CyberSecurity MALAYSIA

www.cybersecurity.my

eSecurity

The First Line of Digital Defense Begins with Knowledge

Vol 52 - (1/2022)

Why Public Wi-Fi should be Avoided?

Overview of 5G Security Challenges and Solutions

The disadvantages of Smart Toys/ IOT Toys

"It takes 20 years to build a reputation and a few minutes of cyber-incident to ruin it." - Stephane Nappo

ISSN 1985-1995

9 771985 199003

Your **cyber safety** is our **concern**

Securing Our Cyberspace

CyberSecurity Malaysia is the national cybersecurity specialist and technical agency committed to provide a broad range of cybersecurity innovation-led services, programmes and initiatives to help reduce the vulnerability of digital systems, and at the same time strengthen Malaysia's self-reliance in cyberspace. Among specialised cyber security services provided are Cyber Security Responsive Services; Cyber Security Proactive Services; Outreach and Capacity Building; Strategic Study and Engagement, and Industry and Research Development.

For more information, please visit
www.cybersecurity.my

For general inquiry, please email to
info@cybersecurity.my

Stay connected with us on
www.facebook.com/CyberSecurityMalaysia and
www.twitter.com/cybersecuritymy

MINISTRY OF
COMMMUNICATIONS AND DIGITAL

CyberSecurity
MALAYSIA

CyberSecurity Malaysia
200601006881 (726630-U)

Level 7, Tower 1,
Menara Cyber Axis,
Jalan Impact,
63000 Cyberjaya,
Selangor Darul Ehsan,
Malaysia.

T: +603 - 8800 7999
F: +603 - 8008 7000
E: info@cybersecurity.my

www.cybersecurity.my

Best Brand Internet Security 2008 & 2009

CERTIFIED TO ISO/IEC 27001:2013 CERT. NO. : ISMS 0014

ACB ISMS 02
SAMM 456

Status Company

WSIS PRIZES 2020 WINNER www.wsis.org

THE MALAYSIA BOOK of RECORDS

WELCOME MESSAGE FROM THE CEO OF CYBERSECURITY MALAYSIA

Dear Readers,

Welcome to the latest edition of our e-Security Bulletin. We are committed to bring you the most up-to-date and relevant information on a wide range of security topics, and we hope that you will find this issue to be both informative and useful.

In this edition, we have gathered a selection of interesting articles about potential cyber threats and vulnerabilities. We believe that staying informed is crucial to protecting yourself and your organization, thus we hope that this bulletin will assist you in doing so.

As you read this message, the number of Internet of Things (IoT) devices that are connected and active is growing rapidly. These smart devices, which can include smartphones, smart watches, home appliances, cars, and others make our lives more convenient and enjoyable by allowing us to exchange information in real-time. However, the interconnected nature of the IoT ecosystem, which includes hardware and software solutions, communication networks, data processing algorithms, and people using it, also makes it vulnerable to cyber-attacks. Unauthorized access to any part of the ecosystem can disrupt services and threaten business continuity. In this issue, we present articles on the various threats and vulnerabilities within the IoT ecosystem, as well as proactive and reactive solutions for protecting against these attacks.

Among the highlights that may interest you are as follow:

- Why Public Wi-Fi should be Avoided?
- Overview of 5G Security Challenges and Solutions
- The disadvantages of Smart Toys/ IOT Toys
- Augmented Cybersecurity Reality: The Prospects and Challenges
- The OIC-CERT 5G Security Framework- Uniformity in Moving Forward
- Blockchain Technology and The Rise of Smart Contracts

We take this opportunity to remind you on the importance of taking the necessary precautions to ensure the safety of your personal and sensitive information. Whether you are at home or at work, it is essential to be vigilant and to follow best practices for protecting your data and devices. If you have any questions or concerns, please don't hesitate to contact us for more information or guidance.

Thank you for reading. We hope you find this edition of our security bulletin to be valuable, and we look forward to bringing you even more informative content in the future.

Safety and security don't just happen. It requires commitment from all of us.
Be Smart Be Safe.

Thank you and warmest regards,

Dato' Ts. Dr. Haji Amirudin bin Abdul Wahab, FASc
Chief Executive Officer, CyberSecurity Malaysia

EDITORIAL BOARD

READERS' ENQUIRY

Knowledge Management, Level 1, Tower 1, Menara Cyber Axis, Jalan Impact, 63000 Cyberjaya, Selangor Darul Ehsan, Malaysia.

PUBLISHED AND DESIGNED BY

CyberSecurity Malaysia,
Level 7, Tower 1, Menara Cyber Axis,
Jalan Impact, 63000 Cyberjaya,
Selangor Darul Ehsan,
Malaysia.

TABLE OF CONTENTS

Operationalizing Cyber Threat Intelligence with MITRE ATT&CK in MyCERT

By | Md Sahrom Abu

Introduction

Security experts have long been looking for ways to predict, prevent, and respond to cyber threats. This has resulted in a recent surge in demand for threat intelligence. However, in the absence of a reliable structure, it is difficult to operationalize cyber threat intelligence. Therefore, security teams require strategies or frameworks to assist them in analysing and mitigating the risks that their organisations face.

The amount of time taken by threat intelligence analyst to identify a threat is very crucial as it can determine the chance of privilege escalation, lateral movement, data exfiltration, or system disruption should intelligence lifecycle take longer time to complete. To prevent this, security teams need to leverage on indicators of compromise (IOCs) collected through various sources to be able to predict threat attackers' behavior through mapping of their tactics, techniques, and procedures (TTPs). This is where the integration of MITRE ATT&CK framework and Threat Intelligence Platform (TIP) become relevant.

The MITRE ATT&CK framework is a tool developed by the MITRE Corporation. It is designed to provide a library of information on all existing TTPs that threat actors employ across sophisticated real-world attack campaigns [1]. When combined with threat intelligence, it enables security teams to acquire adequate evidence for identifying future attacks and taking necessary precautions to eliminate threats.

An Overview of MITRE ATT&CK framework

MITRE ATT&CK is a documented collection of information about the malicious behaviors advanced persistent threat (APT) groups have used at various stages in real-world cyberattacks. ATT&CK, which stands for Adversarial Tactics, Techniques, and Common Knowledge, includes detailed descriptions of these groups' observed tactics (the technical objectives they're trying to achieve), techniques (the methods they use), and procedures (specific implementations of techniques), commonly called TTPs.

MITRE organises data into matrices, which are big tables with links to extensive explanations that can aid in identifying and understanding adversarial behaviour. Attackers might employ a variety of techniques to accomplish the same goal, MITRE groups them into 14 tactics that are often used by adversaries to attack corporate networks. Figure 1 illustrates the density of the Enterprise ATT&CK matrix using MITRE ATT&CK Navigator.

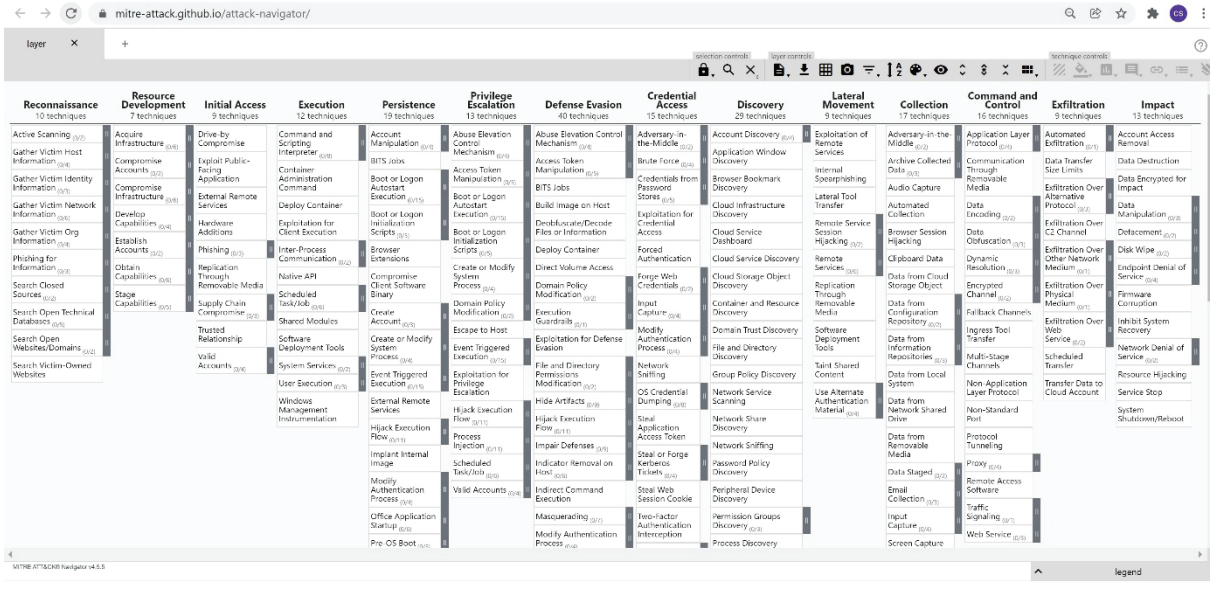


Figure 1: The density of the Enterprise ATT&CK matrix using MITRE ATT&CK Navigator

Before diving into the matrix, it is crucial to understand how MITRE ATT&CK define tactics, techniques, and procedures.

- **Tactics:** Describes the immediate technical objectives (the "what") attackers are trying to achieve, such as gaining ***Initial Access,*** maintaining ***Persistence,*** or establishing ***Command and Control***. Invariably, attackers must use multiple tactics to complete an attack successfully.
- **Techniques:** Describes the "how"—the methods attackers use to carry out a tactic. All tactics in each matrix have multiple techniques; the Enterprise matrix breaks some techniques down further into sub-techniques. An example of this is the Phishing technique.
- **Sub-techniques:** More specific methods on how threat actors reach their tactical goals (i.e., Spearphishing Attachment, Spearphishing Link, and Spearphishing via Service)
- **Procedures:** Describes the specific implementations of techniques and sub-techniques APTs have used (sometimes in clever or novel ways), or it can refer to specific malware or other tools attackers have used. As shown in Figure 2, there is a list of Procedures that describe specific implementations of ***Initial Access*** technique.

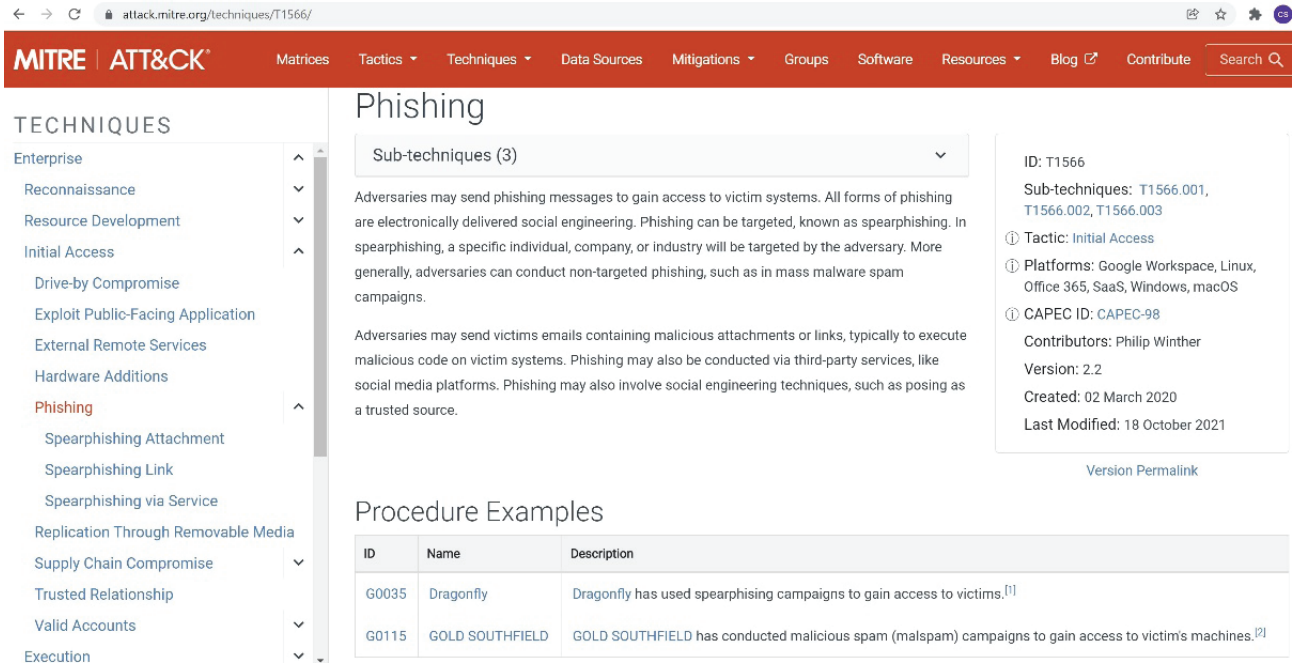


Figure 2: The Procedure that describes specific implementations of Initial Access technique

The term matrix can be misleading as the concept of rows that span the width of all columns is comparable to that of a spreadsheet. However, the whole matrix becomes significantly less intimidating once the representation of 14 separate columns are formatted more like individual organization charts, as illustrated in Figure 3. Henceforth, associated techniques and sub-techniques appear beneath each tactic.

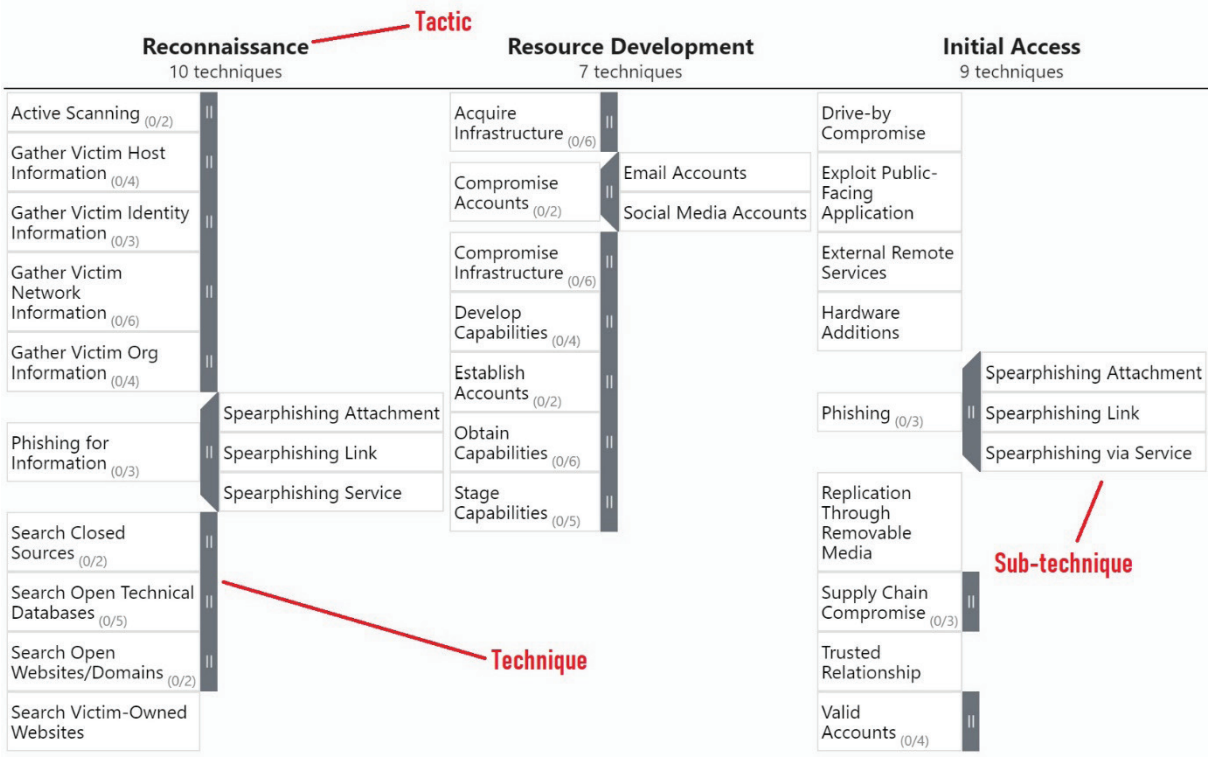


Figure 3: The Columns in the ATT&CK Enterprise matrix represent distinct tactics, each with associated techniques and sub-techniques

Using MITRE ATT&CK with Threat Intelligence

To understand the behavior of adversaries, we need to break down an attack lifecycle and analyze each phase of an attack. MITRE ATT&CK provides an ultra-modern approach to analyzing attacks by cataloging threat actor TTP into a matrix. It offers a holistic knowledge base for security operations center (SOC) teams to examine the threat actor's movements across their network. By using the ATT&CK framework for threat intelligence operations, an advanced threat intelligence platform (TIP) provides contextualized insights into the TTP leveraged by threat actors each step of the way.

An advanced TIP has a built-in MITRE ATT&CK Navigator that enables security teams to visualize and track adversaries' footprints by mapping tactics and techniques to reported incidents. This helps them identify trends across the cyber kill chain and associate them with reported intel, generating actionable insights to make informed decisions earlier in an attack lifecycle

MITRE ATT&CK is very useful for threat intelligence analysts as it outlines threat actor behavior in a standardized manner. Threat actors can be tracked with links to TTP in ATT&CK Navigator that they have been known to use. This provides security defenders an insight into their operations as well as weaknesses and strengths. Developing MITRE ATT&CK Navigator entries for specific threat actors is a convenient way to visualize an organization's weaknesses and strengths against those adversaries.

Communicating intelligence to different organizations will be made easier when every party speaks the same language. Standardizing ATT&CK references increases efficiency and establishes a common understanding. Therefore, ATT&CK is available as a STIX/ TAXII 2.0 feed, making it easy to integrate into existing tools.

Operationalizing cyber threat intelligence with MITRE ATT&CK in MyCERT

The reality is that breaches happen constantly. The key is to respond to them quickly and effectively. Many businesses tend to be reactive when responding to threats. It is, however, possible to start being proactive with the Malware Information Sharing Platform and Threat Sharing (MISP) and MITRE Enterprise ATT&CK integration. MISP is an open-source software solution for collecting, storing, distributing and

sharing cyber security indicators and threats about cyber security incidents analysis and malware analysis [2]. In contrast, MITRE ATT&CK can provide a structured way to describe adversary TTP and behaviors. Threat hunting starts with intelligence, and ATT&CK delivers the basis for hunters to build their hypotheses and search for threats.

For example, MyCERT uses MISP and MITRE Enterprise ATT&CK to look at APT28 [3] and commonly used techniques so that cyber threat analysts can successfully hunt down unknown threats.

Step 1 – Create an event for threat

MISP can help connect the dots between adversaries' behavioral attributes and indicators of compromise. Furthermore, MISP correlations can find relationships between attributes and indicators from malware or attacks campaigns. Correlation support analysts in detecting clusters of similar activities and pivoting from one event to another. Figure 4 shows an event about APT28 Autoit Zebrocy Progression.

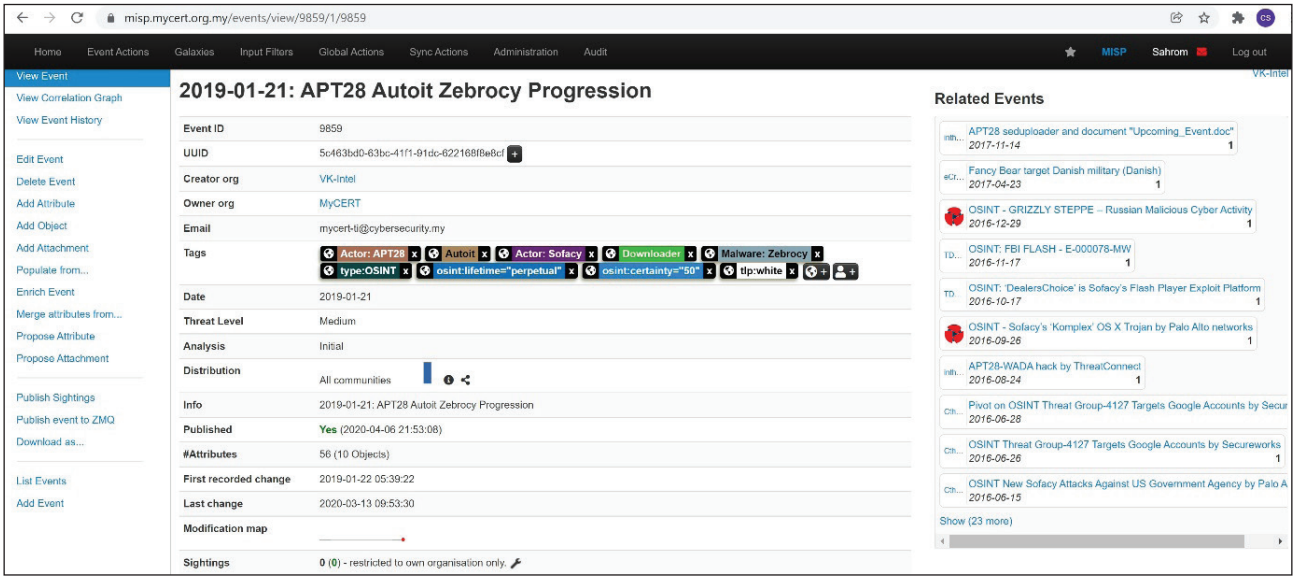


Figure 4: An event about APT28 Autoit Zebrocy Progression

Step 2 – Understanding the threat

While IOCs might help with the scope and early detection, threat actors can swiftly change them. MITRE ATT&CK can provide extensive TTP information, enabling more robust security against malicious threats. MITRE ATT&CK also includes mitigations that can be utilized to implement proactive defenses.

The integration of MISP and MITRE ATT&CK helps a threat intelligent analyst correlate clusters of similar activities and pivot from one event to another. Apart from that, integration can also help visually identify TTP and associated mitigations which may be related to a particular threat. Figure 5 depicts the correlation of activities for APT28 and common technique used by APT28 threat actors. The SOC team can now look into the relevant actions for mitigation provided by MITRE ATT&CK.

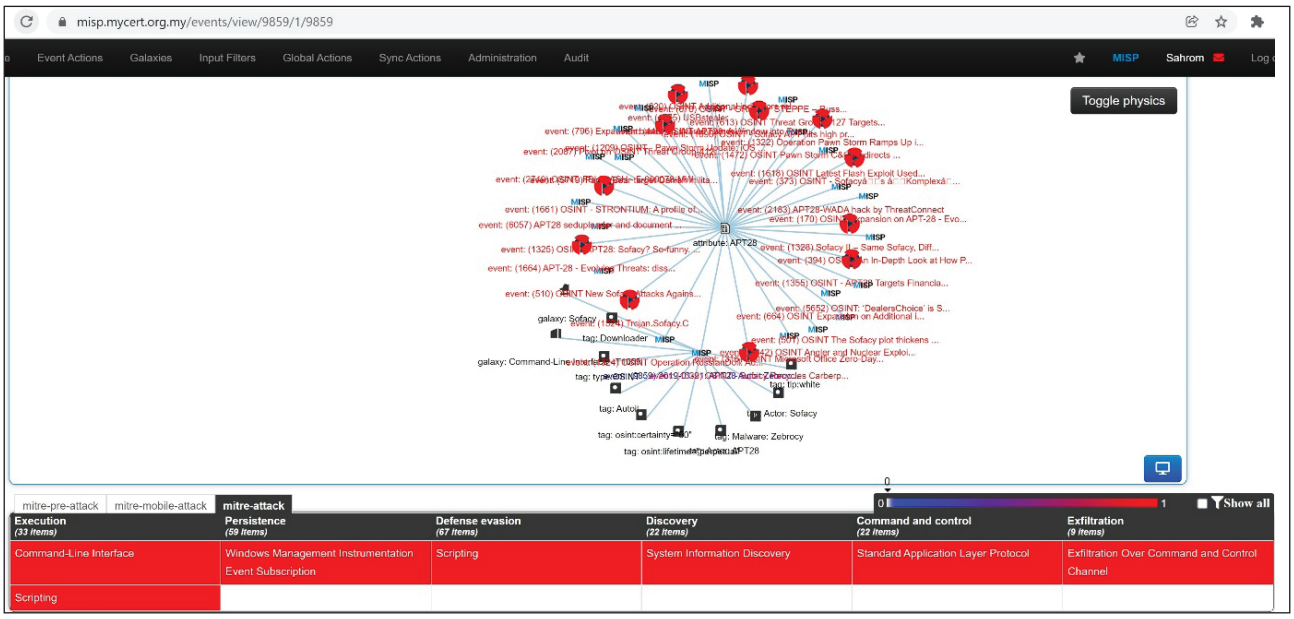
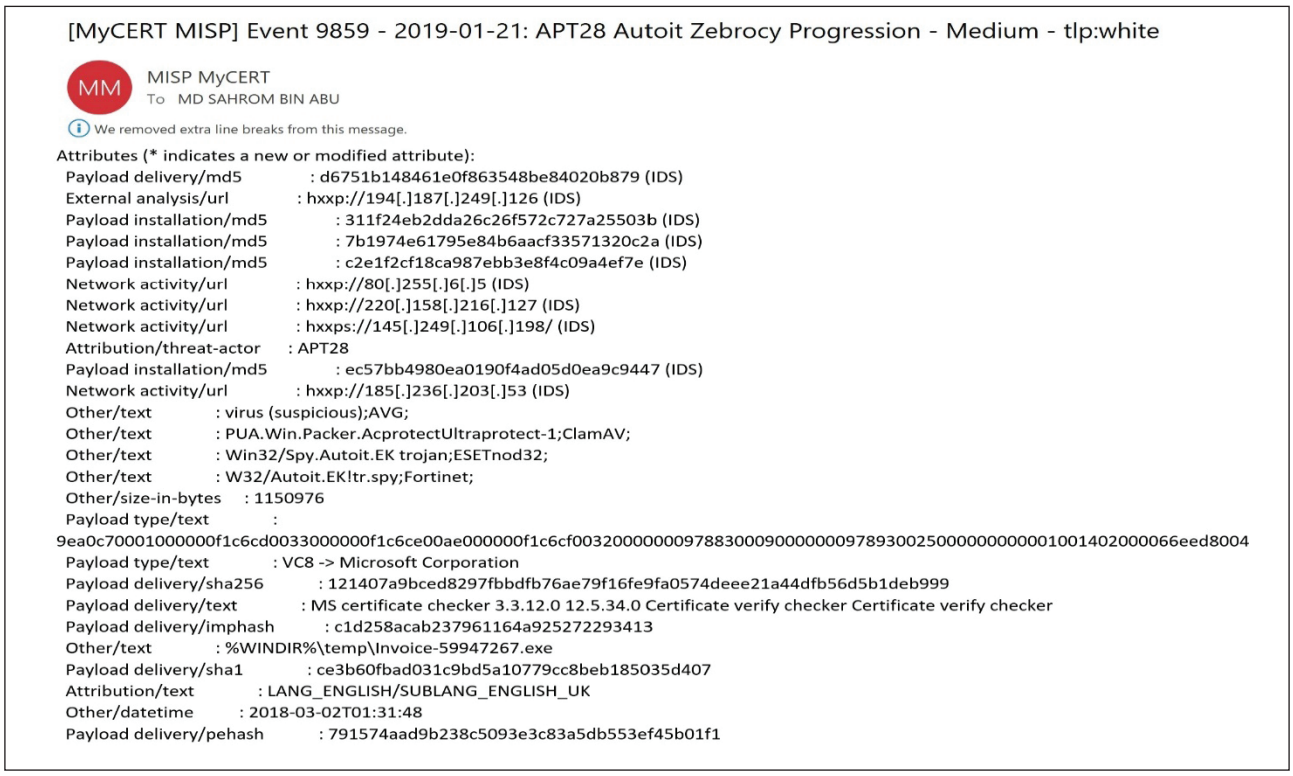


Figure 5 – Correlation graph and common technique used by APT28 threat actor

Step 3 – Consume and Sharing of Threat Intelligence

Once we know how a threat actor target a business, it is possible to start preparing appropriate defenses that can help identify, mitigate and ultimately, prevent them from impacting our businesses. These include:

- Coordinating First Level Incident Handler via ticketing systems to respond to takedown and escalation.
- Produce alert/advisory using information related to the IOC gathered from the Threat Intelligence analysis.
- Produce Threat Intelligence Report - There are two types of report with different content and format produced namely: Internal and External report. Circulation of report must adhere to Traffic Light Protocol (TLP) [4].
- Disseminate any actionable intelligence with community who subscribes to MyCERT MISP to prevent the spread of malware as shown in Figure 6.



[MyCERT MISP] Event 9859 - 2019-01-21: APT28 Autoit Zebrocy Progression - Medium - tlp:white

MM MISP MyCERT
To MD SAHROM BIN ABU

We removed extra line breaks from this message.

Attributes (* indicates a new or modified attribute):
Payload delivery/md5 : d6751b148461e0f863548be84020b879 (IDS)
External analysis/url : hxxp://194[.]187[.]249[.]126 (IDS)
Payload installation/md5 : 311f24eb2dda26c26f572c727a25503b (IDS)
Payload installation/md5 : 7b1974e61795e84b6aacf33571320c2a (IDS)
Payload installation/md5 : c2e1f2cf18ca987ebb3e8f4c09a4ef7e (IDS)
Network activity/url : hxxp://80[.]255[.]6[.]5 (IDS)
Network activity/url : hxxp://220[.]158[.]216[.]127 (IDS)
Network activity/url : hxxps://145[.]249[.]106[.]198/ (IDS)
Attribution/threat-actor : APT28
Payload installation/md5 : ec57bb4980ea0190f4ad05d0ea9c9447 (IDS)
Network activity/url : hxxp://185[.]236[.]203[.]53 (IDS)
Other/text : virus (suspicious);AVG;
Other/text : PUA.Win.Packer.AcprotectUltraprotect-1;ClamAV;
Other/text : Win32/Spy.Autoit.EK trojan;ESETnod32;
Other/text : W32/Autoit.EK!tr.spy;Fortinet;
Other/size-in-bytes : 1150976
Payload type/text :
9ea0c70001000000f1c6cd0033000000f1c6ce00ae000000f1c6cf00320000000978830009000000097893002500000000000010014020000 66eed8004
Payload type/text : VC8 -> Microsoft Corporation
Payload delivery/sha256 : 121407a9bced8297fbbdfb76ae79f16fe9fa0574deee21a44dfb56d5b1deb999
Payload delivery/text : MS certificate checker 3.3.12.0 12.5.34.0 Certificate verify checker Certificate verify checker
Payload delivery/imphash : c1d258acab237961164a925272293413
Other/text : %WINDIR%\temp\Invoice-59947267.exe
Payload delivery/sha1 : ce3b60fbad031c9bd5a10779cc8beb185035d407
Attribution/text : LANG_ENGLISH/SUBLANG_ENGLISH_UK
Other/datetime : 2018-03-02T01:31:48
Payload delivery/pehash : 791574aad9b238c5093e3c83a5db553ef45b01f1

Figure 6 – Dissemination of actionable intelligence to subscribers through email.

Conclusion

Threat actor behaviors and tactics change regularly. Many threat actors shift behaviors and attack techniques as existing methods become less effective. MITRE is constantly streamlining and improving their knowledge base of data to handle this challenge. At the same time, MISP has a built-in MITRE ATT&CK Navigator that enables security teams to visualize and track adversaries' footprints by mapping tactics and techniques against reported incidents. Operationalizing MISP with MITRE ATT&CK can help MyCERT identify trends across the cyber kill chain and associate them with reported intel, generating actionable insights to make informed decisions earlier in an attack lifecycle.

Once we identify a risk from a threat actor, it is essential to stay vigilant. This can be a challenging task in a landscape of escalating threats. There is no replacement for human knowledge and analysis in threat hunting, but we can make it easier by providing current, detailed and accurate information to enable more informed judgements and quicker responses.

Reference

1. B. E. Strom, D. P. Miller, K. C. Nickels, A. G. Pennington, and C. B. Thomas, "MITRE ATT & CK Ò : Design and Philosophy," no. July 2018, 2020.

2. C. Wagner, A. Dulaunoy, G. Wagener, and A. Iklody, "MISP: The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform," in Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security, 2016, pp. 49–56, doi: 10.1145/2994539.2994542.

3. FireEye, "APT28: A window into Russia's cyber security," p. 45, 2014, [Online]. Available: https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf.

4. Cybersecurity and Infrastructure Security Agency, "Traffic Light Protocol (TLP) Definitions and Usage." https://www.cisa.gov/tlp (accessed Feb. 10, 2022).

Behind The Scene: Privacy Certification In Malaysia

By | Mohd Rizal bin Abu Bakar & Ikmal Halim bin Jahaya

Certification is traditionally used by organizations and industries to demonstrate or exemplify quality and also to differentiate between the best from the rest in terms of quality. It can take several forms and involves participation from across multiple industries and stakeholders. Unfortunately, it is often poorly regulated.

Privacy certifications are developed as a conformity assessment process for data privacy through periodic reviews by external and accredited auditors to ensure data privacy policies and implementation comply with the requirements as set by recognized authorities and legal framework.

Current Certification Scenario

Data privacy certification has faced a long history of troubled implementation. Certain countries chose not to pass data protection laws and opted for self-regulatory methods of protecting the privacy of data in order to gain the trust of Personal Identifiable Information (PII) principals/owners.

Under the 12th Malaysia Plan launched in August 2021, one of its objectives was to focus on strengthening the well-being, security and enhancing efforts on defense and security by adapting and capitalizing on 4IR (4th Industrial Revolution). The end result is to increase productivity, efficiency and quality; whilst prioritizing the safety of workers and reducing the dangers associated in high risk work environments.

Adapting to new technologies and strategies often come with several drawbacks. 4IR technologies such as AI, IoT, Cobots, AR, VR and Big Data, which help in devising strategies and making key business decisions, involves massive data management and interpretation that often lead to high cyber threat risks.

The Malaysia Cyber Security Strategy (MCSS), under the 12th Malaysia Plan was implemented to help mitigate and manage cyber threats such as data breaches; where the number has skyrocketed to a staggering 5.5 million malware and botnet infections as of 2020.

MCSS is a comprehensive cybersecurity strategy that addresses major areas of concern and countermeasures involving CNII, citizen and industry protection from cyber threats.

One of the five pillars of MCSS is Pillar IV: Enhancing Capacity and Capability Building, Awareness and Education. Aiming to address the challenges posed by evolving cyber threats, it calls for continuous identification and enhancement in areas of expertise and skill sets at the national, sectoral and organizational level in the cybersecurity domain.

Under the Capacity & Capability Building Plan, two key strategies were planned. Strategy 8 focuses on the National Cyber Security Capacity and Capability Building; while Strategy 9 looks at improving the approach to implementing Cyber Security awareness programme.

The 12th Malaysia Plan also targets improvisation and cultivation of local cyber security expertise in order to reduce reliance of foreign talents in the field.

Integration of all population registration systems to allow data sharing among relevant agencies will be established under the national digital identification policy. Thus, offering a trusted and secure comprehensive framework for digital transactions and data flow between agencies involved in the processing of data.

Under this initiative, PDPA 2010 will also be revised to provide PII owners with more rights and control over personal data, as well as a clear and concise method on data handling using technology besides defining accountability of businesses in protecting personal data and privacy.

Way Forward

Development of privacy certification in Malaysia is the right way forward and in line with Malaysia's Cyber Security Strategy, to build

trust and security in the cyber environment, not solely for national security purposes, but also to support the government's initiative in IR4, and Digital economy for the country's advancement.

Certification Initiatives

The Malaysia Digital Economy Corporation, the country's principal agency for driving the digital economy, is currently spearheading efforts to enhance the number of local qualified professionals, including new talent development, up-skilling, and reskilling activities.

In order to promote knowledge acquisition and enrichment among current cyber security specialists, the government will grant extra money and scholarships. This will aid in the development of a new generation of cyber security experts who are well-educated and highly skilled.

Currently, Cyber Security Malaysia is implementing the Global Accredited Cybersecurity Education (ACE) Scheme in order to expand the number of local cyber security experts. It is a comprehensive professional certification scheme developed inhouse to certify and recognise cyber security workers in accordance with ISO/IEC 17024 for people certification, ISO/IEC 9000 for processes certification, and ISO/IEC 27001 for security management certification.

Compliance to cyber security standards is crucial amongst government and CNII agencies, enterprises and the general public. Adherence to cyber security standards requires good human interaction and attitude towards technology.

ISO/IEC 27701: An Extension to ISO/IEC 27001

When a society and its economy is increasingly driven by data, the focus will shift from preservation to value extraction from data itself; and the most valuable asset is information. With the emergence of new technologies, platform-based business models and adoption of smart working practices, it is not surprising that the number of vulnerabilities in computer networks has skyrocketed.

As a result, new holistic approaches are required to address the growing complexity of cyber threats. Information system security (ISS) focuses on the need to strike a balance between security and legal compliance on one hand, and cost and agility of operations on the other. ISS standards and frameworks such as ISO/IEC 27001 plays a critical role in technological, organizational and managerial approaches over the years and is the third most widely used certification worldwide. It ensures information confidentiality, integrity and availability as well as compliance with legal requirements.

The standard sets the requirements for building, implementing, maintaining and continuous improving an Information Security Management System (ISMS) within an organization. Known for its generic requirements, it is designed for organizations of all types and sizes. Global companies such as Netflix, Amazon Web and most recently, Facebook's Workplace have been certified under ISO/IEC 27001. To date, more than 60,000 organizations globally are ISO/IEC 27001 certified. This proves that certification is an important aspect in protecting our most valuable assets.

ISO/IEC 27701, also most commonly known as Privacy Information Management System (PIMS), was created as a standard data privacy extension to ISO 27001. Released in 2019, the standard helps companies which are required to implement systems to support data privacy regulations such as European Union's General Data Protection Regulation (GDPR) and other data protection regulations.

The extension is a framework to manage data privacy for controllers and processors of Personally Identifiable Information (PII). Its objective is to minimize any threats to individuals and organizations' privacy rights. Implementation of this standard demonstrate to customers and stakeholders that you have strong procedures in place to comply and support GDPR and other related privacy regulations.

The PIMS standard is a natural progression from ISMS certification. It includes additional requirements and guidelines whereby the substantial overlap of system and technical requirements of both standards make it an attractive adoption option.

To be certified under ISO/IEC 27701, an organization must have an existing ISO 27001 certification, or have implemented ISO 27001 and ISO 27701 as a single implementation audit. Getting certified with the ISO shows that the organization has an effective quality management system which will boost confidence

of stakeholders and facilitate effective business agreements.

When data privacy is involved in business transactions and processes, ISO 27701 promotes trust by ensuring all parties involved have high privacy standards. Some companies no longer use the term quality but refer to specific ISO standards as the way of doing business since every aspect of the company is included in the scope of the management system, from sales and planning through delivery and post-delivery activities (Hammar, 2014).

Combination of multiple ISO standard way of compliance may even encourage the redeployment of effort, time, money, and human talent involved in any previous improvement projects. With the reuse, organizations could reap a larger benefit due to reduced effort and costs involved with the implementation of a new model compared to an institutionalized model.

ISO 27701 will also enhance an organization's risk management and security. With the implementation, the severity of potential project risks or data leaks can be identified early (Pardo et al., 2016). In addition, the standard is perfectly aligned to other security standards, privacy regulations/laws and jurisdictional requirements, such as Malaysia's Privacy Data Protection Act 2010—thus, eliminating the worry on the privacy laws differing from GDPR. The standard was developed to provide for working with personally identifiable information and incorporate other privacy laws and jurisdictional specifics into ISO 27701.(ISO 27701, The Privacy Information Management Standard - ISMS.Online, n.d.)

In addition to providing confidence to individuals, other organisations with whom it collaborates, and supervisory agencies, as well as regulatory compliance, certification must also promote accountability. It demonstrates that a business should operate to the highest global standards. But to obtain the maximum benefit from any investment in this area, it is important to work with a certification body that has had its own technical competence, impartiality, performance capability and integrity assessed and aligned to internationally recognised standards.

The GDPR framework does not limit its role to only supervisory authorities. Based on Articles 42(5) and 43(1) GDPR, certification schemes can be issued either by the supervisory authority or by private or other public bodies (Hornung & Bauer, 2019) provided they are accredited accordingly. This flexibility is well received by supervisory authorities which may experience lack of resources in terms of expertise, fundings and time to monitor compliance amongst controllers of PII.

By allowing private and public bodies to assume the role of certifiers, the supervisory authorities could shift their focus and allocate resources to complement their role as a monitor, thus achieving the aim of the regulator as an additional layer of safeguard in the data protection mechanism (Kamara & De Hert, 2018).

GDPR is Giving Advantages More than We Think

By | Aliya Farhana binti Mohd Nasran

Data privacy has become a critical issue globally as Internet usage continues to proliferate over the years. For a business to run safely and successfully, data must be protected and kept away from malicious actors. Thus, there is a need to establish a framework that can effectively protect businesses. The adoption of GDPR helps significantly in data privacy protection as it accords more controls and rights to individuals to manage their personal data and privacy. The GDPR legislation sets out a framework for data protection compliance throughout the European Union (EU) and is enforced in processing of any personal or sensitive data, etc.

Introduction: Birth of GDPR

GDPR (General Data Protection Regulation) was first introduced as a regulation for data privacy and guidelines for other countries that confronted challenges in providing the best protection of citizens' data on the internet. This is also to prevent businesses from misusing any information to which they are accountable. To understand the implementation of GDPR, it is useful to know its origin, history and evolvement.

Back in 1995, when Data Protection Directive was in force and the Internet usage was still relatively low, no one knew how much data would one day occupy their lives. At that time, each member country was left to establish its own data protection laws. This created a lot of problems as it was only a 'Directive', not 'Regulation'. These two terms have vastly different meanings. A directive is a goal established by the European Union (EU) which requires each country to establish its own laws and regulations.

The Directive created more complications as data sharing across borders became more common. Due to cross-border nature of data sharing, administrative expenses and time were incurred in order to trace each country's data.

The safety of data transmission is also another major concern as it cannot be guaranteed once the data move out of the EU. Hence, GDPR was created to reduce such problems and standardize data protection law across the entire EU, thus ensuring data protection during transmission, and setting out rights and privileges for individuals to control their own personal data.

Why Was the GDPR Drafted and How It Can Be the Solution

As technology evolved rapidly over the years, legislation enacted in the 90s such as Data Protection Directive became irrelevant as more international data transfer were handled by businesses. Hence, a new set of data protection rules which are future-proof became necessary.

The digital age is upon us. Sectors such as education, entertainment, and healthcare have become substantially digitalized. The common practice across all these sectors is that personal data is invariably collected and processed since web and data movement have become indispensable in the operations of countless organizations. It is no wonder we are in dire need of a legislation such as GDPR to cater to the way tech companies conduct their business. Almost every platform such as Google, Bing, etc offers free services but at the same time they collect data from users that are personal, private, or sensitive which later get processed and monetized. When people use Google's search engine, their actions and movement will be tracked and transformed into data points. The information became valuable to third parties for advertisement purposes.

An example on misuse of data was Facebook when on 16 March 2022, the global social media network giant was fined $18.6M due to a string of historical data breaches of GDPR committed in 2018. In that particular case, the Irish Data Protection Commission (DPC) received no less than 12 breach notifications from the company between 7th June 2018 and 4th December 2018. It was discovered that Facebook's parent company, Meta, infringed Articles 5(2) and 24(1) of GDPR. They had failed to provide proper technical and organizational measures which would allow it to display the security measures

it applied in practice to protect EU users' data.

A data security expert, Thomas Stoesser, gave his views on the issue which stressed the importance of data privacy and the significance of being GDPR compliant.

"...Companies need to realize that GDPR is a data privacy regulation that has teeth. By now, many companies have been fined by the Data Protection Commission in Ireland, including big brands like Google, British Airways, and Marriott. These are just a few of the multi-million Euro fines that have been handed out in the past four years since GDPR became enforceable. It should be clear by now that more big fines will be handed out if organizations fail to take data privacy seriously. The former information commissioner Elizabeth Denham pointed out something a couple of years that many companies don't yet seem to understand: The personal data that they are processing, and storing is not their property. They have only been entrusted with it. That is a big difference. So, what can organizations like Meta do to protect their customer's data adequately? It may seem obvious, but they need to take a serious approach to data security."

Benefits of GDPR

Although GDPR may be regarded as a tedious necessity to many businesses and enterprises, the regulation can facilitate efficiency and productivity as well as enhance numerous organizational activities. Below are five benefits of GDRP compliance:

A. Enhance Organization Cybersecurity

An organization would not dare take the risk of not complying with GDPR as they know the implications of data breaches. Implementing GDPR requires a company to formulate a security strategy and implement administrative and technical standards to protect the personal data.

According to Cyber Security Breaches Survey 2017, 68% of big companies in the UK have encountered a cyber-attack at least once. As technology evolves, attacks by cybercriminals become much more sophisticated. Having a GDPR-compliant framework in the workplace will also enhance cybersecurity practices. This is proven as GDPR mandates privileged and identity access management that allows only authorized access to vital data in an organization, ensuring that data would not fall into the wrong hands.

B. Improve Data Management

To be GDPR compliant, it is critical to know the sensitivity of information collected. By auditing the data, it will enable an organization to minimize data collection, manage better storage and enhance data management processes. To do that, firstly, there is a need to identify and dispose of redundant, obsolete, and trivial files, also known as "ROT" that have no significant value to a business. Clearing it up will erase redundant information such as an old customer's personal information.

Secondly, after every data has been analyzed, GDPR also requires them to be indexed and globally searchable. This will help tremendously in handling data subjects, particularly those who requested their data to be deleted and forgotten. Additionally, this will also motivate an organization to improve data storage management to achieve productivity and efficiency while dealing with fully searchable, precise, and attainable data.

C. Reduced maintenance costs

Combined with disposal of insignificant ROT information, an organization will dramatically reduce the cost of storing data that is irrelevant and therefore, no longer need to pay for data maintenance costs and incurring man-hours for such exercise.

D. Boost Audience Loyalty and Trust

GDPR compliance will enable the organization to build more faith and trust with its customers. In the process of collecting data and obtaining consent from data subjects, organizations need to illustrate how their information will be handled, leading to better understanding and higher degree of trust among customers.

E. Greater decision-making

Based on GDPR, no automated decisions can be made on an individual's personal data. Instead, the regulation outlines the right to allow for human intervention which ultimately reduces the chances for arbitrary decisions.

As a result, an organization's data will become more secure and easier to access and additionally, individuals have full comprehension of its underlying value. This perception will in turn assist an organization in identifying the unmet

needs of its customers. By utilizing customer information more efficiently, an organization will yield better decision-making and thus, achieve a better return on investments.

Experts' Opinion on GDPR: Two Years after the Implementation

Two years after the implementation of GDPR, several experts have shared their own perspectives in data protection and privacy to review the past, present, as well future of GDPR. Below is an extract of some of the opinions from practitioners, policymakers, and academics across the world.

According to Stephen Wong, a Hong Kong Privacy Commissioner for Personal Data, the effect of the GDPR was positive considering data protection has been updated and compliance requirements must be explicit.

"*...It was indeed a trendsetter and catalyst for change, given its updated data protection conventionally and the explicit compliance requirements on the part of the organizations established outside the EU in specific circumstances.*"

He continued to touch on the risk-based approach method in data protection.

"*...The adoption of a risk-based approach in data protection is another key to the effective implementation of the GDPR. The approach determines the level of data protection through an assessment of potential harm, allowing data controllers to proactively manage the risks involved with their business operations. This pragmatic approach is well poised to be welcome by the business community.*"

Eduardo Ustaran, a co-head of the Hogan Lovells Privacy also shared his views on the risk-based approach that remarkably helps in GDPR.

"*...Perhaps the greatest success of the GDPR so far has been the introduction of the risk-based approach to compliance and regulatory action. Data is all around us, and its protection is a responsibility that needs constant recalibration. A static and prescriptive law would have been incapable of addressing the nuances of the digital economy. Fortunately, the GDPR is not that. The GDPR has flexibility and common sense at its core, and thanks to that, we should regard it as a framework that can adapt to the privacy and cybersecurity needs of our challenging world.*"

Malaysia's PDPA vs EU's GDPR

The Malaysian government has also been working towards establishing robust data privacy and protection since 2010. The result was the enactment of Malaysia Personal Data Protection Act (PDPA). Comparing Malaysia's PDPA and EU's GDPR, both legislations share mutual objectives which is to protect the data subjects' rights and their personal data. However, Malaysia's PDPA came into effect five years before the GDPR. Therefore, GDPR has granted more rights to data subjects. There are also notable differences between PDPA and GDPR as shown in Figure 1 below.

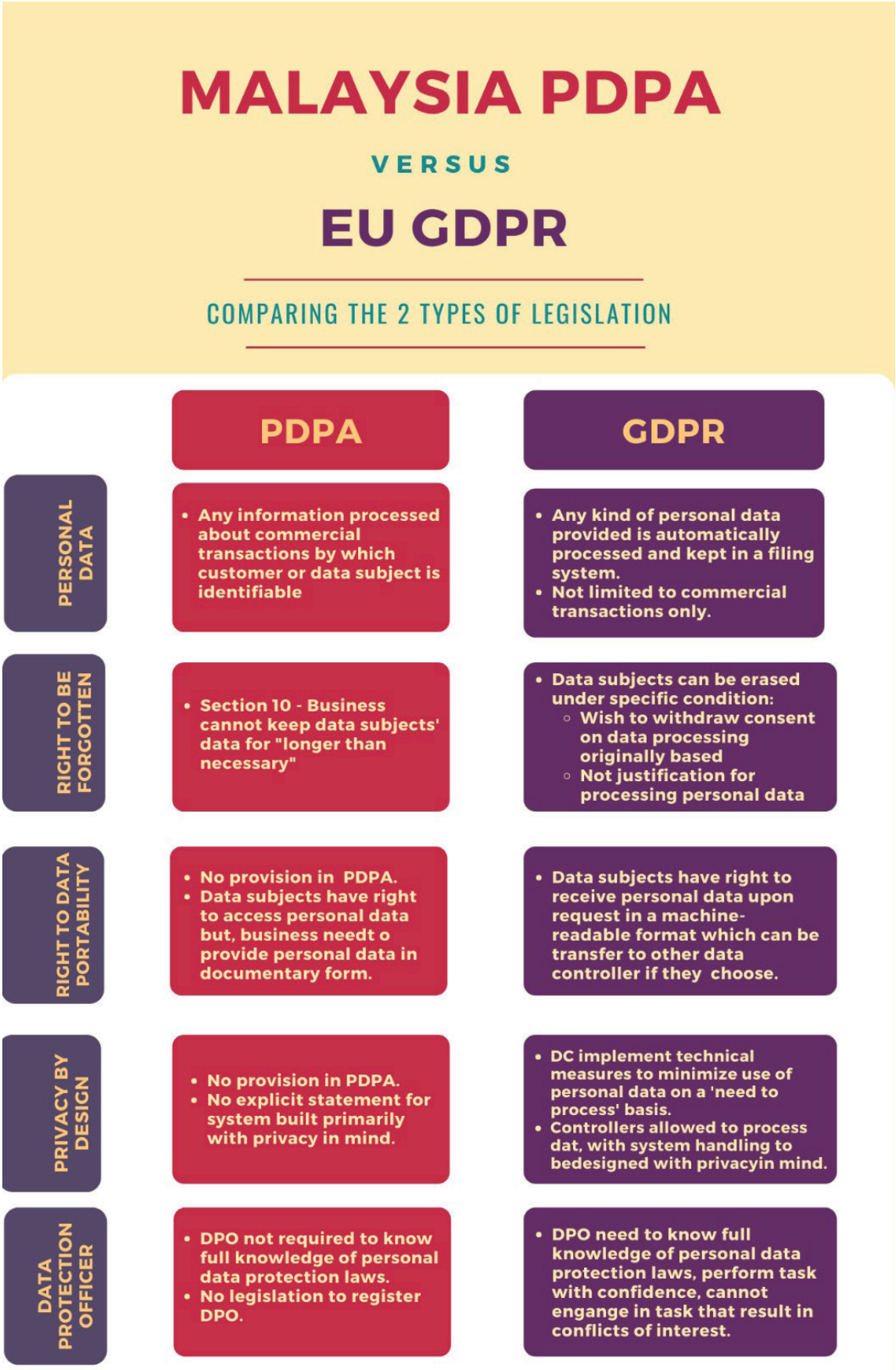


Figure 1: Difference between Malaysia PDPA and EU GDPR

Conclusion

Technology evolves rapidly every day and so should data protection framework. GDPR should not be the end of a journey but a good and stable foundation for the future. As Data Protection Authorities across member states in the EU gain better understanding, GDPR enforcement will potentially be expanded and refined. It has been three years since the implementation amidst continuing data subject complaints and data breaches. Data Protection Authorities are now beginning to be more effective and will continue to be in seeking companies to implement GDPR compliance. The coming years will undoubtedly see on-going discussion among members of Data Protection Authorities on best practices to collaborate and optimize efforts in enforcing GDPR. Although it is undeniable that GDPR implementation has progressively enhanced companies' security measures and safeguarding the privacy of people, consistency across the region remains a challenge among regulators. Therefore, it many take a few more years to establish a standard baseline and compliance in the EU.

Reference

1. Afifi-Sabet, K. (2021, August 20). What is GDPR? Everything you need to know. IT PRO. Retrieved March 12, 2022, from https://www.itpro.co.uk/general-data- protection-regulation-gdpr

2. Fimin, M. (2018, March 29). Five Benefits GDPR Compliance Will Bring To Your Business. Forbes. Retrieved March 7, 2022, from https://www.forbes.com/sites/forbestechcouncil/2018/03/29/five-benefits-gdpr- compliance-will-bring-to-your-business/?sh=49eacc65482f

3. Hazlegreaves, S. (2018, April 16). The five key business benefits of GDPR. Open Access Government. Retrieved March 16, 2022, from https://www.openaccessgovernment.org/the-five-key-business-benefits-of- gdpr/44554/

4. Healey, R. (2021, January 18). Malaysia PDPA vs. GDPR: A Quick Breakdown. Formiti. Retrieved March 24, 2022, from https://formiti.com/malaysia-pdpa-vs- gdpr-a-quick-breakdown/

5. Heine, I. (2021, September 13). 3 Years Later: An Analysis of GDPR Enforcement. Centre for Strategic and International Studies. Retrieved March 17, 2022, from https://www.csis.org/blogs/strategic-technologies-blog/3-years- later-analysis-gdpr-enforcement

6. iHASCO: A Citation Company. (2020, October 19). A very brief history of the GDPR. iHASCO. Retrieved April 10, 2022, from https://www.ihasco.co.uk/blog/entry/3008/brief-history-of-the-gdpr

7. International Association of Privacy Professionals. (2020, May). The GDPR at Two: Expert Perspectives. IAPP. Retrieved March 29, 2022, from https://iapp.org/resources/article/gdpr-at-two-expert-perspectives/

8. Lomas, N. (2022, March 15). TechCrunch is part of the Yahoo family of brands. TechCrunch. Retrieved April 5, 2022, from https://techcrunch.com/2022/03/15/facebook-2018-breaches-dpc-decision/

Virtual Private Network (VPN)

By | Nur Fazila Selamat, Mohd Faisal Abdullah & Mohd Nor A'kashah Mohd Kamal

What is A Virtual Private Network (VPN)?

VPN stands for Virtual Private Network. A VPN serves two main purposes which is to hide a user's IP address and encrypt web browsing data [2]. It allows a user to browse the web or data securely and with more privacy. Also, it acts as a preventive mechanism against data being stolen, tracked, or recorded. VPN works by encrypting users' traffic as well as rerouting users' data packets through VPN servers [1]. This process hides the user's actual IP address and makes it look like browsing from the selected VPN server's location rather than the actual one [1].

Below are the most common reasons why people use a VPN [2] [3] :

a. Protect privacy on public WiFi.
b. Browse the web anonymously.
c. Communicate securely.
d. Access restricted sites.
e. Access better entertainment options.
f. Avoid bandwidth throttling.
g. Hide browsing activity from governments.

Types of Virtual Private Network (VPN)

Here are 4 main types of VPN [4]:

a) Remote Access VPNs
A remote-access VPN is used to connect the Internet to a private network such as an office network. Remote-access VPNs are also called **client-based VPNs** or **client-to-server VPNs**. VPN encryption is required to keep the data private as it travels securely to and from the private network. Without a VPN, the Internet is an untrusted link in communication.

Image 1: How Remote Access VPN works.

How to connect Remote Access VPNs?

Step 1: A VPN server will verify the user whether he/she is allowed to access the network or not.

Step 2: Once the user is authenticated, the client and server will initiate an encrypted tunnel between them.

Step 3: Now, the user is able to access the resources through the VPN server. The user is able to access any data or files via the company's internal network.

b) Personal VPN Services
A personal VPN service allows a user to connect to the Internet via a third-party server. This type of service connects to a VPN server which acts as a middleman between the user's device and the online services that the user wants to access. The personal VPN is also called a 'consumer' or 'commercial' VPN. It will encrypt users' connection, hide identity online, and let users spoof their geographic location.

Image 2: How Personal VPN works.

The top 5 recommended services for personal VPN are ExpressVPN, NordVPN, CyberGhost, IPVanish and Surfshark [5].

How to connect Personal VPNs?

Step 1: From the VPN service provider, install software onto the user's device such as smartphones, routers [6], etc.

Step 2: Connect to a server in the user's VPN provider's network. If users want to protect their privacy, the user should connect to a local server for faster speed.

Step 3: Now users may browse the internet as usual.

c) Mobile VPNs

Mobile VPNs are no different from remote-access VPNs as both types of networks are connected to a private network and require software (as users usually need to install software on their device or configure their operating system). However, if the user is unlikely to have a steady connection on the same network for the duration of the session, a mobile VPN is a preferable solution [4]. By using a mobile VPN, the VPN connection persists even if the user switches their device off for a while. Mobile VPNs tend to be used by mobile workers to ensure consistent availability or for the convenience of having a VPN that tolerates connection changes [4].

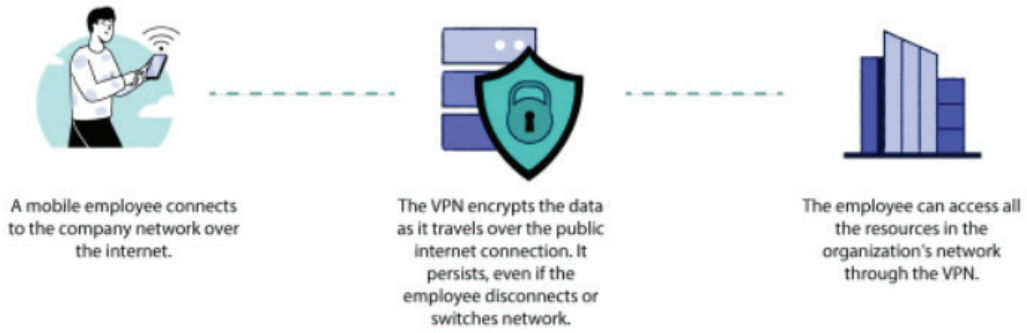


Image 3: How Mobile VPN works.

How does Mobile VPNs work?

Step 1: The user connects to the VPN and is then authenticated. The authentication medium might include passwords, physical tokens, or biometric devices.

Step 2: The VPN tunnel is initiated between the user's device and the server. In a mobile VPN, the VPN tunnel connects to a logical IP address that is tied to the device, and independent of the Internet connection.

Step 3: As the user switches between networks, the VPN connection remains active. The VPN connection remains available when the device is switched back on, even if it is turned off to save battery life.

d) Site-to-site VPNs

Unlike 3 other types of VPNs which connect individual users to a network, a site-to-site VPN is a connection between two networks on different sites. For example, if a company had two offices, a site-to-site VPN can be used to combine them into a single network called an Intranet. It also can join up two or more networks, to create a combined single network. This type of network is also known as a network-based VPNs.

Image 4: How Site-to-Site VPN works.

How Does Site-to-site VPNs work?

There are several technologies that can be used to implement a site-to-site VPN such as IPsec tunnel, Dynamic MultiPoint VPN (DMVPN), and L3VPN [4].

i. IPsec Tunnels

IPsec tunnels can be developed using firewalls and network routes. By using an IPsec tunnel, it encrypts the traffic between connected networks. This can take two forms [4]:

- A route-based IPsec tunnel – It allows any traffic between the networks through. It's like wiring the networks together.
- A policy-based IPsec tunnel – It sets up rules that decide what traffic is allowed through, and which IP networks can communicate to which other IP networks.

ii. Dynamic MultiPoint VPN (DMVPN)

Dynamic MultiPoint VPN (DMVPN) offers a solution that enables sites to connect to the DMVPN hub router using dynamic IP addresses where IPsec tunnel is unable to offer [4].

The network architecture is hub-and-spoke, reflecting the fact that most traffic travels between branch locations (spokes) and the main site (hub), rather than between branches. However, utilizing a DMVPN, branch sites can still communicate to one another. It only necessitates some more configuration [4].

iii. MPLS-based Layer 3 VPN (L3VPN)

MPLS-based Layer 3 VPN is more suitable for large companies than IPSec and DMVPN [7]. MPLS (Multiprotocol Label Switching) is a method of routing packets over a network using any transport medium (such as fiber, satellite, or microwave) and any protocol capable of providing guaranteed quality of service and global connectivity [4].

Service providers can employ MPLS to construct a Layer 3 VPN. The OSI network model, which uses numerous layers to illustrate how communications are turned from electrical, radio, or optical signals into application data, is referred to as "Layer 3." Layer 3 denotes that the VPN is formed at the 'network layer' [4].

When it comes to latency-sensitive and business critical traffic, MPLS-L3VPN is more dependable and provides a better user experience and quality of service [7]. However, MPLS-L3VPN is more expensive than other solutions because of its flexibility and broader coverage [7].

L3VPNs are also known as Virtual Private Routed Networks (VPRNs).

Advantages and Disadvantages of VPN

Advantages of a VPN

The benefits of a VPN can be realized in the workplace. VPNs are ideal for remote work, employees can use them to establish secure connections to their workplace access, no matter where they are. Using a VPN for business ensures that valuable users and company data are secured, even when working from home. The following are some of the advantages of using a VPN for home and business use:

a) Bypass Geo-locked Content
Most popular entertainment websites have different content accessible in specific regions, some content is only available in a particular Geo-location. By using a VPN to make your connection appear as if it is coming from the region where the content is available, we can easily enjoy our favourite entertainment no matter where we are.

b) Safety
Your network traffic is made to appear to come from somewhere other than your own when you use a VPN. This encryption of network traffic protects VPN clients because anyone seeking to steal data would instead obtain it from the VPN server.

The user's IP address, location, and other sensitive information are all protected using a VPN. Using a VPN protects the user's IP address, location, and other sensitive information from prying eyes.

c) Secure Connection for Remote Work
Businesses today are required to consider Internet safety more than ever. With more people working remotely, confidential corporate and customer information are at a higher risk of theft.

If we have a distributed workforce, or working remotely, a secure connection to our company network is vital. A remote-access VPN encrypts online traffic, allowing us to access resources and keep data safe while working across any Internet connection.

d) Cost-Effective Security
Although new security solutions are released on a daily basis, the cost of new software, hardware, and firewall solutions can be prohibitive. You can avoid paying hefty license costs or incurring huge expenses by using a VPN service. VPN eliminates the need for those functions by making our connection invisible and encrypted online.

e) Gaming Pros
If you have access to high-speed bandwidth, using a VPN for gaming can be beneficial. A VPN can safeguard your network from DDoS attacks and rouge players attempting to gain access to it. Due to a VPN's region-free characteristics, you can choose which servers to connect to when playing a game, although one may encounter latency in some cases. Some video games are only available in only certain areas, and a VPN may be prepared to support by our access to them.

Disadvantages of a VPN

Before deciding to use a VPN, understanding its disadvantages is important. In most cases, the advantage(s) far outweighs the disadvantage(s). Below are some disadvantage of using a VPN [9]:

a) Slow Connection Speeds

- The nature of encryption: The encryption protocols process will take time to secure data packets. Thus, the stronger the encryption, the more time it will take
- The distance between client and VPN servers: The farther the VPN servers, the longer the data passage to the servers. This is due to increased travel time for requests and responses.
- The VPN server workload: The speed will be lower should the VPNs have limited server load capacity.

VPN Protocol(s)

Different VPNs use different ports to build a secure connection over the Internet. It is dependent on the VPN service provider's capabilities. A list of VPN protocols and commonly used ports are shown below [10]:

a. **Point-to-Point Tunneling Protocol (PPTP)** uses TCP port 1723.
b. **Layer Two Tunneling Protocol (L2TP)** uses TCP port 1701, UDP Port 500 and UDP port 4500.
c. **Internet Protocol Security (IPSec)** uses UDP ports 500 and UDP ports 4500.
d. **Secure Socket Tunneling Protocol (STP)** uses TCP port 443.
e. **OpenVPN** uses TCP/UDP port 1194 and TCP port 443.

Conclusion

Due to the recent COVID-19 pandemic, VPN usage surged in most organizations. Many companies decided to implement a "work from home" policy during that critical time and VPN service has since become an essential service upon which organization relies. When employers mandated all employees to work from home, using a safe and secure method of connection to the corporate network remains crucial. VPN provides a secure connection between a user and the Internet. Utilizing a VPN ensures that data is encrypted and no one can steal information from the computer.

There are four (4) types of VPN that have been highlighted and users may choose based on their preference. For corporate or organizations, remote access, mobile VPNs or Site-to-Site VPNs are ideal. For individuals, a personal VPN is the best and most affordable option.

Before deciding to use a VPN, it is important to understand the advantages and disadvantages of each type of VPN. There are several factors of VPN that need to be considered such as quality of service, cost, availability, speed and target user (i.e enterprise, individual, small or large enterprise/company, etc). However, before considering all the factors above, defining your personal or business requirements is critical to ensure the product (VPN) outcome is aligned to an organization's expectations.

References

1. What is VPN? How It Works, Types of VPN. Retrieved from https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn

2. What Are VPNs Used For. Retrieved from https://www.top10vpn.com/what-is-a-vpn/what-are-vpns-used-for/

3. Global VPN Usage Statistics in 2020. Retrieved from https://www.top10vpn.com/research/global-vpn-usage-statistics/

4. The 4 Main Types of VPN. Retrieved from https://www.top10vpn.com/what-is-a-vpn/vpn-types/

5. The Best VPN Services of 2022. Retrieved from https://www.top10vpn.com/best-vpn/

6. How to Install a VPN on Your Router. Retrieved from https://www.top10vpn.com/vpn-setup/router/

7. VPN vs MPLS: What's the Difference?. Retrieved from https://community.fs.com/blog/vpn-vs-mpls-difference.html

8. VPN Service. Retrieved from https://en.wikipedia.org/wiki/VPN_service

9. Disadvantages of a VPN. Retrieved from https://vpnoverview.com/vpn-information/disadvantages-vpn/

10. What Port Does VPN Use?. Retrieved from https://www.thevpnexperts.com/faq/what-port-does-vpn-use/

Wireless Sensor Network: Security Requirements And Attacks

By | Nor Amirah Binti Ahmad & Ahmad Hisyamudin bin Salleh

Introduction

Wireless Sensor Network (WSN) is an emerging technology which has gained considerable following. Due to its wide acceptance, WSN is now being used in various fields and applications such as industrial monitoring, military security system, air pollution monitoring, and healthcare monitoring.

Common functions of WSN include broadcasting, multicasting and routing. WSN comprises thousands of sensor nodes that are placed in remote regions. The components of these sensor nodes include sensing component, on-board processing, communication, storage capabilities and computing capabilities [1]. Through such advancement, the sensor nodes are not only capable of data collection, but also in-network analysis, correlation, and amalgamation of its own sensor data and data from other sensor nodes [1]. The sensor nodes not only communicate with each other but also with a base station (Sink/Gateway) using their wireless radio signals. The base station acts as a gateway between the sensor nodes and end users. The sensor nodes will sense, monitor, and collect physical attributes such as temperature, humidity, pressure, wind, and much more. The data or information collected from the base station is then sent to the user or application for further processing or network reporting as shown in figure 1.

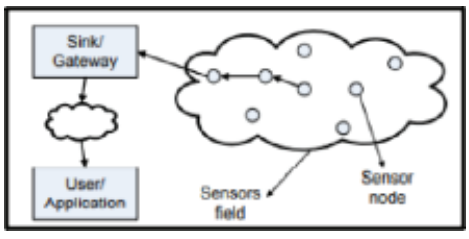


Figure 1: Wireless Sensor Network [2]

WSN is used for many applications. The basic requirement of every application is a secured network. Security is essential for this network. If the network is not secure, it may affect the functioning of these networks in the application. WSN should be secured to prevent an attacker from sabotaging the delivery of sensor node information since these networks are built for remote surveillance and unauthorized adjustments in the sensor data could lead to inaccurate information or data for the decision makers. While transmitting information or data in a network, it is important to ensure that security is maintained. Generally, providing security is the most challenging issue in WSN since it is difficult to keep a constant watch over the sensor nodes/network.

Security Requirements

The primary security requirements for WSN include confidentiality, authentication, availability and integrity; while its secondary requirement is security secure localization. Security in WSN is intended to protect resources, data and information against any type of cyber-attack.

Confidentiality

To maintain confidentiality, data access is restricted to authorized personnel only. Data should not be leaked across to an adjacent sensor network.

When one sensor node sends extremely sensitive data to a destination, it travels through the network via multiple sensor nodes. Therefore, to ensure security in data, network protocols use encryption techniques with a secret key, to enable messages to be transferred in encrypted form through the channel. Encryption also protects against traffic analysis attacks.

Authentication

Authentication is very important in WSN because the attacker can easily inject messages. The receiver sensor node must ensure that data used in any decision-making process comes from a reliable source. The purpose of data authentication is to ensure that identities of communication sensor nodes are protected.

Availability

In the WSN, availability means that the network services are accessible during a denial of service (DoS) attack. The security protocols ensure the availability of data in the network by fixating low energy and storage through reusage of code in the network [3].

The availability of a node is determined by the ability to use the resources and whether the network is available for the messages to be relayed [4].

Integrity

Integrity refers to maintaining consistency and correctness of a message. It means that when a message is sent to other sensor nodes within a network, it is not modified by any malicious intermediate nodes.

Secure Localization

To help identify the position of sensor nodes in a wireless sensor network, location based information is required. Some cyber-attacks target sensor nodes' location. Therefore, secure localization is a crucial factor during network security implementation.

Attacks

An attack on WSN can be categorized into two: active attacks and passive attacks.

Active Attacks

An active attack means an attacker tries to monitor, listen to and modify the content or flow of data in a communication channel.

In this article, we list the main types of active attacks in WSN:

a) HELLO Flood Attack
In WSN, in order to establish communication with the neighbours, a HELLO message is broadcasted by a sensor node. The receiver sensor node determines the source sensor node is within the range of data transmission and sends its sensed data or information to the broadcaster. In a HELLO Flood attack, the attacker broadcasts the HELLO message with high transmission power [5]. Pretending that HELLO message is coming from the base station or sink node, the data packets are then sent to the attacker node by the sensor nodes that receive the HELLO message. The attacker has the ability to edit or modify the data packet, as well as drop it. A lot of energy is wasted as a result way and this also causes, network congestion.

b) Blackhole attack
A black hole attack is one of the active and dangerous. In a black hole attack, when data packets pass through a malicious sensor node which acts as a black hole, allowing the attacker to modify the contents or data [9].

c) Denial of Service attack (DoS)
DoS attack is a general cyber-attack which can target any layer of the OSI model of WSN such as data link layer and network layer etc. The attackers can inject fake broadcast packets to force the sensor node to execute extensive signature verification. The DoS attack impacts the layers in the network and its related functions. DoS attack can cause radio jamming, network protocol interference, thus resulting in exhaustion of the sensor battery. The consequences of this type of attack are interruption, interception and authenticity [3].

d) Wormhole Attack
A wormhole attack is the most dangerous and difficult attack in a wireless sensor network. The attacker of wormhole attack keeps track of the packets and builds a tunnel with other sensor nodes from different communication networks. The attacker forwards the packets through this tunnel. However, this attack can be prevented with pocket leashes and geographic and temporal leashes. This is because a receiver can detect packets traveling over long distances [9].

e) Node Capture Attack
In the WSN, node capture attack is another serious threat. The intruder carries out a variety of operations and compromises the entire network. The node capture attack deletes or removes some of the sensor nodes and redeploys them to carry out multiple attacks. A redeployed malicious sensor node is used to change the data or content in the communication channel within WSN [9].

f) Sinkhole Attack
A sinkhole attack prevents the sink node (base station) from receiving the complete and accurate data from the sensor nodes. In this attack, a malicious sensor node makes itself receptively attractive to its neighboring sensor node in order to direct more traffic to itself. As a result, the malicious sensor node attracts all traffic intended from the sink node. Other than that, the malicious sensor node can conduct a more serious network attack, such as selective

forwarding, altering, or dropping the packet [12].

Passive Attacks

A passive attack means an attacker is monitoring and observing the flow of data in the communication channel. It does not change the data on the network. The main aim of a passive attack is to get the data, scan the open ports and ascertain vulnerabilities of the network [11]. There are several listed passive attacks in WSN which are:

a) Eavesdropping Attack
This is the most common attack on data privacy. An eavesdropping attack does not affect the network's integrity. In the operational network, the malicious sensor node detects the message. The attacker eavesdrops on the data or information to find out the communication channel and violates the communication network's privacy [9].

b) Traffic Analysis Attack
The attacker will analyze and examine the patterns followed in the communication channel. Next, the attacker will reveal the pattern to the opponent to harm the wireless sensor network using any type of active attacks [9].

Security Protocols in WSN

The following are protocols proposed by different researchers to solve the security issue in WSN. These protocols will help maintain security in a network.

a) Sensor Protocols for Information via Negotiation (SPINs)
In SPINs, a sensor node advertises the ADV packet containing the metadata. Should any receiver sensor node shows an interest in the data or content, then that sensor node will send a request for the said data using REQ packet. After receiving a request, the advertiser sensor node will send the DATA packet to the requestor sensor node. SPINs protocol is the protocol that has efficiency and latency properties. It performs best in small size networks.

The SPINs protocol has two secure building blocks which are SNEP (Sensor Network Encryption Protocol) and TESLA (Timed Efficient Stream Loss-tolerant Authentication) [8]. Confidentiality, authentication, and integrity are all provided by SNEP. It uses the encryption mechanism. The MAC (Message Authentication Code) is used to authenticate data. It adds 8 bytes to the message and makes it secure.

Meanwhile, digital signatures are used in TESLA to authenticate data packets. After receiving the packet containing a secret key, the base station computes a MAC and deliver authenticated packet back to the source. Node ensures that the sink does not reveal the computed MAC key to other nodes after receiving a packet. With this, receiving sensor node ensures that the data packet is original, authentic and no changes have been made to it [3].

This security protocol will help in tackling all the security threats faced by WSNs such as Sybil attack, wormhole attack and many more [13].

b) LEAP
Localized Encryption and Authentication Protocol or LEAP is a security protocol for large-scale distributed sensor networks that uses an efficient key management approach. LEAP protocol uses multiple keys mechanism to ensure confidentiality and authentication to the data packet.

Four keys are used for each sensor node: individual, pair wise, cluster, and group keys. The first one is individual key. It is a unique key used for the communication between the source and the base station or sink node. Next is pair wise key. It is shared with other sensor nodes. Next is cluster key. This is used for locally broadcast messages and shared by the sensor node and all of its neighboring sensor nodes. And lastly, the group key is a globally shared key that is utilized by all network sensor nodes. The LEAP protocol is used to defend against HELLO floods attack, sybil attack and wormhole attack [5].

c) TINYSEC
TinySec is the first fully-implemented link layer security architecture for wireless sensor networks. Integrity, confidentiality, and authentication are all supported by this protocol. In TinySec, to achieve confidentiality, encryption is done by using CBC (Cipher-block chaining) mode with cipher text stealing and authentication performed using CBC-MAC [10]. The TinySec protocol has two types of security options. TinySec-AE is for authenticated and encrypted messages, while TinySec-Auth is for authenticated messages. The data payload is encrypted in TinySec-AE, and the received data packet is authenticated using a MAC. While the entire packet is authenticated with a MAC in TinySec-Auth mode, the data payload is not encrypted [5].

TinySec security protocol can be used to defend against DOS attack [12], wormhole attack and sinkhole attack [14].

Conclusion

WSN has become a popular technology. Without good security and deployment of sensors, networks will be exposed to various attacks. This article focuses on WSN's security requirements, security attacks and counter-measures. The biggest challenge for a sensor network is its security. Some applications such as a military security system requires secure communication. To achieve such security requirements, various protocols have been proposed such as TinySec, LEAP and SPINs. The network must be secured to avoid any intruder from attacking data transmission.

References

1. W. Dargie and C. Poellabauer (2010). Fundamentals of Wireless Sensor Networks Theory and Practice, USA: John Wiley & Sonspp. 125-161.

2. Pereira and Simoes V.N (2016) Performance Measurement in Wireless Sensor Networks. pp 11-12

3. Raja W. A., & Kashif N. Q (2014) Security Issues and Attacks in Wireless Sensor Network.

4. Tanveer Z., & Albert Z. Security Issues in Wireless Sensor Networks

5. Jitender G., & Shikha S. (2016). Security Issues in Wireless Sensor Network – A Review.

6. Furrakh S., Maruf P., & Aeslan A. (2016). A survey of Active Attacks on Wireless Sensor Networks and their Countermeasures. International Journal of Computer Science and Information Security (IJCSIS),14(12).

7. Kamal S., Pranjul M., & Sonam (2014). Various Security Attacks in Wireless Sensor Network: "A Survey". International Journal of Engineering Research & Technology (IJERT) 3(4).

8. Adrian P., Robert S., Tygar J. D & et al. (2002). SPINs: Security Protocols for Sensor Networks. ACM Journal of Wireless Network 8(5) pp 521-534.

9. Keerthika M., & Shanmugapriya D. (2021) Wireless Sensor Network: Active and Passive attacks – Vulnerabilities and Countermeasures.

10. Chris K., Naveen S., & David W. (2004). TinySec: A Link Layer Security Architecture for Wireless Sensor Networks.

11. Active and Passive Attacks. Retrived from https://www.encryptionconsulting.com/active-and-passive-attacks/

12. Rashid N., et al (2013). DAP-LECP: Dos Attack Preventation and Low Energy Consumption Protocol for Wireless Sensor Networks. International Journal of Computer Applications.

13. Adam U. A., and Patel M. (2020) Enhacing the Security of Spin Framework by Combining Min AES with Geoenryption. International Journal of Computer Science and Mobile Computing, 9(10) pg. 45-63

14. Olakanmi O. O., and Dada A. (2020) Wireless Sensor Networks (WSNs): Security and Privacy Issues and Solutions.

Overview of 5G Security Challenges and Solutions

By | Farhan Arif Mohamad, Shahrin Baharom, Ahmad Dahari Jarno & Mohammad Asyran Fitri Dunya

5G, known as 5th generation mobile network, is set to fire up the new 4th Industry Revolution (4IR). As the latest standard of wireless communication through mobile network, 5G is regarded as the biggest evolution from 1G, 2G, 3G and 4G (with LTE). After all, it has the capabilities to deliver higher multi-Gbps peak data speeds, ultra-low latency in performance, reliability in delivering multimedia contents with massive network capacity, better availability and user experience when streaming online contents.

The invention of 5G originates from a consortium known as 3GPP (3rd Generation Partnership Project) driven by the GSMA (Groupe Spécial Mobile Association) technical working group comprising international equipment telecommunication vendors, services providers, government agencies and NGOs.

The 5G wireless mobile network technology enables all forms of communication between human and machines by connecting them seamlessly via mobile communication networks. Unlike 4G and other previous mobile network generations, 5G enables technology integration for new and existing technologies such as Internet of Things (IoT) devices, autonomous technologies, and smart city. The broader range of services offered by 5G networks also makes some cyber security solutions and architectures of previous networks obsolete. This article provides an overview of 5G technology, its cybersecurity challenges and possible solutions.

5G Technology Overview

5G is the fifth generation mobile network. It is a new global wireless standard after 1G, 2G, 3G and 4G networks. As the first generation of mobile network, 1G introduced a proper platform for wireless communication through mobile network, enabling consumers to communicate through voice call on a mobile wireless network. 2G is an evolution of 1G from the perspectives of data transmission with use cases of text messaging. Consumers are provided with new features of sending text messages through mobile network as well as multimedia messaging with content such as pictures and audio. As 3G was introduced to the mobile carriers and telecommunication service providers, multimedia content evolved where consumers can browse the Internet through a phone. As a result, smartphone concepts emerged, where consumer can browse the Internet with better multimedia messaging capability. Comparatively, 3G has gone through a longer adoption than 1G and 2G.

As demand for more content and data usage via mobile devices surged, 4G with LTE was introduced to replace an overloaded 3G network, whereby consumers can send more data through the mobile devices. As an improved version of 3G, 4G gave rise to social communication platforms such as social media, blog, video streaming with a new breakthrough in faster Internet connection. But as demand continued to surge, LTE was introduced as an improved version of 4G technology.

Unlike 4G and 3G, where multimedia content and social media communications had been the breakthrough technology for telecommunication industry; 5G is meant to deliver better quality services where 4G fell short. With 4G LTE, faster connectivity had been achieved, but for consumers, this was still not good enough. 5G addresses the need of more data and faster connectivity, thus allowing them to have real-time control on the multimedia content itself, rather than just receiving it. 5G is designed to enable bi-directional communication between the individual and the technology (system, devices etc) enabling users to control communication just from the palm of their hands.

5G Use Cases

The following are a list of possible use cases of 5G mobile network technology that are applicable to the industry sectors which implement 4IR.

No.	Use Case	Example And Description
1.	Manufacturing Automation	**Automated Guided Vehicles (AGV):** · AGV include tractors, pallet movers and forklift. · For example, 5G can help these vehicles move more efficiently and autonomously around factory compound.
2.	Automotive	**Autonomous vehicles/ Cellular vehicle-to-everything(C-V2X):** · Vehicle to network or V2N, connecting vehicle to 5G (base station) for updated information such as real time traffic and routing. · Vehicle to vehicle or V2V, short range communication between vehicles on the same road. Can avoid collision, identify slow or stationary vehicle and share real time information such as warning event ahead. · Vehicle to infrastructure or V2I, infrastructure for road divider, signboard, or road block. Vehicles such as ambulance, police or fire truck can be alerted on traffic signal priority request. · Vehicle to pedestrian or V2P, both need short range communication and connection to base station. Allows for safety alerts to be sent from vehicle to pedestrian and cyclist. **Autonomous Platooning Driving** · 5G is the most promising enabler of truck platooning in which long convoys of trucks are automatically governed and require only a single driver in the lead vehicle.
3.	Healthcare	**Telemedicine:** · Doctor can remotely perform consultation session with a patient through a mobile device. **Personal health system:** · Wearable devices allow users to monitor, diagnose, and treat chronic disease. For example, an Apple watch can collect and analyse data about a user and share it with the hospital for further monitoring.
4.	Retail	**Geo-Targeted Advertisement Precision:** · Better responsiveness through 5G will make geo-targeted offers more accurate and timelier. · 5G devices can be located with high precision within a few centimetres as compared to 4G which use GPS technology precise that results in tolerance within meters. · Can help small businesses like café or local shops located in densely populated areas to promote their business by providing services such as customer-centric discount coupons or events.
5.	Media and Entertainment	**Cloud gaming:** · Cloud gaming is any game-based service where the game is hosted remotely in the cloud instead of locally on a console or computer. · Allow users to connect wirelessly from physical location of their console.

Table 1: 5G Use Cases

5G Cyber Security Challenges

Just like any other mobile network technologies and wireless network technologies, 5G technology and its capabilities are always exposed to the danger of cybersecurity threats. As the mobile network evolves, it becomes more reliable with faster network speed and multiple technology connectivity. 5G allows all network connected technologies to interact with one another with unlimited boundaries, leading to further opportunities for attacker and threats to be lurking in 5G mobile network.

One of the major cybersecurity challenges resulting from massive device interconnectivity is new security vulnerabilities and attacks. Device communication and automation without any human intervention could lead to the creation of new loopholes for cyber-attacks. Technical flaws could open up opportunities for attackers to compromise any automated devices undetected, resulting in massive damage, impacting industries and organisations.

In addition, 5G comes with advanced data transmissions which allows fast and seamless data transfer and enables proficiency in mobile network connectivity. It uses software-defined networking that leverages cloud computing software defined network (SDN) advancement similar to mobile edge computing. 5G core networks enables cloud computing capabilities that allows efficient data processing through cloud SDN that managed subscriber information, mobile devices management and subscriber billing information. These sensitive data are at risk of security breaches if the 5G core network is not properly configured. Cloud computing security control implementation needs to be enforced to mitigate this risk.

Furthermore, through the efficient network connectivity of 5G, high speed data transfer enables consumer to communicate quickly, boosting productivity and efficiency. However, high speed data transfer allows large volume of data being transferred, resulting in data exfiltration. Consequently, consumers are exposed to vulnerability exploitation and cyber-attacks such as accidental malware application downloads which leads to faster spread of computer virus. Additionally, unnoticed denial of service attacks (DoS) and others, could cause disruption to any business operations.

With ultra-reliable low latency communications (URLLC), 5G mobile network enables live communication capabilities that allows telemedicine to perform remote surgeries by medical professionals. The new technology also realizes the feasibility of autonomous vehicles operating on the road with higher efficiency. With high speed data transfer supported by low latency capabilities, all devices in the 5G network are vulnerable to cyber-attacks such as malware, large scale denial of service attacks (DoS), privacy compromise due to unwanted cross data sharing, data disclosure of devices due to no IP address protection and other threats that are likely to pose risks to 5G consumer.

5G Proposed Cybersecurity Solutions

The introduction of 5G technology will definitely bring efficiency and better communication to consumers. Through 5G deployment trial projects to gauge adoption period and acceptance by local community on the 5G technology, cybersecurity need to be in place to create a secure ecosystem for the mobile network. In this article, three cybersecurity solutions are proposed to ensure a secured 5G ecosystem.

Firstly, by understanding the capabilities of 5G enabled Software-Defined Networking (SDN) security through implementation of cloud network security controls, it can become one of the potential cybersecurity solutions to be implemented in 5G mobile network technology. Through the security features of SDN such as defining secure virtualization network stages, monitoring through intelligence gathered from network resources, network learning states and flows, secure SDN provides network-wide consistent security policies and supports both instant threat identification. In addition, secure SDN architecture supports both extremely reactive and proactive security monitoring, traffic analysis, and reaction systems to facilitate network forensics, changes in security policies, and new security service(s) insertion.

Secondly, infrastructure-level attacks on 5G mobile network can be averted by continuous monitoring of users resource consumption and blocking malicious requests based on an IP address blacklisting via the Network Functions Virtualization (NFV) security controls. The NFV architecture with its security controls protects virtual functions in physical entities within a communications network. Insider threats can also be mitigated by the NFV security function by using identity and access management methods. Infrastructure-level attacks can be

further mitigated by continuously monitoring subscribers and operator resource consumption with the capability of blocking malicious requests based on an IP address blacklisting.

Thirdly, location privacy and anonymity-based approaches are recommended in which the subscriber's real identity is masked, and pseudonyms used instead. Under such circumstances, enabling security control via encryption-based procedures is favoured by ensuring all communication is encrypted before being sent to a Location-Based Services (LBS) provider. In addition, common location privacy threats such as timing and boundary attacks, can be mitigated through location cloaking methods.

Aside from these proposed cybersecurity solutions, mobile equipment vendors, as one of the key stakeholders in 5G ecosystem, should also ensure that all developed products run through proper security evaluation and testing by 3rd party labs. Promoting secured 5G ecosystem mobile network rests in two domains, namely secure deployment of systems and secure mobile equipment usage. Getting certification such as NESAS and Common Criteria for mobile network equipment leads to higher assurance of 5G secure ecosystem implementation.

Overall, there are also other vulnerabilities, threats and risks as adoption of 5G technology matures. From time to time, cybersecurity controls and solutions in 5G deployment and implementation need to be reviewed to ensure the ecosystem is safe from cyber-attacks.

Conclusion

5G is the main driver for industry changes that utilizes enhanced cloud computing technologies, including Software-Define Networking (SDN), Network function virtualization (NFV), and mobile clouds, to support the operations of mobile and IoT devices as well as other system. All these connected technologies with their own set of security issues could result in an insecure and untrusted network. The integration of various devices, services and new networking technologies increases security threats, thus necessitating the development of new security solutions for efficient and secured communication across industries and organizations. As such, the critical urgency of cybersecurity for mobile network ecosystem specific to 5G must be aligned with the technology implementation drivers across consumers, government agencies and service providers.

References

1. Ahmad, I., Kumar, T., Liyanage, M., Okwuibe, J., Ylianttila, M., & Gurtov, A. (2018). Overview of 5G security challenges and solutions. IEEE Communications Standards Magazine, 2(1), 36-43.

2. Dutta, A., & Hammad, E. (2020, September). 5G security challenges and opportunities: a system approach. In 2020 IEEE 3rd 5G World Forum (5GWF) (pp. 109-114). IEEE.

3. Mijumbi, R., Serrat, J., Gorricho, J. L., Latre, S., Charalambides, M., & Lopez, D. (2016). Management and orchestration challenges in network functions virtualization. IEEE Communications Magazine, 54(1), 98-105.

4. Sezer, S., Scott-Hayward, S., Chouhan, P. K., Fraser, B., Lake, D., Finnegan, J., ... & Rao, N. (2013). Are we ready for SDN? Implementation challenges for software-defined networks. IEEE Communications magazine, 51(7), 36-43

Augmented Cybersecurity Reality: Prospects And Challenges

By | Mohd Ridzuan Bin M Shariff, Muhamad Zaim Bin Mohd Rozi & Noor Azwa Azreen Binti Abd Aziz

Introduction

Throughout the years, the world has gone through many technological advances and breakthroughs. We have made many inroads and overcome technical barriers which once seemed impossible. No one could have ever imagined advanced technologies such as artificial intelligence, robotics and automation, as well as virtual and augmented reality. Many believed these things only happen in the movies but not real life. The world has certainly made a giant leap in technological advancement, knowledge, and skills to make them into reality.

The Fourth Industrial Revolution (4IR) and smart cities are already at our doorsteps, while the digitalization era seems to be near its peak. Even so, constant improvements and advancements in the country's technological capacity will continue to boost the digital environment, resulting in better and improved services across all sectors such as public, economy, banking, education, social and security. New and emerging technologies such as Cloud Computing, Internet-of-Things (IoT), Blockchain, Big Data, Artificial Intelligence (AI), and Machine Learning (ML) are already being implemented and adopted in today's digitalized world.

Augmented Reality

Augmented Reality is an emerging technology that provides virtual information to the physical environment. Augmented reality (AR) is a mix of real-life exposure and virtual reality. It enriches user interaction with near-reality feel through the use of computer-generated graphic layers.

Augmented Reality Around The World

In 1968, computer scientist Evan Sutherland invented the first Augmented Reality (AR) technology. However, the early versions focused on simulation for industrial, aviation and military purposes. Today, AR has become more advanced and its application can be found in almost every field.

The emergence of smartphones and advanced camera systems have further improved AR applications. As reported by Datareportal, there are 5.31 billion people worldwide who use smartphones[1]. Through a smartphone, AR is utilised as an information provider. It is also commonly used in museums and art galleries. AR provides the necessary visual or auditory information through apps or wearables to those interested to learn more about certain subjects[2]. This creates a more interactive ambience for individuals to gain knowledge on objects of interest. Currently, it is the younger generation who commonly participates actively in AR technology, especially those used in social media. An example of AR in social media is the Instagram AR filter that has a wide range of design, sound, and effects for entertainment purposes.

Types of AR

There are several types of AR: projection-based AR, recognition-based AR, location-based AR, outlining-based AR and superimposition-based AR.

- **Projection-based AR:** Video projection technique that can extend and reinforce visual data by launching images on the surface of 3D objects or space
- **Recognition-based AR:** Image recognition that depends on the identification of logo or user-defined images to operate
- **Location-based AR:** Digital compass, GPS, accelerometer, and other similar technologies that identify a device's location and position with high accuracy
- **Outlining-based AR:** Special cameras that are built for human eyes to outline specific objects such as boundaries and lines to help in certain situations
- **Superimposition-based AR:** Through object recognition, the augmented image replaces the original image. This technology is commonly used in the health industry

Application of AR for Consumers

Not surprisingly, AR is also commonly used in Global Positioning System (GPS) applications. AR

acts as a compass to detect device orientation. When it comes to smart cars, AR technology is used to determine speed, best pathway, and the most appropriate action when a car faces an obstacle in front. There are many promotional videos of the well-known self-driving Tesla car which highlights how drivers can take their hands off the steering wheel, allowing AI to determine the most suitable and safest drive[3].

Marketing. Several big organisations have started implementing AR to provide visualization options for users who are making purchasing decisions on how to decorate a house. Amazon provides a feature that enables users to insert items such as furniture in their room digitally. As stated on the Amazon site, "Show with confidence" is to ensure that a potential buyer is completely satisfied that the furniture purchased is suitable for the room size, space, and surrounding[4].

Gaming Industry. Meanwhile, the gaming industry has been actively developing AR technologies from first-person shooters, strategy games to role-playing adventures. The most popular AR game is *Pokémon Go*, an android game in which a player needs to travel to certain areas to catch digital Pokémon with the player's smartphone camera. Furthermore, AR is more common within the gaming community due to a variety of themes that can be applied to the gameplay. Ease of access to AR features within the smartphone that also provides a positive view on promoting various AR games.

Military. Not surprisingly, the military also deploys AR for training purposes. AR can be used to create almost real-life combat situation to train soldiers without the risk of injury or death. Military training is expensive and it could also put lives in danger. Another reason AR is being used extensively in the military especially the Airforce is that it injects realism especially for fighter pilots using flight simulators. Concurrently, it also saves costs and eliminates significantly any element of danger.

Healthcare. AR allows medical professionals to simulate surgery techniques and determine the best approach to handling patients' cases. It helps avoid unnecessary risks and improves the chance of patient survivability during a surgery.

Even other industries such as entertainment, sports, business, and many more have started to embrace AR due to its many benefits.

The potential benefits of using AR are as follows:

- Enhances real-life experience
- Reduces cost significantly
- Ease of use and user friendly
- Practices and improve work skills
- Converges with other modern or niche technologies

AR in Malaysia: Challenges & Cybersecurity Measures

Malaysia is currently undergoing a massive digital transformation towards creating a digital economy and becoming a leading digital nation. Due to today's competitive environment, Malaysia has started embracing new technologies to stay ahead of the curve in industrial revolution. Augmented Reality (AR) and Virtual Reality (VR) technologies have been making headway in training and improving employees' skills within a safe confine. Most industrial challenges are due to the lack of skilled and experienced employees in conducting operations with proper procedures especially in dangerous environments such as in oil and gas, automotive, aerospace, and other heavy engineering activities.

Challenges. There are still some challenges implementing AR technology:

- **Costly**. Even with accessibility to various AR technologies, only a handful of companies are willing to invest in these technologies due to high budget requirements and investments in developing industry applications.
- **Confidentiality issues**. The requirement to generate, analyse and collect significant data sets could be considered one of the prime drawbacks of augmented reality. With such data collection, confidentiality is put into question. In addition, some AR systems can capture the surroundings in real-time which raises a legal issue similar to recording someone's chat, shooting casual photos of an individual and their properties, which is generally prohibited.
- **Psychological impact**. Several healthcare studies have shown that prolonged use of AR may cause headaches, visual disorder, ataxia, and user societal behaviour. Virtual information injected into a real environment creates impact to user cognition which in turn could result in intense psychological reactions and even lead to post-traumatic stress disorder[5].
- **New data, new security threats**. Due to AR technology's popularity, many companies

started investing in AR without considering its risk implications. Most AR devices rely on online data to operate which is already fraught with cybersecurity threats.

Cybersecurity. Cybersecurity is not just about installing anti-virus solutions and hiring cybersecurity advisors. It is an ongoing team effort that is constantly evolving alongside technology development and cybercriminal activity. Cybersecurity uses AR to provide cybersecurity training to employees, create a robust security infrastructure through visualisation, and provide new opportunity to spread public awareness through a new medium.

In future, AR applications may even replace our common monitor display. AR uses people's perceptions to provide the necessary information. Within the cybersecurity space, one can set up AR as an alert or detection system in the network. AR can streamline network monitoring and security which in turn creates a better understanding by sharing visualisations with other members of the team. Information no longer needs to be transferred by words. It can be done via an animation, GIF, or essentially "show, don't tell".

Cybersecurity Measures. Nevertheless, cybercriminals can and will exploit AR technology to the fullest through malware, social engineering attack, ransomware, denial-of-service, fraud, and much more. With many companies starting to invest in big data and data analysis, AR data is also being collected and analysed, making them more valuable and worth stealing by cybercriminals. Hence, to tackle the risks and threats posed by AR, strong cybersecurity measures are required:

- **Security by design**. AR is designed to bring immersion within user interactivity between the physical and digital world. As such, cybersecurity must be implemented early and designed with "poka-yoke" or 'mistake-proof' in mind.
- **Avoid disclosing information that is too personal.** Internet of Things (IoT) is now pervasive. It is almost impossible to withhold personal information due to wide access of IoT on many sites. However, the power is still in the user's hands. Ensure users only share or provide information to the trusted devices and legitimate sites.
- **Review privacy policies:** Ensure that privacy policies are understandable and easy to comprehend to avoid any complicated issues.
- **Security monitoring**. There is a wide variety of devices that have AR capabilities, but each has different purposes with few similarities. Security monitoring collects and analyses information to identify any unusual behaviour or unauthorised activity network throughout multiple devices.
- **Practice cyber hygiene:** This can be done by using comprehensive antivirus software, regularly updating firmware, using complicated passwords, and changing passwords periodically. Never share personal information and always be aware of the latest methods used by cybercriminals.

Way Forward

Augmented reality has existed for quite some time but its growth in recent years has been exponential. The pandemic and increased reliance on digital technologies have forced governments and industries to keep up with citizens' demand for better services. Even AR has started to become commonplace within smart devices. Nevertheless, AR has not reached its full capabilities. There are still unexplored areas and untapped opportunities. However, AR technology raises new issues and challenges. AR will become a staple within any smart city and the cybersecurity community must adopt the right aptitude to ensure the safety of any user and device that incorporates AR technology.

AR is one of the most highly anticipated technologies that brings both huge benefits and risks. Applying AR entails managing between convenience, privacy, and security; while at the same time defending against cyber threats that are constantly infiltrating through the thin veil of our digital world.

References

1. https://datareportal.com/reports/digital-2022-global-overview-report

2. https://www.thestar.com.my/metro/metro-news/2022/03/17/experience-ar-interaction-at-the-museum

3. https://futurism.com/the-byte/tesla-full-self-driving-code-secret-augmented-reality-view

4. https://www.amazon.com/adlp/arview

5. https://www.verdict.co.uk/ar-and-vr-psychological-effects-2019/

Why Public Wi-Fi Should Be Avoided?

By | Mohamed Anwer Mohamed Yusoff & Muhammad Nazmie Mat Nasir

Introduction

A public network Wi-Fi is a free network for users to gain access to the Internet. Public Wi-Fi can be found in common areas such as airports, cafes, shopping centers, restaurants and hotels. These places usually allow visitors access to the Internet for free. Public Wi-Fi are so widespread and common that most people connect to the them without considering the risk. Even though it sounds innocuous to log on the Internet through public Wi-Fi and check your social media account or use it to browse news articles, standard procedures that require a login, namely perusing email or checking your bank account, could become risky . A public Wi-Fi network is innately less secure than a private one since you do not know who set it up or who else is connected to it. Preferably, it is better to utilize your mobile phone as a hotspot instead of using public Wi-Fi.

When users use public Wi-Fi, they should take precautions first as their information is vulnerable to theft or manipulation when sent through open Wi-Fi, particularly public Wi-Fi that does not require a password to access its network. Even if a public Wi-Fi network requires a password, it probably does not have encrypted traffic protecting it. Assuming the Wi-Fi network does encrypt the information, hackers can still decrypt once they know the pre-shared key.

What Are the Risks Using Public Wi-Fi?

When using public Wi-Fi, there are dangers and risks that are associated with these unprotected networks. The users connected to public Wi-Fi will be exposed to risk of information leakage as hackers can access their devices and retrieve data and information from them. Furthermore, most of the free public Wi-Fi connections have lax or non-existent security, exposing users to a myriad of risks and dangers. There are several types of risks when using public Wi-Fi that users need to be aware of, such as the following:

Man-in-the-Middle Attacks

Man-in-the-Middle attacks is a form of eavesdropping where a “man” (or a device) is placed in the middle of a connection between your device and the router, service, or site through free open Wi-Fi, and blocks information sent to and from your device. Anything you send or access over the unsecured connection is at risk— from photos, contact information, and financial data to logins, passwords, and access authorizations. Man-in-the-middle attacks usually include sneaking around or sniffing, and there are modest, highly accessible, and simple-to-utilize devices and programming that hackers can utilize to perpetrate a man-in-the-middle attack, making it a low-cost and profoundly common type of cyber-attack. When the devices are connected to the Internet, data is sent from point A (devices) to point B (website), and this vulnerability will allow the attacker to get in between these transmissions and read them. As a result, what we thought was private is not so.

Unsecured Networks

Since public Wi-Fi is generally offered as a free service, the routers utilized in these networks are frequently loaded with factory defaults and devoid of any encryption capability. Without encryption, any information you send or receive through the connection can be perused by any individual who blocks or eavesdrop on that information.

Malware

Malware can be distributed through unsecured Wi-Fi connections. If the device or the system has a software vulnerability, a hacker can slip in any malware or virus directly. Hackers can exploit flaws in an operating system or software by writing code to target a specific vulnerability and then inserting malware into devices. Malware is known as malicious software that gives an unauthorized user access to a system, device, or network. This malware can been used to steal or sabotage data and information. There are many ways in which malware or other unauthorized program, files, or data can be introduced into a network, for example through phishing, email attachments, and download links. If the devices allow file-sharing across a network, hackers can easily access and plant infected software on the devices.

Malicious Hotspots

A malicious hotspot is a rogue access point connected to a network that tricks users into a trap by making them think that they are connecting to a legitimate network as the name sounds reputable. For example, users may think a free Wi-Fi connection at an airport labeled “Airport Lounge” is safe by virtue of its name, but it is actually operated by a hacker. Users may connect to the network believing that it is the airport’s complimentary Wi-Fi connection and thinking they have selected the correct one. Instead, it just connects to a rogue hotspot set up by the hackers, who can now access and view any sensitive data and information on users’ devices.

Snooping and Sniffing

Cybercriminals can buy special software kits devices to assist and help them eavesdrop on Wi-Fi signals. This method allows the hackers to enable access to all data and everything users are doing online, starting from viewing entire website pages users have previously visited (which can contain private information that was filled out while visiting that page) to being able to capture your login credentials and even hijack your account.

How To Stay Safe on Public Wi-Fi?

As a user, it is advisable to prevent unsafe public Wi-Fi issues by refraining from using public Wi-Fi altogether. However, if you must use public Wi-Fi to connect to the network, follow these tips to stay safe and protect your information:

Use a VPN

It is essential to use a virtual private network (VPN) to connect to public Wi-Fi as it is private, although unsecured. Using the VPN will hide and prevent the data, for example, the user’s IP address and search history, from being tracked and recorded by sites that you visit. Furthermore, if the hackers manage to access your devices in the middle of the user’s connection, the data will be strongly encrypted. Since most hackers are after an easy target, they will probably dispose of the data and information taken rather than putting it through a lengthy decryption process.

Turn Off Sharing

When connecting to public Wi-Fi, users must disable sharing from the system preferences or control panel, depending on their operating system; otherwise, set Windows to disable sharing by selecting the "Public" option the first time connecting to a new or unsecured network. This is important as it is unlikely for you to want to share anything.

Keep Wi-Fi Off When You Don't Need It

Users must keep the Wi-Fi off when they are not using it. Even if you are not actively connected to the Wi-Fi, the Wi-Fi’s hardware in the computer still transmits data between any network within range. There are safety measures in place to prevent this minor communication from compromising you, but not all wireless routers are the same, and the hackers are a smart bunch. Moreover, if you use your devices to do work such as (Word or Excel) documentation, it’s better for you to keep the Wi-Fi off.

Never Use Hidden Networks

Normal Wi-Fi access points send reference points that contain data which nearby devices need to find and connect to the network. For example, the network SSID and the sort of encryption it supports. Hidden networks do not behave in the same way, but rather requires the user to have previous information about the network. Assuming you have devices that are configured to connect to a trusted hidden network of your own, those devices will continually call out the name of the network you hid, making the network an open target for anybody who can catch those reference point transmissions.

Keep the Firewall Enabled

Turning on the firewall can prevent hackers from gaining access into the user’s system. Although a firewall will not provide full protection, it should be always enabled. A firewall acts as an additional boundary that protects the user’s devices from data-based malware threats. It effectively monitors the information packets that come from the networks and checks whether they're protected. If it can detect or see of any malicious information packet, the firewall will block it. By blocking a certain kind of information, the firewall protects your computer or network and safeguards your information from attackers.

Conclusion

Digital security is very important nowadays, and we need to understand the risks of public Wi-Fi and the security problems that users will encounter when using it. As we know, many users prefer to use the public Wi-Fi because it is free, but they overlook the security risks that they may be exposed to. Public Wi-Fi is not secure and hence, Internet users could fall victim to data thefts carried out by hackers. The best way to protect our data and information is not to use public Wi-Fi at all, as this eliminates risks of hackers spying or accessing your device without being found out. Users should remember that public Wi-Fi networks are very risky. As such, they should refrain from entering sites that need sensitive personal information. For example, bank account number and information for different sites, user should disable File-sharing features because it is difficult to control different users on a similar network. If you still need to connect to public Wi-Fi in emergency cases, the steps mentioned above should help to minimize any potential risks.

Reference

1. *https://www.researchgate.net/publication/351947401_Privacy_Issues_of_Public_Wi-Fi_Networks*

2. *https://www.globalsign.com/en/blog/staying-safe-using-public-wifi*

3. *https://www.fin.gov.nt.ca/sites/fin/files/public_wifi_security_risks.pdf*

4. *https://f.hubspotusercontent10.net/hubfs/367813/Dangers%20of%20Public%20WiFi%20Whitepaper.pdf*

5. *https://medium.com/@.Qubit/is-public-wifi-safe-the-risks-of-public-wi-fi-4e3a7cd15752*

6. *https://www.kaspersky.com/resource-center/preemptive-safety/public-wifi-risks*

The OIC-CERT 5G Security Framework- Uniformity In Moving

By | Mohd Shamir Hashim, Noraini Abdul Rahman & Raja Nur Zafira Raja Sharudin

Introduction

Within an increasingly interconnected world, cybersecurity has become a central concern of all parties to ensure minimal disruption to digital transmission and management. The fifth generation (5G) wireless technology represents a complete transformation of the telecommunication networks that will boost the realisation of Fourth Industrial Revolution (4IR) where billions of devices will be connected to the Internet. It is predicted that 5G networks will have more than 1.7 billion subscribers worldwide by 2025. Against such backdrop, the 5G digital transformation will continue to introduce new dimensions of attack vectors, surfaces, and vulnerabilities through the connected digital systems.

As the world moves into uncharted territory with 5G technology, it is imperative to proactively safeguard existing and new digital platforms against cyber threats. The OIC-CERT's 5G Security Framework provides a guide for all governments, telecom providers and users in securing this new technology.

OIC-CERT 5G Security Working Group

The Organization of the Islamic Cooperation-Computer Emergency Response Team (OIC-CERT) recognises that 5G is another disruptive technology bringing in new cybersecurity challenges in the digital transformation age. Just like any other IT entities and in line with its cybersecurity objectives, the OIC-CERT strives towards preventing the loss of information availability and integrity in the 5G networks and related services and applications. The main focus is to maintain confidentiality of users' information and prevent data leakage during transmission in the network or in storage of all connected devices. To address some of the key challenges, the OIC-CERT has developed OIC-CERT 5G Security Framework, which among others, classifies the different 5G cybersecurity related threats, areas, roles, and responsibilities. The OIC-CERT is an international cybersecurity platform for information-sharing and developing capabilities for the members mainly among the Organization of the Islamic Cooperation (OIC) country community. Established in 2009, the OIC-CERT serves as a platform for member countries to explore and develop collaborative initiatives and possible partnerships in matters pertaining to cybersecurity in order to strengthen resilience in cyberspace. To date, the OIC-CERT has 57 members from 27 OIC countries and is an affiliate institution of the Organisation of Islamic Cooperation (OIC).

With the emergence of 5G, members are of the opinion that there is a need to look into the security aspect of this upcoming technology and thus, the OIC-CERT 5G Security Working Group (WG) was formed. This WG is jointly led by Cybersecurity Malaysia, an agency under the Ministry of Communications and Digital Malaysia (KKD) and also the OIC-CERT Permanent Secretariat; as well as Huawei UAE, an OIC-CERT commercial member. Currently, the WG consists of members from 10 countries which are Bangladesh, Brunei Darussalam, Indonesia, Pakistan, Somalia, Tunisia, Malaysia, Morocco, Oman, and the United Arab Emirates.

The OIC-CERT Board Meeting No. 02/2021 has endorsed the establishment of the OIC-CERT 5G Security WG with the following objectives:

- Identify 5G related cybersecurity risks taking into account the perspectives of stakeholders and maintaining a risk register
- Develop recommendations and establish a 5G security standard that serves as a reference model for member countries to develop their own National 5G cybersecurity standards
- Provide recommendations for developing an OIC-level 5G security framework that will harmonise the requirements allowing for cross-recognition among the OIC member countries
- Develop an Information Sharing and Analysis Centre (ISAC) capable of CERT response in the era of 5G and Cloud Computing for OIC member countries through the OIC-CERT

OIC-CERT 5G Security Framework

The OIC-CERT 5G Security Framework is an advanced control agreement that establishes the global norms for a safe and secure operation of the next-generation networks. This framework covers areas such as international cooperation, risk assessment and management, cybersecurity maturity, authentication and identity management, privacy protection and compliance with international laws.

The OIC-CERT 5G WG has developed a framework comprising three major documents. The first document focuses on sufficiently identify existing 5G cybersecurity threats, while the second is aimed at constructing a 5G cybersecurity baseline technical specification to provide all fundamental requirements and references for the purpose of effectively mitigating identified and upcoming risks. Since this is a framework developed for the use of various OIC-CERT and OIC countries, the third document defines a cross-recognition assurance methodology in order to guarantee harmonized 5G cybersecurity certification schemes and cross-recognised certification results among the member countries. This document also specifies the roles and responsibilities of all stakeholders in implementing 5G cybersecurity, basic requirements, references, as well as certification mechanism. Furthermore, the cross-recognition assurance methodology shows how to harmonize designing, implementing, maintaining, and optimizing cybersecurity conformity assessment among the members, so that individually certified security assurance will be mutually recognized.

Way Forward – Roll out plan

The OIC-CERT believes that no party should be left behind and therefore, connectivity based on a secure robust infrastructure is critical for the community and businesses. The cooperative and shared approach of the OIC-CERT 5G Security Framework will enable a path to greater digitalisation, trusted online services, and digital economic growth. It also enables the OIC community at large to share the same level of trust among the countries in a volatile global environment.

The OIC-CERT 5G Security Framework provides the necessary mechanism for its members to strategize and plan for adoption of 5G technology. It will enable agility and provisions for localised security requirements to be incorporated to address the fast pace, ever rapidly changing and challenging global environment in today's digital era.

Commencing in Malaysia, a workshop session for telecom operators was held in February 2020 and hosted by CyberSecurity Malaysia and supported by the Malaysian Communications and Multimedia Commission. The workshop session aimed to create awareness on the importance of 5G security, to develop a common 5G security framework for risk assessment and management, and develop a common standard among the OIC member countries, which can then be used to mitigate any technical difficulties in rolling out the 5G technology. The event marked the beginning of the OIC-CERT 5G Security Framework adoption roll-out, with a series of similar workshops to be held in various OIC-CERT member countries. Regulators and major local telecommunication operators were given an overview of the OIC-CERT 5G Security Framework, developed exclusively for the OIC community and thus, heralding a new Islamic Golden Age. The expected outcomes will be determined based on feedback and acceptance of the framework and shall act as a reference document, leading to the formation of task forces which could make modifications to the framework for local use.

The roll-out continued at GISEC 2022, the Middle East and Africa's most influential and connected cybersecurity event, held in Dubai, United Arab Emirates in March 2022. Two (2) major entities were introduced to the framework —National Agency for Computer Security of Tunisia and National Telecom Regulatory Authority of Egypt. Both organizations have shown positive response and will study the framework accordingly for adoption. These activities will continue throughout the year covering Africa and Asia region.

References

1. A. Cheang, X. Gong & M. Yang, Achieving 5G Security Through Open Standards, OIC-CERT Journal of Cybersecurity Volume 3, Issue 1 April 2021.

2. Hulk Zhang, Aloysius Cheang, Xiaoxin Gong & Yang Ming, OIC-CERT 5G Security Framework, OIC-CERT Journal of Cybersecurity Volume 4, Issue 1 April 2022.

3. https://www.oic-cert.org

How Apple iCloud Works

By | Muhammad Nasim Abdul Aziz & Kamarul Baharin Bin Khalid

Introduction

Cloud storage is commonly used among users who need extra storage for their data and information as they either lack space to store them on their hard drive devices or for easy sharing between devices. Cloud storage requires the internet in order for users to store their digital data on servers supplied by cloud providers or hosting companies. These cloud storage providers are responsible for ensuring that data is always accessible, available, and secured (Wu *et al.*, 2010). Some of the most used cloud storages services are OneDrive, Google Drive, Dropbox, and Apple iCloud.

Apple iCloud is a cloud storage service designed specifically for Apple devices such as MacBooks, iPads, iPhones, Apple Watches, and other Apple devices. A lot of cloud storage has been created since the start of its creation for every user to save their data in one convenient location that can be accessed anywhere in the world (Apple Inc., 2020). With iCloud, the storage in Apple devices' hard drives can be minimally utilized by syncing data between local storage and iCloud storage and thus, allows for data storage in iCloud to be accessed via other devices by users. Figure 1 below shows several Apple devices that use iCloud.

Figure 1: Apple devices using iCloud

iCloud Storage Service

iCloud is a cloud storage service specially integrated for Apple based devices. iCloud can also be utilized by other brand's products to store their data using an Internet browser or by installing iCloud client applications (apps). When using iCloud, Apple users can access their photos, files, passwords, music, and other data that are stored in the cloud. iCloud backs up Apple platform data from supported devices to iCloud mail, calendars, Find My iPhone, iCloud Photos, Apple Music Library, and other services (Pathak, 2020). As data is stored in iCloud, all data is automatically updated across all Apple devices.

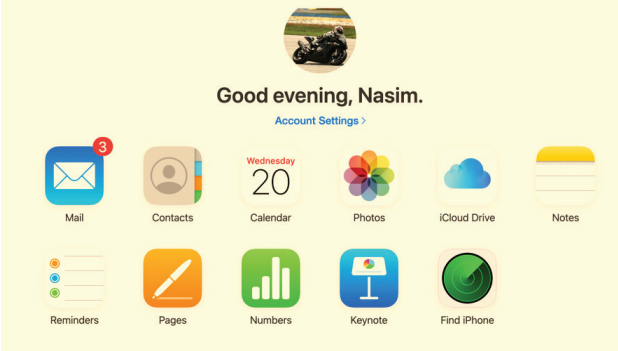


Figure 2: Stored data of user account in iCloud

Cost of the service provided by Apple iCloud varies according to storage size. Apple users will automatically get free storage for 5GB. However, they can upgrade their plan to 50GB for RM3.90, 200GB for RM11.90 and 2TB for RM39.90. The storage can be shared among family members and provides for easy sharing of photos, files, notes, and other data (Apple Inc, 2022). Figure 2 shows some of the data that is kept by iCloud and integrated across all of its Apple devices.

Apple uses end-to-end encryption, which allows only authorized users to access their information on trusted devices by signing in with their Apple ID. The data stored in iCloud also uses two-factor authentication where a user account can only be accessed on trusted devices that are verified as Apple products.

How Icloud Works?

Apple iCloud storage has its own unique management for its own devices that may differ from other cloud storage. It basically consists of two main sections, one section is to store data across all shared devices and the other section to store data, or so-called backup, for a particular device being used. These options are switched on by default, but users can opt out if they do not wish to use them. To use iCloud, users are required to sign into their devices using their

Apple ID. They can customize which data to store in iCloud according to their preferences by turning on or off in the device settings app.

Diagram 1 below illustrates Apple iCloud storage that contains two main sections in which data is stored. The First Section stores application data such as YouTube, Shopee, Waze, and Facebook as backup. This section of the cloud space does not share data among all devices and is specific to the gadgets used. For the Second Section, data stored in this segment are data across Apple's devices, such as iPhoto, iMessage, Files, Notes, Calendar and so on. The data stored in these two iCloud sections is based on specific or integrated backup data.

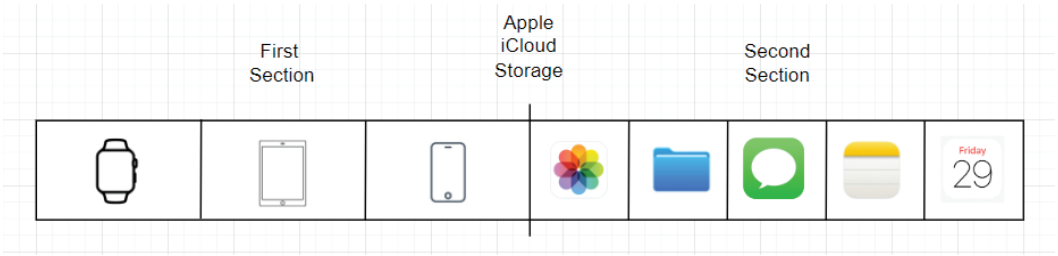


Diagram 1: Apple iCloud Separated into Two Main Sections

1. Specific iCloud Data Storage

As shown in Diagram 1, specific data from an Apple device is stored in the first section of iCloud storage as backup. Backup data from specific apps such as YouTube, allows Apple devices to store their data in the First Section. All other Apple devices, such as iPhone, iPad, Apple Watch and iPod, will back up their data to the iCloud segment in this First Section.

This storage can only be useful if an Apple device is able to utilize similar backup actions that are compatible with its Apple operating system (iOS). This is why only certain data is backed up in the First Section. Diagram 2 illustrates the data backup in which Apple devices (iPhone, iPad, and iPod) store the apps' data to Apple iCloud Storage according to the devices.

For storage of apps in Diagram 2, only First Section of Apple iCloud storage is required. It does not necessarily need to connect to all apps in iCloud as users prefer specific apps rather than having similar apps on all their Apple devices.

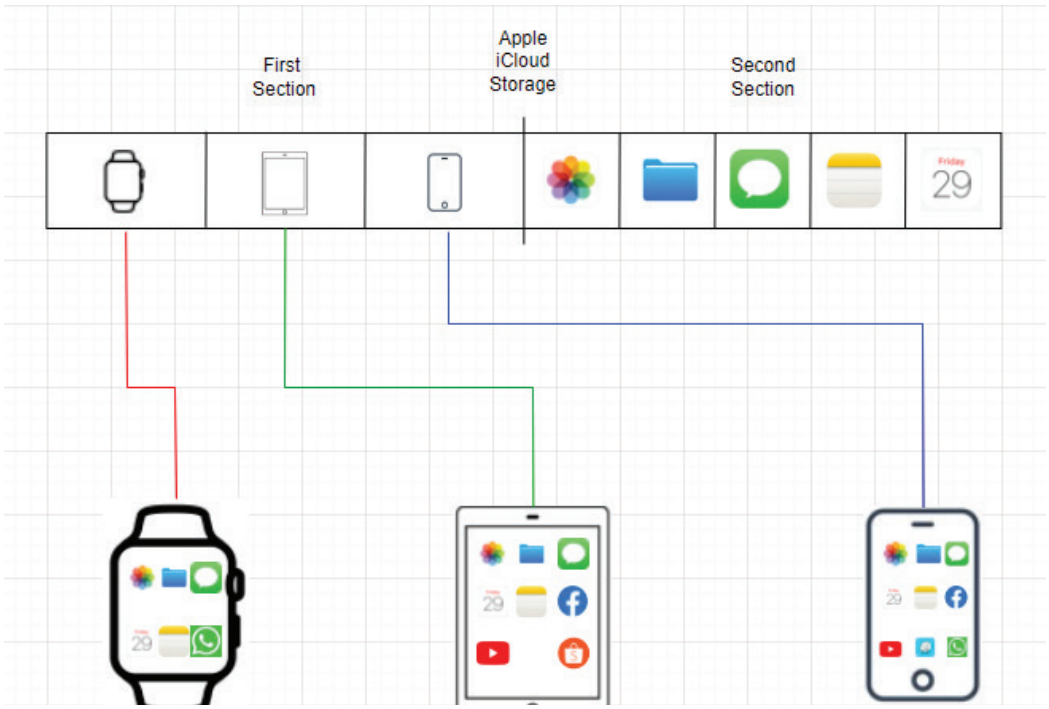


Diagram 2: Specific data storage in the First Section

2. Integrated iCloud Data Storage

Photos, messages, calendars, and other data that are useful to Apple device users must be saved and accessed in Apple iCloud storage. This sort of data must be synced and updated across all the devices, so users can use the data without having to transmit from one device to another manually. This is shown in the Second Section of Diagram 3 below, which illustrates significant amount of data that is uploaded onto Apple iCloud storage.

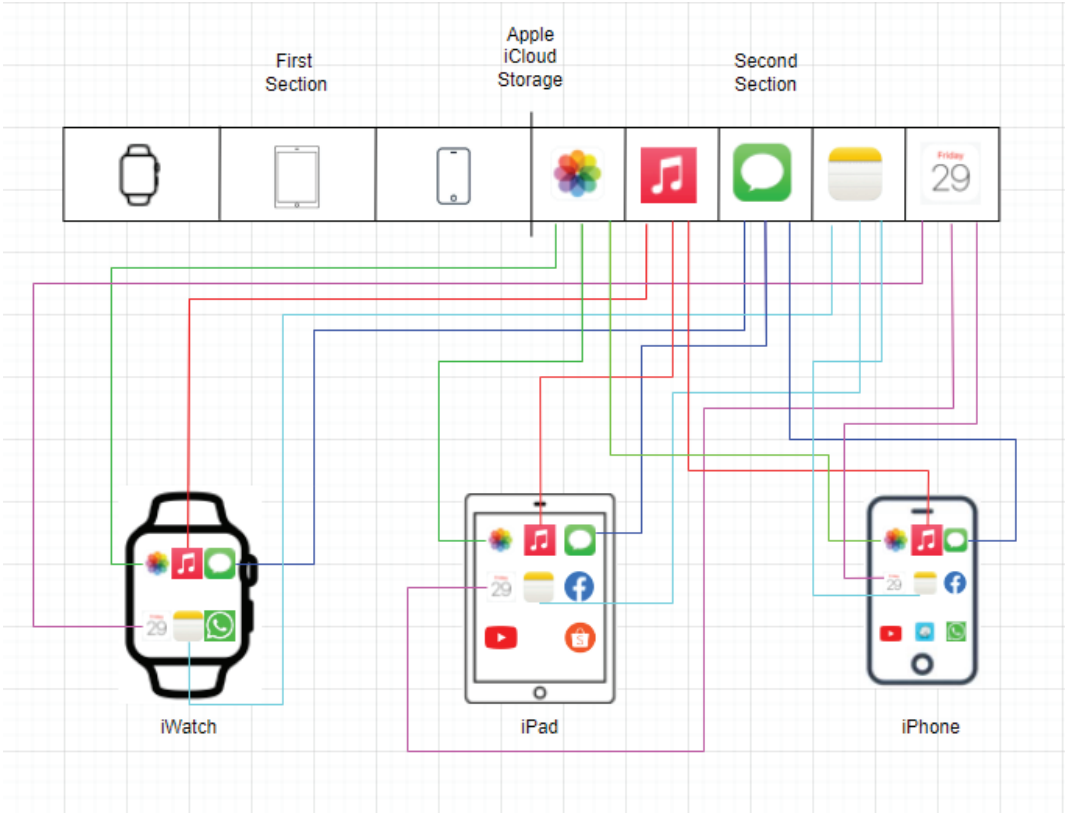


Diagram 3: Integrated data storage in Second Section

Uploaded data in the Second Section can be used across Apple devices and shared with other members that are allowed access to such data. For example, a user that wishes to share photos with his/her family member can open a shared iPhoto album and grant access to that individual. In this way, the user transmits an up-to-date shared picture, which allows the receiver to download the image without compromising the picture resolution.

iCloud users can also determine what data they wish to upload to iCloud storage by switching On or Off for specific apps. Contents that wish to be shared or collaborated via Files, Notes, or other apps can be allowed access and everyone can view the latest changes. Data will also be updated by the user through Apple devices connected via iCloud, such as in the Calendar apps.

It should be made known that all Apple devices can use iCloud for data storage backup, except for the iMac. The iMac syncs its data in desktop and document folders directly to iCloud and uses time machine to back up its data.

Conclusion

Data stored in iCloud uses two-factor authentication and is encrypted to allow only trusted devices to access them. Users can share information stored in iCloud, decide who can view their content, make changes, or experience real-time data utilization wherever access is available. In conclusion, iCloud is an easy way to store, share, and secure data for Apple-based devices. It allows users to buy Apple products with minimal storage space in their devices on the condition that they subscribe to iCloud storage.

References

1. Apple Inc. (2020) Apple Services now available in more countries around the world, https://www.apple.com. Available at: https://www.apple.com/newsroom/2020/04/apple-services-now-available-in-more-countries-around-the-world/.

2. Apple Inc (2022) iCloud User Guide, Apple Inc. Available at: https://support.apple.com/en-my/guide/icloud/mm74e822f6de/icloud.

3. Pathak, K. (2020) What Is Apple's iCloud and What Does It Back Up?, How-To Geek. Available at: https://www.howtogeek.com/669830/what-is-apples-icloud-and-what-does-it-back-up/.

4. Wu, J. et al. (2010) 'Cloud storage as the infrastructure of Cloud Computing', Proceedings - 2010 International Conference on Intelligent Computing and Cognitive Informatics, ICICCI 2010, pp. 380–383

Rise Of Ransomware During Covid-19

By | Intan Suraya Binti Samsuni & Mohamad Hafiz bin Rahman

Introduction

Ransomware is known as one of the leading cybersecurity threats that affect both organizations and individuals. Ransomware is considered a very serious threat when it comes to networks and devices. The main targets are usually Internet users and servers to encrypt user files or the entire operating system. A ransom will be demanded from the victim in order to get the decryption key to restore the data or system upon payment. Ransomware can be categorized as a malware that can affect the vulnerability of the user's system, compromising a system to enable individual access and eventually encrypt all the files that have been targeted.

Ransomware can be categorized into two main types: Locker Ransomware, which locks the computer or device, and Crypto Ransomware, which will prevent users from accessing their files by encrypting them. Locker Ransomware blocks the interactions between the user and device, by resetting the PIN code. Sometimes, it also does a full-screen window popup, which makes it hard for the user to interact with the device and the window will only disappear if the victim pays the ransom. It is different from Crypto Ransomware, whereby it will encrypt the user's data and demand payment before releasing the decryption key.

However, in some cases, Locker Ransomware and Crypto Ransomware occasionally appear together. Ransomware is becoming increasingly sophisticated, and the criminals who use it are hitting larger targets, such as hospitals, banks, and government organizations, in search of higher monetary rewards.

Ransomware During COVID-19

The rise of ransomware during Covid-19 has now become one of the main worries of any organization as their workers use and depend on digital tools when working from home. The attackers exploit the opportunity presented by the pandemic to target the victims and get profits from them. Many organizations received cyber threats during this pandemic, and as a result, the cybersecurity threat landscape changed dramatically. According to SonicWall, there were 304.7 million ransomware attackers in the first half of the year 2021, a 151% increase since 2020. After posting record highs in both April and May, SonicWall recorded another new high of 78.4 million ransomware attacks in June 2021 alone.

Ransomware volume showed massive year-to-date spikes in the U.S. (185%) and the U.K. (144%). Accounting for 64% of all recorded ransomware attacks, Ryuk, Cerber, and SamSam were the top three ransomware families in the first half of the year, as recorded by SonicWall Capture Labs. The top five regions most impacted by ransomware in the first half of 2021 were the United States, the United Kingdom, Germany, South Africa, and Brazil. Across the U.S., the five hardest-hit states were Florida (111.1 million), New York (26.4 million), Idaho (20.5 million), Louisiana (8.8 million), and Rhode Island (8.8 million).

Tactics and Techniques of Attackers

One of the common techniques employed during a ransomware attack is spear phishing. Spear phishing occurs when attackers drop malicious attachments or links in order to infect systems. Attackers also gain access to the user's system by injecting malicious codes. This will result in the user losing his or her ability to connect to their system.

Aside from that, the attackers also gain various access controls to numerous types of resources and platforms by stealing, hacking, and reusing the credentials of an individual or organization's accounts. This usually happens to famous people, whose personal accounts are often hacked easily. Why do attackers like to hack famous individuals? Hacking famous individual accounts is the easiest way to obtain money as they are most willing to pay any ransom amount so as to regain their personal data stored in the account. Another common technique used frequently by attackers is to encrypt the data. They execute malicious programs that users attempted to download in their system and execute ransomware from a remote website.

Preventive Measures

Ransomware attacks will keep increasing if nothing is done to stop them. One of the best ways to prevent ransomware is by conducting a comprehensive compromise assessment. The assessment will examine the digital assets of an organization and determine if there was any breach that has not been detected. Next, it will conduct a simulation exercise whereby a real-life scenario is created to detect phishing scams and immediately respond to make sure the activity stops and does not cause any further damage. In addition, a cyber security awareness session will be conducted to educate employees and third-party contractors on how fast cyber threats, especially ransomware, emerge in today's society and its impact as well as the required cyber security skills to counter them.

Public awareness is critical as it could stop cyber threats such as phishing scams and ransomware from getting worse. Because many ransomware variants now attempt to find and delete accessible backups, it is critical to keep offline backups of data or save data on separate networks. It is also important for organizations or individuals to patch their operating systems, software, and firmware as soon as manufacturers release the updates. Changing passwords regularly on the network system and avoiding the use of same pattern of passwords for different accounts could prevent data from getting stolen by an irresponsible party. Setting up or installing any antivirus and anti-malware is one of the best solutions for automatic updating as the user must conduct a regular scan to avoid getting any cyber threat attacks.

One of the positive outcomes of Malaysia being a target of cyberattacks, is the resultant nationwide drive to improve cybersecurity and stay ahead of ransomware menace. Malaysia's government developed the Malaysia Cyber Security Strategy 2020-2024 with a budget of RM1.8 billion to improve the country's readiness in addressing cyber threats, earning fifth ranking out of 194 nations in the Global Cybersecurity Index 2020. The government also announced plans to adopt cybersecurity law in 2021, which will help strengthen cybersecurity and improve nationwide enforcement.

Conclusion

The escalating cyberattacks during the pandemic has resulted in a higher demand for security skills across all industry sectors. Ransomware attacks will keep causing damage to organizations, individuals, and others if no major action is taken. The education sector is expected to be hit as most schools rely on digital media to minimize the number of students in one classroom. As the attacks evolve dynamically, urgent measures need to be taken to protect this sector.

Paying the ransom is not the only way, as it does not have any guarantee as to whether the data can be decrypted or not. Thus, the best way to avoid a ransomware attack is to minimize the possibility of getting one. While technology has become one of the best tools for cybercriminals to carry out cyber threats during this pandemic, it is also used by cybersecurity teams to counter the attacks. Their contribution in leveraging the latest technology to secure Malaysia's cyberspace certainly deserves our commendation.

References

1. Bhattacharya, S., and C. R.S. Kumar. 2017. "Ransomware: The CryptoVirus Subverting Cloud Security." 2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies, ICAMMAET 2017 2017-January: 1-6.

2. Gonzalez, Daniel, and ThaierHayajneh. 2018. "Detection and Prevention of Crypto-Ransomware." 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference, UEMCON 2017 2018-January: 472-78.

3. Symantec Corporation. Internet security threat report, 2016

4. Nabe C., 2020. "Impact of Covid-19 on Cybersecurity." 2020, Deloitte Website URL: https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html

5. Yas Tripathi. 2020. "Zoom App User Data Is Being Sold For 23 Lakh on Dark Web: Reports." Republicworld.com URL : https://www.republicworld.com/technology-news/apps/zoom-app-user-data-is-being-sold-for-rs23-lakh-on-dark-web-reports.html

6. Tan Kim Chuan. 2019. "The Rise and Evolution of Ransomware during COVID-19." Kpmg. 2019

7. Ransomware Activity Targeting the Healthcare and Public Health Sector. 2020 URL: https://www.cisa.gov/uscert/ncas/alerts/aa20-302a

Blockchain Technology And The Rise Of Smart Contracts

By | Muhammad Naqib bin Zahid, Isma Norshahila Mohammad Shah, Hazlin Abdul Rani & Nor Azeala Mohd Yusof

Introduction to Blockchain and smart contract

Innovative and disruptive technologies are necessary to help find better ways to deploy systems and software solutions more effectively. Blockchain is one such example, which has an immense potential to be used in a variety of applications, including Internet interaction systems, public services, Internet of things (IoT), and financial systems. Academic and industrial spheres have given blockchain technology and cryptocurrencies a lot of attention. Satoshi Nakamoto first invented the concept of blockchain in 2008 [1], and was later implemented in a digital currency system named Bitcoin in 2009. Following the introduction of Bitcoin, new blockchain-related ideas began to evolve and be adopted, resulting in the rapid evolution of this technology.

Blockchain technology has a larger global economic and industrial potential. Countries such as China, Australia, Dubai, Bangladesh, and Singapore have all embraced the use of blockchain technology. Malaysia is not left out either. The government has devised several strategies, and initiatives to stimulate the country's economic growth using blockchain technology. Blockchain technology is one of the essential technical aspects in advancing digitization in the Malaysian economy, as stated in the 12th Malaysia Plan. According to the Malaysia Digital Economy Blueprint (MyDigital) 2030 [2], the government recommends integrating new digital assets and technologies into businesses and services. Among the initiatives outlined in MyDigital is the use of blockchain to accelerate the use of the Malaysian Health Data Warehouse.

A blockchain is a digital form of a public ledger that is fully distributed to the blockchain network's members or nodes. Distributed ledgers, unlike traditional databases, do not have centralized data storage and administration functions. It is also backed up by primitive cryptography, which ensures the security and integrity of information. Its distributed and immutable nature makes it ideal for use in digital asset transactions such as property ownership transfer, recording transactions, and tracking digital assets to ensure transparency, security, trustworthiness, and value. The blockchain is based on a protocol that combines three well-known technologies: cryptography, peer-to-peer networking (P2P), and game theory.

A smart contract is a distributed software program that uses blockchain technology. Nick Szabo, a computer scientist and cryptographer, first proposed this concept back in 1997 [3]. Nick Szabo believes that by combining clear, logical observations with the validation and enforcement of cryptographic protocols, the functionality of smart contracts can be developed much more effectively from the basic idea he proposed. However, his concept of smart contracts did not gain traction until the advent of blockchain technology, which enabled it to be fully implemented.

In general, smart contracts are computer protocols that facilitate, validate, and enforce digital contracts created by two or more parties [4]. Smart contracts are self-contained, self-verifying agents that are stored in the blockchain. They are made up of fields and functions. Once deployed in the blockchain, they have a unique address where users/clients can interact. It is referred to as a 'contract account' to distinguish it from an 'external account,' controlled by public-private keys used by humans. Furthermore, the code stored in blockchain after deployment is a low-level stack-based bytecode representing the high-level programming language (a JavaScript-like language) in which the smart contracts were initially written. As a result, because the bytecode is publicly available on the blockchain, smart contracts' behavior is entirely predictable, and any node in the network can inspect their code.

Blockchain technology has seen a rapid increase in the use of its applications across various domains, thanks to smart contracts. Among them are smart contracts' ability to improve the insurance process by automating the claims system when specific incidents occur, allowing for a smoother supply chain process, and leveraging a wide range of applications in business, commerce, and governance.

Like all existing computer programs, these blockchain and smart contracts are vulnerable to programming code vulnerabilities. As with all new technologies, they are the target of hackers who will try to exploit them for personal gain. As these blockchain and smart contracts grow in popularity and acceptance, best practices for implementing such codes must be established [5].

How Smart Contracts Functions

"Smart contracts" refers to a computer code that automatically executes all or portions of a contract and is stored on a blockchain-based platform. The majority of smart contracts are written in Solidity, a programming language that is specifically designed for such computer systems.

A smart contract code can either be the whole representation of the parties' agreement or augmented from a traditional text-based contract by carrying out specific requirements, such as sending payments from Party A to Party B. The code is duplicated across several blockchain nodes, delivering security, permanence, and immutability that only a blockchain can provide. This duplication ensures that the code is effectively performed as each new block is added to the network. If the parties have signaled that specified parameters have been satisfied by commencing a transaction, the code will perform the step triggered by those parameters. The code will not take action if no such transaction has been achieved. These processes can be visualized in Figure 1.

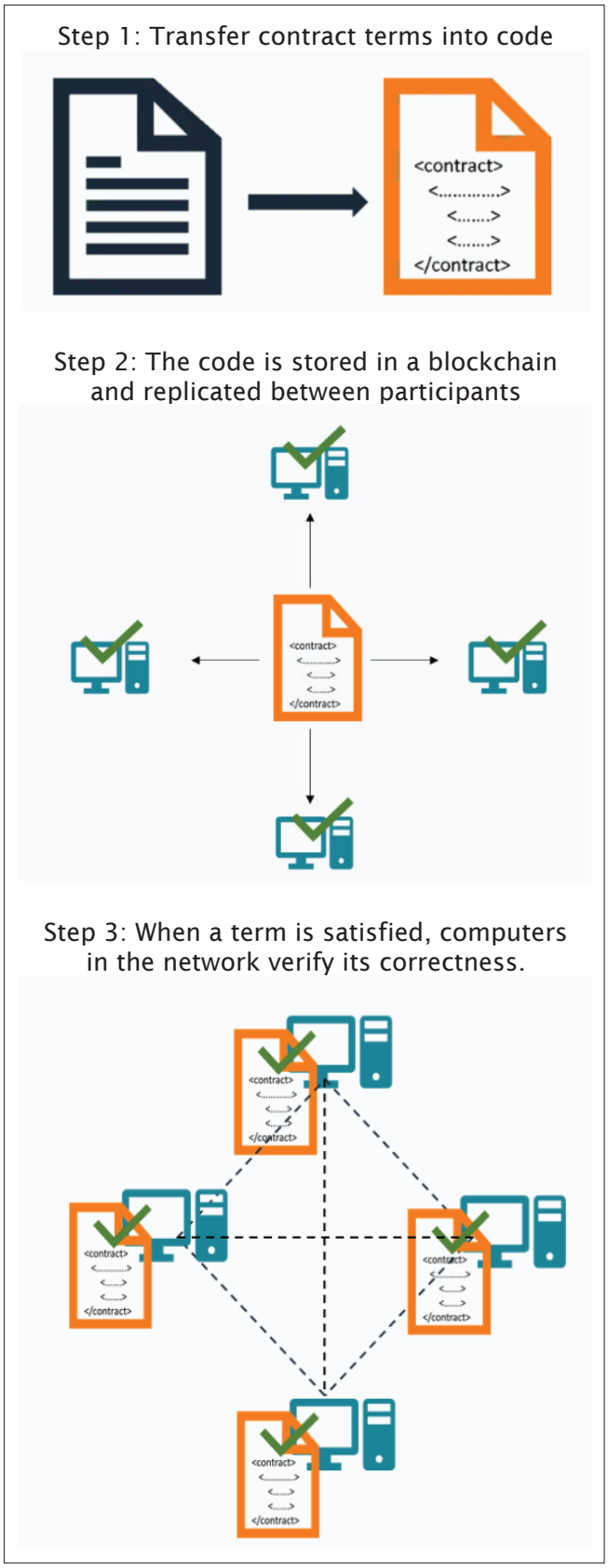


Figure 1: How smart contract works

(Source: Smart Contracts, [6])

For the time being, a smart contract's input parameters and execution phases must be precise and objective. In other words, if "x" happens, go to step "y." As a result, smart contracts' actual functions are quite basic, such as automatically sending a certain amount of cryptocurrency from one party's wallet to another when a specific criteria is met. Smart contracts will grow more complicated and capable of managing sophisticated transactions as the usage of blockchain spreads and more assets are tokenized or placed "on-chain."

An additional step is necessary before a built smart contract can be performed on certain blockchains: payment of a transaction fee for a contract to be added to the chain and performed. In the case of the Ethereum blockchain, smart contracts are performed on the Ethereum Virtual Machine (EVM), and this payment is known as "gas." It is made using the Ether cryptocurrency. The more complicated the smart contract (depending on the transaction processes to be completed), more gas will be required to execute it. As a result, gas serves as a critical gatekeeper to keep overly complicated or many smart contracts from overloading the EVM.

Smart contracts are now best adapted to automatically execute two types of "transactions" in many contracts; securing the payment of monies upon specified triggering events and imposing financial penalties if particular stipulated conditions are not accomplished. Human involvement is not required in each situation after a smart contract is executed and functioning. As a result, expenses related to contracting process execution and enforcement are reduced.

Smart contracts can also reduce what are known as procure-to-pay gaps. When a product is delivered to a warehouse and scanned, a smart contract might be initiated to request for necessary approvals. Once granted, payments will automatically be effected from the buyer to the seller. Sellers would get paid faster, while purchasers' account payable fees would be reduced. This process makes financial operations easier for both parties. On the enforcement side, if a payment is not received, a smart contract might be configured to disable access to an Internet-connected item. In addition, access to some materials may be restricted automatically.

Adoption of Smart Contracts/ Smart Contracts Applications/ Smart Contracts Benefits

Smart contracts provide numerous advantages, particularly for businesses, governments, and individuals. One of their key advantages is that smart contracts are secure and efficient. Since smart contracts run on blockchains, it is deemed safe. As blockchain is immutable, the contracts' records are secure and cannot be easily altered by third parties. The decentralization of a blockchain contributes to the security of smart contracts by ensuring that no single entity or authority has complete control of the blockchain, hence improving trust in smart contracts. Transparency and traceability of transactions can be assured because every transaction is recorded on the blockchain, boosting trustworthiness of smart contracts.

Since smart contracts are digital, they save time. A deal can be executed in a matter of minutes when all terms are met. This is significantly faster than manual contracts, which can take days to complete due to time zones and conditions confirmation. Smart contracts are also less expensive because they do not require the use of law offices or intermediaries to mediate. Related parties also do not need to go through legal compliances and/or middlemen to mediate a contract, which might take days or weeks.

Smart contracts can be used in various industries, including the supply chain. Multiple stakeholders are involved in the supply chain industry, which is a complex field. Due to the complexity, it's challenging to keep track of every event during a delivery process, making it difficult to pinpoint the root cause of problems and the responsible party. Every event or transaction that occurs within a smart contract is recorded. This will provide a thorough record of the transaction and delivery of the merchandise. Clients and suppliers are kept updated about the product's delivery stages and any complications that could arise. Because records are encrypted to a block, the information provided can be trusted and relied upon, enhancing vendor-client trust.

Smart contracts are also used in the healthcare industry. With traditional methods, maintaining the confidentiality and security of patients' medical records could be challenging. Medical records held in the hospital system are vulnerable to tampering and data breaches. The use of blockchain could eliminate any uncertainty about the patients' records because

the records are encrypted, preventing any unrelated parties from reading them. They are immutable, therefore any tampering is not possible. Physicians worldwide could access the record through a connected network, enhancing treatment efficiency. Patients could also use the records as documentation when filing a claim with their insurance provider.

Property ownership could be accomplished more easily with the use of a smart contract. Acquiring assets or intellectual property can be time-consuming and costly. Furthermore, small and medium-sized businesses could struggle since they lack the financial resources to pay for the services. Unaffiliated inventors face difficulties to register their intellectual property because they do not always have the financial ability. A smart contract could make intellectual property registration easier. Because the process is straightforward, the cost of registering property is lowered significantly, and creators can quickly register their work.

The Internet of things can benefit from smart contracts. One of the biggest fears about the Internet of things is that it could be hacked. Hackers can gain access to any device that is connected to the Internet. Any tampering with the device could result in serious accident as it interacts with the Internet and humans. For example, a life-threatening catastrophe might occur if a traffic light connected to the Internet is hacked. Smart contracts can lower the probability of devices being tampered with due to the encryption feature. As an added advantage, a device's history can be easily traced, through smart contract’s records, thus ensuring transparency.

Smart contracts are also transforming financial services. Trust is critical in financial services. Some organizations may need days or months to verify the authenticity of a transaction before executing it. As an example, in traditional banking, transferring funds from one bank account to another takes three days. This is not limited to banking; it is also practised in other services such as insurance and payment. Transparency is also mandated in financial services, as money leakage is a major concern. In terms of speed and security, smart contracts could take financial services to the next level. Smart contracts will execute promptly once all preconditions are met, saving a significant amount of time when making transfers or payments. Transactions that previously take days might now be completed within minutes. Many other services could be accelerated because of this. Smart contracts also increase the assurance of any transaction because they are immutable and always recorded in a blockchain, thus allowing enterprises and clients to trace their money's movement.

With the benefits of smart contracts, many corporations seek to implement them in their operations. For example, the Union Bank of Switzerland (UBS) built a payment stream for unbanked clients by implementing a micro contract that executes automatically. In music industry, a streaming music network uses a smart contract to ensure intellectual property ownership of songs played. Another application is healthcare service provider which stores patients' medical data as encrypted smart contracts in a secure network for access by physicians.

As blockchain and smart contracts are useful in transforming business operations, major corporations are eager to incorporate them into their systems. While some are still in exploratory stage, others have implemented in real life. This might hasten the adoption of smart contracts across the ecosystem, including finance, commerce, business, and governance.

Limits, Challenges, and Security of Smart Contracts

Despite the rapid development of blockchain and smart contracts, they are not without limitations and obstacles. One of the major constraints of smart contracts is that they are difficult to alter once deployed due to their immutability. After the contract has been deployed on the block, it is difficult to amend its terms and conditions. To modify a smart contract, the majority of the nodes must agree, and getting a majority agreement for a change is difficult. In the case of a standard contract, one can easily amend any term in the agreement by either party, intermediaries, or legal offices. For any contract amendment in a smart contract, this process could take a long time and cost a lot of money.

One of the critical limitations of smart contracts is the possibility of contract loopholes. Creating a contract is a time-consuming process in which the agreement, terms, and conditions must be set down and understood by both parties and the contract's developer. Developers must then establish a contract that contains all agreed-upon conditions and adheres to them. Poorly skilled work could give rise to loopholes in the contract, allowing unforeseen events to disrupt the basis of a contract. Consider the

case of reentrancy. A reentrancy attack has been known to occur in a smart contract. An adversary completes a transfer twice without recording the initial transfer in the contract, giving the impression that only one transfer was completed. This could occur due to a flaw in the contract, allowing a malevolent actor to hijack a transaction. Although reentry is an old problem, it still exists today. This is just one of the numerous issues that could arise due to contract flaws.

Precision is another significant limitation when building smart contracts. Because computer programs cannot grasp ambiguous phrases, smart contracts cannot interpret ambiguous contract terms. Just as traditional contract requires human lawyers to mediate the terms to be precise, a smart contract also requires lawyers to ensure the terms are precise and executable. There is a limitation in implementing smart contracts as both lawyers and developers must understand one another's requirements in order for the terms and conditions to be appropriately created. The contract agrees to the lawyer's terms and the lawyer can understand and evaluate the contract written. Vague phrases are harmful to a contract, whether traditional or smart. In the past, vague terms can be clarified through spoken and written language; however, it is more difficult to do so in computer programming languages since spoken, and computer programming languages operate differently.

Smart contracts are limited by its silo operation. Due to the nature of blockchains and the environment within it, interoperability between blockchains is currently difficult. As a result, a contract created and deployed in one blockchain could not interact with another contract written and deployed in another blockchain. Both contracts must be implemented in the same blockchain to interact. This could result in a contract having to be rewritten due to language variations, resulting in additional operating costs for rewriting. Not to mention the experts' limitations, especially in languages.

Some hurdles must be overcome first before smart contracts can be used or adapted widely in the current system. Although smart contracts have been around for at least five years, they are relatively in their infancy. Many constraints are imposed on smart contracts, and resoluttions to these limitations require a significant amount of work before smart contracts can be refined and adopted easily. Furthermore, expertise in this field is low. Therefore, the development of smart contracts is still limited. Smart contracts is even more difficult for the public to understand as compared to ordinary commercial contracts. From the administrative to the legislative levels, society needs to understand blockchain. Even though a smart contract is technically secure, its security is still under heavy scrutiny due to its novelty. In addition, there are not many reliable security verifications. Even though technologies for contract verification exist, they are either not yet fully developed or require a highly qualified expert to implement.

The learning curve for blockchains is another significant challenge for coders lawyers, judges, and the legal system. A smart contract still falls under the jurisdiction of the law. However, due to the barrier of computer languages, it is difficult to bring a breach of contract to court. Lawyers and judges may need to learn how to understand smart contracts, and there is a lack of expert witnesses who can be called to testify to legitimate interpretations.

Governance difficulties are also hampering the adoption of smart contracts. Traditional contracts encountered numerous obstacles and challenges before the government could fully regulate contract governance. Because smart contracts are still in the early stages, governments are still debating on how to regulate or even tax contract transactions. Therefore, smart contract regulations will take some time to be established.

While smart contracts could be utilized for simple transactions the same could not be applied in complicated systems, such as a distributed autonomous community. Because the social ecosystem is complex, it is difficult for smart contracts to be incorporated. Creating an ideal contract to address such difficulty is possible but making it a reality will be difficult and require the involvement of many parties due to the scarcity of professionals in the sector. Because the general public does not comprehend the nature of smart contracts, education on the technology must take place first to lessen the fear of new technology adoption.

Limitations in smart contracts are obstacles that must be addressed before the public can use smart contracts. As of now, smart contracts can only be used by large corporations and governments because they are the only ones who can afford to implement them. Experts are likewise in short supply in this field. Since this is a new technology, few professionals could help advocate it. This applies to other technical aspects of this technology as well, such as smart contract debugging, testing, and

verification. It is essential to ascertain whether smart contract security is genuinely secure or merely conceptually secure.

With regards to smart contract security, at present, the only means to secure smart contract security is to scrutinize every line of code, use smart contract analysis tools, or formal verification of smart contracts (Rouhani & Deters, 2019). A group of developers will team up to inspect every line of code in a contract to guarantee that it is free of flaws. This strategy may reduce contract risks, but it is time-consuming and may not uncover any inherent weaknesses.

Security analysis tools such as OYENTE or SECURIFY can also be used to verify the code. These tools will extract information from the contract code and display any vulnerabilities discovered. Although this strategy is more time-efficient, such tools are still new and under development, which reduces the tools' reliability. Furthermore, such technologies cannot detect all the contract's weaknesses.

Finally, formal verification could be employed to verify smart contracts security. Formal verification is transcribing the functions' specification of a code in a proof assistance tool and using a formal method to ensure that the contracts' functions operate as specified. This method might uncover all vulnerabilities in the contract with a single tool; however, transcribing the code requires a master. Such masters are in short supply worldwide, so hiring one to perform formal verification on a smart contract could be onerous.

General Best Practices for Smart Contracts

When it comes to security, best practices are important to ensure a smart contract can defend itself against bugs and vulnerabilities. Some of the best practices that developers can adopt in their philosophies and approaches are:

1. Be ready for failure
All significant contracts are always prone to errors. Hence, a smart contract must have the ability to respond when errors occur. One way is by pausing the contract or breaking the circuit whenever things go wrong. Furthermore, formulating an effective upgrade strategy with improvements and methods to fix bugs and loopholes can also make smart contracts ready for error. Additionally, limiting the maximum usage rate and managing the total amount well are ways to manage a smart contract effectively.

2. Ensure careful rollouts
This practice can help detect and resolve bugs before the full production phase. This can be done by thoroughly testing the contracts, rolling them out in incremental phases with increased usage and testing in each phase, providing bug bounties from as early as the Alpha TestNet releases, or adding tests at the discovery of every new attack vector.

3. Always keep the contracts simple
The more complex the contracts, the more likely potential errors and bugs will occur. Hence, the best way to reduce the chances of errors is by keeping them simple. The first step to implementing this practice is by ensuring the contract logic is simple. If possible, code or tools used in writing the contracts must already been written before. The code can be modularized to reduce the size of the contracts and functions. Not all parts of the system should be converted into blockchain technology. Only parts of the system that need decentralization need to use blockchain.

4. Stay updated and keep track of new developments
A smart contract developer must constantly stay updated with any new security developments or changes. The written smart contracts must be regularly checked to see if there are any bugs and errors. Should any tool or library be used in writing the contracts, the developer must ensure that the version used is the latest. If not, the tool or library must be updated to the latest version as soon as possible. The developer must be open to adopting new security techniques in securing smart contracts.

5. Be attentive to blockchain properties
Ethereum programming can be handled competently by developers with enough programming experience. However, they must be alert of certain pitfalls and blockchain properties. Developers must be aware of any external contract calls as they are exposed to malicious code and tampering with control flow. They must keep in mind that anyone from public functions can view private data in smart contracts, including attackers as they are also regarded as 'public.' On blockchain, timestamps are imprecise. Miners can alter or impact the time of a transaction's execution in mere seconds. Another two important factors that must be considered during writing contracts are the block gas limits and gas costs as well as approaches to random number generation, mostly for gameable and non-trivial.

6. Consider fundamental trade-offs
An ideal smart contract system should be modular, supports upgradeable components, and is able to reuse code without duplicating it in software engineering. However, an ideal smart contract may or may not share the same approach from a security architecture's standpoint. Hence, when assessing a smart contract system's security and structure, a balance between these trade-offs must be struck. Find a balance by making an optimal mix of properties like duplication, reuse, modular, monolithic, up-gradation, and rigidity.

7. Duplication and reuse in contracts
Reusing contract code should be encouraged where possible and done by using previously deployed and proven contracts. On the other hand, developers should not rely on duplication if previously self-owned contracts that have been deployed are not available.

8. Monolithic and modular contracts
Monolithic contracts normally keep all data readable and identifiable only locally. This is acceptable unless such localization is too extreme that it impedes data flow. This can impact optimizing the code review efficiency.

9. Rigid and upgradeable contracts
There is a fundamental trade-off between security and 'malleability' of smart contracts. Malleable patterns make contracts complex and can also increase the risk of potential attacks. Hence, developers must emphasize simplicity over complexity if smart contracts were to perform limited functions for a pre-defined period.

Future of Smart Contracts

Smart contracts are currently utilized in transactions involving cryptocurrencies or blockchain corporations. They will become increasingly popular once our society gains a deeper understanding and confidence in blockchain technology. The bigger question is whether smart contracts can be used to enforce non-monetary agreements which may be more difficult to manage. Should this obstacle be overcome, the number of financial component agreements using smart contract will grow significantly.

References

1. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/en/bitcoin-paper

2. Economic Planning Unit (EPU). (2021). Malaysia Digital Economy Blueprint. Prime Minister's Department, Putrajaya, Malaysia. Retrieved from https://www.epu.gov.my/sites/default/files/2021-02/malaysia-digital-economy-blueprint.pdf

3. Szabo, N. (1997). The Idea of Smart Contracts. Retrieved from Nick Szabo's Essays, Papers, and Concise Tutorials: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html

4. Wang, S., Ouyang, L., Yuan, Y., Ni, X., Han, X., & Wang, F.-Y. (2019). Blockchain-enabled smart contracts: architecture, applications, and future trends. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2266-2277.

5. Benabbou, C., & Gürcan, Ö. (2021). A Survey of Verification, Validation and Testing Solutions for Smart Contracts. 2021 Third International Conference on Blockchain Computing and Applications (BCCA) (pp. 57-64). IEEE.

6. Smart Contract, https://corporatefinanceinstitute.com/resources/knowledge/deals/smart-contract/

7. Best Practices For Ethereum Smart Contracts, https://www.leewayhertz.com/best-practices-for-ethereum-smart-contract/

8. Challenges for the Adoption of Smart Contracts, https://scalablesolutions.io/news/challenges-for-the-adoption-of-smart-contracts-2/

9. Benefits Of Smart Contract Adoption, https://blaize.tech/article-type/smart-contracts-with-blockchain-how-it-can-help-startups-be-more-cost-efficient/

10. Smart Contracts, https://corporatefinanceinstitute.com/resources/knowledge/deals/smart-contracts/

11. The promise of smart contract adoption is held back by crypto silos, https://cointelegraph.com/news/the-promise-of-smart-contract-adoption-is-held-back-by-crypto-silos

12. Smart Contracts: Adoption Value for Enterprises and General Use Case, https://antgrasso.medium.com/smart-contracts-adoption-value-for-enterprises-and-general-use-case-3c8303b387c3

13. What Are The Advantages And Disadvantages Of Hospital Management System?, https://healthcaretech.bcz.com/2020/08/06/what-are-the-advantages-and-disadvantages-of-hospital-management-system/

14. Smart Contracts and Financial Services, https://www.deltecbank.com/2022/02/15/smart-contracts-and-financial-services/?locale=en#:~:text=Smart%20contracts%20are%20tamper%2Dresistant,to%20finance%20smart%20contracts%20bring

15. Rouhani, S., & Deters, R. (2019). Security, Performance, and Applications of Smart Contracts: A Systematic Survey. IEEE Access, 7, 50759-50779. https://doi.org/10.1109/access.2019.2911031

Biometric Acceptance In Malaysia: Part 2

By | Nur Iylia Binti Roslan, Nor Zarina Binti Zamri, Ahmad Dahari Bin Jarno, Farhan Arif Bin Mohamad & Mohd Muslim Bin Mohd Aruwa

Abstract - Malaysia has adopted and used biometric fingerprint technology across ICT products and systems since 2001 when MyKad was first introduced to Malaysian citizens. Since then, the technology has sparked a dramatic change in trends where more diverse biometric modalities have emerged. A survey was conducted to find out the readiness and acceptance level of biometric technologies among Malaysians. The survey found that, there is an unmet need for defining security testing requirements in the national testing program. Through the study, security testing requirements of biometric technologies are being adopted in the product lifecycle for devices and systems. These have led to a certain unique proposed list of criteria to fulfill the needs and demands. The criteria defined must be able to fulfill and balance in the aspects of biometric usability, acceptance of usage and performance.

At the same time, these initiatives of defining the criteria have also steered technological innovation and exploration into uncharted territories and unlimited heights.

Introduction

In the previous article - *"A Biometric Acceptance in Malaysia Voyage Part 1"*, the Technology Acceptance Model (TAM) was used to identify the readiness of Malaysians in accepting the adoption of biometric technologies in Information Technology (IT) ecosystem. Within the TAM study, there are four main aspects to consider before any technology will be used, namely through External Variable, Perceived Usefulness, Perceived Ease of Use and Behavioral Intention. These main aspects needed to be defined and understood within the framework of TAM analysis before any type of technology can be adopted. Figure 1 shows an example of a TAM framework.

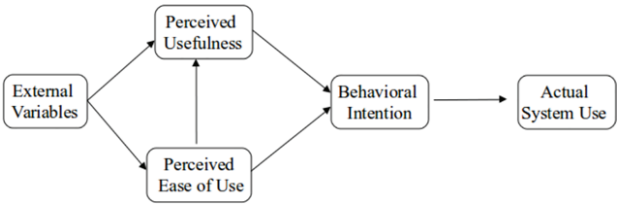


Figure 1: TAM framework (Ventash & Davis, 1996) [1]

Based on the overall view of biometric acceptance and technology adoption, users' feedback played a pivotal role in this research. If users are confident of a technology and it meets their demands, they are more willing to use the technology. Therefore, we highly recommend that a product be tested and certified in order to achieve biometric acceptance and technology adoption.

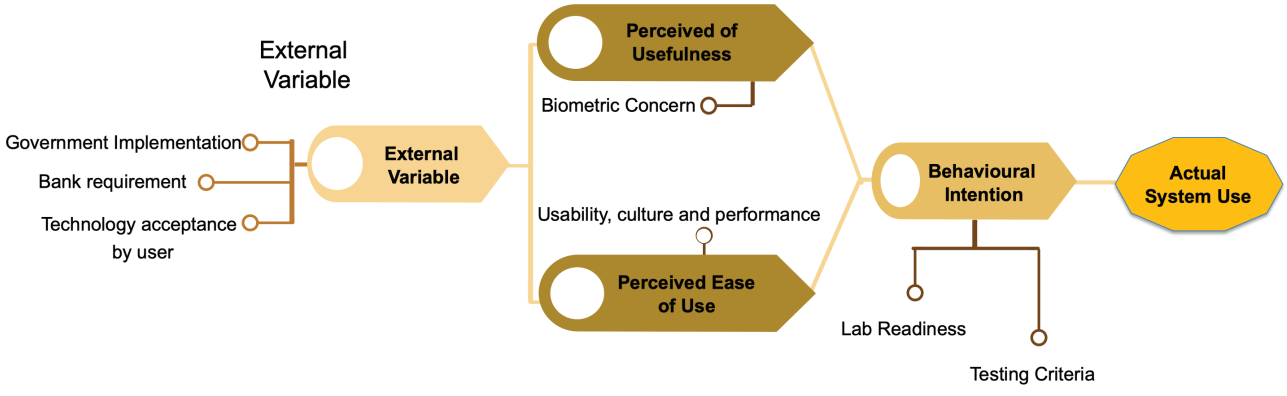


Figure 2: Summary Content Base on TAM

Figure 2 illustrated the flow of all the four main criteria that leads to the proposed requirements to define the Lab Readiness and Testing Criteria. These two aspects will influence the behavioural intention of users in accepting the biometric implementation through a technology implementation from the view of actual system usage experience. This article will describe the journey of CyberSecurity

Malaysia Security Evaluation Facility (CSM MySEF) in the research, development and experience to uncover the biometric security and its technology.

CSM Mysef Voyage In Biometrics Security Testing

CSM MySEF started the journey in biometric back in 2016, where its researchers and evaluators attended training by well-known trainers in biometric technology. To put into practice of what had been learned, the first evaluation in fingerprint biometric challenge began in 2017. From there, CSM MySEF managed to improve the testing methods and continuously research other biometric modalities. In 2019, CSM MySEF expanded into other biometric modalities such as facial and finger vein through joint ventures with local universities to gain further understanding on biometric technologies from development process. The evaluation facility gradually attained its capabilities in biometric security testing field, eventually devised Security Functional Requirements (SFRs) for biometric security testing on specific modalities, as well as successfully developed test methodologies.

Biometric Projects

Here, we review some of the biometric projects that were previously executed. Two projects were successfully executed in 2018:fingerprint access control evaluation and fingerprint device evaluation for border control operation. Both projects were executed by adopting the Common Criteria evaluation methodology with additional security testing criteria that were requested by the client related to performance testing in terms of time taken to execute the verification and identification process. Both projects were performed based on similar SFRs.

Identifying The Gap In TAM

In order to understand the flow of biometric testing and acceptance in technology implementation, there was a need to identify the gap in the elements in TAM. Figure 3 summarizes the points for external variables, biometric concerns and balance between usability, culture and performance.

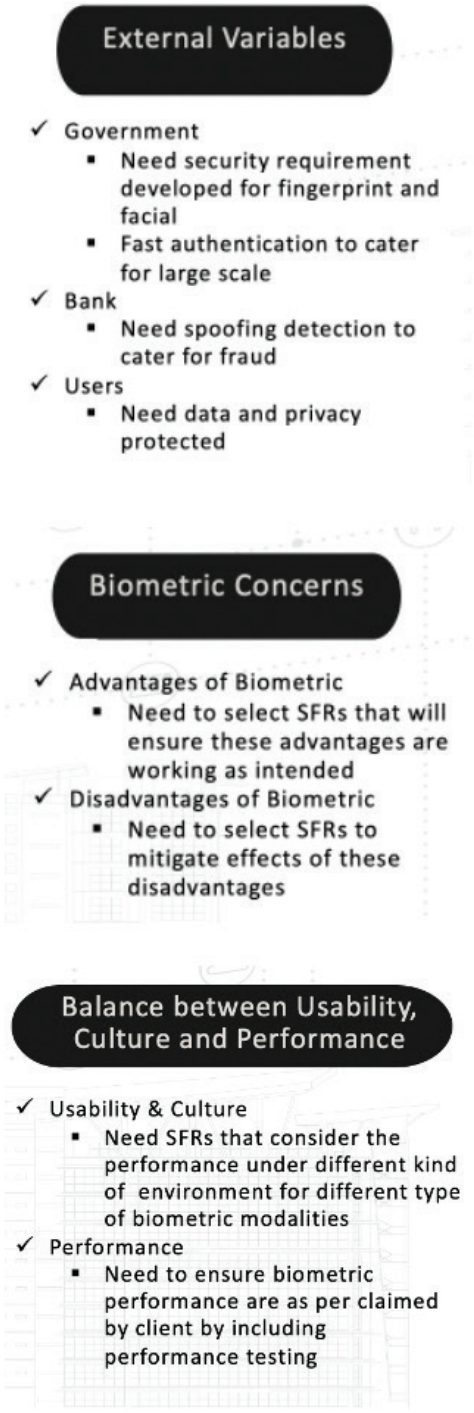


Figure 3: Gap for each element in TAM

Based on external variables criteria, there is a need to develop the requirements for fingerprint and facial, as the government is dealing with a large scale identity management system. Thus, the system needs to be efficient, error-free and secure. As for the financial sector, fraud issues have been a major threat to the industry, thus their concerns are more on the presentation attack issue. Whereas for community, they need the confidence of the technology implementation, to ensure privacy of their biometric data is protected.

Biometric has both advantages and disadvantages. There is a need to define the SFRs towards instilling more confidence on the benefits of biometric implementation. Implementing several testing methods on the biometric solution will help identify and correct its weaknesses.

As for usability culture and performance, it can be balanced through performance and penetration testing.

Identifying The Gap In Previous Biometric Projects

Figure 4 illustrates the testing criteria gap in projects. In this figure, the current SFRs and proposed SFRs are specified. It can be observed that through this basis of comparison, the proposed SFRs were not tested due to the client's defined scope which lacked importance of assurance levels and the testing details. We can see that previously some of the SFRs were not addressed. This is maybe due to the level of assurance and testing according to the scope set by client.

Testing Criteria — Based on past biometric projects

		ATE		AVA	
	Security Functional Requirements (SFRs)	Current SFRs	Proposed SFRs	Current SFRs	Proposed SFRs
1	Identification & Authentication (FIA)	✓	✓	✓	✓
2	Security Audit (FAU)	✓	✓	✓	✓
3	User Data Protection (FDP)	✓	✓	✗	✓
4	Protection of the TSF (FPT)	✓	✓	✓	✓
5	Security Management (FMT)	✓	✓	✗	✗
6	TOE Access (FTA)	✗	✓	✗	✗
7	Trusted Path (FTP)	✗	✓	✗	✗
8	Cryptography (FCS)	✗	✓	✗	✗
	Security Non-Functional Requirements	Current SFRs	Proposed SFRs	Current SFRs	Proposed SFRs
1	Performance Testing	✗	✓	✗	✗

Figure 4: The gap in previous biometric projects. Check mark symbols show that the SFRs have been executed while the cross symbols show that the SFRs have not been executed.

Proposed Testing Criteria Improvement

Figure 5 and Figure 6 are the proposed testing criteria. Figure 5 will address the gap identified in TAM (Figure 3) and Figure 6 will address the gap identified in the past biometric projects (Figure 4). These proposed criteria shall be evaluated based on these terms: external variables, biometric concerns and balance.

Special SFRs are those SFRs that are not defined or made available as testing criteria in any public references or may be still under research and development. Thus, in the proposed SFRs, there might be a need for modification based on the client's requirement as the scope of testing deems it to be.

	External Variables	Related SFRs	Special Case SFRs
1.	Government (Specific Bio Modalities)	BEM, BVM (if 1:1)	Timing of identification & verification
a)	Fingerprint	FPSPP + FPSPP OSP	
b)	Face Recognition	Can based on FPSPP + FPSPP OSP - modified to face with different species (Presentations and Attacks, and Spoofs)	
2.	Bank	BEM, BVM (if 1:1)	
a)	secure	BEM , BVM (if 1:1)	
b)	highly resistant to spoofing	PAD evaluation [ISO/IEC 30107] + [ISO/IEC 19989-3] + BEAT (AVA_VAN) Extended - FPT_SPOD Biometric Spoof Detection	
c)	have a minimal false acceptance rate	[ISO/IEC 19792] + [ISO/IEC 19795] under ATE_COV & ATE_FUN	
3.	User	BEM , BVM (if 1:1)	BiocPP for Smartphone - use case 2

Figure 5: Proposed testing criteria that addresses external variables

	Biometric Concerns - Advantages	Related SFR	Special Case SFR
1.	Ease of work	FIA	
2.	Non-shareable	FAU,FCS, FDP,FIA	
3.	Increase Security	FDP, FIA ,FPT, FTA	
	Biometric Concerns - Disadvantages	**Related SFR**	**Special Case SFR**
1.	False positives & inaccuracy + add in FRR (Biometric related Error Rate)	FIA , FMT	
2.	Privacy issue	FAU, FCS,FDP , FTP	1.FPR - unable to address regeneration issue+ Org policies) 2.FDP_RIP.2 Full residual information protection
3.	System Performance	FIA	FRU (Non Critical)
	Balance between Usability, Culture & Performance	**Related SFR**	**Special Case SFR**
1.	Usability	AGD -Environmental Influences	
2.	Culture	[ISO/IEC 19792] + [ISO/IEC 19795] + [ISO/IEC 19989-2] ATE_COV & ATE_FUN	
3.	Performance	[ISO/IEC 19792] + [ISO/IEC 19795] + [ISO/IEC 19989-2] ATE_COV & ATE_FUN	

Figure 6: Proposed testing criteria that addresses biometric concerns, usability, culture and performance.

Proposed Testing Methodology Improvements

Let's consider the proposed improvements for testing methodology in biometric technology. There are three areas that can be helpful in achieving an efficient and comprehensive testing. The first is performance testing. Based on our experience, performance testing was not executed, as the product was not developed by the client. Therefore, they were unable to provide access to the product test data and algorithm. Though, the need for performance testing is important as it gives confidence on the biometric component in the product based on the error rate(s) data produced.

Secondly, it is recommended to have checklists to cater for different biometric modalities. The checklist shall enlist mandatory and optional security functional requirements. They can be in different formats to support developer, tester and research in developing test methods. This helps to keep all parties on the same page.

The third recommendation is to understand the criteria before testing is conducted— the need to make the correct assumptions, threat analysis and risk calculation. One must determine the environment requirements based on biometric modalities. These environments have to be researched, whether it is indoor or outdoor in order to get the best replication of the actual operational environment.

Proposed Common National Testing Requirements

To ensure that the testing criteria on the proposed SFRs are used and defined appropriately across the nation, a Common National Testing Requirement should be considered. The proposed SFRs are as such:

- Identification and Authentication (FIA);
- Security Audit (FAU);
- User Data Protection (FDP);
- Security Management (FMT); Protection of the TSF (FPT_SPOD); and
- TOE Access (FTA).

Additionally, two SFRs, which are Trusted Path (FTP) and Cryptography (FCS), are also required if there are components that support the biometric functionalities in the form of cryptographic process and secure communication.

As discussed in this article, non-functional testing criteria, which are performance testing using [ISO/IEC19795], [ISO/IEC19792], [ISO/IEC19989-2]) and penetration testing need to be considered and performed. Some examples of penetration testing are as below.

- Specific to Biometric Modalities (Ref: BEAT, Biometric itc Tool Box, ISO/IEC 30701)
- PAD evaluation [ISO/IEC 30107] + [ISO/IEC 19989-3] + BEAT (AVA_VAN)

It is also suggested in the Common National Testing Requirement that performance testing, Biometric Testing Checklist and Prerequisite for Biometric Testing are included.

Conclusion

In Part 1, it was highlighted that the test lab or evaluation facility needs to be updated with the latest trends in biometric. This can be achieved by using the Technology Acceptance Method. By analyzing TAM, we are able to identify the method of promoting user acceptance in biometric technology.

Since biometric has unique characteristics, it needs to be addressed differently from other technologies. By building confidence in testing, indirectly we can influence more Malaysians to accept biometric technology.

Last but not least, the testing criteria and requirements need to cover all the scope established by the target audience.

References

1. Davis, F. D. Perceived usefulness, perceived ease of use, and user acceptance of information technology", MIS Quarterly, 13 (3): 319–340. 1989

2. FICO Survey: Malaysians Keen on Biometrics as They Struggle with Banking Passwords.2020

3. A Survey of User Preferences on Biometric Authentication for Smartphones.International Journal of Engineering & Technology, 7 (4.15) (2018) 491-495

4. [BEAT]N. Tekampe; et al. BEAT: Towards the Common Criteria evaluations of biometric systems.

5. [BEM] Biometric Evaluation Methodology Supplement. 2002

6. [BVM] Biometric Verification Mechanisms Protection Profile v1.3. 2008

7. [FPSPP] Fingerprint Spoof Detection Protection Profile, version 1.8, November 2009

8. [FSPPP OSP] Fingerprint Spoof Detection Protection Profile based on Organisational Security Policies v1.7.2009

9. [ISO/IEC-19795-1]ISO/IEC 19795-1:2006 Information technology -- Biometric performance testing and reporting -- Part 1: Principles and framework. 2006.

10. [ISO/IEC-19795-2]ISO/IEC 19795-1:2006 Information technology -- Biometric performance testing and reporting -- Part 2: Testing methodologies for technology and scenario evaluation. 2006.

11. [ISO/IEC-30107-3]ISO/IEC 30107-3:2017 Information technology — Biometric presentation attack detection — Part 3: Testing and reporting. 2017.

12. [ISO/IEC-19989-2]ISO/IEC 19989-2:2020 Information security — Criteria and methodology for security evaluation of biometric systems

13. [PresentationsAttacksSpoofs] Stephanie Shuckers. Presentations and attacks, and spoofs, oh my.. 2016.

Baseline of Security Defense (BoSD) Implementation for ICT Products

By | Noraziah Anini Binti Mohd Rashid & Nur Sharifah Idayu Mat Roh

Introduction

A few decades ago, cybersecurity as a topic was viewed rather coldly by all, with little emphasis placed on product development lifecycle.

Fast forward to the 20th century, the world has witnessed how advanced and sophisticated security attacks such as malware breaches, phishing, ransomware, etc had compromised the security of the information system. New emerging threats and vulnerabilities, being the most probable and damaging attacks, are the most significant risks that need to be managed well. Based on a Forbes (global media & publishing company) report, 2021 saw 50% more cyber-attacks per week on corporate networks than the previous year 2020 [1].

Security implementation in ICT products is actually very critical and companies should take into consideration the associated risk level during the technology development of a product.

It is inevitable that equipping a product with an advanced security defense would incur considerable investment [2]. However, there are still several baseline mechanisms which can be implemented *(which may not be too expensive)* for security defense that product developers could integrate during a product development lifecycle. In simpler terms, if developers want to bring their product to the market, it must at least be equipped with some basic security capabilities to protect the integrity, confidentiality, and availability of the product as well as user data from the privacy aspect. This article outlines several security baseline mechanisms that are suitable across several product types.

Baseline of Security Defense (BoSD)

Due to the diversity of technologies or product types, implementing baseline security mechanisms may involve various methods. This is to ensure that the product can still perform as expected even during running of security mechanism and able to provide users with high level of security assurance and confidence.

The following are several (but not limited to) baselines for security mechanisms that can be integrated into the product:

1. Several best practices to implement the BoSD
2. Type of products applicable to deploy the respective BoSD
3. Examples of security attacks that can be prevented by implementing the respective BoSD

BoSD#1: Secure Password Policy

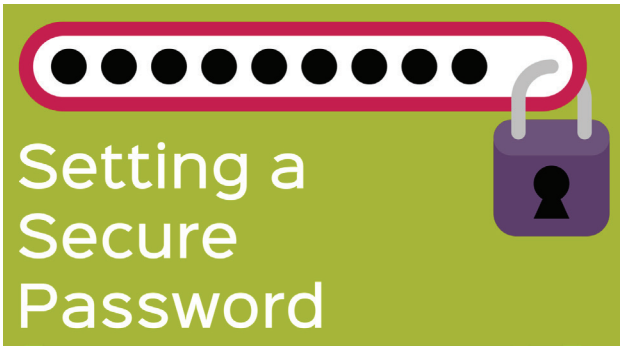


Figure 1: BoSD 1-Setting secure password

A secure password is one that is hard to crack. The password's strength is largely determined by a few factors. For example, the length of the password, the usage of alphanumeric characters, password change history, hashed and salted password, etc.

Some of the Best Practices [3]:

a. Require a period password reset.
b. Emphasize password complexity (adding special characters, capitalization, and numbers).
c. Monitor and filter new passwords created against list of common and compromised passwords. The list should be regularly updated.

Type of products that are applicable to deploy BoSD#1 (not limited to):
Web application, Desktop application, Authentication system.

Prevent Security Attacks (not limited to):
Dictionary attack, Man-in-Middle attack, Brute force attack, Offline password cracking, Eavesdropping, Online password guessing.

BoSD#2: Lock Account After Multiple Unsuccessful Attempts

This BoSD plays a significant role in preventing a brute force attack. The system shall define the number of unsuccessful attempts allowed and resulting action that the system will execute once the number of unsuccessful attempts is reached. In usual practices, the step can be considered as such: a) Lock the account until a certain specific time before the user is allowed to attempt login again, or; b) Lock the account until the system administrator unlocks it. Either way, the action taken shall take into consideration its impact.

Some of the Best Practices: [4] Section 5.22, [5] Section AC-7:

a. Completion of CAPTCHA challenge before attempting login
b. User needs to wait for a period of time after several failed attempts
c. Accepting authentication requests only from a whitelist of IP addresses
d. Automatic account lock in the event of unknown or unverified authentication attempts
e. Considering wiping data on mobile device once authentication fails after several attempts
f. Limiting biometric attempts on a similar basis as limiting attempts of login
g. Use an alternate authentication factors or enable multifactor authentication mechanism.

Type of products that are applicable to deploy BoSD#2 (not limited to):
Web application, Mobile application, Biometric Authentication system.

Prevent Security Attack (not limited to):
Brute Force attack.

BoSD#3: Use the Hypertext Transfer Protocol Secure (HTTPS) for the Header

A Hypertext Transfer Protocol Secure (HTTPS) is applicable on the website platform, which involves implementation of an encryption and Secure Socket Layer (SSL)/Transport Layer Security (TLS) certificate. These implementations ensure that the data transmitted is secure and the integrity of shared information is maintained. Figure 1 shows a comparison between HTTP and HTTPS implementation on how data transmitted (password) can be exposed to attackers.

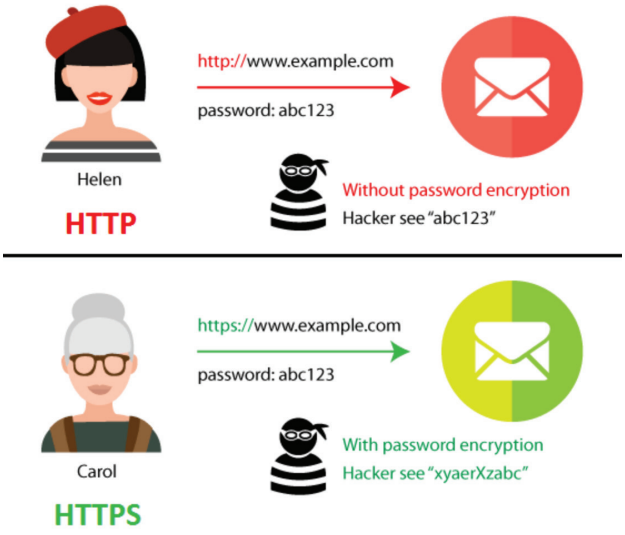


Figure 2: HTTP vs HTTPS [6]

Some of Best Practice: Implementation of [7], [8] Guidance:

a. Initiate HTTP Strict Transport Security (HSTS).
b. Implement X-Frame-Options (XFO).
c. Setting the header in X-Content-Type-Options
d. Enable Content-Security-Policy
e. Initiate X-Permitted-Cross-Domain-Policies
f. Enable Referrer-Policy
g. Clear-Site-Data
h. Enable Cross-Origin-Embedder-Policy
i. Enable Cross-Origin-Opener-Policy
j. Enable Cross-Origin-Resource-Policy
k. Enable Cache-Control

Type of product that is applicable to deploy BoSD#3 (not limited to):
Web application.
Prevent Security Attacks (not limited to):
Information Sniffing, SSL Stripping attack, Session Hijacking, Clickjacking, Cookie hijacking, Cross-site scripting.

BoSD#4: Interactive Session Locking/ Termination

Unattended or idle sessions for a certain period may attract multiple security attacks involving an attacker posing as legitimate user. It is recommended to set a pre-defined session idle

timeout to avoid any mishaps later. The user is also encouraged to consistently log out or end the session process once an activity is completed.

Some of Best Practice: [2] Section AC-12, [9] Session Replay Attack, [10] Session Hijacking.

a. User-initiated logouts
b. Termination message once logout
c. Timeout warning message
d. Encrypt the session data
e. Set the lifespan for the session to be shortest possible
f. Change the session key after login
g. Introduce additional methods for identity verification

Type of products that are applicable to deploy BoSD#4 (not limited to):
Web application, Mobile application.

Prevent Security Attacks (not limited to):
Session Replay Attack, Session Hijacking, XSS.

BoSD#5: Event logging

Event logging will generate audit trail which includes:

1. What type of event has occurred
2. When event has occurred
3. Source of event
4. Outcome of event
5. Identity of individual associated with the event

Developers should protect the record from unauthorized deletion and/or modification to maintain its security and integrity. They can also take action to protect the audit record as follows:

Some of the Best Practices [5] Section AU-9:

a. Store the record information in a different system or system component than the system or component being audited (as backup or long-term storage of audit records)
b. Implement cryptographic protection
c. Control authorized access to the audit record
d. Set the audit record as read-only access

Type of products that are applicable to deploy BoSD#5 (not limited to):
Web application, network device, biometric device.

Prevent Security Attack (not limited to):
Audit log manipulation.

Conclusion

Implementing the above security defense mechanism will help minimize the number of vulnerabilities and risks associated with a particular technology and product type. This article has listed several security defenses which developers can consider as a baseline of first-line defense for IT products. The listed defense baseline mostly require only a few IT product configuration/setting tweaks and does not involve large monetary investment. However, if the developer decides to implement additional security mechanisms in their products, several essential security functions have been highlighted under the Common Criteria Scheme [11] and these can be accessed for free at https://www.commoncriteriaportal.org/cc/.

References

1. https://www.forbes.com/sites/chuckbrooks/2022/01/21/cybersecurity-in-2022--a-fresh-look-at-some-very-alarming-stats/?sh=23ca5b4b6b61
2. https://www.embroker.com/blog/cyber-attack-statistics/
3. https://www.auditboard.com/blog/nist-password-guidelines/
4. https://pages.nist.gov/800-63-3/sp800-63b.html
5. Security and privacy controls for information systems and organizations. (2020). National Institute of Standards and Technology. http://dx.doi.org/10.6028/nist.sp.800-53r5
6. https://seopressor.com/blog/http-vs-https/
7. https://centrinetcorp.com/2017/07/26/10-website-security-best-practices-can-implement-today/
8. https://owasp.org/www-project-secure-headers/
9. https://campus.barracuda.com/product/webapplicationfirewall/doc/49058327/session-replay-attack/
10. https://www.keyfactor.com/blog/what-is-session-hijacking-and-how-does-it-work/
11. Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components. 2017. https://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R5.pdf

The Disadvantages of Smart / IOT Toys

By | Shazwani binti Salleh & Mohamad Nasrul Taufiq bin Salleh

The Internet of Things (IoT) has made almost all devices to be intelligent. A wired robot toy for example, is capable of enriching a child's playtime with complex and ever-changing settings, and it can continue to evolve and be modified thanks to app upgrades. The Internet of Things, or IoT, applies to the millions of physical items around the planet currently linked to the Internet; many of which store and exchange data. Due to the advent of highly affordable computer processors and the ubiquity of cellular networks, everything can be converted into an IoT, from a tiny pill to a gigantic airplane. Practically any physical entity may be turned into an IoT computer, whether it can be wired to the Internet to be monitored or transmit data. The technology helps children create, play, and even code its own content into toys. Linked toys not only spark children's interest in STEM by teaching them to appreciate logical reasoning, but also allow them to enable their own research to come to life in real time. STEM is a program focused on an interdisciplinary and practical approach to teaching students in four different fields — science, technology, engineering, and mathematics.

In an era where everything exists and anything can be gained from communication, the world of toys is rapidly evolving. IoT enabled toys are getting smarter, more integrated and sophisticated. According to industry association statistics, domestic product revenues in the U.S. reached approximately $22 billion in 2014, and that figure has been gradually increasing ever since, particularly with the latest connected distributor opportunities (Gibbons, 2018). Unfortunately, IoT is no longer a novel concept for children nowadays. Research by the University of Iowa showed that 90 per cent of children under the age of 2 were able to use a tablet. But issues such as laptops and smartphones are not the only concerns. Parents, especially, ought to be cautious with any toy that contains cameras or receivers, has GPS or web based networking, or demands and stores information. In brief, double-check any toy that has the potential to expose your kids or their data to third parties (Ranger, 2020).

"Smart" and "linked" toys designed to amuse, improve protection, and even link parents to their children when they are away from home are gaining traction in the marketplace. Such apps may offer opportunities for parents to improve privacy and protection through awareness of privacy settings and strategic usage. Unfortunately, they can also lead to more aggressive means of technology utilization to track, stalk, intimidate, or damage them (Norton Online, 2020).

What Are IoT Toys?

Internet of Things (IoT) toys are toys for children equipped with unique sensors and software to give customized experiences for children. IoT robots, unlike ordinary robots, can store, access, and exchange knowledge over the Internet (User, 2018).

Consequently, these toys are, also called Internet-connected or associated toys. IoT toys are often digitally advanced, depending on their purpose, because they are often linked to an Internet website or network. When you conduct a quick search on YouTube, you will find numerous intelligent toys on the market. Furby is one of the first known smart toys. This robotic toy, which replicates the language learning cycle through the child's constructive encouragement, became a big hit in the late 90s. Later other smart toys entered the market, including the popular Anki Cozmo, the Kano Machine, or the Woobo too (David, 2019).

According to David (2019), in his research titled "Are smart toys beneficial for your children?" smart toys can contribute to children's development. The use of sensors, microphones, or Internet-connected software allows more immersive and imaginative toys to be developed, which can respond to the feelings of children and provide different functionalities and ways to play. Intelligent robots can help with the development in motor and cognitive ability.

According to Market Research Specialist Anna Bryk, all IoT toys are either directly or indirectly linked to the Internet. For example, Wi-Fi is used for direct connectivity to wireless access stations, and Bluetooth is used for indirect connectivity by linking a gadget to an Android or iOS smartphone that has Internet access.

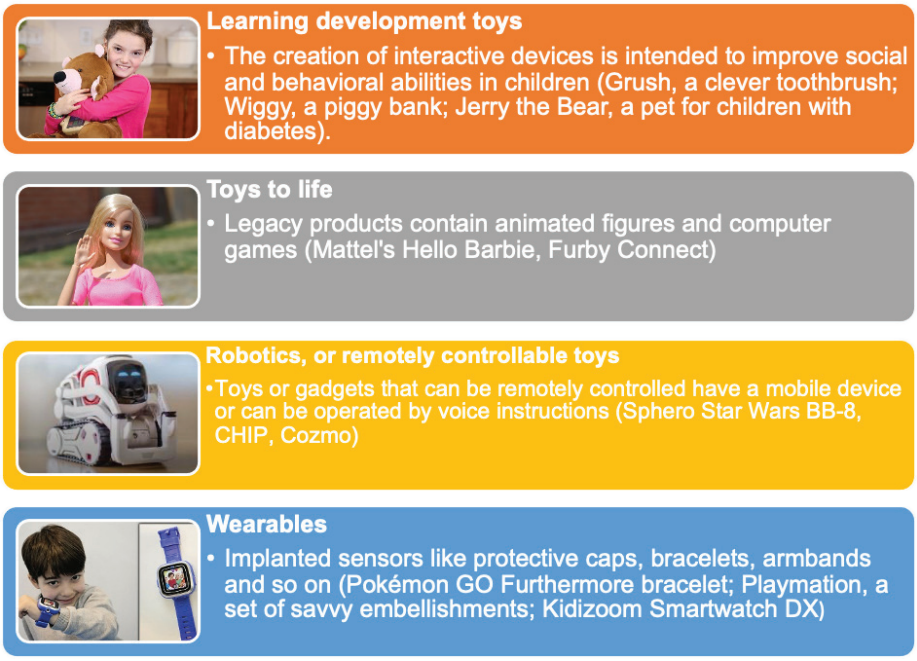


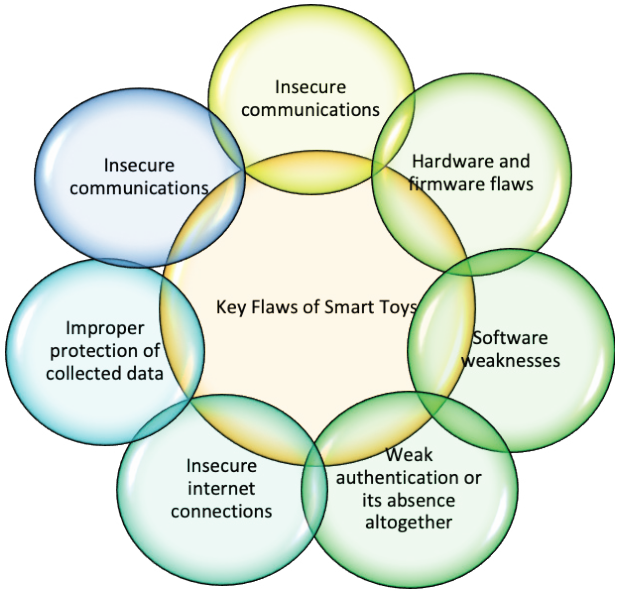
Figure 1: Types of IoT's Toys

She added that although an Internet link enables toys to communicate with kids, it raises many concerns regarding privacy and protection. Furthermore, the link of a robot to cloud storage makes it a vulnerable target for cyber attackers. We now have the option to purchase toys that could even listen and talk to your kids, read stories, ask questions, and check the Web for details. Many toys come fitted with screens, microphones, and speakers to enable children to communicate.

There are also concerns over protection and privacy threats involved with speech recognition. The distinction between "language recognition" and "speech recognition" is critical. Voice recognition is a device's capacity to recognize spoken phrases. It could be common to access digital assistants such as Amazon's Alexa or Google Home from mobile phones or home automation.

Do Smart Toys Have Disadvantages?

As with all digital technology advancement, there are always some drawbacks. Many privacy advocates and parents are worried about IoT toys, and with a good reason, particularly those fitted with a camera and a microphone or GPS. Although there are benefits of playing with smart toys as highlighted by product manufacturers, several disputes about security violations, however, have created a lack of trust in smart toys. This even extends to smart watches for children. As demonstrated by the computer platform "Which?" 4 out of 7 smart toys checked could be easily hacked. Connected toys' key flaws typically fall in the following areas:



Figures 2: Key Flaws of Smart Toys

Smart toys are often blamed for providing so much more of a sequential nature as opposed to traditional 'open-ended' toys as well. Typically, smart toys are built with a more constrained framework, identified by the constraints of their own code or technologies, which restricts their play value. That's why using technology in a way that promotes creativity or enables new modes of play is very critical. Smart toys are not designed to spoon-feed its users through talking or teaching; instead, they are programmed to facilitate and lead the kids to

develop the creative skills on their own. Secret surveillance by an intruder, a friend, or a third party is the biggest concern associated with such items. Most smart toys may also pose risks to data privacy. Many toys, for example, may be linked by Bluetooth, enabling people in close proximity, such as neighbours, to access the product. Some do not provide protection against third parties or visitors, which may, for example, allow unwanted access to video or audio to anyone who offers the product as a present. The stolen information could be used to track, monitor, or threaten them.

Strategies to Increase Privacy and Safety

Parents should be mindful and conscious of what is at risk when deciding to buy a smart toy. Understanding the advantages and dangers of IoT Toys is key. Before purchasing a new product, parents need to learn what type of device has been embedded, what type of capabilities it offers (why is it beneficial, is it appropriate for children's age, is it educational?), how does it communicate and link to the Internet, and what kind of personal details it requires to fully operate it. Knowledge is "control", and results in better judgement and decisions (McReynolds, et al., 2017).

As with many other ICT resources and goods, one should adhere to certain "fundamentals" and best practices in order to leverage the benefits. They include the following:

- Update your username and password shortly upon ordering and update your password periodically.
- Pick a strong password (with capital letters, icons, and numbers) or a Lock.
- If not in service, switch off the machine.
- Sign on to a protected network (password protect or VPN Wi-Fi).
- Include only minimal personal information, use fictional details where possible.

Parents must also review the user facts and guidelines on the computer, or via the software or website that regulates it. They can reach out to the vendor and seek to reclaim ownership of any information given or its related account. It is also necessary to take measures in improving network and Wi-Fi protection.

It is possible for cyber-attackers to obtain possession of a wired toy without adequate protection and privacy, transform it into a spying or listening tool, and interact directly with an infant. Criminals can also potentially monitor the location of a child with the purpose of socializing, kidnapping, or even attacking them via a connected toy.

Cyber criminals may discreetly capture an infant's voice recordings and turn it into pornographic materials to threaten parents with a ransom. It is the responsibility of a parent, to protect your children, both online and offline. Although IoT toys come with several advantages and enjoy web-connected functionality, they may also present security threats that pose a danger to sensitive data and personal information. Parents can minimize such risks with the right knowledge. Be conscious and constantly educate yourself about the risks involved.

References

1. David. (2019, August 22). Are smart toys beneficial for your children? Retrieved March 30, 2020, from https://melbot.es/smart-toys-risks-benefits-for-kids/

2. Gibbons. (2018, March 13). The Future of IoT with Kids. Retrieved March 30, 2020, from https://readwrite.com/2018/03/05/future-iot-kids/

3. IoT Health Privacy. (2018). Retrieved March 30, 2020, from https://www.techsafety.org/iot-health-privacy

4. McReynolds, E., Saraf, A., Hubbard, S., Cakmak, M., Lau, T., & Roesner, F. (2017). Toys that Listen: A Study of Parents, Children, and Internet-Connected Toys. Association for Computing Machinery. doi: 10.18411/a-2017-023

5. NortonOnline. (2020). Connected toys and what you need to know about them. Retrieved from https://us.norton.com/internetsecurity-iot-connected-toys-and-what-you-need-to-know-about-them.html

6. Ranger, S. (2020, February 3). What is the IoT? Everything you need to know about the Internet of Things right now. Retrieved March 30, 2020, from https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/

7. User, S. (2018, February 2). IoT Toys: A New Vector for Cyber Attacks. Retrieved March 30, 2020, from https://www.apriorit.com/dev-blog/521-iot-toy-attacks

Enhancing ICS Security Network Using Firewall and Data Diodes

By | Ts. Dr. Solahuddin Bin Shamsuddin, Ahmad Hazazi Bin Zakaria & Mohd Faizal Bin Sulong

Securing Industrial Control System (ICS) networks has become one of the most critical priorities to the industry because of its devastating impact to the environment, people safety and reputation. ICS networks carry a lot of sensitive information. In the event that they were compromised, it can cause havoc in control systems, thus allowing attackers to launch waves of cyberattacks. Among the top cyberattacks in ICS according to Waterfall Security firm are zero-day ransomware, ICS insiders, vendor backdoor, compromised remote site and cell-phone WIFI [1]. ISA-95 Purdue model has laid out some best practices to perform a network segmentation in ICS [1]. This segmentation and network separation is important to create defences-in-depth in the network system and enable better network management. Generally, ICS network consists of two main parts: IT network and OT network. The connectivity of IT into the OT legacy system has put the ICS to greater risk. Therefore, a better network security control must be implemented.

There are several methods and devices that can control network traffic in ICS. Firewall and data diode are among the popular options as these two carry similar functions but has better security controls towards the ICS environment. Firewalls are software-enforced network security system that act as barrier between two network segments. Firewalls are able to filter and block malicious network traffic. It will inspect all packets entering and leaving its guarded segment and use a set of pre-configured rules to distinguish between good and bad packets. Data diode, on the other hand, is a hardware-enforced unidirectional network communication device that secures information by allowing data to travel in only one direction to another segment. It is physically impossible for data to be transferred in from the other direction. Two main parts of data diode is transmitter and receiver [2]. Most often, the transmitter will be installed and placed in the network segment which is more secure; whilst the receiver will be on the less secure network segment. Such separation is necessary in order to protect highly sensitive and manipulative data, which is known as an air gapped network.

The main differences between data diode and firewall is that the former is a hardware based while latter is software based. A data diode is a hardware that enforces a one-way data flow on the physical layer. This means any data information exchange cannot occur on the network where the data diode is placed. As shown in Figure 1, there is no return path from IT network to OT network, and all threats are blocked. Hence, data diodes are invulnerable to software bugs, zero-days exploits, or misconfiguration that plague firewall solutions.

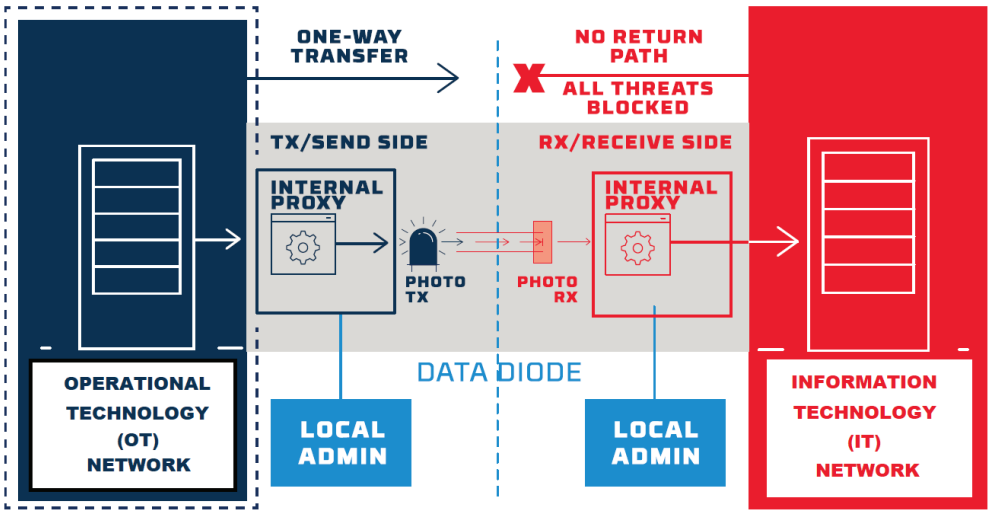


Figure 1: Unidirectional Data Diode communication

On the other hand, firewall is software based. It is embedded with complex programmable logic array, algorithm, listing, rules and many other software requirements to operate. Firewall is able to keep up with latest technology as it can be reconfigured to the latest setting and parameters. It has more flexibility than data diode when it comes to thwarting cyberattacks.

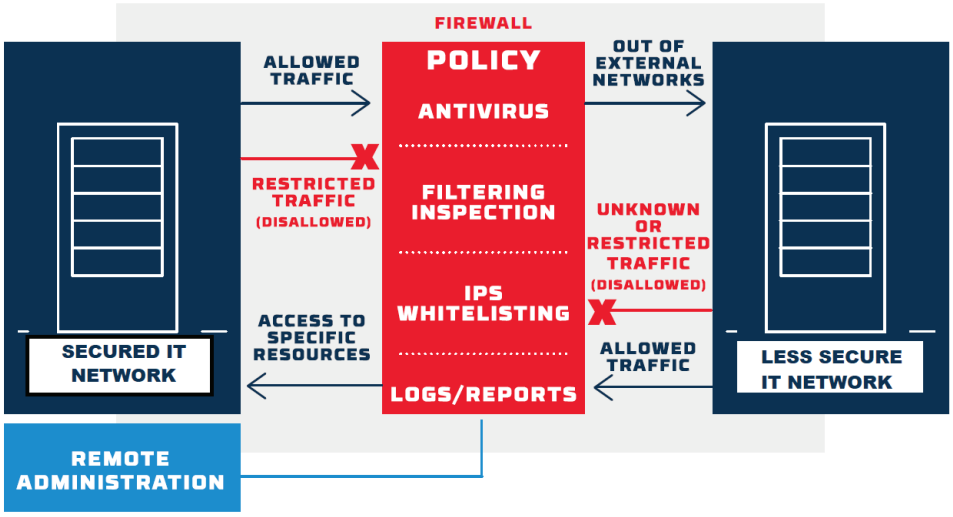


Figure 2: Firewall communication layout

In electronic components, a diode is an electric circuit component that allows current to flow only in one direction. This concept also applies to a data diode where it only allows data transfer to flow in one direction. There are two communication parts in a data diode that act in concert. One side is a sending part with no receiving capability, while vice versa for the other part. These two parts create a barrier in between them known as an air gap network as previously mentioned. This condition prevents any data leakage, or attacks from any external threat while safeguarding the sending and receiving network. In order to ensure one way path communication is established between the sending and receiving part, a protocol is "broken" in between known as protocol break. Protocol break is a process of eliminating and re-establishing data transfer protocol before the data reaches its destination. This will prevent any data in transit from being tampered, changed or compromised. In contrast, there is no such protocol in firewall. Firewall inspects, logs and audits each data that passes through it [3]. Any restricted traffic is not allowed to leave the secured network and any unknown traffic is barred from entering the secured IT network. Any data allowed to pass through are those that comply with the firewall's filtering rules and included in IPS whitelisting as shown in Figure 2. The data is what we refer to as a packet, which contains information such as where it comes from, its destination and content. If the packet information abides by the firewall rules, the data is allowed to pass through [4]. A data packet could sometimes be tampered by malicious actor in order to comply with the firewall rules and penetrate the network. However, a proper rules configuration and thorough packet inspection setting in the firewall can prevent such malicious packet to get past.

Before the industrial revolution of ICS that connects operation technology (OT) to information technology (IT), ICS was an isolated and disparate network. Based on the ISA 95-layer, level 0, 1, 2 and 3 is considered as the OT [5]. OT requires less software updates and patches to the programmable logic controller (PLC) systems, and most of the devices are sensor and processing-based units [6]. The nature of ICS environment itself does not require a direct connection the IT part. This is similar to the characteristics of a data diode which is hardware based and it requires no software updates. In other words, data diode is a preferred choice as it is low maintenance and easy to manage. Thus, all efforts can be focused on data availability rather than confidentiality because the network is more secured with data diode. In contrast, periodic software update is mandatory in the firewall from time to time. Latest updates include bug fixes to reduce risk of software problems in the future. Firewalls require a connection to the Internet thus is deemed riskier to an ICS network. However, through software updates, firewall is able to detect the latest bugs and malware. New rules in the firewall setting can also be fully optimised according to the network administrator.

Implementing data diode and firewall into an ICS network enhances its security owing to its clear network segmentation. In a complex ICS network with enormous amounts of data transfer and processing devices connected to it, network segmentation will help manage the network more efficiently. Regardless of high or low security network, firewalls and data diodes protect the data from the malicious actors. As depicted in Figure 3, firewall acts as a barrier that separates the two network segments. However, persistent and sophisticated attack vectors could put the firewall at risk and eventually break it. Data diode is highly resistant against cyber-attacks due to its unique strength in creating an air gapped network. It separates the network makes it almost impossible for any cyber threats to pass through the network due to segmentation. The exception would be when someone or something physically brought the threat into the network.

Figure 3: Differences of network segmentation in firewall and data diode. [2]

Enhancing control policy remains one of the most critical steps to enhance security in an ICS network environment. Although data diodes provide a unidirectional gateway for data flow, it does not mean that they can prevent any data leakage. Any external connection can still be established via ports if the network layout is not properly constructed [7]. Data leakage could also occur if the data is stored in a portable storage media which can be used by any person within the protected network. Thus, control policy is important to prevent people from indiscriminately using any device for connection that may compromise the security of a protected network. Data diode is unable to detect abnormal network traffic if the malicious software or data is already within the network. It still needs the support from other devices such as a firewall to ensure the network is safeguarded. With an ability to inspect data packet, firewalls can search through the network and provide relevant information for data protection.

As to whether firewall or data diode is better for network security, both have its own specific function that complements each other overall. Priority is to secure the ICS networks using both firewall and data diode in the network. Instead of focusing on which one is better, IT and OT sides need to find synergy in both. Proper network segmentation is critical to enable the network team to deploy extra security in specific segments using either data diode or firewall. In a nutshell, putting the right cybersecurity hardware in the right places can bring about effective controls in network protection.

References

1. *https://www.sans.org/reading-room/whitepapers/ICS/secure-architecture-industrial-control-systems-36327*
2. *https://owlcyberdefense.com/wp-content/uploads/2019/05/19-OWL-DataDiodes-Firewalls.pdf*
3. *https://www.forcepoint.com/cyber-edu/firewall*
4. *https://searchsecurity.techtarget.com/definition/firewall*
5. *https://isa-95.com/technical-isa-88-and-isa-95/*
6. *https://www.automation.com/en-us/articles/2020/isa95-in-the-iot-digitalization-era*
7. *https://www.nexor.com/resources/white-papers/protecting-confidential-information-using-data-diodes/*

The Importance of Data Privacy Legislation Compliance in Cross-Border Transactions

By | Mayasarah Maslizan, Naqliyah Zainuddin, Abdul Alif Zakaria & Wan Zariman Omar

Overview of Cross-Border Data Privacy Protection

Nowadays, data is fundamental to digital and physical commerce, and a vital catalyst for innovation. Businesses and trade today are very much dependent on data transfer from one location to another in order to execute a transaction efficiently. Thus, the Internet and digital services impact organizations, business models, consumer behaviour, and trade processes. Enabling data to be exchanged across borders brings more businesses and consumers into the digital fold, hence drives adoption of data-driven business strategies and stimulates the national economy [1].

We now live in an online world where digital transactions are a part of our everyday life. For individuals, Internet access provides various ways to interact with people and organizations from anywhere in the world, whether within or outside a country or even over a different jurisdiction. International data flows allow instant access to the wide range of goods and services, whereby an order can be made online for delivery, regardless of where the goods are produced [1].

Cross-border data transfers refer to moving data from one country to another, crossing international borders [2]. Almost all firms across every economic sector use electronic payment systems, Internet-based advertising and retailing, and cloud computing in their day-to-day operations. This ability to move data across borders has become a vital and intrinsic part of daily business activities to control and make operations more efficient.

Why Protection of Data Privacy in Cross-Border is Essential to the Business?

Cross-border data transfers enable a globally distributed approach to tasks, which leverages on expertise across multiple locations throughout the world and around the clock [3]. If a person wishes to participate in modern society using digital solutions to communicate, browse, shop, share, and search for information, it is impossible to do so without having personal data collected and shared across the Internet. Personal data makes up a large portion of data being produced and transferred, which then raises concerns about its protection across the border.

Despite the significant benefits to organizations, consumers, and national economies that result from data transfer across borders, changes to global data flows have also increase the risks to privacy. Cybercriminals seek to exploit technology to expose data for financial gain [3]. Given the ease of information transfer at any time and to any place, cross-border data breaches is likely to escalate.

Common Issues in Cross-Border Transfer of Data

Ensuring business operations comply with data protection laws can be costly. Data transfer restrictions increase the financial burdens associated with building bespoke data storage centres in multiple locations to comply with a host of national laws [4]. Some organizations have to invest significant resources to restructure their IT systems to restrict personal data from being transferred to countries with different jurisdictions. On the other hand, some businesses have chosen to avoid capital investments in countries with complicated compliance requirements in the establishment of IT infrastructure. When businesses are discouraged from entering or investing in new markets, consumers and businesses alike may be deprived of digital access to world-class products and services.

Another issue arising in cross-border data transfer concerns cloud computing, in which the data processing and storage take place outside the organizations [5]. It is very difficult for national laws to resolve multi-jurisdictional issues of data protection involving cloud computing or any other new technology. Jurisdictional aspects of data protection can be settled using private international law. However,

the virtual world extends beyond the control of nation-states and is likely to bypass national legal jurisdiction.

Data Privacy Breach Incidents Related to Cross-Border Issues

Data breaches have expanded significantly in 2021 for a variety of reasons, one of which being cross-border privacy. A recent cyber incident at an international social media organization, Socialarks, is an example of a cross-border data leak.

Researchers from Safety Detectives [6], led by Anurag Sen, identified a server belonging to Socialarks that held scraped profiles of over 214 million Facebook, Instagram, and LinkedIn users. The database had around 408 GB of data and 318 million records revealed by the Safety Detectives, including the following data:

i. 11,651,162 Instagram user profiles
ii. 66,117,839 LinkedIn user profiles
iii. 81,551,567 Facebook user profiles

Within hours of discovering the system and its vulnerabilities, another 55,300,000 Facebook profiles were wiped off by cybercriminals. Given the enormity of the data leak, Safety Detectives concluded that determining the entire scope of the potential damage was difficult. Researchers were able to discover users' full names, country of residence, place of work, position, subscriber data, and contact information, as well as direct linkages to profiles from the studied data.

Besides, there was also a case that concerns cross-border access to personal data. The case involved the United States (US) government's efforts to acquire an electronic communication stored by Microsoft on an Irish server [7]. In 2013, a federal magistrate's court in New York granted the Department of Justice (DoJ) a search warrant against Microsoft Corporation under the US Stored Communications Act (SCA). The purpose of a warrant is to access emails and the personal information associated with an account involved in a criminal investigation, specifically in narcotics trafficking. Instead of requesting access to user data through the Mutual Legal Assistance Treaty (MLAT) with Ireland, which allows law enforcement access to data stored abroad, the DoJ went directly to Microsoft with a warrant [8].

According to DoJ [9], a US warrant is sufficient to obtain the content of emails without involving Ireland's jurisdiction. The warrant is valid because Microsoft could obtain the data from the US through access from the cloud. In other words, the US government claims that copying or moving the content of emails that are stored in Ireland can be done directly by providing the emails to the US government. This action is not considered a search and seizure. However, Microsoft mentioned that data held on Irish servers is not subject to US jurisdiction. If the US wishes to access data held outside its jurisdiction, it must use the appropriate international law channels. This argument was supported by the Irish government. Furthermore, Microsoft also highlighted that if the US can use its warrant to seize data held in another country, other countries will in turn use their laws to seize data stored in the US. This action could put Americans' data at risk of seizure by foreign governments. If Microsoft wins this case, US law enforcement will lose the ability to obtain evidence related to significant crimes like terrorism and child pornography. The concern is that organizations could move their data beyond the reach of US authorities by simply storing it outside of the US.

Due to the complexity of this case, the DoJ eventually decided to dismiss the lawsuit against Microsoft as moot in 2016. The US government and Microsoft both agreed that the enacted Clarifying Lawful Overseas Use of Data Act (CLOUD) Act renders the lawsuit moot [10]. In this case, US federal law enforcement and Microsoft came into conflict over the validity of the SCA warrant for data stored on a server in Dublin, Ireland. In these types of cross-border situations, the establishment of a CLOUD Act would have provided a clear new procedure to allow foreign countries who have adequate and robust privacy and civil liberties protections to enter into mutual agreements with the US to obtain direct access to electronic evidence, wherever it may be located, in order to combat serious crime and terrorism.

Data Privacy Legislations in Cross-Border Transfer of Data

The European Union's General Data Protection Regulation (GDPR) implementation has resulted in significant improvements on protection of personal data and privacy worldwide. GDPR applies to organisations operating within the EU and those operating outside the EU that provide goods or services to EU customers or businesses. Apart from GDPR, organizations must also comply with other data privacy

laws such as the California Consumer Privacy Act (CCPA) and China's Personal Information Protection Law (PIPL), if their business operates in the US or China as well.

The general consensus highlighted in several data protection laws, such as GDPR (EU), CCPA (US), and PIPL (China) is that the transfer process of personal data outside to a foreign country is allowed under very limited circumstances. Both PIPL and GDPR require organizations to use a transfer mechanism when transferring personal information to a foreign country or organization [11]. Based on PIPL, personal information collected and generated within China must be stored locally by critical information infrastructure operators and personal information processors that reach the limit set by the Cyberspace Administration of China (CAC). They must pass a security assessment administered by the CAC if they are required to provide data outside of the country. While the GDPR prohibits the transfer of personal data outside the EU, there are three (3) exceptions [12] to the rule, which are as follows:

i. The personal data is covered by an 'adequacy decision' – foreign country or organization has a legal framework in place that provides adequate protection for the rights and freedom of individuals;
ii. The cross-border transfer is covered by 'appropriate safeguards' - ensure that data subjects' rights and freedoms are effectively protected; and
iii. The cross-border transfer is justified under one 'derogation' – obtain consent from the data subject, important reasons of public interest, establishment, exercise, or defence of legal claims, etc.

Meanwhile, the CCPA, a state law of United States of America, does not govern the transfer of personal information across international borders, but it does overlap and may conflict with certain PIPL and GDPR cross-border transfer restrictions [11]. For example, CCPA requires organisations that hold personal data to meet some of the same contractual obligations as GDPR and PIPL, such as contractual addendums between a "business" and its "service providers" (as those terms are defined under the CCPA) that [13]:

i. Identify the specific reason for sharing/ disclosing personal information; and
ii. Third-party recipients must have the same level of privacy safeguards as the CCPA.

Conclusion

Data privacy protection will affect businesses and users' decisions on where they should run their services and perform online browsing. Increasingly, an organization's reputation for the responsible management of personal data will be an asset that can lead to more website traffic, conversions, and a positive impact on profits. For this reason, every country has enacted data privacy laws or acts to regulate how information is collected, how data subjects are informed, and what control a data subject has over their information once it is transferred. Failure to follow applicable data privacy laws/acts may lead to fines, lawsuits, and even prohibition of service use in certain jurisdictions. In addition, even if a company is based in a jurisdiction that has not implemented comprehensive data privacy legislation, it is essential to consider where the potential customers might reside and what regulations apply. If organizations intend to do any business in the US, UK, China, etc., they should get familiar with the requirements imposed by these countries.

References

1. *"Cross-Border Data Flows Realising benefits and removing barriers," no. September, 2018.*
2. *"How to achieve cross-border data transfers in compliance with the law."*
3. *R. O. N. The, E. Of, and P. Laws, "Report on the cross-border enforcement of privacy laws."*
4. *"Business without Borders: The Importance of Cross-Border Data Transfers to Global Prosperity."*
5. *"Data Protection under Cloud Computing: A Jurisdictional Aspect."*
6. *The top data breaches of 2021 (https://www.securitymagazine.com/articles/96667-the-top-data-breaches-of-2021)*
7. *"Microsoft's Supreme Court Case Has Big Implications for Data" https://www.wired.com/story/us-vs-microsoft-supreme-court-case-data/*
8. *"The Microsoft Ireland Case and the Future of Digital Privacy" https://www.justsecurity.org/32076/microsoft-ireland-case-future-digital-privacy/*
9. *"Microsoft Ireland Case: Can a US Warrant Compel A US Provider to Disclose Data Stored Abroad?" https://cdt.org/insights/microsoft-ireland-case-can-a-us-warrant-compel-a-us-provider-to-disclose-data-stored-abroad/*
10. *"Supreme Court dismisses warrant case against Microsoft after CLOUD Act renders it moot" https://techcrunch.com/2018/04/17/supreme-court-dismisses-warrant-case-against-microsoft-after-cloud-act-renders-it-moot/*
11. *"Cross-Border Data Transfers: PIPL vs. GDPR vs. CCPA" https://www.jdsupra.com/legalnews/cross-border-data-transfers-pipl-vs-9241114/*
12. *"What are the requirements for 'cross-border data transfers' under EU Data Protection Law?" https://medium.com/golden-data/what-are-the-requirements-for-cross-border-data-transfers-under-eu-data-protection-law-e59bfce908f0*
13. *"California Consumer Privacy Act (CCPA)" https://oag.ca.gov/privacy/ccpa*

Automatic Software Updates

By | Muhammad Arman bin Selamat & Dania Syahirah binti Zakry

Most devices today will have automatic updates turned on by default. An automatic software update is a patch or a set of changes to the software to update, fix, or improve it as soon as these updates are available. If users set their software to be updated automatically, all pending updates will be installed immediately, regardless of whether they are postponed or waiting for a maintenance window to open.

Changes to the software will usually either fix bugs, fix security vulnerabilities, remove outdated features, add new security features, or improve performance and usability. The user experience will be enhanced through all of these updates. For instance, the most common software updates are Microsoft Windows, MacOS, mobile applications, iOS, Android, Java, and many more.

Installing software updates is not just to ensure that the system runs effectively, but also to protect their devices against cyber-crime threats.

Nevertheless, some users often delay software updates for various reasons, such as a slow Internet connection or being in a hurry to complete their tasks. Therefore, automatic software updates are very useful to these people. If an update is ready to be installed on a Microsoft Windows computer device, the software update notification will pop up a window to notify the user. However, in order for the update to be properly installed, the user must click a button. The user can accept the software update immediately by clicking the "Restart now" button, or else the user is allowed to schedule it for another time by clicking the "Pick a time" button, while the "Snooze" button is to ignore the software updates as in Figure 1.

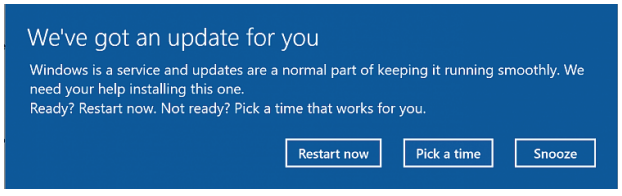


Figure 1: Windows update installation pop-up.

For this reason, users should set their software updates to automatic to help them avoid postponing their tasks. Users can enable this feature in the settings on their device, as shown in Figure 2 and Figure 3 below. Hence, the device software can be kept constantly up-to-date whenever there is a new update from the developer.

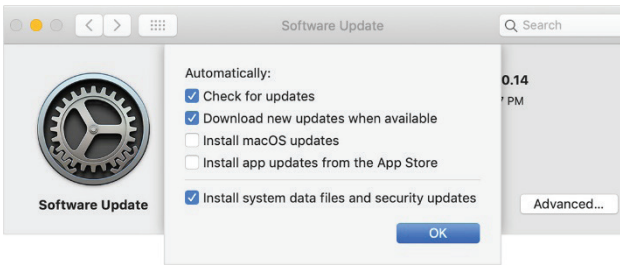


Figure 2: MacOS Software Update Setting

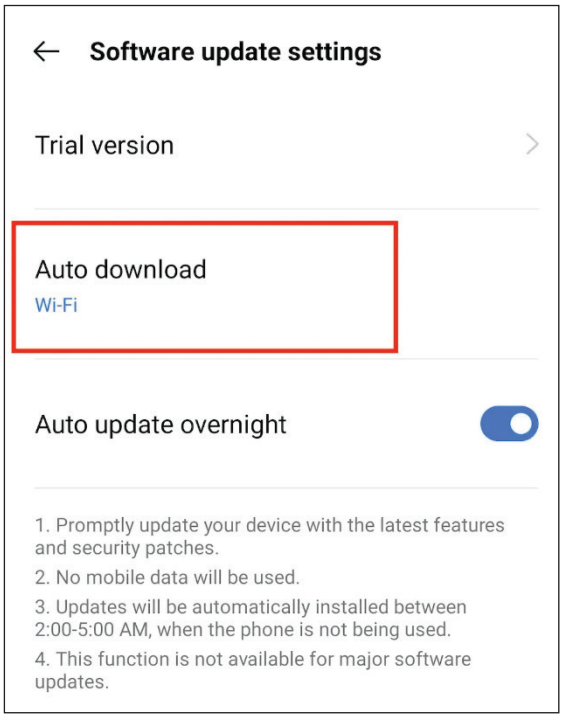


Figure 3: Android Software Update Settings

Advantages of Automatic Software Updates

1. Prevent Cyber Threats

One of the pros of automatic software updates is that it helps users update security flaws in the software. From time to time, after the software has been released, there will always be new

vulnerabilities discovered later in the software. Hackers love security flaws because weaknesses or security holes in software would give them an advantage. Thus, it will be easier for them to launch a cyber-attack on the user's device.

Sometimes, security is not just limited to the device user. Another party might be involved, especially with devices that belongs to an organization. Some of the data inside the device belongs to the organization, and some to the user. Hence, updating software could prevent cybercrime incidents like data breach or malware infection.

2. Good Software Experience

It is common to have bugs in software after it has been released. Most of the updates from the developers are intended to fix minor or major bugs or add a new feature. These updates can optimize users' experiences and yield performance improvements when using the software. If the users do not update their software when the new version comes out, disruption or errors can occur, leading to other problems. To avoid issues with your software, turn on the automatic software update feature to avoid running your software with bugs or glitches.

3. Save Time and No Interruption

A scheduled automatic software update can save users a lot of time. Humans can be forgetful. As such, automatic software updates will help them continue to run their devices using the latest software version effortlessly. Some software updates are scheduled by the software developer to be updated during midnight when users are less likely to use their devices, such as the iOS update example in Figure 4 below.

Figure 4: iOS Update Schedule

Therefore, the software updates will not disturb users who are using their devices during working hours.

Disadvantages of Automatic Software Updates

1. Lack of Compatible Device

Some software updates might not be compatible with the user's device or system, which could cause unintentional issues. For instance, not every Apple iPhone device can be updated with the latest iOS 16. Apple will usually stop updating their old devices which are five to six years old. The main reason is hardware compatibility, and from a business standpoint, an incentive for users to upgrade their devices.

Furthermore, Apple announced that it will no longer be supporting major iOS updates for iPhone 6 or iPhone 7 model. Hence, users cannot get the latest software updates unless they upgrade their device to the latest model. The same goes for Windows software. Due to minimum system requirements and hardware compatibility, not every PC can be upgraded to the latest Windows 11 OS. All current and future PCs will need a processor of 1GHz or faster with at least two (2) cores on a compatible 64-bit processor or system on a chip (SoC) with at least 4GB of RAM.

2. Cost and Time Consuming

Specific software may take a long time to download and install, especially if the size is large and there is no option to schedule an installation at a preferred time. While the software is being downloaded and installed, the user cannot work on the device, which can negatively impact a business since time is money.

Users may also need to spend money to update their software, such as Windows. Windows 11 will only be a free upgrade for Windows 10 users, but not the older version. Developers can choose to release numerous updates through the years, which may be cost-consuming and expensive to buy.

3. Lose Track of Changes

Users can lose track of changes to the software, especially when the changes do not require the user's intervention. As a consequence, users may need some time to learn how to use the latest features of the software that has been updated. However, this is only a minor drawback of an automatic software update.

Conclusion

Automatic software updates is more than just downloading the latest features to your device and fixing bugs. Rather, it contains critical updates that ensures that your devices are safe from cyber threats.

References

1. *https://www.tenforums.com/tutorials/76305-turn-off-windows-update-restart-notifications-windows-10-a.html*
2. *https://support.apple.com/en-us/HT207005*
3. *https://helpdeskgeek.com/how-to/how-to-turn-off-automatic-updates-on-android/*
4. *https://iphone-tricks.com/tutorial/3869-how-to-install-ios-updates-overnight-automatically*

Asas Dan Skop Percukaian Negara

By | Tormizi Bin Kasim, Siti Noriah Nordin, Nur Nadira Mohamad Jafar, Shamsul Hairy Haron & Muhammad Faizal A. Rahman

Pengenalan

Pencukaian boleh didefinisikan sebagai satu bayaran yang wajib tetapi bukannya denda yang dikenakan oleh kerajaan ke atas penggunaan pendapatan, kekayaan atau asas-asas lain untuk faedah rakyat bersama. Hasil kutipan cukai biasanya digunakan oleh kerajaan untuk mengurus, mentadbir dan membangunkan negara

Sejarah Percukaian Di Malaysia

Cukai pendapatan yang pertama diperkenalkan di Persekutuan Tanah Melayu pada 1947 di bawah Ordinan Cukai Pendapatan 1947. Ordinan Cukai Pendapatan yang pertama diperkenalkan di Sabah pada 1957 dan di Sarawak pula pada 1961. Secara tidak langsung, Persekutuan Tanah Melayu, Sabah dan Sarawak mepunyai Ordinan Cukai Pendapatan tersendiri. Bagi tujuan penyelarasan, pada tahun 1967, Parlimen memperkenalkan Akta Cukai Pendapatan (ACP) 1967 yang berkuatkuasa di seluruh Malaysia mulai 1 Januari 1968.

Cukai pendapatan di Malaysia bersifat kewilayahan. Ini bermakna cukai dikenakan ke atas pendapatan yang bersumber dari Malaysia. Pendapatan yang bersumber dari luar Malaysia akan dikenakan cukai sekiranya dibawa masuk ke Malaysia dan diperolehi oleh mereka yang bermastautin di Malaysia sahaja. Mereka yang tidak bermastautin tidak dikenakan cukai terhadap pendapatan yang dibawa masuk ke Malaysia

Ideologi Percukaian Sejagat

Ideologi cukai ialah kaedah pemikiran yang digunakan dalam merangka sistem pencukaian. Di antara beberapa sifat dan peranan idealogi cukai adalah:

1. Ia cuba merasionalisasikan kaedah pencukaian yang diamalkan dalam satu sistem pencukaian.
2. Ia cuba menjustifikasikan nilai-nilai yang diambil dan digunakan di dalam pencukaian
3. Nilai-nilai di atas disebut sebagai prinsip yang ditekankan dalam system pencukaian

Asas ideologi pencukaian sejagat boleh dikenalpasti kepada tiga asas iaitu:

a. Ideologi keupayaan

Ideologi keupayaan atau kebolehan membayar menerangkan bahawa cukai perlulah dikenakan berasaskan kebolehan pembayar cukai untuk membayar cukai. Kebolehan membayar diukur daripada pendapatan yang diperolehi dan kekayaan yang dimiliki oleh pembayar cukai. Andaian ini adalah apabila pendapatan dan kekayaan semakin tinggi atau banyak, semakin banyaklah jumlah yang boleh disumbangkan dalam bentuk cukai.

b. Ideologi sekatan dan penghalang

Ideologi ini memandang cukai sebagai satu sekatan dan halangan kepada perkembangan dan kestabilan. Di sini, cukai dianggap amat berbahaya dan akan mengurangkan minat untuk bekerja. Ia juga mengurangkan minat untuk melabur hingga menyebabkan penyekatan perkembangan sumber modal di dalam ekonomi.

Ideologi ini menekankan supaya sekatan dan halangan perlulah dihapuskan daripada dalam sistem pencukaian supaya ia tidak memberi kesan negatif terhadap sistem ekonomi.

c. Ideologi keadilan

Asas ideologi keadilan ini ialah ‘keadilan di antara yang sama’. Ia menekankan bahawa orang yang mempunyai kedudukan yang sama daripada segi pendapatan dan kekayaan perlulah dikenakan cukai pada kadar yang sama. Begitu juga orang yang berkedudukan berbeza daripada segi pendapatannya akan dikenakan kadar cukai yang berbeza. Daripada kenyataan di atas, ada dua peringkat keadilan yang perlu ditegakkan iaitu keadilan melintang dan keadilan menegak.

Keadilan melintang ialah keadilan di antara pembayar cukai yang mempunyai kedudukan yang sama. Di sini penekanan adalah untuk memastikan supaya pembayar cukai yang

mempunyai kedudukan yang sama dari segi pendapatan dan kekayaan dikenakan cukai pada kadar yang sama.

Keadilan menegak ialah satu usaha membezakan di antara pembayar cukai yang mempunyai kedudukan yang berbeza. Ia merupakan dasar diskriminasikan pembayar cukai mengikut kedudukan pendapatan dan kekayaannya. Di sini, pembayar cukai akan dikenakan kadar cukai yang berbeza berasaskan kedudukan pendapatan dan kekayaannya.

Objektif Percukaian

Apabila sesuatu diperkenalkan, ia perlulah mempunyai objektifnya yang khusus. Objektif ini termasuklah objektif umum dan khusus. Objektif umum pula berkait dengan dasar umum sesuatu pencukaian seperti keadilan dan sifatnya. Objektif khusus berkait terus dengan satu-satu cukai yang tertentu seperti untuk menghasilkan pendapatan atau mewujudkan galakan terhadap kegiatan tertentu.

Di antara objektif-objektif khusus pencukaian adalah:

a. Cukai sebagai sumber pendapatan kerajaan

Cukai merupakan sumber pendapatan utama kebanyakan kerajaan negara-negara di dunia sama ada negara maju atau membangun. Umpamanya di Malaysia bagi tahun 2000, cukai telah menyumbangkan kira-kira 90% daripada jumlah pendapatan negara. Sumber pendapatan daripada cukai ini digunakan untuk mentadbirkan negara dan untuk diagihkan semula ke dalam ekonomi melalui projek-projek pembangunaan atau bantuan terus kepada penduduk tempatan.

Bagaimanapun, objektif ini berpendapat pendapatan tidak boleh dijadikan sebagai objektif yang tunggal kerana ia boleh menyebabkan wujudnya kezaliman ke atas penduduk jika pencukaian disalahgunakan oleh kerajaan.

b. Cukai sebagai penggalak pertumbuhan ekonomi

Bagi kebanyakan negara membangun, sistem pencukaian adalah dianggap sebagai satu saluran dan kaedah begai menggalakkan perkembangan ekonomi. Kerajaan dan kebanyakan ahlinya berpandangan bahawa pembangunan ekonomi boleh berkembang pesat dengan adanya galakan daripada sistem pencukaian dan juga dengan adanya sistem pencukaian yang dapat meminimumkan sekatan dan perkembangan ekonomi.

c. Cukai sebagai alat pengagihan semula pendapatan dan kekayaan

Jika berasaskan kepada prinsip 'Robin Hood', cukai ialah satu proses mengagihkan semula kekayaan daripada orang yang kaya kepada orang yang miskin. Cukai merupakan sumbangan daripada orang yang mampu dan mempunyai lebihan pendapatan kepada kerajaan untuk diagihkan semula kepada orang miskin dan yang memerlukan. Ini juga selaras dengan prinsip dalam Islam yang mementingkan kesejahteraan masyarakat. Kesejahteraan jiran dan masyarakat hanya boleh diwujudkan jika kita dapat memastikan yang setiap orang dalam ekonomi mencapai satu taraf hidup yang sempurna. Ini hanya dapat dilakukan dengan mengutip cukai daripada pembayar cukai yang mempunyai kemampuan yang tinggi dan mengagihkannya semula kepada orang yang sangat rendah taraf hidupnya bagi mengecilkan jurang perbezaan taraf hidup di antara kedua golongan ini di dalam satu sistem ekonomi.

Objektif pengagihan semula pendapatan dan kekayaan merupakan salah satu objektif dan strategi serampang dua mata (di samping perkembangan ekonomi) dalam rancangan ekonomi negara. Walaupun dalam sistem pencukaian di Malaysia, objektif ini tidak dinyatakan dengan jelas, ia masih dianggap sebagai satu objektif yang penting, memandangkan kepada sistem pencukaian berjadual mengikut tingkat pendapatan individu.

Ketiga-tiga objektif di atas boleh dikatakan sebagai objektif utama dan penting dalam sistem pencukaian bagi negara Malaysia.

Jenis – Jenis Cukai Pendapatan

Dalam sistem pencukaian di Malaysia terdapat dua (2) jenis cukai iaitu, cukai langsung yang dipungut oleh Lembaga Hasil Dalam Negeri (LHDN) dan cukai tidak langsung yang dipungut oleh Jabatan Kastam Di Raja.

Cukai langsung terdiri daripada cukai pendapatan, cukai pendapatan petroleum, duti setem dan cukai keuntungan hartanah. Manakala cukai tidak langsung terdiri daripada cukai jualan, cukai perkhidmatan, cukai import

dan juga cukai eksport.

Prinsip - Prinsip Am Percukaian

Semua pendapatan yang diperolehi di Malaysia, pada amnya dikenakan cukai dan tertakluk kepada Akta Cukai Pendapatan 1967. Akta ini menggariskan panduan am taksiran cukai yang biasanya bergantung kepada prinsip-prinsip berikut:

a. Taraf pemastautinan
Implikasi cukai adalah berlainan di antara pemastautin dan bukan pemastautin.

b. Entiti
Kesan cukai adalah berlainan antara pelbagai entiti khususnya antara individu dan syarikat.

c. Bentuk perolehan
Perolehan hasil adalah tertakluk kepada cukai manakala perolehan modal terkecuali daripada dikenakan cukai.

d. Penerimaan hasil
Cukai dikenakan apabila hasil telah diterima atau apabila hasil dianggap telah diterima.

e. Tempoh berkait
Taksiran cukai pendapatan bergantung kepada keberkaitan sesuatu pendapatan yang diterima dengan tempoh yang berkaitan.

f. Potongan
Belanja yang berlaku bagi memperolehi pendapatan atau hasil layak dijadikan potongan daripada pendapatan berkenaan, kecuali kes-kes tertentu.

g. Perjanjian Pelepasan Cukai Duaganda
Ini melibatkan pendapatan yang di perolehi dari luar Malaysia dan dibawa masuk ke Malaysia setelah dikenakan cukai di negara di mana ia diperolehi. Kesan cukai mungkin berbeza terhadap pendapatan berkenaan, kerana Malaysia mempunyai perjanjian yang berlainan antara beberapa negara lain.

Asas Skop Percukaian

Asas skop cukai pendapatan ialah batasan definisi pendapatan yang boleh dicukai di sesebuah negara. Ia biasanya berkait dengan siapa pembayar cukai dan juga di mana pendapatan itu diperolehi. Amnya, terdapat tiga asas skop pencukaian yang boleh digunakan:

a. Skop Seluruh dunia

Skop seluruh dunia menekankan jenis atau kualiti pembayar cukai dan asasnya ialah warganegara. Jika seseorang itu menjadi warganegara di sesebuah negara, semua pendapatannya tidak kira di mana ia diperolehi akan ditaksirkan sebagai pendapatan bagi negara tersebut. Prinsipnya ialah seseorang warganegara itu memerlukan tapak asas dan perlindungan daripada negara yang dia menjadi warganegara.

Sebagai balasan ke atas perkhidmatan dan perlindungan kewarganegaraan ini, pembayar cukai perlulah menyumbangkan sebahagian daripada pendapatannya, tidak kira di mana ia diperolehi, dalam bentuk cukai. Kesannya, semua pendapatannya daripada seluruh dunia akan ditaksir di negara yang dia menjadi warganegara. Skop pencukaian ini adalah amat luas dan meliputi semua sumber pendapatan daripada seluruh dunia yang diperolehi oleh seorang warganegara.

b. Skop Perolehan

Skop ini menekankan di mana pendapatan diperolehi. Cukai hanya akan dikenakan ke atas pendapatan yang diperolehi di sesebuah negara tidak kira siapa yang memperolehinya. Asas ini menghadkan hanya pendapatan yang diperolehi dalam negara ini akan dicukai di negara ini juga. Dalam zaman teknologi yang tinggi ini, adalah amat susah untuk menentukan di mana sesuatu pendapatan itu diperolehi. Ini akan menyukarkan proses taksiran dan pungutan cukai. Banyak pembayar cukai yang menjalankan kegiatan perniagaan di sebuah negara tetapi menerima pembayaran di negara yang lain, amat susah untuk menentukan di mana sebenarnya pendapatan itu diperolehi.

Dalam kebanyakan kes, pendapatan sedemikian tidak akan ditaksirkan kerana kekurangan maklumat. Kemudian apabila wang dibawa masuk ke dalam negara itu, ia tidak pula boleh dicukai kerana ia bukan diperolehi di negara tersebut semasa wang dibawa masuk. Skop in adalah lebih sempit daripada skop seluruh dunia.

c. Skop Perolehan dan Penghantaran (remit)

Skop ini meliputi semua pendapatan yang diperolehi dalam sesebuah negara oleh sesiapa sahaja dan pendapatan yang dibawa masuk oleh orang yang tinggal di dalam negara ini juga boleh diandaikan sebagai telah diperolehi di negara ini dan boleh dicukaikan.

Masalahnya ialah siapakah orang yang patut dicukai ke atas pendapatannya yang dibawa masuk? Ada dua kriteria penentuan yang boleh digunakan. Pertama ialah kewarganegaraan. Jika diandaikan bahawa tiap-tiap warganegera duduk dan tinggal dalam negara tersebut, dia perlulah dicukaikan ke atas pendapatannya yang dibawa masuk. Bagaimanapun, seorang warganegara tidak semestinya tinggal di negara tersebut. Oleh itu, asas bermastautin dianggap lebih sesuai kerana tidak kira sama ada seseorang itu warganegara atau tidak, asalkan ia bermastautin di negara itu ia boleh diandaikan menjalankan urusan dengan negara tersebut dan memperolehi pendapatan daripada negara tersebut.

Asas mengenakan cukai ke atas pendapatan yang dibawa masuk adalah kerana pendapatan itu akan dibelanjakan dalam negara tersebut dan ini menunjukkan kaitan rapat di antara pemilik pendapatan dengan negara yang dia tinggal.

Apabila sistem pencukaian di perkenalkan di Malaya di bawah Ordinan Cukai Pendapatan 1947, kerajaan telah menggunakan asas perolehan. Walau bagaimanapun, setelah menyedari skop ini tidak begitu praktikal, pada tahun 1968, pindaan dibuat dan mengubah skop ini kepada skop perolehan dan penghantaran yang lebih bersifat kewilayahan. Skop ini boleh dikatakan lebih praktikal kerana skop ini lebih sempit dari skop seluruh dunia tetapi lebih luas dari skop perolehan

Sistem Taksiran Cukai

Taksiran ialah proses mengumpul maklumat pendapatan dan data-data berkait dengan aspek pencukaian bagi tiap-tiap pembayar cukai, membuat pengiraan cukai kena bayar dan mengumumkan jumlah kena bayar kepada pembayar cukai.

Sistem taksiran yang diamalkan di Malaysia sekarang ialah Sistem Taksiran Diri (STD) ataupun taksiran tahun semasa menggantikan (STR) yang diamalkan sebelum ini. Taksiran tahun semasa dimaksudkan pendapatan yang diperolehi dalam suatu tahun semasa ditaksirkan cukai dalam tahun yang sama. Dalam Belanjawan 1999, pindaan telah dicadangkan bahawa cukai pendapatan berasaskan tahun semasa akan dilaksanakan dalam tahun 2000. Ini bermakna pendapatan yang diperolehi dalam tahun 2000 akan dikenakan cukai dalam tahun itu juga.

Dalam STD, ada dua fungsi yang penting iaitu fungsi utama dan fungsi bukan utama. Dalam fungsi bukan utama, terdapat aspek-aspek pengiraan cukai pendapatan yang perlu dibuat oleh pembayar cukai itu sendiri.

Perkara-perkara ini meliputi pengiraan cukai pendapatan termasuk:

- pengiraan jumlah pendapatan
- pengetahuan tentang pendapatan-pendapatan yang dikecualikan cukai
- pengiraan pendapatan boleh dikenakan cukai dan
- pengiraan jumlah cukai pendapatan yang perlu dibayar

Dalam STD, jumlah cukai yang perlu dibayar dikira oleh pembayar cukai sendiri. Ia menjadi tanggungjawab penuh pembayar cukai. Sebaliknya, bagi fungsi utama STD iaitu pengesahan, penyemakan dan pengauditan ke atas jumlah cukai yang dibayar oleh pembayar cukai adalah tanggungjawab LHDN. Secara tidak langsung, pegawai-pegawai penaksiran dalam Sistem Taksiran Rasmi akan diberikan tugas-tugas lain, seperti pengauditan dan penyiasatan. Dalam STD, tumpuan diberikan kepada aspek pencegahan. Memandangkan LHDN akan dapat mengurangkan kerja-kerja penaksiran dalam pelaksanaan tetapi mempunyai masa untuk pengauditan dan penyiasatan maka, sistem baru ini secara tidak langsung boleh menjimatkan kos pentadbiran tetapi meningkatkan hasil cukai dan ini adalah intipati STD.

Selain Malaysia, negara-negara yang telah menerimapakai STD ialah negara-nagara maju seperti Amerika Syarikat, United Kingdom, Australia, New Zealand dan Jepun.

Sebelum STD diperkenalkan, sistem taksiran yang diamalkan ialah Sistem Taksiran Rasmi (STR). STR bermaksud cukai yang dikenakan pada sesuatu tahun adalah berasaskan kepada pendapatan yang diperolehi dalam tahun sebelumnya. Ini bermakna pendapatan yang diperolehi dalam tahun 1998 akan dikenakan cukai pendapatan dalam tahun 1999. Di sini, tahun 1998 dikenali sebagai tahun asas manakala tahun 1999 dikenali sebagai tahun taksiran. Tahun asas adalah tahun di mana pendapatan seseorang diperolehi manakala tahun taksiran adalah tahun di mana cukai akan ditaksir dan dibayar.

Dalam STR, pembayar cukai hanya perlu mengisi borang nyata pendapatan dengan memberi

semua butir pendapatan bagi tahun taksiran dan LHDN akan membuat taksiran ke atas jumlah pendapatan yang dilaporkan. LHDN akan memaklumkan kepada pembayar cukai mengenai jumlah cukai pendapatan yang perlu dibayar bagi tahun taksiran itu.

Ini bermakna dalam STR pembayar cukai tidak dikehendaki membuat taksiran sendiri terhadap pendapatan masing-masing, tetapi perlu mengisytiharkan jumlah pendapatan dalam borang nyata pendapatannya. STR tidak diamalkan di negara-negara maju dengan alasan ia suatu sistem yang tidak berkesan dan produktif.

Dengan pelaksanaan sistem "taksiran tahun semasa" atau STD dalam tahun 2000, pembayar cukai akan membayar cukai dalam tahun 2000 atas pendapatan tahun 2000 juga. Bagaimanapun, oleh kerana taksiran dalam tahun 1999 akan dikenakan cukai dalam tahun 2000 dan bayaran perlu dibuat dalam tahun itu juga (tahun 2000). Ini bermakna pembayar cukai perlu membayar cukai pendapatan untuk dua tahun dalam tahun 2000.

Untuk meringankan beban pembayar cukai daripada membayar cukai pendapatan dua tahun dalam satu tahun, Kerajaan akan melepaskan pendapatan yang diperolehi dalam tempoh asas 1999 daripada cukai pendapatan. Ini bermakna pembayar cukai tidak dikenakan cukai atas pendapatan bagi tempoh asas 1999 dalam tahun 2000 dan cukai yang perlu dibayar dalam tahun 2000 adalah atas pendapatan bagi tempoh asas 2000 sahaja. Walaupun, pendapatan tahun asas 1999 dilepaskan dari cukai pendapatan, pembayar cukai dikehendaki melaporkan pendapatan tahun tersebut dalam Borang Nyata Pendapatan bagi tahun taksiran 2000.

STD memang merupakan satu sistem yang mempunyai banyak kelebihan berbanding STR. Bagaimanapun, untuk memastikan STD berjaya, pungutan cukai haruslah dibuat dengan baik. LHDN perlu mengemaskinikan sistem pulangan ('refund') berikutan dengan potongan berlebihan ke atas pendapatan pembayar cukai dalam masa yang lebih singkat, iaitu antara dua minggu hingga tiga minggu selepas borang nyata diserahkan

Kesimpulan

Sebagai pentadbir hasil yang bertanggungjawab, Kerajaan sentiasa peka dalam meningkatkan kecekapan kutipan hasil pendapatan negara. Inisiatif yang dijalankan akan menambah baik penyampaian perkhidmatan dan mempermudah prosedur seterusnya meningkatkan pematuhan cukai. Sebagai komitmen dalam menyokong inisiatif pembaharuan fiskal, pelaksanaan rangka kerja Strategi Hasil Jangka Sederhana (MTRS) akan memperkemas dasar cukai, menambah baik pentadbiran cukai dan memperkukuh rangka kerja perundangan cukai. Di samping itu, Kerajaan akan terus menilai ekosistem hasil secara menyeluruh melalui penglibatan komuniti perniagaan untuk membangunkan dasar hasil yang baik selaras dengan amalan terbaik antarabangsa. Usaha tersebut akan memastikan janaan hasil berterusan yang amat penting dalam usaha membina ruang fiskal yang mampan dan kemampuan keberhutangan.

Rujukan

1. Md.Zyadi Md. Tahir. 2002. Percukaian. ISBN:9789836214782. Dewan Bahasa dan Pustaka.

2. Carlos Alberto de Souzu. 2002. Taxation and Education. Rio De Janeiro

3. Choong Kwai Fatt. Malaysia Taxation: Principles and Practice. 2021. Mph. online.com

4. https://www.hasil.gov.my/individu/pengenalan-cukai-pendapatan-individu/siapa-kena-cukai/

5. http://gst.customs.gov.my/ms/hl/SitePages/officials_statement.html

6. https://budget.mof.gov.my/pdf/1999/hasil/seksyen2.pdf

7. https://belanjawan2000.treasury.gov.my/pdf/bajet/ucapan/ub21.pdf

Peranan Ibu Bapa Dalam Memastikan Penggunaan Internet Yang Selamat Bagi Generasi Muda

By | Mohd Shamil bin Mohd Yusoff

"Perkembangan teknologi digital yang dinamik sememangnya memberi banyak faedah, bukan sahaja kepada kemajuan ekonomi dan pembangunan fizikal, malah perkembangan sosio budaya Keluarga Malaysia. Berdasarkan mandat yang diberikan oleh pihak Kerajaan, sebagai pusat pakar teknikal keselamatan siber, CyberSecurity Malaysia sentiasa berusaha untuk meneruskan kelangsungan membudayakan amalan dan penggunaan teknologi dan Internet secara positif, beretika, dan bertanggungjawab khususnya kepada generasi muda dalam Keluarga Malaysia." Petikan kenyataan Ketua Pegawai Eksekutif, CyberSecurity Malaysia.

Dalam kepesatan evolusi teknologi digital masa kini, kita perlu memberi perhatian sewajarnya terhadap penggunaan teknologi dan Internet oleh generasi muda. Ini kerana kemajuan teknologi serta akses kepada Internet turut memberi pelbagai impak kepada golongan tersebut.

Jika dahulu, generasi muda lebih cenderung melakukan aktiviti fizikal seperti berbasikal, bermain bola serta lain-lain aktiviti di luar rumah, namun dengan adanya peranti digital seperti telefon pintar, tablet serta akses Internet, mereka kini lebih gemar untuk berada di dalam rumah dan menggunakan kemudahan tersebut. Lebih parah apabila ada dalam kalangan mereka yang mengalami ketagihan Internet.

Dengan kepesatan teknologi digital, penggunaan peranti serta akses kepada Internet dan media sosial telah meningkat dengan ketara. Berdasarkan Kajian Tanda Aras Tahap Kesedaran Keselamatan Siber Dalam Kalangan Murid dan Ibu Bapa 2021/2022 yang dilaksanakan oleh CyberSecurity Malaysia, berlaku peningkatan pemilikan telefon pintar dalam kalangan generasi muda sebanyak 17.18% serta pertambahan kadar melayari media sosial sebanyak 60% berbanding hasil dapatan Kajian Tanda Aras Kesedaran Keselamatan Siber yang dilaksanakan pada tahun 2016.

Kajian Tanda Aras Tahap Kesedaran Keselamatan Siber Dalam Kalangan Murid dan Ibu Bapa 2021/2022 melibatkan 16,908 responden yang terdiri daripada 13,953 murid sekolah rendah dan menengah, termasuk murid pendidikan khas. Kajian ini juga melibatkan sejumlah 2,955 ibu bapa di seluruh negara. Ia dilaksanakan sewaktu negara berada di dalam kemelut kesihatan akibat penularan pandemik COVID-19. Kejutan budaya pada waktu tersebut mengakibatkan generasi muda lebih tertumpu kepada aktiviti pembelajaran dalam talian (PDPR) disebabkan oleh Perintah Kawalan Pergerakan (PKP) sepanjang tempoh dua tahun. Keadaan ini menyebabkan generasi muda perlu memiliki peranti digital untuk melaksanakan aktiviti-aktiviti PDPR.

Penggunaan peranti digital oleh generasi muda dalam tempoh tersebut meningkat disebabkan oleh keupayaan mereka menggunakan teknologi untuk pelbagai tujuan antaranya mencari maklumat bagi meningkatkan ilmu pengetahuan, memperkasa kemahiran diri, berkomunikasi serta membina jati selain untuk bersosial. Walaupun teknologi dan Internet digunakan untuk pelbagai tujuan positif, namun wujud penggunaan secara melampau tanpa batasan masa sehingga menyebabkan berlaku ketagihan, tingkahlaku yang tidak bermoral, tidak beretika dan tidak bertanggungjawab.

Kajian yang sama turut mendapati ketagihan Internet disebabkan kurangnya kesedaran mengenai konsep Kewarganegaraan Digital (KD). Konsep KD menekankan bahawasanya kurang kawalan yang efektif oleh ibu bapa adalah di antara punca berlakunya peningkatan risiko keselamatan siber dan menyebabkan generasi muda terdedah dengan pelbagai ancaman dan jenayah siber.

Generasi muda perlu diberi pendedahan serta pendidikan dari awal secara konsisten mengenai amalan terbaik penggunaan teknologi, Internet dan media sosial. Malah, ibu bapa disaran untuk cakna dan mengambil tahu aktiviti anak-anak mereka di dalam talian. Peranan ibu bapa sangat penting dalam membentuk sahsiah dan keperibadian anak-anak sejajar perkembangan teknologi masa kini.

Justeru, artikel ini menggariskan beberapa langkah bagi kawalan dan pemantauan yang boleh dijadikan panduan oleh ibu bapa dalam memainkan peranan sebagai ibu bapa siber.

- Sentiasa berkomunikasi dan berdialog secara terbuka dengan anak-anak. Luangkan masa sama ada di dalam talian atau bersemuka bersama anak-anak anda. Wujudkan suasana mesra dan harmoni semasa bersembang dengan anak-anak terutamanya dalam memberi pemahaman kepada mereka tentang keperluan bertindak secara bijak dan rasional apabila anak-anak menghadapi ancaman dan bahaya di alam siber.
- Awasi corak penggunaan peranti digital anak-anak seperti letakkan komputer di kawasan terbuka di dalam rumah dan berwaspada dengan aktiviti anak-anak sewaktu mereka menggunakan peranti dan Internet.
- Sentiasa cakna akan perubahan sikap anak-anak, contohnya, dari seorang yang periang kepada seorang yang pendiam serta perlakuan seperti mengurungkan diri dan menghabiskan masa berada di dalam alam siber seperti di laman media sosial.
- Ketahui aktiviti anak-anak dan rakan mereka di dalam talian. Biasakan diri dengan kata laluan anak-anak, penggunaan nama mereka pada skrin dan minta agar mereka berkongsi identiti setiap individu yang terdapat dalam senarai rakan mereka terutamanya di akaun media sosial. Ini bagi memastikan anak-anak tidak berkomunikasi dengan orang yang tidak kenali (*stranger*) di dalam talian.
- Ketahui akaun media sosial yang dimiliki oleh anak-anak. Jika anda tidak pasti sama ada anak anda mempunyai akaun media sosial, lakukan carian di akaun media sosial tersebut atau melalui enjin carian seperti Google dengan menaip nama anak anda.
- Semak secara berkala senarai rangkaian anak-anak di media sosial. Sebaiknya, pastikan anda juga berada di dalam senarai rangkaian anak anda.
- Ambil tahu jenis permainan dalam talian yang sering digunakan untuk melihat maklumat yang anak-anak muat naik atau kongsikan. Berhati-hati dengan informasi yang dimuatnaik oleh anak anda, malah lihat juga apa yang dihantar oleh orang lain mengenai anak anda.
- Pantau serta kawal aktiviti muat naik foto, video serta informasi oleh anak-anak di dalam talian. Ini kerana bahan yang dimuat naik tersebut berkemungkinan akan menyebabkan mereka terdedah kepada ancaman siber yang berupaya mejejaskan imej dan reputasi.
- Sekiranya anak-anak memuat naik bahan kerja-kerja sekolah, pastikan ia mematuhi peraturan hak cipta manakala bahan tersebut juga tidak mengandungi sebarang maklumat yang boleh dikenal pasti secara peribadi.
- Pastikan anak-anak tidak menggunakan kamera web (*webcams*) yang terdapat pada peranti digital dan menggunakannya hanya untuk tujuan tertentu seperti pembelajaran dalam talian. Jika untuk tujuan lain, pastikan ia berada di bawah pengawasan ibu bapa. Jangan sekali-kali benarkan kamera web digunakan oleh anak anda sewaktu mereka berada di dalam bilik tidur atau kawasan peribadi yang lain.
- Pastikan anda sentiasa mengingatkan anak-anak untuk berfikir (secara rasional) sebelum mereka memuat naik sesuatu perkara di dalam talian kerana informasi atau bahan yang dimuat naik tidak dapat dihapuskan atau ditarik balik. Tiada informasi atau bahan yang boleh diklasifisikan sebagai privasi di alam siber kerana apa jua maklumat yang dimuat naik akan menjadi tatapan umum. Justeru, berwaspadalah dan ketahui risiko tentang perkongsian maklumat peribadi dalam talian.
- Pastikan tetapan privasi pada peranti digital anak-anak untuk menghadkan siapa yang boleh melihat profil anak-anak remaja anda. Minta anak remaja anda untuk tunjukkan tetapan akaun media sosial mereka, jika anda mempunyai akses kepada akaun anak-anak, maka semak tetapan tersebut.
- Aktifkan tetapan penapis yang bersesuaian untuk menyekat laman web yang tidak sesuai untuk diakses oleh anak-anak seperti pornografi, keganasan, perjudian, aktiviti kumpulan samseng dan tingkah laku tidak sopan.
- Selain menyediakan kawalan ibu bapa, kemas kini sistem pengendalian secara berkala dan pasang tembok api serta perisian anti-virus dan anti-perisian pengintip yang terkini.
- Sentiasa berkongsi informasi dengan anak-anak dan maklumkan kepada mereka tentang risiko serta bahaya pertemuan secara bersemuka dengan seseorang yang mereka tidak kenali di dalam talian tetapi mempunyai jaringan di dalam rangkaian.

- Maklumkan kepada anak-anak bahawa mereka boleh berkongsi dan memaklumkan kepada anda sebarang perasaan seperti takut, tidak selesa atau keliru dengan seseorang yang meminta maklumat peribadi atau pengenalan diri, atau mencadangkan untuk berjumpa dengan mereka.

Kesimpulan

Generasi muda hari ini hidup di dalam dunia yang dinamik dan saling berhubung dengan pantas. Idea, sumber, jaringan malah tindakan berada di hujung jari mereka dimana teknologi digital telah mengubah gaya hidup dan menjadi sebahagian dari budaya kita. Pastinya ia membawa bersama pelbagai risiko, terutamanya untuk anak-anak remaja yang sikapnya ingin mengetahui dan menyelami sesuatu perkara.

Jika ditanya seorang remaja adakah mereka sanggup melepaskan peranti digital seperti telefon pintar atau akses Internet mereka selama sehari, jawapannya pasti tidak. Inilah dunia mereka dan inilah cara mereka mengendalikan dunia siber yang bergantung sepenuhnya kepada sikap dan tingkah laku mereka.

Kini, ibu bapa serta ahli keluarga lain hampir mustahil untuk berbual secara bersemuka tanpa gangguan peranti digital yang berterusan. Sudah menjadi kebiasaan untuk meneruskan sesuatu perbualan jika ahli keluarga masih kekal menggunakan peranti. Hasilnya, hubungan menjadi renggang dan komunikasi pula semakin menjadi tidak efektif. Maka, wujudlah pelbagai permasalahan sosial dalam institusi keluarga dan masyarakat.

Justeru, jangan sekali-kali berasa takut untuk membawa isu keselamatan siber dan berbincang tentangnya dengan generasi muda khususnya anak-anak di pelbagai peringkat usia. Sebagai ibu bapa, pastikan mereka berupaya untuk memberi pemahaman kepada anak-anak mengenai pentingnya untuk bertindak secara wajar, positif, beretika dan bertanggungjawab, malah mampu untuk mengamalkan sikap kawalan kendiri tatkala menggunakan teknologi dan Internet.

Perjelaskan kepada anak-anak mengenai risiko, ancaman serta bahaya yang bakal mereka hadapi seandainya teknologi dan Internet disalahgunakan. Jika anda ibu bapa yang cakna tentang keselamatan siber, nyatakan juga kesan penggunaan teknologi dan Internet yang negatif dari perspektif undang-undang serta hukuman ke atas perbuatan gangguan siber, sexting, buli siber dan sebagainya. Jadilah ibu bapa siber yang berupaya membentuk institusi keluarga digital yang berilmu.

Corporate Office:
CyberSecurity Malaysia
Level 7, Tower 1, Menara Cyber Axis,
Jalan Impact, 63000 Cyberjaya,
Selangor Darul Ehsan,
Malaysia.

Tel: +603 8800 7999
Fax: +603 8008 7000
Email: info@cybersecurity.my

www.cybersecurity.my

@cybersecuritymy
CyberSecurityMalaysia
cybersecurity_malaysia
CyberSecurityMy

MINISTRY OF
COMMMUNICATIONS AND DIGITAL

ISSN 1985-1995