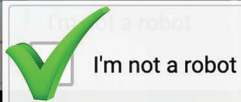


eSecurity

www.cybersecurity.my

The First Line of Digital Defense Begins with Knowledge

Vol 54



CAPTCHA Security: Understanding the Risks and How to Prevent Them
Ethics in Vulnerability Assessment and Penetration Testing
Understanding the Technology Behind Cryptocurrencies

"Update regularly, defend constantly. Don't wait for the breach to teach."

ISSN 1965-1995



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



CyberSecurityMalaysia



CyberSecurity Malaysia



cybersecuritymy



cybersecurity_my



cybersecuritymy



MINISTRY OF DIGITAL



CyberSecurity Malaysia

(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

Customer Service Hotline:

1 300 88 2999
www.cybersecurity.my



WELCOME MESSAGE FROM THE CEO OF CYBERSECURITY MALAYSIA

Dear Esteemed Readers,



Welcome to our latest edition of the eSecurity Bulletin. In an age where digital threats loom large and digital security concerns are ever-evolving, staying informed is paramount. This bulletin aims to provide you with insights, strategies, and knowledge to navigate the complex landscape of digital security effectively.

As we embark on this journey through the pages of our bulletin, we are met with a diverse array of articles that encompass a wide spectrum of cybersecurity topics. From understanding the vulnerabilities inherent in CAPTCHA security to exploring the advancements in biometric authentication, each article offers valuable insights into safeguarding our digital identities and systems against malicious actors.

Furthermore, in an era where cyber threats know no borders, it is essential to examine the global frameworks governing responsible state behavior in cyberspace. The exploration of the United Nations' framework for responsible state behavior underscores the need for international collaboration in addressing cyber threats effectively and promoting a safer digital environment for all.

Moreover, as technology evolves, so too must our standards and practices for ensuring information security. The overview of ISO/IEC 27001:2022 provides us with a comprehensive understanding of the latest standards for information security management systems, empowering organizations to stay ahead of emerging threats and regulatory requirements.

In addition to understanding the technical aspects of cybersecurity, it is equally important to address the human element. Articles on cybersecurity policies and governance highlight the importance of establishing clear guidelines and protocols to mitigate risks effectively and foster a culture of security within organizations.

Ethical considerations in vulnerability assessment and penetration testing remind us of the ethical responsibilities inherent in cybersecurity practices. By upholding ethical standards and integrity, we not only protect our organizations but also contribute to building trust and credibility in the digital ecosystem.

Furthermore, as cybercriminals continue to adapt and evolve, it is crucial to remain vigilant against emerging threats such as the evolution of the Macau scam and the risks associated with tap-and-pay apps. By understanding these threats and implementing proactive measures, we can better protect ourselves and our organizations from falling victim to malicious activities.

The bulletin also delves into the underlying technology of cryptocurrencies, offering readers a deeper understanding of this transformative innovation and its implications for cybersecurity. Additionally, discussions on cyber insurance and ransomware attacks provide valuable insights into mitigating financial risks associated with cyber threats and leveraging emerging opportunities in the cybersecurity landscape.

As we navigate the complexities of data management and analytics, articles on video analytics and NTFS permission management offer practical strategies for controlling data storage and interaction, thereby enhancing security and compliance within organizations.

Finally, I invite you to engage with our Cyber Security Crossword Puzzle, a fun and interactive way to test your knowledge and reinforce key concepts in cybersecurity.

In closing, I extend my heartfelt appreciation to the contributors, editors, designers and readers who have made this bulletin possible. By sharing knowledge, insights, and best practices, we empower ourselves and our organizations to confront the challenges of cybersecurity with confidence and resilience.

I encourage you to immerse yourself in the wealth of information presented in this bulletin, to engage in discussions, and to continue your journey toward greater cybersecurity awareness and preparedness. Together, we can build a safer and more secure digital future for generations to come.

Thank you for reading.

Be Smart, Be Cybersafe.

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

EDITORIAL BOARD

Chief Editor

Roshdi bin Hj Ahmad

Editorial Team

Fazlan Hj Abdullah

Yuzida Yazid

Designer & Illustrator

Zaihasrul bin Ariffin

Nurul Ain binti Zakariah

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

| | | |
|-----|---------------------------------------------------------------------------------------------------------------------------------|----|
| 1. | CAPTCHA Security: Understanding Cyber-Attack Risks and How to Prevent Them | 1 |
| 2. | Biometric Security Features in Digital Identity System | 4 |
| 3. | United Nations' Framework for Responsible State Behaviour in Cyberspace (Part 1) | 7 |
| 4. | ISO/IEC 27001:2022 – An Overview Of The New ISMS Version | 12 |
| 5. | How Hackers Can Drain Your Bank Account with Tap-And-Pay Apps | 16 |
| 6. | Cybersecurity Policies And Governance | 18 |
| 7. | Ethics In Vulnerability Assessment And Penetration Testing | 21 |
| 8. | Evolution Of Macau Scam: How To Protect Personal Information And Avoid Being A Victim Of Fake Apps | 27 |
| 9. | Understanding The Technology Behind Cryptocurrencies | 30 |
| 10. | Current And Future Trends of Cyber Insurance and Ransomware Attacks: An Insight for Cybersecurity Business Opportunity | 35 |
| 11. | Data Collection for Video Analytics and Its Application | 40 |
| 12. | Controlling Data Storage and Interaction Using NTFS Permission Management | 43 |
| 13. | Cybersecurity Crossword Puzzle | 47 |

CAPTCHA Security: Understanding Cyber-Attack Risks and How to Prevent Them

By | Ahmad Azizul Iqram bin Musa & Zul Hafiy Ikmal bin Mohd Marzuki

Introduction

CAPTCHA is considered one of the most common methods used for human validation before submitting online forms on websites that requires user interaction and authentication. Websites use CAPTCHA to verify whether an actual user or an online bot is attempting to access a web page. CAPTCHA is an acronym that stands for “Completely Automated Public Turing test to tell Computers and Humans Apart.”

Computer scientist Alan Turing created a test in 1950 known as the Turing test to test a computer’s ability to perform and display human traits through written communication. The test became the foundation for future computer scientists to develop and create the CAPTCHA based on its fundamentals and methodology. A reverse Turing test is the best description for CAPTCHA because the test is given by the computer instead which is the opposite of a standard Turing test conducted by a human.

Internet users normally encounter CAPTCHA for security reasons whenever they want to login via their access to various website. The verification test is designed not to be difficult for humans to complete but meant to ensure bots could not complete it. In other words, it should be nearly impossible for bots to solve CAPTCHA.

CAPTCHA is recognized as one of the most efficient methods to reduce the exploitation of a website by automated bots. It ensures that the system could not be overloaded with bots by verifying the user’s authenticity through solving a simple problem to differentiate between humans and computer bots. The CAPTCHA security technique is crucial as it prevents malicious bots from gaining access to the websites to perform unwanted behaviour. However, as secure as CAPTCHA is designed to be, there are still identified risks that need to be highlighted.

Background

CAPTCHA is designed to determine and verify whether an online user is a real human and not an automated bot that is used for malicious intent. Threat actors are constantly mounting cyber-attacks to gain access to the system. The risk of any website being exploited and illegally accessed is increasing by the day and security threats are growing at an alarming rate.

CAPTCHA is also used to prevent spam on websites, such as registration forms spamming, data scraping, and bot raiding. It is an effective filter as only humans can solve, and not bots. It is critical to implement CAPTCHA as it could increase the capability of a website significantly. For example, if an automated bot tries to access a website even with the right credentials, the bot will still encounter difficulty or is unable to validate CAPTCHA. Hence, implementation of CAPTCHA could prevent unauthorized access by ensuring that all the actions performed on the website, are by a real human.

In addition, CAPTCHA could ensure fair and uninterrupted websites services for users. By blocking access of automated bots, all features of a website are available. This also helps improve user experience by reducing spam bots and unwanted content.

The implementation of CAPTCHA is vital to keep websites safe. However, as artificial intelligence becomes more advanced, it is now more difficult to prevent bots from trying to access websites. As a result, other more advanced approaches need to be developed to match the bot's advancing capability to bypass.

Problem and Risks

Problems in implementation of CAPTCHA were identified early during its development. Users who were visually impaired found it difficult to solve text-based CAPTCHA because they were unable to interpret the letters and numbers due to their disability. This will prevent these users from accessing the websites. Even for normal

2

users who did not have problem with vision, the combination of deformed alphanumeric was frequently too difficult to decipher.

The latest version of CAPTCHA, developed by Google, also known as reCAPTCHA requires users to pick images that match the description given. For example, the test requires one to pick all images that contain crosswalks. Users need to pick every block from the divided images of the crosswalk to solve the test. This feature often frustrates users due to the time limit set to complete the test and some are difficult to solve. Consequently, users are more likely to leave the web pages rather than fill out the CAPTCHA to continue their access.

Apart from causing user frustration and disengagement, CAPTCHA technology also results in client-side website attacks. CAPTCHA plugins are available and can be found on WordPress libraries or repositories such as GitHub. The source code of the plugins can be viewed, and threat actors will find a way to probe if there are any vulnerabilities. According to the MITRE CVE database, there are at least 10 vulnerabilities related to reCAPTCHA and 86 vulnerabilities related to CAPTCHA. The type of cyber-attacks that were identified from the database includes cross-site scripting (XSS), cross-site request forgery (CSRF), SQL injection, and brute-force attacks.

Security Issues

According to cyber security researchers who have conducted research and written paper on CAPTCHAs, the feature is highly vulnerable to cyber-attacks. Perceived as bad user experience, a time-wasting and annoying method that gives bad user experience, all CAPTCHA types are practically vulnerable whether it is image-based or text-based. Owing to its alphabetic and numeric properties, it is easy for the threat actors to recognize by using CAPTCHA algorithms and machine learning for image processing.

By classifying the type of Machine Learning models available and their properties, researchers have also shown how bots and Machine Learning (ML) models could be the cause of all these attacks. They have demonstrated that CAPTCHAs are vulnerable to ML approaches, particularly when Deep Learning methods are used. As a result, threat actors are motivated to design botnets, with Deep Learning and Machine Learning models to bypass all CAPTCHA security systems in all web application.

A recent phishing attack campaign saw CAPTCHAs being exploited through bypassing email security filters and theft of credentials. The researchers explained that:

"Because the content of this attachment is a seemingly harmless reCAPTCHA, and the mail client will not be able to solve the CAPTCHA, the email client will have no way of determining the safety of the actual attachment's content."

How To Prevent

A few patch improvements have been taken to prevent these bots from aggressively bypassing CAPTCHAs. One method is to utilize multi-factor authentication to verify that only authorised users have access to the systems. For example, sending a user message on one-time passcode needed to go to the next stage on the website.

Strong Recognition Mechanism is also another option that can be considered. CAPTCHA attacks can be reduced by using advanced security measures, such as robust character recognition techniques for detecting bots.

To establish a secure traffic connection, it is also recommended to install a trusted third-party service that stops the bots in their tracks and protects the bots from malware and human fraud.

In addition, conducting a security awareness would be a better approach for every organization to deploy honeypots as an alternative to CAPTCHA.

If the organization needs to rely on CAPTCHA method, it is recommended for them to continuously inspect, monitor, and scan the websites every day to minimize the risk of being attacked by threat actors.

Conclusion

Cyber-attacks on CAPTCHA pose a significant risk to the security of all online systems and services. CAPTCHA is a useful method for defending websites against automated assaults, but it could still be exploited by attackers. Using a mix of security measures such as two-factor authentication, strong passwords, and other authentication mechanisms is the most effective technique to prevent CAPTCHA related cyber assaults.

It is also necessary for companies to routinely update its software and hardware to fortify security and patch any vulnerabilities.

Enterprises should also consider utilizing web application firewalls to identify and stop malicious traffic.

References

1. <https://cybersecuritynews.com/why-website-captchas-are-vulnerable-to-cyber-attacks/>
2. <https://cheq.ai/blog/how-click-farms-and-bots-bypass-captcha/>
3. <https://threatpost.com/cyberattackers-captchas-phishing-malware/168684/>
4. <https://medium.com/@harshalcoep/captcha-bypass-on-critical-websites-dea8da74e9a>
5. <https://www.iosrjournals.org/iosr-jce/papers/Vol22-issue3/Series-4/D2203042329.pdf>
6. https://www.researchgate.net/publication/329484616_CAPTCHA_Design_and_Security_Issues
7. <https://www.ijser.org/researchpaper/Review-of-various-CAPTCHA-generating-systems-and-vulnerabilities.pdf>
8. <https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=6a423297c2b9b930f6b4b394ec06b7b1151d93a1>

Biometric Security Features in Digital Identity System

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

Digital Identity also known as Digital ID, is the next generation credential management system for organization, government and community. Evolved from the concept of physical identity management such as national identity card and combined with a digital system that performs IT user identification, authentication and verification, Digital ID enables convergence of identity management system that cuts across physical document to digital platform.

Biometric recognition is a technology that captures human biometric modalities to be used as information or criteria for digital identification system. Information or data such as fingerprint minutiae, facial image etc. that are captured by biometric readers (e.g., fingerprint reader, facial recognition camera etc.) In enabling the biometric security features of identification, authentication and verification in an IT system, biometric recognition feature is also implemented in other systems such as for medical devices and law enforcement monitoring

The combination of Digital ID and Biometric Recognition Feature technologies to form a digital identity system, plays a critical role in ensuring the user of the system are identified, authenticated and verified. Through defined standard operating procedures that enables the usage of credentials created in the IT system. The objective of this combination is meant to mitigate issues of unidentified credentials, identity theft, fraud and scammers.

Digital Identity System with Biometric Features Support

Digital identity system is designed to elevate the common credential management systems which are basically used by organizations, communities, banking and government sectors to communicate, share information and trade secrets through the Internet.

To make the proposed system more efficient than other common credentials systems,

biometric and PKI are embedded as a support and security features of the digital identity system.

Aside from PKI capability, biometric for digital identity system also serves to enhance user experience with easier access, reduce the issues of forgotten password and missing mobile token. Although these are not major issues in identity management system, cyber criminals were capitalizing on the mistakes made by a user due to negligence.

Based on a study conducted by FICO, a data analytics entity, report titled “**Consumer Digital Banking Survey**” stated a “significant number” of Malaysians do not safeguard their passwords when doing online banking. Additionally, the survey also revealed Malaysia’s growing interest in biometric technologies.

This data suggests that the acceptance of biometric technology in Malaysia is reflective of the challenges faced.

For a technology meant to enhance user experience, biometric features in digital identity system have evolved to provide security protection capability and mitigating effects of human negligence.

Biometric security feature in Digital Identity System can be categorised into three components which are biometric identification, authentication and biometric verification.

Biometric Identification in Digital Identity System

Biometric identification allows a person to be identified and authenticated based on recognizable, verifiable, unique and specific data. The aim to is to capture an item of biometric data from this person. Similar to using a username and password in IT system, by either replacing or adding value to the existing identification and authentication process flow, biometric identification provides the IT system

with better security in ensuring the persons accessing the IT system are legitimate. Security with a strict criterion of enforcement mitigates the threats of unknown users (ghost credential). Biometric identification requires a set of hardware and software that captures biometric data during account registration based on specific criteria of data enrolment process. Aside from user account registration and biometric enrolment, biometric identification uses the same process for user identification.

Biometric identification is designed to provide better security protection on the identification process, even though feedback from IT developer sees it as a redundancy in user management.

Within the process itself, the IT system compares scanned features to a user's recorded digital identification using physical traits such as fingerprints, face image scans, or even voice recorded patterns. Biometrics is critical for identification as it forms the initial layer of security control implemented in an IT system which is often considered impenetrable and secure. Biometric modalities data are particularly well-suited as one of the factors in Multi-Factor Authentication (MFA.)

Biometric identification is also grouped under "biometric verification," which encompasses the following:

- **Biometric Identification:** Perform search and compare the user's biometric data to a credential enrolment stored in the database.
- **Biometric Verification:** The process of confirming user biometric claim by comparing user scanned biometric data to the biometric reference data stored in the identity card, reader or database.

Biometric recognition is considered an effective method of identification and verification since it is extremely difficult, if not almost impossible, to forge without a considerable amount of effort.

In the digital identity system, biometric identification feature plays an important role in mitigating brute force attack attempts on a login page or phishing attack on the digital identity of users by acting as first layer protection on digital identity system attacks.

Biometric Authentication in Digital Identity System

Next in the process flow is biometric authentication. It is undeniable that biometric authentication offers significant advantages over more traditional means of verification (such as: username and password, token-based authentication, CAPTCHA etc.). However there are still several biometric characteristics that need to be recorded and analysed.

The process of biometric authentication is to prioritize the log in access by validating the credential provided based on a biometric data matching process. Unlike biometric identification with the purpose of identifying legitimate user using his/her biometric to prove the user is a human behind the keyboard and screen, biometric authentication process is to ensure the provided biometric comes from the trusted devices owned or operated by legitimate user(s) during the process of log in to the digital identity system.

Without identifying the devices that are trusted by the digital identity system, the process of logging into the system will not proceed, which is intended to identify cases of breach related to legitimate user impersonation using correct credential during biometric identification.

However, there is still low maturity in enabling biometric authentication feature, as the technology is still new compared to the digital identity system. Apart from fingerprint readers that have matured through technology evolution, facial recognition cameras, iris detection cameras, voice recorder devices are not yet fully matured and accepted as trusted devices due to the lack of live detection capability and possibly low quality in detection algorithm.

Nonetheless, combining both biometric identification and authentication features as first security protection layers provides higher confidence for users in the implementation of digital identity ecosystem.

Use cases of Biometric Identification and Authentication

When examining business operations that rely on physical verification, it is critical to note that biometric identification and authentication in both enterprise and consumer contexts, require rigorous implementation across all sectors.

Additionally, biometric security features can help prevent unrecognized access and lower IT expenditures by minimising overhead associated with lost credentials or breaches caused by phishing attempts.

Biometric security features are critical in specialised operations and businesses in various ways, such as the following:

- a. **Financial Services:** Biometrics can help financial entities combat fraud and identity theft. By using electronic Know Your Customer (eKYC) technology, that utilises digital verification such as fingerprint and/or face images captured, as a form of identity confirmation.
- b. **Healthcare:** Similar to eKYC, healthcare providers employ digital identity system to enable doctors and nurses to identify patients based on their physical traits and correlate the information collected to their entire medical history. This helps minimize investment for unwanted medical supplies and preventing misuse of medicine by irresponsible patients.
- c. **Automotive:** As the automotive industry continues to innovate with electric and self-driving vehicles, manufacturers and third-party firms are creating biometric identification and authentication system that could be used in conjunction with or substitution of traditional key start systems. Physical human interaction through facial identification and authentication can assist in preventing vehicle theft.

Biometric Verification in Digital Identity System

The next process flow on biometric identification and authentication, is biometric verification that verifies human biometric modalities when the digital identity system is connected to service provider(s) that does not have direct access to the biometric database(s).

Biometric verification enables the digital identity system to move outside of its secure ecosystem through 3rd party integration. Dealing with untrusted devices such as user smartphone, proxy servers hosted by 3rd party service provider(s) and external network that lack security protection can jeopardize the digital identity system.

Without any direct connection to the back-end system to perform seamless identification and authentication, process biometric verification allows a user of the digital identity system to perform similar process. This is, however, done through an untrusted platform, but protected via security features such as liveness capability, mutual handshake of trust between systems or devices and PKI validation process on the status of operations (request and response).

Assuming the digital identity system uses a user smartphone to perform biometric verification via the front facial camera, the facial image(s) sent by the smartphone will need to go through liveness verification at the service provider proxy server to ensure the images sent meet the biometric data specification. This method allows the verification process to be performed without any direct connection to the source biometric database(s). Likewise, liveness verification can be performed along with biometric enrolment process within the procedure of user account registration. This may be applicable if the front end devices are located in public such as self-service kiosk in banks or government agencies.

Biometric verification can also be performed either during biometric enrolment or user account verification by 3rd party service provider(s) that serves the main purpose of mitigating fraud or identity theft or impersonation. Similar to the objective of biometric identification and authentication, biometric verification feature adds more value and security capabilities in digital identity system that could mitigate concerns on the digital identity system ecosystem.

Conclusion

As Malaysia transitions to a digital economy, digital identity management system will emerge as one of the key features of digital economy initiatives. Even if the adoption and acceptance rates of biometric features and its security capabilities are still low, these features can solve issues and challenges related to human negligence, whilst adding a high value of trust and assurance to the process flow of a digital identity system implementation.

Reference

1. <https://id4d.worldbank.org/guide/biometric-data>

United Nations' Framework for Responsible State Behaviour in Cyberspace (Part 1)

By | Mohd Rizal bin Abu Bakar

In the past, war and conflicts between countries, also known as States, were reported primarily in traditional media such as television, radio, and newspapers. The Iraq invasion and war crimes in Bosnia Herzegovina were examples of conflicts widely covered in the mainstream media. However, what the public knew was limited to what was shown in the media, as national security concerns and secrets restricted free access of information.

Today, through advancements in technology from the Internet, social media, open source to Artificial Intelligence, and the Metaverse, states no longer need to rely solely on traditional warfare involving ground troops, paratroopers, and tanks to resolve conflicts. Wars can start and end in cyberspace without any physical invasion or military intervention.

Cyber warfare is not a new phenomenon as States have been using interception methods such as communication signals, radar, and satellite tracking for some time. However, with the enhancement in digital technology and the Internet, cyber warfare used by States and non-state actors have evolved, with cyber-attacks now targeting all levels from government and private sectors to individual Internet users.

The modus operandi of cyber-attacks includes DDoS attacks, intrusion attempts through phishing, business email compromise, cyber fraud, Crimeware-As-a-Service, and e-commerce data interception, all committed by either State or non-state actors primarily to obtain valuable data of their adversaries..

However, due to the anonymity of the Internet and the vastness of the digital landscape, it is difficult to hold accountable those responsible for cyberattacks. The United Nations member states have addressed this issue in 2021 by agreeing on a framework for responsible state behaviour in cyberspace¹ through the UN's Open-Ended Working Group (OEWG)². This framework, based on norms developed by the United Nations' Group of Governmental Experts (UNGGE)³ in 2015, politically binds all member states to be accountable for their actions, policies, legislations, and operations in cyberspace. With these agreed norms,

activities and intentions of states in cyberspace can be subjected to assessments; and may be reprimanded (or sanctioned if the need arises) if they are found to have been negligent in preventing an incident or used their cyber capabilities irresponsibly.

The UNGGE and OEWG facilitate inter-governmental negotiations and consultations; at times, with non-government organisations and the civil society. ASEAN state members have been participating in such meetings since 2004 including Malaysia as shown in Figure 1 below:

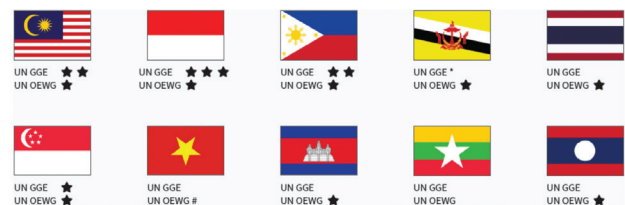


Figure 1: ASEAN member states' participation in UN norms processes since 2004-2021. Stars indicate a country's membership of the UNGGE, and its active participation in the OEWG as determined by written submissions or oral statements.

What are the accepted norms and what do they do?

In international relations, norms are commonly accepted standards of behaviour or conduct that are expected among states. Norms can relate to various aspects of a state's behaviour, such as diplomacy, human rights, arms control and the use of force. Cyber norms dictates the way each state should behave in cyberspace, and seek to establish expectations and guidelines on how state practices should continue or change.

As an example, one of the cyber norms is that states should not knowingly allow their territory to be used to launch cyber-attacks against other states. This norm reflects the reality that some states have been using third-party servers or compromised computers in other countries to launch and conduct cyber-attacks, targeting critical infrastructures such as power grids, water and transportation systems. Such norm establishes a standard that all states should follow in order to prevent such behaviour.

In general, norms in cybersecurity is critical to maintain international security and stability, highlighting the need for states to work together and establish common understanding and cyberspace behavioural guidelines. By implementing current state practices and establishing future expectations, norms can help promote a more secure, resilient cyberspace whilst reducing the potential conflict and instability specifically in the area of international relations.

3. To serve as a point of reference to hold other actors responsible for behaviour not aligned to UN norms of responsible state behaviour.

Governments of states that support the UN norms can highlight their efforts that promote predictability, trust and confidence in cyberspace at the UN General Assembly.

The United Nations' 11 Norms

The 11 norms of responsible state behaviour in cyberspace as introduced in UNGA Resolution 70/237, in practice, are used by governments in three ways:

1. To use as guidelines to reassure other states of their good intentions and behave as constructive members of the international community.
2. To serve as a point of reference to guide a state's national cybersecurity policy and national cybersecurity investments.

Implementing the United Nations Normative Framework for Responsible State Behaviour in cyberspace

While planning the United Nations Normative Framework proves to be an obstacle, implementation is another challenge altogether. As internationally agreed political agreements are discussed, planned and negotiated through an inter-governmental process, the policies, language, terminology, processes and legislations can be indistinctive.

For that reason, states need to adapt this framework and norms to form their own approach in embracing the UN normative framework. The UN framework of responsible state behaviour in cyberspace consists of four components as shown in Figure 2:

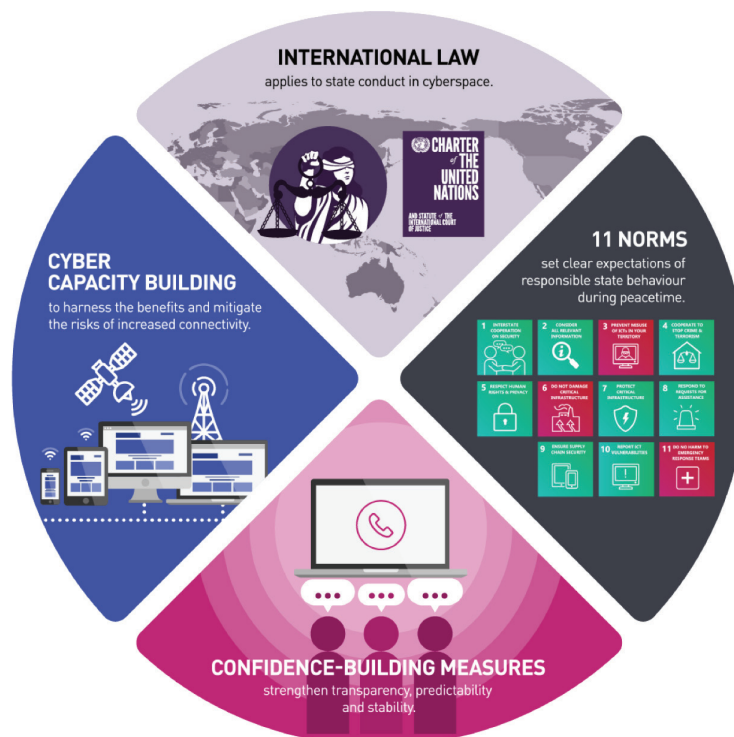


Figure 2: Four components in the UN framework of responsible state behaviour in cyberspace.

Framework Component 1: International Law

The International law component of the framework refers to the Charter of the United Nations in relation to state conduct both offline and in cyberspace⁴, consisting of major principles on international relations; from state sovereignty to prohibition of the use of force in international relations (i.e. military deployment).

Framework Component 2: 11 Norms

Norms typically codify existing state practices. The UN norms introduced in UNGA Resolution

70/237, set the standards of what the international community considers responsible on the basis of observed states' behaviour in the past and concurrently. With these agreed norms, activities and intentions of states can be subjected to assessments. States are commended on their response to an incident or its best practices can be showcased to other states as best global practice. In contrast, states can be penalised if they did not take action to prevent an incident, or prevent any irresponsible use of their cyber capabilities.

The 11 norms set defined expectations on how states behave responsibly during peace time, and should be viewed in its entirety and not selectively or randomly. The UN 11 norms are defined in the diagram below and elaborated in part 2 of this article:

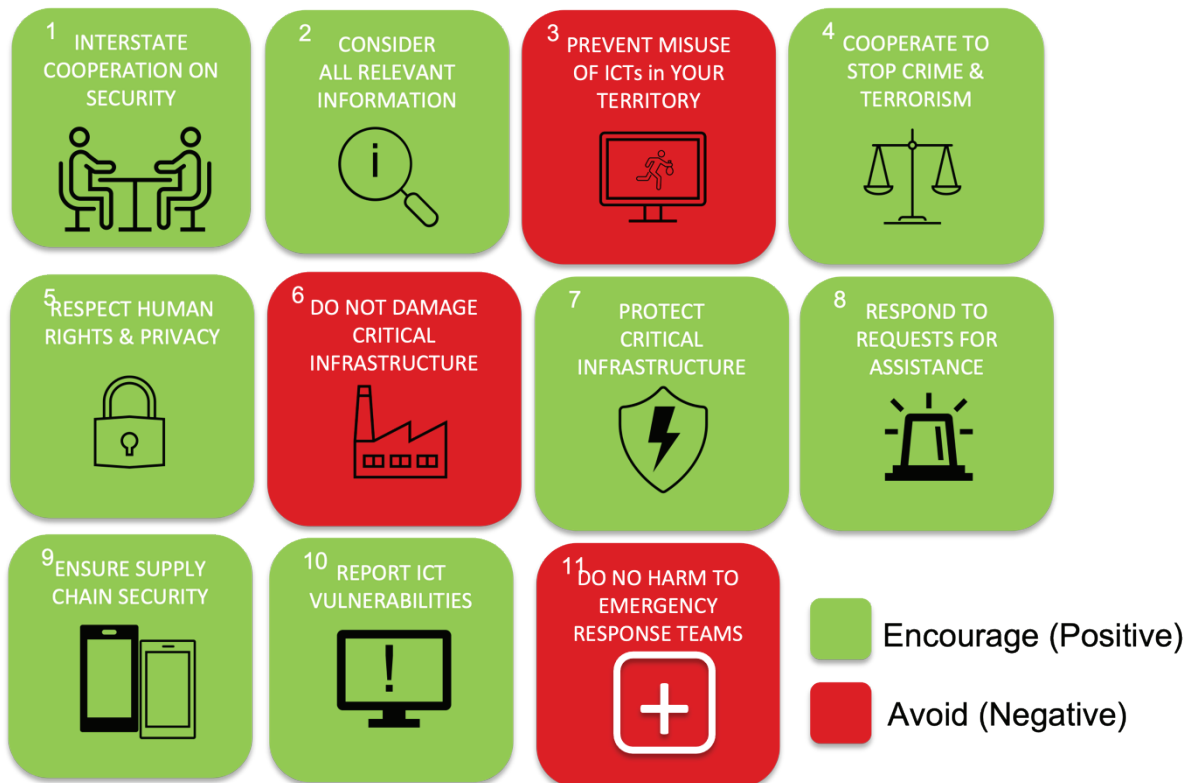


Figure 3: The UN 11 norms on responsible state behaviours in cyberspace (<https://documents.unoda.org/wp-content/uploads/2022/03/The-UN-norms-of-responsible-state-behaviour-in-cyberspace.pdf>)

Governments of states must take note that the above norms form part of a broader framework that includes international law recognition of states, a set of Confidence Building Measures (CBMs) and commitment to coordinated capacity building.

States can demonstrate implementation of the norms in multiple ways. Typically, implementation of norms can occur at three levels:

1. Political endorsement

- a. Voting in favour of relevant resolutions at the UN General Assembly-through subscription of ASEAN leaders' statements and by ministerial statements.

2. National laws, policies & strategies

- a. Integrate norms into national legal frameworks, (cybersecurity/security) strategies and national (cyber) policies.

3. Actions on the ground (active/effective implementation)

- a. Demonstrate implementation by referring to government practices through capabilities, mandates, procedures and actions to prove its ability and willingness to act.

However, implementation of UN norms relies on the government of states. Effective implementation hinges heavily on a government’s ability and willingness to consult and collaborate with multiple industries, civil society organisations, technical communities and academia and most importantly, its ability to implement a whole-of-government approach (every ministry, agency and linked agencies/ companies).

To be more inclusive, views, expertise and capabilities of non-government stakeholders need to be taken into consideration as an integrated approach encompassing a national action plan or cybersecurity road map.

Creating a national approach to cybersecurity and implementing the UN norms is neither a straight forward approach nor a short term process. It requires a gradual process to enhance understanding, maturity levels and reassurance on the topic of cybersecurity (Figure 3).

| Awareness | Recognition | Assessment | Understanding | Plan & Act | Implement |
|---------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|
| Build awareness across government of its international responsibilities. Can be achieved through trainings, talks, awareness campaigns on the UN norms. | Lay the foundation for a cross-government recognition that the government is committed to the UN's framework and is willing to be guided by it through its national and international cybersecurity activities. | Assess implementation efforts by third party (i.e. auditing, certification) or through a whole-of-government mapping. | Outcome of assessment is used to inform and educate the government of its strengths and weaknesses. | Domestic investments in particular areas of cybersecurity-requesting assistance from global cyber capacity building community or to offer expertise to others. | Implementation of UN Norms is at par with its own means and capabilities. |

Table 1: Step-by-step process for implementation of UN Cyber norms

Demonstrating Implementation

To minimize threats to global peace and security and prevent conflicts, it is imperative for nations to exhibit proactive efforts and intentions. Therefore, documentation and reporting play a vital role in this process. To effectively communicate a state's perspectives, accomplishments and capabilities, the following avenues can be utilized to showcase implementation:

1. Reporting through the United Nations’ Secretary-General

- On invitation by the UN Secretary-General, governments can share their efforts taken at national level to strengthen information security and promotion of international cooperation in cybersecurity on invitation by the UN Secretary-General.

2. UN OEWG Submissions

- Submissions or statements via the OEWG, which is then shared by the UN Secretariat to other member states, chair(s) and non-government stakeholders.

3. ASEAN Regional Forum (ARF)

- The semi-annual meeting on ICT security offers ASEAN member states a platform to exchange views on regional and global ICT landscape on their respective states' efforts and initiatives.

4. Recognition by third party

- By engaging third-party organisations to perform external assessment and report via a capacity-building relationship, ASEAN member states can utilise academia, think-tanks and other sectors such as ASEAN-ISIS (Institutes of Strategic and International Studies), NEAT (Network of East Asian Think-Tanks), CSCAP (Council for Security and Cooperation in Asia and the Pacific).

Why should states make an effort to implement UN cyber norms

States should adopt international norms such as the UN norms for responsible state behaviour in cyberspace in order to achieve the following outcome:

1. **Enhance cyber resilience:** Implementation of these norms would lead to a significant increase in a state's national cybersecurity maturity levels, bolstering its capacity to defend against malicious activities, both domestic and international, and respond proactively.
2. **Bolster international credibility:** By supporting the norms and providing guidance to governments on national cybersecurity policy, states can demonstrate their commitment of being responsible members of the international community.
3. **Contribute to norm-setting:** Adherence to these norms allows states to help shape a shared understanding on what constitutes responsible state behaviour in cyberspace and align with international expectations.
4. **Ensure assurance, accountability, and transparency:** When a large number of states implement UN norms effectively, it increases assurance that each state is willing and able to prevent tensions and conflict. Furthermore, it adds to the accountability and transparency of state activities in cyberspace.

The second part of this article shall provide more details about the framework component of 11 UN Norms, OSCE Cyber Norms, Confidence Building Measures (CBMs) and Capacity Building. It will also discuss the efforts made by Malaysia, specifically by CyberSecurity Malaysia in supporting the UN's framework for responsible state behaviour in cyberspace as a technical agency, which helped in its own Transformation Plan.

Reference

1. UN Norms of responsible state behaviour in cyberspace (<https://documents.unoda.org/wp-content/uploads/2022/03/The-UN-norms-of-responsible-state-behaviour-in-cyberspace.pdf>)
2. UNOEWG (<https://www.un.org/disarmament/open-ended-working-group/>)
3. UNGGE (<https://www.un.org/disarmament/group-of-governmental-experts/>)
4. Charter of the United Nations (https://ccdcoe.org/uploads/2018/10/UN_-Official-compendium-of-national-contributions-on-how-international-law-applies-to-use-of-ICT-by-States_A-76-136-EN.pdf)

ISO/IEC 27001:2022 – An Overview Of The New ISMS Version

By | Aliya Farhana binti Mohd Nasran, Nur Shafiqah binti Nor Aztawakal, Ameerul Aziz bin Thaib & Noor Aida binti Idris

On October 25, 2022, the world's leading information security standard, ISO/IEC 27001, was updated after nine years and its new version is known as ISO/IEC 27001:2022 Information Security, Cybersecurity, and Privacy Protection. This is a revised and updated version of ISO/IEC 27001:2013, which provides a comprehensive and integrated approach to managing information security risks. It also helps organizations ensure the confidentiality, integrity, and availability of their information assets. Although there are only minor changes in this revision, it is still useful to review them carefully. This document provides a thorough overview of the changes and improvements made in ISO/IEC 27001:2022.

ISO/IEC 27001 - A Quick Overview

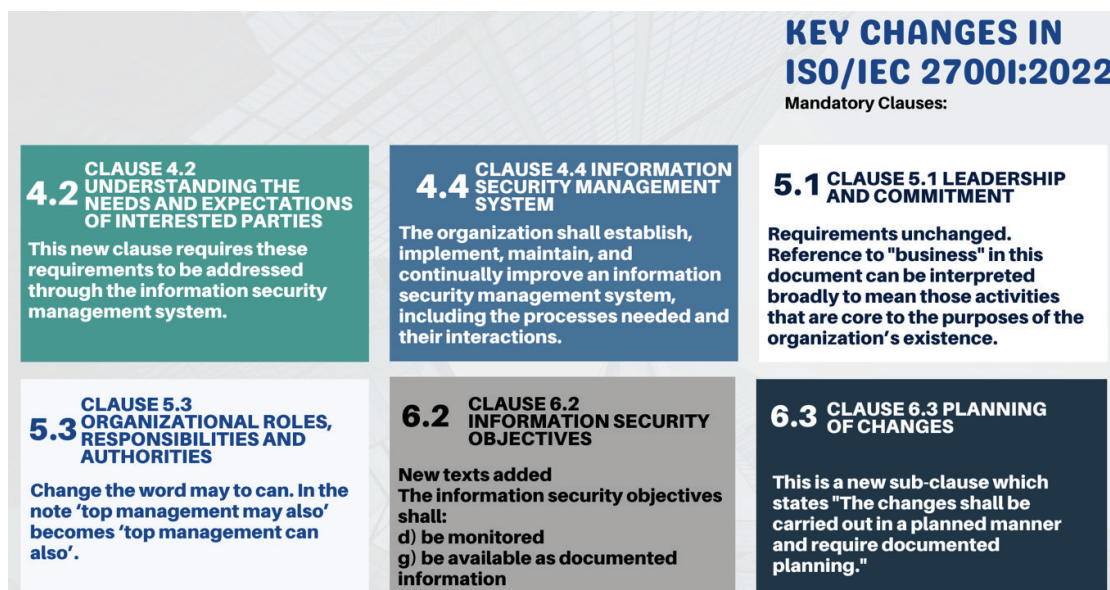
ISO/IEC 27001 is an international standard that provides a universal framework for information security management. It outlines the requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS). The standard

provides a systematic and risk-based approach for identifying, assessing, and managing information security, taking into account the context of the organization, its information security risks, and the controls necessary to mitigate those risks. It is designed to provide a framework for organizations to improve their security posture and demonstrate their commitment in information security to stakeholders including customers, regulators, and investors.

ISO/IEC 27001 prescribes a set of requirements that organizations must meet in order to achieve certification. These requirements cover various aspects of information security management, such as risk assessment and treatment, security controls, monitoring, and continual improvement. The standard is technology-neutral and can be applied to organizations of all sizes and types in any industry. By implementing ISO/IEC 27001, organizations can demonstrate their commitment to protecting sensitive information, build trust with customers and other stakeholders, and comply with legal and regulatory requirements.

Key Changes in ISO/IEC 27001:2022

The new version of ISO/IEC 27001:2022 has the same number of clauses as ISO/IEC 27001:2013, but the wordings have changed slightly. The changes help align ISO/IEC 27001 as the same as other ISO/IEC management standards. Key changes to the mandatory clauses in ISO/IEC 27001:2022, are elaborated in the figure below:



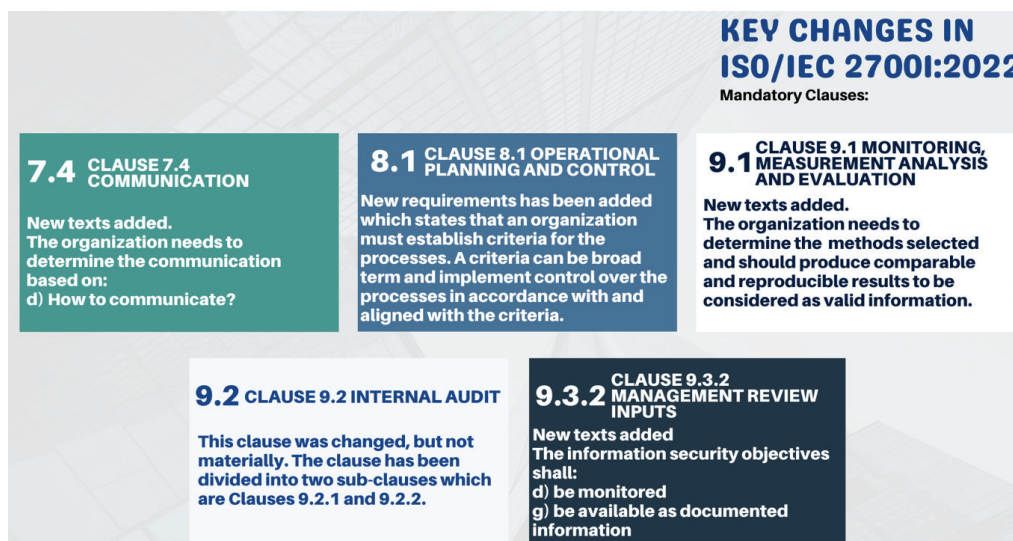


Figure 1: Key Changes in ISO/IEC 27001:2022

Changes to Annex A Control Structure

ISO/IEC 27001 Annex A is the most significant annex of all ISO standards, as it contains a vital instrument for managing information security risks: a list of security controls (or safeguards) that should be used to enhance the security of information assets. The ISO/IEC 27001 controls are outlined in ISO/IEC 27001 Annex A, which are devised from ISO/IEC 27002. The following figure illustrates the significant changes made to Annex A, which are reflected in the changes made in ISO/IEC 27002:2022:

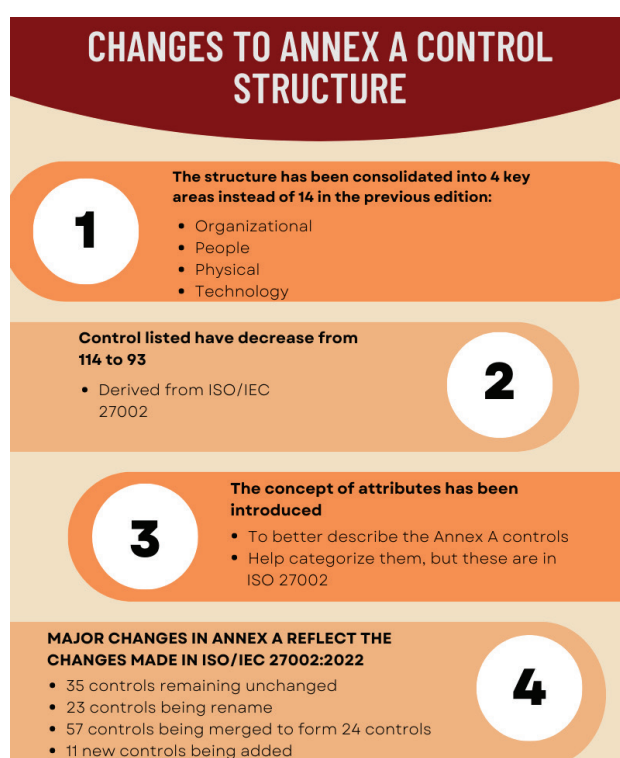


Figure 2: Changes to Annex A Control Structure

Benefits of ISO/IEC 27001:2022 Certification

Being ISO/IEC 27001:2022 certified can benefit an organization in many ways. It demonstrates one's dedication to security standards and the openness of the company to feedback from outsiders. Additionally, it implies that an organization gets along well with fellow auditors and is open to making adjustments as needed. The changes made in this new revision reflect the evolution in working methods and associated threats. Besides that, the revised standard enable a more flexible and evident implementation.

The key benefits of securing ISO/IEC 27001:2022 certification are as follows:

- 1. Improved information security posture:** By implementing ISMS and the controls as outlined in ISO/IEC 27001:2022, organizations can improve their overall security posture, ensure is reflected in the current digital business profile, and simultaneously reduce their information security risks.
- 2. Increased confidence:** ISO/IEC 27001:2022 certification demonstrates an organization's commitment to information security and provides stakeholders with increased confidence in their ability to protect sensitive information.
- 3. Competitive advantage:** Organizations that are ISO/IEC 27001:2022-certified may have a competitive advantage over their peers because they have demonstrated their commitment to information security.

- 14
4. **More flexible control:** Adopt the most flexible control structure which aligns easily with international cybersecurity frameworks.
 5. **Improve efficiency:** By aligning it with the most recent harmonized structure for management systems, organizations can increase the effectiveness of their management system.

For the new clients, certification against ISO/IEC 27001:2013 is allowed until 30th April 2024. Upon successful completion of the transition audit, the certificate document will be revised to show compliance with ISO/IEC 27001:2022. It is important to note, however, that the expiration date of the current certification cycle will remain unchanged.

This means that organizations should begin updating their controls and processes to comply with the requirements of this new revision as soon as possible. Additionally, they need to revisit their risk assessment and Statement of Applicability (SOA) to ensure the revised set of controls are applied appropriately and effectively, bringing an organization's ISMS in line with their digital business risk. The transition timeline for ISO/IEC 27001:2022 is illustrated in the figure below:

Transition Period

According to the International Accreditation Forum's publication, "Transition requirements for ISO/IEC 27001:2022", any company currently certified against ISO/IEC 27001:2013 has until 31st October 2025, a period of approximately 2 years from now, to transition to the new revision.

ISO/IEC 27001:2022 Transition Timeline

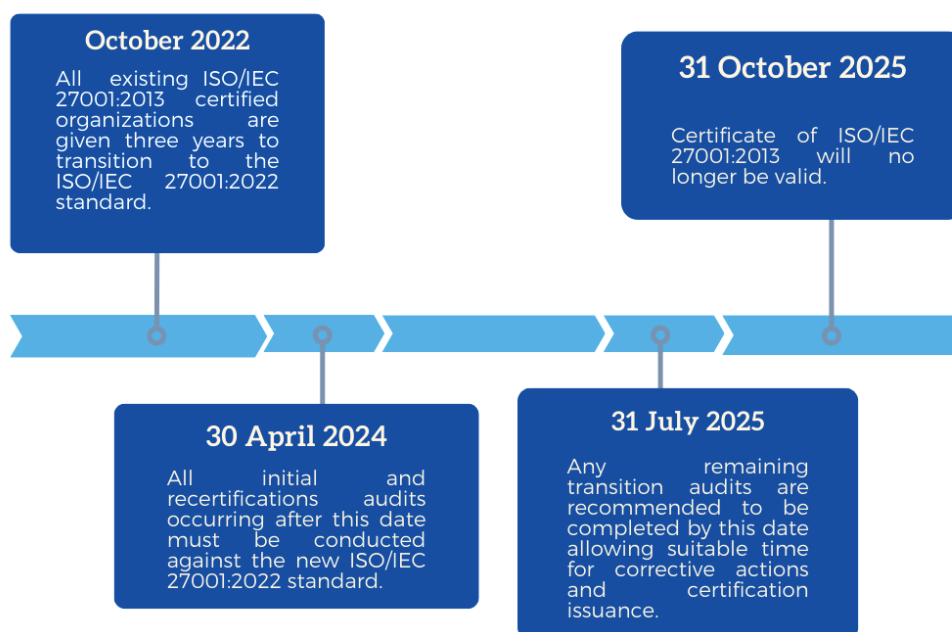


Figure 3: ISMS Transition Timeline Period

Certified organizations are given a three-year window for transition. The transition audit can take place either as part of a scheduled surveillance/recertification review or as a separate audit, provided that the objectives of the transition audit can still be met. Remote transition audits are also permissible if the requirements are fulfilled. If the transition audit is conducted simultaneously with a recertification

review, a minimum of half (0.5) auditor day will be required to verify the certified client's transition. However, if the transition occurs during a surveillance audit or a separate audit, a minimum of one full day (1.0) is necessary.

Please contact us Certification Body (CB) at certification@cybersecurity.my or visit <https://iscb.cybersecurity.my> for more details.

Conclusion

The previous update of ISO/IEC 27001 occurred almost 10 years ago. But due to new technology risks, one can expect more frequent changes and updates in the near future as cybersecurity threats continue to grow exponentially.

In summary, changes made to the new version of ISO/IEC 27001:2022 Information Security, Cybersecurity, and Privacy Protection, are considered minimal, but organizations are still required to revisit their ISMS processes and documents. Each organization needs to provide a timeline for their own transition.

31st October 2025 shall be the final date for organizations to be certified against the new version of ISO/IEC 27001:2022. It is therefore advisable for organizations to contact the Certification Body (CB) to renew their certifications to the latest version.

References

1. <https://advisera.com/27001academy/blog/2022/02/09/iso-27001-iso-27002/>
2. <https://www.a-lign.com/articles/blog-whats-the-difference-between-iso-27001-2013-and-iso-27001-2022#:~:text=Updates%20to%20Clauses%204%2D10,as%20well%20as%20monitoring%20standards>
3. <https://www.standardfusion.com/blog/iso-27001-changes-2022/#:~:text=The%20updated%20version%20of%20ISO,instead%20of%20the%20previous%2014>
4. <https://pecb.com/article/iso-iec-27001---what-are-the-main-changes-in-2022#:~:text=Some%20of%20the%20main%20new,also%20impacted%20ISO%2FIEC%2027001>
5. <https://www.a-lign.com/articles/blog-whats-the-difference-between-iso-27001-2013-and-iso-27001-2022#:~:text=Updates%20to%20Clauses%204%2D10,as%20well%20as%20monitoring%20standards>
6. <https://www.dataguard.co.uk/blog/iso-27001-annex-a-controls#one>
7. <https://www.thecoresolution.com/iso-270012022-is-here-what-does-it-mean-for-you>

How Hackers Can Drain Your Bank Account with Tap-And-Pay Apps

By | Nur Syakirah binti Shahabuddin & Norhamadi bin Ja'afar

Introduction

Tech giants like Apple, Google and Samsung have made smartphones an alternative to the plastic credit and debit cards that we usually carry around. With a few easy settings on our phones, we no longer need to reach into our wallets to take out cash or cards every time we purchase something at the stores. The new way is known as 'tap-and-pay'. With tap-and-pay, it is even possible to pay without having to unlock your digital wallet at all. The App continues to work even when a phone has run out of battery or powered down. Just tap our smartphones at retail terminals and we are good to go.



Figure 1: Tap-And-Pay Application on a device

How Is It Even Possible?

Tap-and-pay has been proven to ease congestion at train turnstiles and bus stops. A commuter's routine has been made easier and quicker, so everyone seems to be happy.

The process appears easy, but is it really safe? After all, we are putting the safety of our money and bank accounts on the line.

A cause for concern was raised by researchers from the University of Birmingham and University of Surrey, England back in September 2021. They showcased that a smartphone could be 'tricked' into making a payment at a train turnstile, while it was actually any random retail terminal. That retail terminal might well be one

that is controlled by cyber criminals to funnel your money straight into their bank accounts. To make matters worse, the tap-and-pay feature could continue operating even when the phone has run out of battery or powered down [1].

Confirming the worst fears, Timur Yunosov, a Russian cybersecurity researcher, has also demonstrated in early 2022 that the same attack could happen to Apple and Samsung smartphones. Yunosov successfully showed how quick and easy it was to empty someone's funds should their phones fall into the wrong hands. [1].

Using an Apple smartphone and Apple Pay, Yunosov was able to empty the linked Visa card account into an overdraft. Using a standard payment terminal which mimicked a transport terminal, the London Underground for example, payment on a Visa card was allowed to go through. Yunosov used a "man-in-the-middle" like device between the locked phone and the terminal to activate payment, bypassing restrictions set up by Visa.

The really easy hack for crooks is to bring a stolen smartphone with touch-and-pay settings turned on, for a shopping spree. They could keep charging the card as they please until the bank reaches the overdraft limit or the cardholder blocked their card.

Of course, the attack could only happen if a crook can physically get hold of a smartphone and hold it up to a fake terminal, and where the e-wallet is using a Visa card. Meanwhile, Mastercard appears to have avoided the problem. Neither Apple nor Samsung has provided any additional protection from this kind of attack, while Visa has yet to provide any kind of fixes despite updates by Mastercard.

How to Stay Safe?

Whom do we turn to should we encounter such theft? Is it Apple, Google, Samsung, Visa or Mastercard?

1. An official response from Apple stated that, "We take any threats to users' security very seriously. This is an issue raised within the internal system in Visa however Visa does not believe this kind of fraud was likely to take place in the real world given the multiple layers of security in place. In the unlikely event that an unauthorized payment was made, Visa has made it clear that their cardholders are protected by Visa's zero liability policy" [2].
2. An official response from Mastercard stated that, "Cardholders can remain confident that any payment using Mastercard is safe and secure; they are always protected whenever and wherever they choose to pay. Our fundamental priority is to deliver security in every Mastercard transaction. We use the latest technologies across cyber, biometrics, and AI to identify and stop any threat of fraud at every step of a purchasing process. This academic scenario was raised to us via the responsible disclosure program, and while it was extremely limited outside of a laboratory environment, we have since addressed the potential problem." [2].
3. An official response from Visa, "Visa cards connected to mobile wallets with transit features are secure and cardholders should continue to use them with confidence. Variations of contactless fraud schemes have been studied in laboratory settings for more than a decade and proven to be impractical to execute at scale in the real world. Multiple layers of security are used to protect payments and consumers can benefit from Visa's zero liability guarantee. Visa takes all security threats seriously and continuously evolves its payment security capabilities to protect cardholders from any latest real-world threats" [2].

Conclusion

Our reliance on technology has increased over the years, but with today's rapid technological development, security is invariably doing catch up with each innovation. Nevertheless, it is still possible to protect your privacy and enhance security on smart devices to avoid any theft from your e-wallet apps. Just simply turn off the quick tap payment feature in your phone settings. Otherwise, one may compromise security for the sake of convenience.

References

1. <https://rapidtelecast.com/how-hackers-can-drain-your-bank-account-with-apple-and-samsung-tap-and-pay-apps/>
2. <https://www.forbesmiddleeast.com/innovation/cybersecurity/how-hackers-can-drain-your-bank-account-with-apple-and-samsung-tap-and-pay-apps>
3. <https://www.trustedreviews.com/how-to/how-to-use-samsung-pay-4230716>
4. <https://cult.honeypot.io/reads/5-ways-hackers-steal-your-money/>
5. <https://www.garlandtechnology.com/blog/how-hackers-stole-millions-from-banks>

Cybersecurity Policies And Governance

By | Mohamad Nasrul Taufiq bin Salleh & Shazwani binti Salleh

Cybersecurity has emerged as a critical concern for individuals, corporations, and governments across the world. The widespread use of digital technology has made individuals and businesses alike vulnerable to cyber-attacks. Hence, cybersecurity rules and governance are crucial in protecting individuals, corporations, and governments from the consequences of cyber threats. This article takes a look at cybersecurity policies and governance, as well as the various frameworks that businesses can use to strengthen their cybersecurity posture.

What is Cybersecurity?

Cybersecurity is a set of techniques, technologies, and processes used to safeguard all computers, digital devices networks, and data from unwanted access, use, disclosure, interruption, modification, or destruction. Cyber threats are hostile activities that exploit weaknesses across computer systems and networks. Phishing attacks, malware, ransomware, and denial-of-service assaults are some examples of cyber threats

What is the Importance of Cybersecurity?

Cybersecurity ensures confidentiality, integrity, and availability of information. Protection of data from unauthorized access is referred to as confidentiality. Protection from illegal alteration is referred to as integrity, while the protection of data from unlawful deletion is referred to as availability. Cybersecurity is also essential in preventing financial losses, reputational damage, and legal obligations as a result of cyber incidents.

Policies for Cybersecurity

A cybersecurity policy represents a set of rules, standards, and processes that a company uses to secure the confidentiality, integrity, and availability of its data and systems. It is an important component of an organization's overall cybersecurity program because it

provides a structure for managing cybersecurity threats. A cybersecurity policy should be based on the organization's risk management framework, which involves identifying and assessing cybersecurity threats, adopting risk-mitigation controls, as well as monitoring and reporting on control efficacy.

Cybersecurity Policy Elements

Purpose

The purpose of a cybersecurity policy should be clearly defined and consistent with an organization's broader mission and objectives. The policy must explain why cybersecurity is important and what it aims to achieve. An example could be to secure the confidentiality, integrity, and availability of sensitive information, to protect against financial loss and legal liability stemming from cyber incidents, and to the organization's reputation.

Scope

The scope of a cybersecurity policy should clearly identify what the coverage entail. It has to include all assets, such as hardware, software, data, and networks. The policy should also specify the extent to which it is applicable. For example, it must apply to all employees, contractors, and third-party service providers who have access to the organization's information and systems.

Responsibilities and Roles

All parties involved in a cybersecurity program, including senior management, employees, contractors, and third-party service providers, should have their roles and duties clearly defined. The policy should explicitly define who is in charge of developing, maintaining, and monitoring security controls, as well as the exact duties and responsibilities. It needs to state that the Chief Information Security Officer (CISO) must be in charge of administering the cybersecurity program and ensuring that security measures are implemented. It could also outline employees' obligations in reporting security issues, adhering to security standards, and completing security training.

Management of Risk

A cybersecurity policy should establish the risk management framework for the organization, including processes for detecting, assessing, and managing cybersecurity threats. It has to specify the organization's risk tolerance as well as how it will prioritize and allocate resources to handle cybersecurity threats. The framework should be founded on industry best practices and standards, such as the NIST Cybersecurity Framework or ISO/IEC 27001.

Security Measures

The policy should identify all security procedures that will be implemented by the organization to mitigate cybersecurity threats. All cyber security controls must be based on industry best practices and standards, such as the CIS Controls or the NIST Cybersecurity Framework. In addition to type of controls, the policy must describe how the controls will be implemented, maintained, and tested. For example, the policy could state that all software must be updated on a regular basis to ensure that known vulnerabilities are addressed.

Management of Incidents

The incident management procedures, including protocols for reporting, investigating, and responding to cybersecurity occurrences, must be clearly defined in the policy. The policy should state who is in charge of responding to such occurrences and what procedures to follow including the mechanisms for escalation for situations that cannot be resolved at the operational level. For example, the policy may require that all security issues be reported to the CISO, who will oversee the incident response process.

Reporting and Monitoring

A cyber security policy should specify the procedures for monitoring and reporting on the efficacy of cybersecurity measures as well as the overall cybersecurity program. The frequency of monitoring and reporting must also be specified. For example, the policy could state that all security incidents have to be documented and investigated, and that the results of the analysis must be reported to management regularly.

Cybersecurity Governance Frameworks

ISO/IEC 27001

ISO/IEC 27001 is a generally accepted global standard that establishes a framework for information security management systems (ISMS). An ISMS is a methodical way of handling sensitive enterprise information. Based on the Plan-Do-Check-Act (PDCA) cycle, which is a model for continuous improvement in cybersecurity risk management, the standard defines roles, responsibilities, and processes to provide a more systematic approach to addressing cybersecurity risks. Organizations must conduct a risk assessment, create an information security management plan, and apply security measures to mitigate identified risks, in accordance to the standard. Organizations also need to regularly monitor and assess the efficiency of their security procedures in order to improve their cybersecurity posture.

NIST Framework for Cybersecurity

The National Institute of Standards and Technology's (NIST) Cybersecurity Framework is a voluntary framework that provides guidelines for enterprises to improve their cybersecurity posture. The framework is intended to assist enterprises of all sizes and types in managing and mitigating cybersecurity risk via five primary functions: identify, protect, detect, respond, and recover. By identifying assets and risks, securing them, detecting and responding to threats, and recovering from cyber catastrophes, these functions provide an organized method to managing cybersecurity risks.

The Framework Core, Implementation Tiers, and Framework Profiles are three components of a framework. The Framework Core represents a collection of cybersecurity tasks, outcomes, and useful references that are shared by critical infrastructure sectors. The Implementation Tiers allow businesses to specify how closely they adhere to the Framework Core. Organizations use the Framework Profiles to match their cybersecurity operations with business requirements, risk tolerance, and resources.

CIS Controls

Controls from the Center for Internet Security (CIS) are a set of best practices for safeguarding IT systems and networks. The CIS Controls are classified into three types: fundamental, foundational, and organizational. Fundamental

controls are basic controls that a company should have in place. Organizational controls are strategic controls that focus on governance and risk management, while foundational controls are additional control features that businesses can adopt to strengthen cybersecurity posture.

Based on real-world threats, assaults, and vulnerabilities, CIS Controls specifies a prioritized approach to cybersecurity. The controls are aligned with industry standards such as the NIST Cybersecurity Framework and ISO/IEC 27001. CIS Controls also include instructions on how to deploy the controls and assess their efficacy.

COBIT

COBIT (Control Objectives for Information and Related Technology) is an IT governance and management framework developed by ISACA (Information Systems Audit and Control Association). COBIT provides a comprehensive framework for managing information technology risks, including cybersecurity threats. The framework is intended to assist enterprises in aligning their IT strategy with their business plan, as well as in managing IT risks in a methodical and organised manner.

Governance and Management Objectives, Governance and Management Practices, Governance and Management Processes, Governance and Management Enablers, and Performance Management make up the five components of COBIT. The framework defines roles, responsibilities, and processes to provide an organized approach to managing cybersecurity risks. COBIT also offers guidelines on how to examine and improve an organization's cybersecurity posture.

CSA Cloud Controls Matrix

The Cloud Security Alliance's (CSA) Cloud Controls Matrix is a pre-defined paradigm for evaluating the security controls of cloud service providers. The matrix presents a set of security rules that enterprises may use to assess cloud service providers' security posture. Controls pertaining to data security, access management, incident response, and compliance are included in the matrix.

The Cloud Controls Matrix is based on industry standards such as ISO/IEC 27001 and NIST Framework. It defines roles, responsibilities, and processes of providing an organized way to analyze cloud service providers' security posture. The Cloud Controls Matrix also explains how to assess the efficacy of security controls applied by cloud service providers.

References

1. <https://resources.infosecinstitute.com/topic/key-elements-information-security-policy/>
2. <https://www.nist.gov/cyberframework>
3. <https://www.cisecurity.org/controls>
4. <https://www.iso.org/isoiec-27001-information-security.html>
5. <https://www.isaca.org/resources/cobit>
6. <https://cloudsecurityalliance.org/research/cloud-controls-matrix/>
7. <https://www.ibm.com/topics/cybersecurity>
8. <https://www.cisa.gov/topics/cybersecurity-best-practices/cybersecurity-governance#:~:text=Cybersecurity%20governance%20is%20a%20comprehensive,Decision%2Dmaking%20hierarchies>
9. <https://blog.box.com/information-security-policy-core-elements>

Ethics In Vulnerability Assessment And Penetration Testing

By | Ahmad Hazazi bin Zakaria, Norhamadi bin Ja'afar & Mohd Faizal bin Sulong

Introduction

Ethics in the broadest sense refers to moral principles that govern a person's behaviour or the conductivity of an activity. In community life, ethics is pursued through diverse cultural, political and religious ideals and practices which give each member guidance on leading a good and virtuous life. Ethics in work life, is often defined in formal codes or standards to which all members of a profession are held accountable, such as medical or legal field.

Penetration testers attack systems to evaluate their security response in an event of a real attack and it is also known as Vulnerability Assessment and Penetration Testing (VAPT). These attacks take the form of authorised penetration tests that attempt to probe a system's defences. These defences are then breached to evaluate the impact of any inherent weaknesses and the test results are used to improve a system's security, thus making them more resilient to future or similar attacks.

VAPT which is part of best cybersecurity practices with the aim to secure—that is, keeping data, computer systems and networks either it is software or hardware safe. VAPT primarily addresses the integrity, functionality, and reliability of human institutions/practices that rely upon such data, systems, and networks. In protecting these institutions and practices, VAPT is essentially protecting the lives of human beings who depend upon them. VAPT is also critical in the protection of credit users, students, power and water customers, voters, investors, inventors, drivers, trains and aeroplane passengers—essentially each and every one of us. This means ethics ultimately plays an important part in human life and environment. Considering the complexity and difficulty of securing online data and systems from a multiplicity of hostile actors exploiting under-resourced security controls—the ethical responsibility borne by cybersecurity professionals is a heavy one. Ethics is what keeps cybersecurity practitioners, focused and clear about their roles and responsibility towards human life and the systems that keep the modern world running.

Problems

Identity theft is one of the most common threats in cyberspace. Personally identifiable information is stolen and used to impersonate victims in financial transactions or any other illegitimate purposes alike. This happens due to the sheer volume of sensitive data that people and organizations are generating today. Hacking and other network intrusions are used to gain sensitive information about individuals. It can be used for blackmailing, extortion and any other unethical or illegal activities. For example, blackmailing is used to force compromised employees to disclose sensitive client information or engage in corporate and government espionage and misconduct.

Most of us do not realize how exposed our lives and property are by not practising good cybersecurity. The inability to personally control, protect and disclose private information is due to the chaotic global data ecosystem. Sensitive information could be exposed and unfortunately, poorly enforced data regulations and policies fail to protect the public from reputational, economic and emotional harm. Hence, public safety and personal data protection within the cyber environment is at risk and this may cause harm to privacy. Privacy harms do not only threaten those who are already exposed to cyber threats, but also the general public who are on the digital grid. For example, sensitive personal data which is not stored securely may be inadvertently exposed by medical providers or legal practitioners.

While performing vulnerability assessment and penetration testing, it is common to find illegal, sensitive and harmful information. This is because the pen testers have permission to roam inside the client system. Cybersecurity is a form of risk management that needs to be properly handled as the resultant risks can significantly impact other parties. A default ethical duty is to disclose those risks when known so that those potentially affected can make informed decisions. For example, if a critical vulnerability is discovered in a client system either within the software or hardware, the penetrators should immediately notify the customers/client so they can install a patch (if available)

22

or to take appropriate defensive measures against the said vulnerability. In many cases, the best method and extent of the disclosure is timely notification. If the vulnerability proves too challenging to discover and the security is team unable to patch a critical network flaw which could impact customers, any delay in notification until a patch is available could be ethically indefensible. There is no 'one-size-fits-all' rule or instruction that one can follow to ensure transparency in cybersecurity practice. Ethics is the cornerstone in such situation. Hence, given the particular facts and options, a critical reflection is necessary on the particular scenario and the specific risks, benefits, trade-offs and stakeholder interests involved, followed by a well-reasoned ethical judgment on the best available resolution.

Practising cybersecurity involves many distinct roles and stakeholders interest. In some cases, ambiguous ethical duties can be one of the great concerns. Divergent roles may also lead to confusion on the expected ethical standards in the cybersecurity community. Thus, careful reflection is necessary to reach a justifiable decision in each particular case. For example, the various ethical standards of a hacker who identifies as a white hat, black hat or grey hat hacker. They are security practitioners who identify themselves as computer hobbyists and informal collectives. Many cybersecurity professionals may feel conflicting loyalties to the interests of the public, government agencies and particular groups within the security community. A cybersecurity researcher will be at odds whether to publish a finding which may undermine a popular encryption key management system for the sake of the community knowledge base. While at the same time, he may also have a client in a cybersecurity consulting firm who will be at risk by such disclosure. Ethically his/her findings could undermine the security firm but such disclosure is for betterment of the cybersecurity community. All of the issues outlined could significantly impact the lives and welfare of others. The issues are ethically wrong and in conflict with what we would expect from cybersecurity professionals. Formulating cybersecurity solutions that are right and justifiable by reasonable professional standards can be challenging and require careful ethical reflection, analysis and problem-solving skills.

Solution

Two of the most important aspects in carrying out work and taking care of company's interests is trust and confidence. To ensure that these two aspects are preserved, we need to establish a workplace where ethical behaviour is the norm:

1. Honesty in assessing needs and resources

Good and careful planning is one of the key success factors in any business. To produce a good plan, honesty needs to be applied. To ensure the project is relevant and meaningful, it is very important to know the common ethical challenges in the work done, the risks encountered during implementation of the project, as well as values of company and employee and beneficial ethics resources available.

2. Create a solid foundation

Establishing a robust and compliant program needs careful preparation in order to create a solid foundation. A holistic ethics program must consists of several key elements:

- a. Written standards of ethical conduct in the workplace
- b. Training on standards
- c. Advisory services on ethical and compliance issues
- d. Provision of a medium to report potential violations confidentially or anonymously
- e. Ethical behaviour performance evaluation.
- f. A comprehensive system to discipline violators

When it comes to ethical compliance, just having these elements is not enough. It is important to ensure employee know-how and a good support system that can help them uphold ethics and comply with all standards of work. Characteristics of an effective ethics and compliance program are:

- a. Freedom to question management without fear
- b. Rewards for following ethical standards
- c. Not rewarding the practice in question, even if it produces good results for the company
- d. Positive feedback for ethical behaviour

- e. The willingness of employees to deal with misconduct
- f. Employees' willingness to seek ethical advice

3. Build a culture of integrity

Building an ethics and compliance program and incorporating it into the day-to-day operations of the organization makes for a strong ethical culture. In such environment, employees at all levels are committed to doing the right thing and upholding values and standards. Leaders who become powerful drivers of the corporate culture, can then promote a strong ethical culture by:

- a. Talking about the importance of ethics
- b. Ensuring that employees are adequately informed about issues that affect them
- c. Keeping promises and commitments to employees and stakeholders.
- d. Recognizing and rewarding ethical behaviour
- e. Holding those who violate standards accountable, including leaders
- f. Displaying ethical behaviour professionally and personally

4. Reassess and revise as needed

Situations and needs are always changing from time to time. A responsible person needs to identify what works, what does not, what is new and fix any weaknesses that appear. Be disciplined and constantly review the state of ethics and compliance organization. Periodic or ongoing risk assessments, follow-up surveys and focus groups could help keep the program relevant and minimize risk.

Every organisation should plan and develop security requirements for assessment. The requirements should be in line with the objectives and scope of the assessment. To perform a security assessment, a code of ethics must be incorporated to ensure morality of work. Apart from providing principles and theories on what is right, ethics helps classify arguments, defend a position, enhance understanding of others and lastly, help determine an appropriate course of action. Professional penetration testers will inevitably rely on professional codes to provide advice on their conduct. Such codes need to be broad enough to cover potential ethical conflicts and concerns, yet specific enough to guide decision-making in actual situations. The

Council of Registered Ethical Security Testers (CREST) provides their members with a code of conduct. It not only stipulates a code of ethics but also good practices including the need to evaluate the impact of new techniques and tools and the requirement to explain project deliverables to clients and also, keep abreast with new rules and regulations.

For information security professionals, the three code of ethics are:

Integrity

- a. Perform duties following existing laws and exercising the highest moral principles
- b. Refrain from activities that would constitute a conflict of interest
- c. Act in the best interest of stakeholders consistent with public interest
- d. Act honourably, justly, responsibly, and legally in every aspect of the profession

Objectivity

- a. Perform all duties in fairly and without prejudice
- b. Exercise independent professional judgment, to provide unbiased analysis and advice
- c. When an opinion is provided, emphasize that it as an opinion and not a fact

Professional Competence and Due Care

- a. Perform services diligently and professionally
- b. Act with diligence and promptness in rendering service
- c. Render only services in which one is fully competent and qualified in
- d. Ensure work performance meets the highest professional standards. Where constraints exist, ensure that work is both correct and complete within the set limits. In one's professional judgment, if resources are inadequate to achieve an acceptable outcome, inform clients and principals accordingly
- e. Be supportive of colleagues, and encourage their professional development. Recognize and acknowledge the contribution of others, and respect the decisions of principals and co-workers
- f. Keep stakeholders informed on progress of work

- g. Refrain from conduct that would damage the reputation of the profession
- h. Report ethical violations to the appropriate governing body on time

Outcome/Lesson

Best cybersecurity practices are proven techniques for doing something that tends to work well. For cybersecurity practitioners, these best practices are like guiding principles which they could adhere to:

| Guiding Principles | Descriptions |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| At all times follow existing laws, and practice values and exercise the highest moral principles | <ul style="list-style-type: none"> Do not engage in unethical or unlawful acts that negatively impact the community, professional reputation, or the information security discipline Act with fairness and justice to all parties and refrain from activities that would constitute a conflict of interest or damage the reputation or be detrimental to the information security profession or association Act in the best interest of stakeholders and consistent with the public interest |
| Protect and maintain an appropriate level of confidentiality, integrity and availability of all sensitive information in any course of professional activities | <ul style="list-style-type: none"> Respect the confidentiality of information acquired during their duties Refrain from using or disclosing, sharing, disseminating or distributing any confidential or proprietary information without proper and specific authority unless there is a legal or professional obligation to do so Avoid misusing any confidential information for personal gain Treat all information received from a client or employer as confidential unless such information is in the public domain Take appropriate steps to minimize or mitigate potential risks, including recommending the engagement of another professional if the need arises |
| Render service with fairness, courtesy and good faith towards clients, colleagues and others, give credit where it is due and accept, as well as give, honest and fair professional comments | <ul style="list-style-type: none"> Exercise independent professional judgment in providing unbiased analysis and advice Exercise restraint when commenting on the work of other members Do not maliciously injure the character or the prospects of business of another member or individual, being just as careful with a colleague's reputation as with one's own |
| Do not engage in any crime or improper practices | <ul style="list-style-type: none"> Do not engage in any crime such as bribery, identity theft, forgery, fraud, financial crime such as credit card fraud or double billing or any other improper practices Reveal any conflict or any possible crime without delay to clients or employers, including interests (direct or indirect) held by close associates, relatives and companions |
| Perform all professional activities and duties following the highest ethical principles | <ul style="list-style-type: none"> Be responsible to safeguard credibility and trustworthiness while rendering services Only render services for which one is fully competent and qualified in Do not engage or be a part of any malicious activities that may harm others Conduct services in the most ethical manner without prejudice |

| | |
|------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Avoid association with those whose practices or reputation might diminish the profession | <ul style="list-style-type: none"> Refrain from any activities that can damage your reputation and profession, or the practice of colleagues, clients, and employer Report ethical violations to the appropriate governing body if needs arise |
| Provide service with competence, honesty and forthrightness | <ul style="list-style-type: none"> Provide a guideline to those involved in the industry and maintain uniform ethical standards, and uphold the trust at all times Be aware of the exact nature and scope of professional activity and do not go beyond specificity Demonstrate personal commitment to ongoing professional development and capability building |

A code of ethics increases the probability that people will behave in the right way. This is achieved by focusing on their actions and partly on sanctions for violations of ethics. In addition, reliance on the code can reduce any consequences in case of unethical behaviour.

An example might be the case of an information system security analyst whose friend asked him to reveal the weaknesses of an organization's system for his benefit. Without the code, it would be a moral choice on his part. The code specifies that should the analyst violate the rules, it would result in him losing his job, and not being a good example to his family. Second, a good code of ethics can lead to actions that result in doing the right thing and for the right reason. Ethical behaviour should become a habit through practice. An effective code allows both parties to pitch their action against standards that have been set. When constantly repeated, such practice will be ingrained in an individual.

For example, in a system security assessment contract, the project duration is long and often difficult to justify. If efficiency alone is the standard, contract analyst will be easily tempted to ignore the rules to expedite the project. However, it is clear that the main principle should be fairness and honesty in carrying out duties. It is therefore difficult to justify an incomplete and improperly drafted contract.

A code of ethics can serve as a professional statement. This ensures commitment of employees to adhere to a set of moral standards specific to their respective professions. Not all individuals are aware of the expected moral standard of each profession and codes can clarify expectations. Codes can also help instill a sense of pride. Pride is a critical emotion in motivating individuals to hold themselves out as professionals.

Conclusion

Adhering to a code of ethics while performing VAPT is tricky and very challenging at the same time. Any discovery of illegal activity in client during VAPT exercise demands a wise judgment on the part of penetration tester. Finding a single hooky copy of an application could amount to violation. For example, for software license violations, depending on how severe it would be, could be raised with the client first before reporting to the authorities. It is more ethical to bring up such findings to the client's manager.

Codes of ethics for ethical hacking are focused on the duties, responsibilities and limits of the ethical hacker in doing his job. Cybersecurity practitioners need to make sure that the client's system and network is properly evaluated for security issues and vulnerabilities. During the course of ethical hacking, it is not surprising that the ethical hacker could come across sensitive, personal, confidential or proprietary information. In this regard, the ethical hacking and code of ethics will help guide the actions of the ethical hacker in handling such information.

The code of ethics must also focus on protecting the client's system or network, as well as ensuring effectiveness of the ethical hacker in doing his job. Education and training of IT professionals, including security specialists, usually focuses on technical knowledge and skills. However, it is equally important to focus on ethics. In the world of IT where physical distance is irrelevant, mischievous minds tend to take advantage for their personal gain. However, the question of ethical behaviour among IT professionals is something that needs to be addressed. There are many professional associations which uphold ethical issues of IT. They have developed their own codes of ethics and professional conduct, which can serve as a guideline for individuals and other organizations. This will help make ethics an integral part of the cyber security profession.

References

1. An Introduction to Cybersecurity Ethics. Shannon Vallor, William J. Rewak, S.J Professor of Philosophy, Santa Clara University
2. Ethical Dilemmas and Dimensions in Penetration Testing. Shamal Faily, John McAlaney, Claudia Iacob
3. Code of ethics for Information Security Professionals. Retrieved from https://www.cybersecurity.my/data/content_files/11/764.pdf
4. A question of ethics illegal discoveries during a penetration test. Retrieved from <https://blog.jonsdocs.org.uk/2019/06/04/a-question-of-ethics-illegal-discoveries-during-a-penetration-test/>
5. The Important of Ethics in Information Security. Retrieved from <https://reciprocity.com/the-importance-of-ethics-in-information-security/>
6. GIAC Code of Ethics. Retrieved from: <http://www.giac.org/overview/ethics.php>
7. Ethical Issues for IT Security Professionals. Retrieved from: <http://www.windowsecurity.com/articles/EthicalIssues-IT-Security-Professionals.html>
8. Ethical principles and information professionals: theory, practice and education. Retrieved from: <http://www.alia.org.au/publishing/aarl/33.2/full.text/iacovino.html>
9. Code of Professional Conduct & Practice. Retrieved from: <http://www.mncc.com.my/code.htm>
10. Ethics Working Group. Retrieved from: <http://www.ethicswg.org/framework>

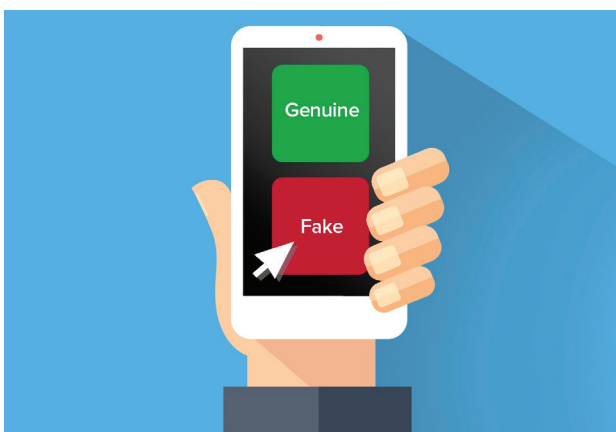
Evolution Of Macau Scam: How To Protect Personal Information And Avoid Being A Victim Of Fake Apps

By | Kamarul Baharin bin Khalid, Muhammad Nasim bin Abdul Aziz, Ahmad Aizuddin Aizat bin Tajul Arif & Muhammad Edwin bin Ambo Rifai

Introduction

Macau Scam is a form of telemarketing fraud which originated from Macau, China and hence, the name given to this particular scam. It starts with a call or message from the scammer posing as a genuine representative from either a financial institution, government agency, or official organisation. In the call, a scammer will ask the victim to provide their personal information, such as their full name, date of birth, and financial information. Next, they will use this information to steal money from the victim's bank account or commit other financial fraud.

In recent years, Macau Scam has evolved through the use of fake mobile applications. Scammers would create fake versions of popular apps, such as banking apps and ask victims to download them. Once the victim has downloaded the app, the scammers would use it to gain access to the victim's personal and financial information, including online banking details.

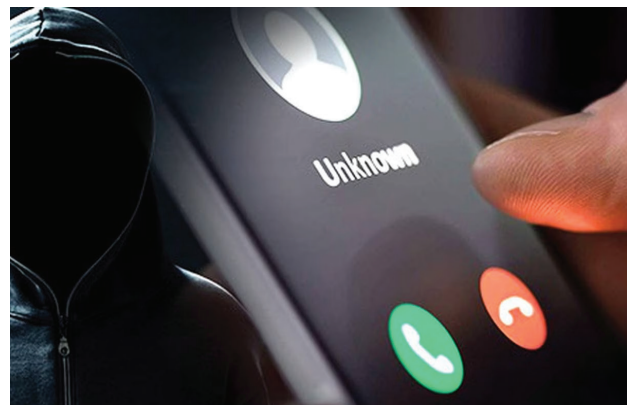


How The Scam Works

The scam begins with an advertisement, message or call from the scammer, who will pose as a representative from an e-commerce,

financial institution, government agency, or official organisation. The scammer will then ask the victim to download a fake mobile application, which the scammer claims is necessary for a transaction or security purposes. Finally, the phoney application will prompt the victim to provide personal and financial information and steal their online banking information including OTP.

Once the victim has provided their personal information in the fake application, the scammers would use the information to access their bank account and steal money via online transactions. They may also use the information for other types of financial fraud, such as opening credit card accounts in the victim's name. The victim may also be at risk of malware infection, harming their device and compromising their personal information.



Scammers will also attempt to create a sense of anxiety or panic surrounding the victim's financial activities by threatening them with frozen bank accounts, unpaid taxes or tax fraud, or withholding investment proceeds. To settle any fabricated threats, scammers will likely demand immediate payment from the victim. There are also instances where victims are lured with promises of lucrative cash prizes, in exchange for the victim's personal information or bank details as a reason to transfer the winnings to them.

Protecting Yourself

To protect yourself from becoming a victim of Macau scams and fake mobile applications, it is important to do some research on the new mobile app and only download from official app store like Google Play Store or Apple App Store. Remember to keep your mobile device and applications up-to-date as this will help ensure you have the latest security updates.

Always be wary of unexpected messages or calls from financial institutions, government agencies, or other official organisations. If you receive a message or call asking you to download an app or provide personal information, do not respond. Instead, contact the organisation directly to confirm if the request is legitimate. Be cautious of "too good to be true" offers in social media advertisements. Scammers often use these advertisements to lure people into downloading fake applications. If an offer seems too good to be true, it probably is.



MASSA, an Android app created by the Malaysia Computer Emergency Team (MyCERT) of CyberSecurity Malaysia, can be downloaded from the Google Play Store. Once installed, users can automate security checks on their Android devices to identify any misconfigurations or potential risks. Additionally, the app can detect suspicious applications not downloaded from the official Google Play Store. Any reports generated by the app can be used to investigate any Android-related incidents. If assistance is required, users can contact Cyber999. Further information can be viewed at: <https://www.mycert.org.my/portal/index>.

If one suspects that he or she is being targeted by the Macau Scam syndicate, it is essential to take immediate action to protect yourself. Such actions include contacting the financial institution to report the fraud and take steps to safeguard personal information and financial accounts. Additionally, you can seek help from the National Scam Response Centre (NSRC) via 997 hotline number.



**CYBER
CRIME ALERT**
ROYAL MALAYSIA POLICE

SEMAKMULE
Muat turun aplikasi **CHECK
SCAMMERS CCID**
di Google Play Store
Semak di laman sesawang
[HTTPS://SEMAKMULE.RMP.GOV.MY](https://semakmule.rmp.gov.my)

CCID INFOLINE
Whatsapp kami : 
013-2111 222
8 pagi - 12 t/malam (Setiap hari)

**NATIONAL SCAM
RESPONSE CENTER
(NSRC)**
Hubungi:
997
8 pagi - 8 malam (Setiap hari)

AKAUN RASMI
  
Dapatkan maklumat terkini di :
@JSJKPDRM
@CYBERCRIMEALERTMP

The hotline provides assistance for online financial scams. If an unauthorised financial transaction is discovered, it is essential to promptly contact the bank's 24/7 hotline or the NSRC's 997 hotline, which is operational from 8 am to 8 pm daily. During the call, briefly describe the scam, personal details, transaction details and if available, the scammer's information.

Conclusion

The Macau Scam has evolved over the years to include fake mobile applications that can steal victims' personal and financial information. Therefore, one needs to be cautious when downloading mobile applications, keep devices and applications up-to-date, and be wary of unexpected messages or calls from financial institutions and other organizations to protect yourself from this scam.

It is also crucial to take the necessary precautions to avoid becoming a victim. One critical step is to stay informed about the latest scams, fraud schemes and to be wary of unsolicited phone calls, messages, and emails. You should also avoid unnecessary sharing of personal or financial information, especially with individuals or organisations whom you do not know or trust.

References

1. What Is a Macau Scam and Why Are You in Danger? <https://loanstreet.com.my/learning-centre/what-is-macau-scam-what-to-do>
2. Two conned of RM18,000 in Macau Scams with new app download tactic <https://www.thestar.com.my/news/nation/2022/02/23/two-conned-of-rm18000-in-macau-scams-with-new-app-download-tactic>
3. Malware https://www.maybank2u.com.my/maybank2u/malaysia/en/personal/security_alert/malware_sa.page
4. 6 ways to manage and protect your precious banking access from online hacks or scams <https://vulcanpost.com/816596/maybank-kill-switch-security-deactivate-online-banking/>
5. How to protect yourself? - <https://www.bnm.gov.my/macauscam>
6. Jenayah Siber, Gelap Mata Tawaran Kebendaan Punca Mudah Terpedaya - <https://youtu.be/-NmGS5vXgow>
7. NSRC - Hubungi Pusat Respons Scam Kebangsaan (Nsrc) Jika Anda Adalah Mangsa Jenayah Siber <https://www.mkn.gov.my/web/ms/2022/11/23/hubungi-pusat-respons-scam-kebangsaan-nsrc-jika-anda-adalah-mangsa-jenayah-siber/>

Understanding The Technology Behind Cryptocurrencies

By | Dr. Abdul Alif Zakaria

Introduction

Cryptocurrency is a digital asset designed as a medium of exchange, similar to traditional fiat currency. However, cryptocurrency operates independent of central banks controls and government regulations. It uses cryptography to secure and verify transactions based on a distributed ledger called blockchain. Blockchain is a technology that maintains a continuously growing list of records called blocks [1]. Each block contains a timestamp, a link to the previous block, and transaction data.

Transactions of cryptocurrency are validated by a network of nodes in the blockchain [2]. When someone makes a transaction, it is broadcasted to the network, and the nodes verify the transaction using complex computation called consensus algorithm. Once verified, the transaction is added to the blockchain, and the recipient shall be credited with the specified amount of cryptocurrency.

Cryptocurrency exchange is a platform that allows users to buy, sell, and trade various cryptocurrencies. These exchanges act as intermediaries between buyers and sellers, providing a platform where buyers and sellers can perform transactions. While there are risks associated with cryptocurrency trading, using a reputable exchange and practicing good

security practices can help minimize those risks. Securities Commission Malaysia has approved four digital asset exchanges (DAX) to operate in Malaysia that include Luno, SINEGY, Tokenize, and MX Global [3]. One of the most popular DAX in Malaysia is Luno which has been a reputable cryptocurrency exchange since 2015. The exchange takes its cyber security very seriously and has implemented various measures to ensure the safety of its user accounts and funds. Luno uses two-factor authentication (2FA) and email confirmation to prevent unauthorized access to user accounts.

Cryptocurrency Technology

There are more than 20,000 cryptocurrencies in circulation worldwide. However, the listing of cryptocurrencies in Malaysian DAX requires permission from the Securities Commission Malaysia. Therefore, citizens are advised to only trade in cryptocurrencies from the approved DAX so that they do not get caught in scams. Table 1 lists different types of cryptocurrencies available in Luno DAX. Luno Malaysia supported five cryptocurrencies at its early stage of operation, including Bitcoin, Ethereum, Bitcoin Cash, Litecoin, and Ripple [4]. Later, a few other coins were included, such as Chainlink, Uniswap, Cardano, and Solana.









| |  |  |  |  |  |  |  |  | |
|-----------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|-----------------------------------------------------------------|
| | Bitcoin (BTC) | Ethereum (ETH) | Ripple (XRP) | Chainlink (LINK) | Uniswap (UNI) | Litecoin (LTC) | Bitcoin Cash (BCH) | Cardano (ADA) | Solana (SOL) |
| Original Author | Satoshi Nakamoto | Vitalik Buterin, Gavin Wood, Charles Hoskinson, Anthony Di Iorio & Joseph Lubin | Arthur Britto, David Schwartz & Ryan Fugger | Sergey Nazarov, Steve Ellis & Dr. Ari Juels | Hayden Adams | Charlie Lee | Roger Ver | Charles Hoskinson & Jeremy Wood | Anatoly Yakovenko, Greg Fitzgerald, Stephen Akridge & Raj Gokal |
| Developer | Bitcoin community | Ethereum Foundation | Ripple Labs Inc. | Chainlink team | Uniswap company | Litecoin Core Development Team | Bitcoin Cash community | Cardano Foundation | Solana Labs & Solana Foundation |
| Release | 9/1/2009 | 30/7/2015 | 2012 | 2017 | November 2018 | 7/10/2011 | 1/8/2017 | 27/9/2017 | 20/3/2020 |
| Programming | C++, Java, Python | C++, Rust & Python | C++ | Solidity, Go | Solidity, TypeScript & React | C++ (Project fork of Bitcoin) | C++, Java, Python (Project fork of Bitcoin) | Haskell | Rust |
| Network | Bitcoin blockchain | Ethereum blockchain | XRP Ledger | Various blockchain | Ethereum blockchain | Litecoin blockchain | Bitcoin Cash blockchain | Cardano blockchain | Solana blockchain |

Table 1: Types of Cryptocurrencies

Bitcoin (BTC) is the world's first and most well-known cryptocurrency. It was created in 2009 by an unknown individual or group under the pseudonym Satoshi Nakamoto [5]. BTC operates on a decentralized network that is not controlled by any central authority. BTC transactions are verified by a network of computers worldwide known as mining.

Ethereum (ETH) is a decentralized platform that enables developers to build decentralized applications (DApps) using smart contracts. Smart contracts are self-executing programs that automatically execute when certain conditions are met. Ethereum was created in 2015 by Vitalik Buterin, and it has since become one of the most popular cryptocurrencies in the world [6].

Ripple (XRP) was created in 2012 to provide fast and affordable cross-border payments, and moreover, it has forged several partnerships with many banks and financial institutions around the world [7]. XRP is used as a bridge currency for payments and it has a relatively low transaction fee compared to other cryptocurrencies.

In 2011, Litecoin (LTC) was developed as a fork of Bitcoin [8]. LTC is similar to Bitcoin in many ways as a means of payment and a store of value. However, LTC has a faster block time and a larger supply base. LTC is often used as a testbed for new Bitcoin features and improvements.

Bitcoin Cash (BCH) was created in 2017 as a result of a hard fork from Bitcoin [9]. The fork was created to address some of the scalability issues that Bitcoin faced, such as slow transaction times and high fees. BCH has a larger block size

than Bitcoin, which allows for faster transaction times and lower fees.

Chainlink (LINK) is a cryptocurrency that was introduced in 2017 by Sergey Nazarov and Steve Ellis [10]. LINK is designed to be a decentralized oracle network that connects smart contracts on the blockchain with data sources and APIs outside the blockchain. In other words, LINK enables smart contracts to access real-world data, such as market prices, weather data, and more. Moreover, LINK is also used as a means of payment and a store of value.

Uniswap (UNI) was launched in 2018 by Hayden Adams that operates on the Ethereum blockchain and uses an automated market maker system to enable peer-to-peer trading of cryptocurrencies [11]. UNI has become increasingly popular in the decentralized finance (DeFi) space, as it provides a decentralized and transparent way for users to trade cryptocurrencies.

Cardano (ADA) was founded by Charles Hoskinson in 2017, who is also one of the co-founders of Ethereum [12]. ADA platform aims to provide a more secure, sustainable, and scalable blockchain network. ADA can be used to pay for transactions on the Cardano network, as well as for staking and governance purposes.

Solana (SOL) was designed by Anatoly Yakovenko in 2017 to provide fast and cheap transactions while maintaining high levels of security and decentralization [13]. SOL uses a combination of sharding, which splits the network into smaller parallel chains and smart contracts, which enable developers to create DApps on the platform.

Cryptocurrency Consensus Algorithm

One key feature that enables cryptocurrencies to operate in a trustless environment is the consensus algorithm [14]. A consensus algorithm is a mechanism used by a cryptocurrency network to verify transactions and maintain the integrity of its blockchain, as shown in Table 2. This section presents different types of consensus algorithms and how they work.

| | Bitcoin (BTC) | Ethereum (ETH) | Ripple (XRP) | Chainlink (LINK) | Uniswap (UNI) | Litecoin (LTC) | Bitcoin Cash (BCH) | Cardano (ADA) | Solana (SOL) |
|---------------------|---------------------|----------------------|--------------------------------------------|--------------------------------------------|--------------------------------------|---------------------|---------------------|----------------------|-----------------------------------------------|
| Consensus Algorithm | Proof-of-Work (PoW) | Proof-of-Stake (PoS) | Ripple Protocol Consensus Algorithm (RPCA) | Based on the underlying blockchain network | Based on Ethereum blockchain network | Proof-of-Work (PoW) | Proof-of-Work (PoW) | Proof-of-Stake (PoS) | Proof-of-History (PoH) & Proof-of-Stake (PoS) |
| Mining Reward | 6.25 BTC | 2 ETH | None | Not fixed (Fees paid by users) | Not fixed (Trading fees) | 12.5 LTC | 6.25 BCH | None | Not fixed (Transaction fees) |
| Block Time | 10 minutes | 15 seconds | 3-5 seconds | None | Based on Ethereum blockchain network | 2.5 minutes | 10 minutes | 20 seconds | 0.4 seconds |

Table 2: Types of Consensus Algorithms

Proof of Work (PoW) is the first known consensus algorithm that has been adopted in Bitcoin, Litecoin, and Bitcoin Cash. The miners have to compete in order to solve complex mathematical problems to validate transactions and add blocks to the blockchain, as shown in Figure 1. This requires a significant amount of computational power and energy consumption. In return, the successful miner will receive some Bitcoin as a reward.

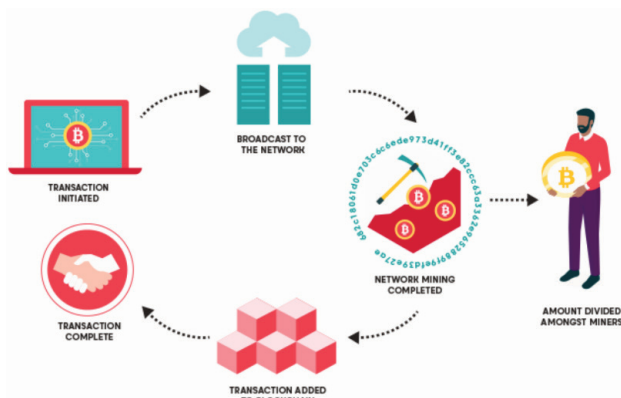


Figure 1: Proof of Work [15]

For the Proof of Stake (PoS) consensus algorithm, the validators are selected to validate transactions and add blocks to the blockchain based on the amount of cryptocurrency they

hold and stake as collateral, as shown in Figure 2. This requires less computational power and energy consumption compared to PoW. PoS is one of the most popular consensus algorithms that has been implemented in Ethereum, Cardano, and Solana.

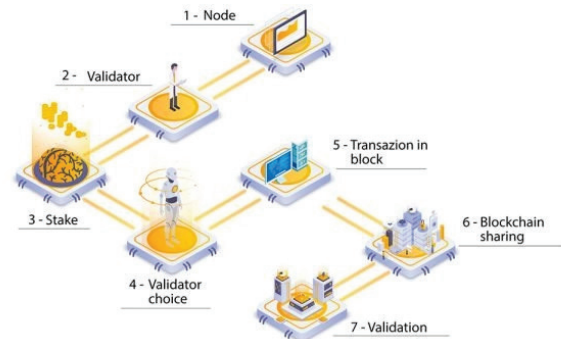


Figure 2: Proof of Stake [16]

In Delegated Proof of Stake (DPoS) consensus algorithm, a smaller group of validators are selected by stakeholders to validate transactions and add blocks to the blockchain, as shown in Figure 3. This allows for faster transaction processing times and lower energy consumption compared to PoW and PoS. Some of the cryptocurrencies that use DPoS include EOS, TRX, and ARK.

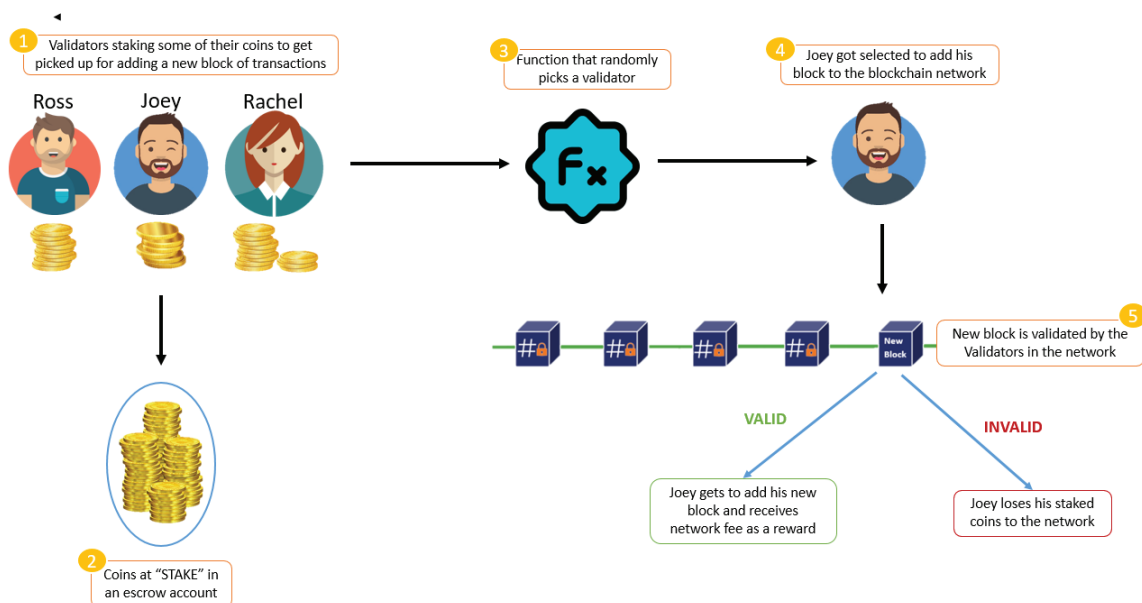


Figure 3: Delegated Proof of Stake [17]

Another consensus algorithm called Proof of Authority (PoA) has been used in CLO, EGEM, and DCR cryptocurrency. PoA is a consensus algorithm used in private blockchains. In PoA, a group of trusted validators is selected to validate transactions and add blocks to the blockchain based on their reputation and authority as shown in Figure 4. This allows for fast transaction processing times and low energy consumption but requires a high level of trust in the validators.

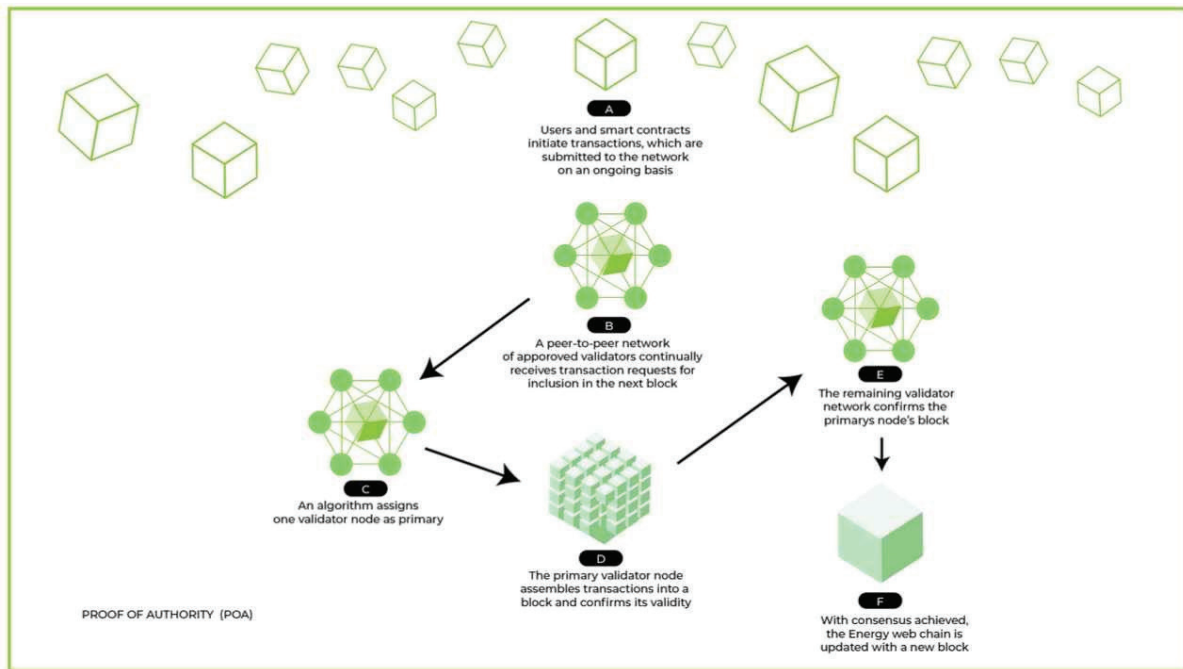


Figure 4: Proof of Authority [18]

Each consensus algorithm has its own advantages and disadvantages, and the choice of algorithm can have a significant impact on the security, decentralization, and scalability of a cryptocurrency network. While PoW is the most widely used consensus algorithm, other algorithms such as PoS, DPoS, and PoA offer more energy-efficient and cost-effective alternatives. Apart from the presented algorithms, there are other types of implemented consensus algorithms, including PoC, PoB, PoI, PoET, LPOS, DAG, PBFT, and DBFT. As the cryptocurrency landscape evolves, we can expect to see more innovation in consensus algorithms that addresses the limitations of existing algorithms.

Cryptocurrency Value

It is important to understand that cryptocurrency is a relatively new and volatile asset class with no intrinsic value. One of the most significant factors that determine the value of cryptocurrency is its adoption [19]. The more people use a particular cryptocurrency, the higher its demand will be, and thus, value. Adoption can be influenced by a variety of factors such as ease of use, security, and acceptance by merchants.

Another factor that can impact the value of cryptocurrency is its underlying technology [20]. The blockchain technology that powers cryptocurrencies can be upgraded and improved over time, making the currency more secure, faster, and more efficient. Cryptocurrencies with superior technology are likely to have higher demand and thus, value.

The overall market sentiment towards cryptocurrency also plays a role in determining its value. Positive news and developments, such as institutional adoption or regulatory clarity, can drive up the value of cryptocurrencies, while negative news, such as government crackdowns or security breaches, can cause prices to drop rapidly.

Finally, scarcity is a crucial factor that determines the value of certain cryptocurrencies. Bitcoin, for example, has a finite supply of 21 million coins, which means that as demand for the currency increases, its value is likely to rise in tandem. Other cryptocurrencies, such as Ethereum, have a different monetary policy and an unlimited supply, which would affect their long-term value, as shown in Table 3.








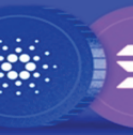

| |  |  |  |  |  |  |  |  |  |
|--------------------|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| | Bitcoin (BTC) | Ethereum (ETH) | Ripple (XRP) | Chainlink (LINK) | Uniswap (UNI) | Litecoin (LTC) | Bitcoin Cash (BCH) | Cardano (ADA) | Solana (SOL) |
| Market Cap Rank | 1 | 2 | 6 | 24 | 19 | 16 | 29 | 7 | 12 |
| Market Cap | RM1,767,076,211,829 | RM782,888,756,885 | RM85,707,284,840 | RM13,913,161,305 | RM19,309,023,726 | RM23,638,196,068 | RM9,856,092,061 | RM50,515,176,074 | RM31,625,899,729 |
| Circulating Supply | 19,313,831 BTC | 120,468,759 ETH | 50,950,912,949 XRP | 491,599,971 LINK | 753,766,667 UNI | 72,454,383 LTC | 19,333,743 BCH | 35,045,020,830 ADA | 382,961,536 SOL |
| Supply Limit | 21,000,000 BTC | Infinite | 100,000,000,000 XRP | 1,000,000,000 LINK | 1,000,000,000 UNI | 84,000,000 LTC | 21,000,000 BCH | 45,000,000,000 ADA | Infinite |
| All-Time High | RM286,777 | RM20,261 | RM13.59 | RM216.69 | RM184.89 | RM1,684 | RM15,423 | RM12.84 | RM1,081 |
| Price | RM91,628 | RM6,505 | RM1.68 | RM28.30 | RM25.64 | RM326 | RM509 | RM1.44 | RM82.40 |
| All-Time Low | RM211.18 | RM1.85 | RM0.00850498 | RM0.606188 | RM4.26 | RM4.15 | RM321 | RM0.082604 | RM2.17 |

Table 3: Values of Cryptocurrencies

Conclusion

Cryptocurrency has advantages compared to traditional fiat currency. However, it also has some potential drawbacks. One of the main concerns is its volatility, which can lead to rapid fluctuations in value. This can make it a risky investment, as the value of cryptocurrency can change dramatically within a short period of time. In summary, the technology that underpins cryptocurrencies is a crucial factor that influences their value. Security, efficiency, functionality, and upgrade capability to blockchain technology can all impact the demand for a cryptocurrency and its overall value. As blockchain technology continues to evolve and improve, the value of cryptocurrencies will likely continue to rise in the longer term.

References

1. Bodkhe, U., Tanwar, S., Parekh, K., Khanpara, P., Tyagi, S., Kumar, N., & Alazab, M. (2020). Blockchain for Industry 4.0: A Comprehensive Review. IEEE Access, 8, 79764-79800.

2. Wu, J., Liu, J., Zhao, Y., & Zheng, Z. (2021). Analysis of Cryptocurrency Transactions from A Network Perspective: An overview. Journal of Network and Computer Applications, 190, 103139.

3. List of Registered Digital Asset Exchanges (<https://www.sc.com.my/regulation/guidelines/recognizedmarkets/list-of-registered-digital-asset-exchanges>)

4. Luno Exchange (<https://www.luno.com/en/my>)

5. Nakamoto, S. (2008). Bitcoin: A Peer-To-Peer Electronic Cash System. Decentralized Business Review, 21260.

6. Buterin, V. (2014). A Next-Generation Smart Contract and Decentralized Application Platform. White Paper, 3(37), 2-1.

7. Schwartz, D., Youngs, N., & Britto, A. (2014).

The Ripple Protocol Consensus Algorithm. Ripple Labs Inc White Paper, 5(8), 151.

8. Lite Coin White Paper (<https://whitepaper.io/document/683/litecoin-whitepaper>)

9. Cash, B. (2019). Bitcoin Cash. Development, 2.

10. Ellis, S., Juels, A., & Nazarov, S. (2017). Chainlink: A Decentralized Oracle Network. Retrieved March, 11(2018), 1.

11. Adams, H., Zinsmeister, N., Salem, M., Keefer, R., & Robinson, D. (2021). Uniswap v3 Core. Tech. rep., Uniswap, Tech. Rep.

12. Why We Are Building Cardano (<https://whitepaper.io/document/581/cardano-whitepaper>)

13. Yakovenko, A. (2018). Solana: A New Architecture for a High Performance Blockchain v0. 8.13. Whitepaper.

14. Bach, L. M., Mihaljevic, B., & Zagar, M. (2018, May). Comparative Analysis of Blockchain Consensus Algorithms. In 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) (pp. 1545-1550). IEEE.

15. What is a Proof of Work (PoW) Blockchain? (<https://www.axi.com.au/blog/education/blockchain/proof-of-work>)

16. Blockchain: The Proof of Stake (PoS) (<https://affidaty.io/blog/en/2019/08/blockchain-the-proof-of-stake-pos/>)

17. Delegated Proof of Stake (DPoS) (<https://www.shiksha.com/online-courses/articles/delegated-proof-of-stake-dpos/>)

18. What Is Proof-of-Authority: Staking Credibility Instead of Coins (<https://phemex.com/academy/what-is-proof-of-authority>)

19. Hayes, A. (2015). What Factors Give Cryptocurrencies Their Value: An Empirical Analysis. Available at SSRN 2579445.

20. Sovbetov, Y. (2018). Factors Influencing Cryptocurrency Prices: Evidence from Bitcoin, Ethereum, Dash, Litcoin, and Monero. Journal of Economics and Financial Analysis, 2(2), 1-27.

Current And Future Trends of Cyber Insurance and Ransomware Attacks: An Insight for Cybersecurity Business Opportunity

By | Shaifullah bin Mat Swadi

Introduction

Malaysia recorded over 20,000 cybercrime cases in 2021 with losses amounting to RM560 million (BERNAMA, 2022). With the rise of ransomware attacks, a type of malware that encrypts a victim's files and demands a ransom payment in exchange for decryption, businesses are increasingly looking towards cyber insurance policies to help protect them from the financial losses and reputational damage associated with such attacks. Hence, cyber insurance has become an increasingly popular means for businesses to mitigate the financial risks associated with cyber-attacks via policies that indemnify the cost of incident response services (Daniel & Rainer, 2021). Cyber insurance is also as an important tool to protect organizations against cyberattack-related losses (Aggeliki, Vasiliki, Stefanos, & Costas, 2023). In balancing between mitigation and protection, various factor must be considered to achieve an optimum economic impact to all parties within the cyber insurance ecosystem. However, as ransomware attacks continue to evolve and become more sophisticated, the effectiveness of cyber insurance policies in mitigating the risks associated with these attacks is being called into question. This paper aims to provide an analysis of the current trends in cyber insurance and ransomware attacks, as well as explore the future challenges that businesses and insurers will face in mitigating the risks associated with such attacks.

Review Of Current Cyber Insurance Trends

Increased Demand For Cyber Insurance

As cyber threats become more sophisticated and widespread, organizations are realizing the importance of cyber insurance. The demand for

cyber insurance has been increasing steadily over the past few years. For example, in United States, it was reported that demand for cyber cover jumped from 60% to reach more than 90% during 2021 (Howden, 2021). A surging demand for managing the ransomware attacks as a result of costly data breaches, coupled with the looming threat of state-sponsored large-scale attacks demonstrate that cyber security is not only a key risk trend for companies but also warrants a sustainable risk management approach beyond traditional insurance coverage (Maxwell, 2023). With cyber insurance policies expanding beyond traditional coverage, latest policies are beginning to include new coverage such as business interruption, cyber extortion, and other cyber-related losses.

Collaboration Between Insurers And Cybersecurity Firms

At present, insurers typically pay for a forensic investigation into what caused each compromise, and the findings contributes to a structured database that would empower analytical work in the future (Daniel & Rainer, 2021). This symbiotic partnership paves a trend for insurers to partner with cybersecurity firms to offer their policyholders additional services such as risk assessments, security posture assessment and incident response services. Emerging threats such as ransomware attacks and similar attacks on critical infrastructure are driving further collaboration and innovation in the cyber insurance industry, as insurers seek to enlarge coverage scope for these new risks. The process of seeking insurance coverage requires prospective policyholders to identify and quantify the exposures that they face in order to determine the amount of coverage that they require, a process that can also be beneficial for informing decisions on investments in cyber security (OECD Publishing, 2017). The collaboration process from identification to recovery enables insurers and cyber security firms to attain synergy. This will help further

36

protect policy holders through the dynamic involvement of cyber security controls to manage the escalating threats.

Review On Current Ransomware Attacks

Ransomware attacks continue to be a major threat to organizations of all sizes and across all industries today. Ransomware attacks have also evolved with the rise of remote working and growing reliance on digital infrastructure. Here are some general updates on ransomware attacks.

Increase In Frequency And Severity Of Ransomware Attacks

The COVID-19 pandemic has witnessed a huge surge in the number of ransomware attacks because users globally have been compelled to migrate into the digital realm as an alternative way of doing business. It is reported that ransomware incidents soared by 485 per cent globally in 2020, thus alarming government and businesses that ransomware attacks have become more frequent and severe (Hayes, 2021). Additionally, cybercriminals are constantly exploring different approaches such as social engineering attacks, which includes phishing attacks, to spread ransomware.

Attackers employing more sophisticated tactics and demanding higher ransoms target critical infrastructure such as hospitals, schools, and government agencies, causing significant disruption and financial damage. A research team found that a cohort study suggests that from 2016 to 2021, ransomware attacks on healthcare delivery organizations increased in frequency and sophistication which exposed Confidential Health Information and caused frequent disruption to health care delivery (T. Neprash et al, 2022).

One research team states that the advancement of ransomware attacks have paved the way for the need of harnessing machine learning to detect general behaviour of ransomware. Ransomware is constantly evolving and can change its code signature easily but not its attack pattern (Beaman, Barkworth, David Akande, Hakak, & Khurram Khan, 2021). Such pressure on technological needs sends an alarming signal that ransomware's rapid evolution requires unique balance between mitigation of threat and solution.

Among the many types of ransoms used for cyber-attacks and most widely known and frequently used includes, Petya, Jigsaw, Trolldesh, Ryuk, Bad Rabbit, WannaCry, Locky, REvil and Maze.

Evolution Of Tactics

Attackers are evolving their tactics to evade detection and maximize the impact of their attacks. For example, some attackers are now stealing sensitive data before encrypting it, and then threatening to release the data if ransom is not paid. Research on PoetRAT portray how tactics evolve in a malware variant targeting public and private sector in Azerbaijan.

The research team highlighted that the Azerbaijan public sector and other important organizations targeted by new versions of PoetRAT leveraged malicious Microsoft Word documents allegedly from the Azerbaijan government. The actor evolved by moving from Python to Lua script. In addition, the attackers improved their operational security (OpSec) by replacing protocol and performing reconnaissance on compromised systems (Mercer, Rascagneres, & Venture, 2020).

Among the evolution of tactics is the rise of double extortion where attackers not only encrypt data but also threaten to release it publicly or sell it on the dark web, if the ransom is not paid. This tactic has become increasingly popular among attackers as it gives them an additional source of leverage and potential income.

Apart from that, another research shows how ransomware attackers have changed their tactics by using inductive content analysis. The said research managed to pinpoint a number of emerging key themes namely: (1) ransomware attackers have adopted more sinister tactics and now commit multiple crimes to maximise their return, (2) the expanded attack surface caused by employees working from home has severely aggravated the risk of malicious intrusion, (3) the preferred attack vectors have changed, with phishing and VPN exploits now back to the fore, (4) failure to adapt common business processes from off-line to on-line interaction has created vulnerabilities, (5) the ongoing laissez-faire attitude towards cybersecurity and lack of preparedness continues to be a nagging problem, and (6) ransomware attacks now pose potentially severe consequences for individuals, whose personal data has become a central part of the game (Lang, Yuryna Connolly, Taylor, & J. Corner, 2022).

Discussion

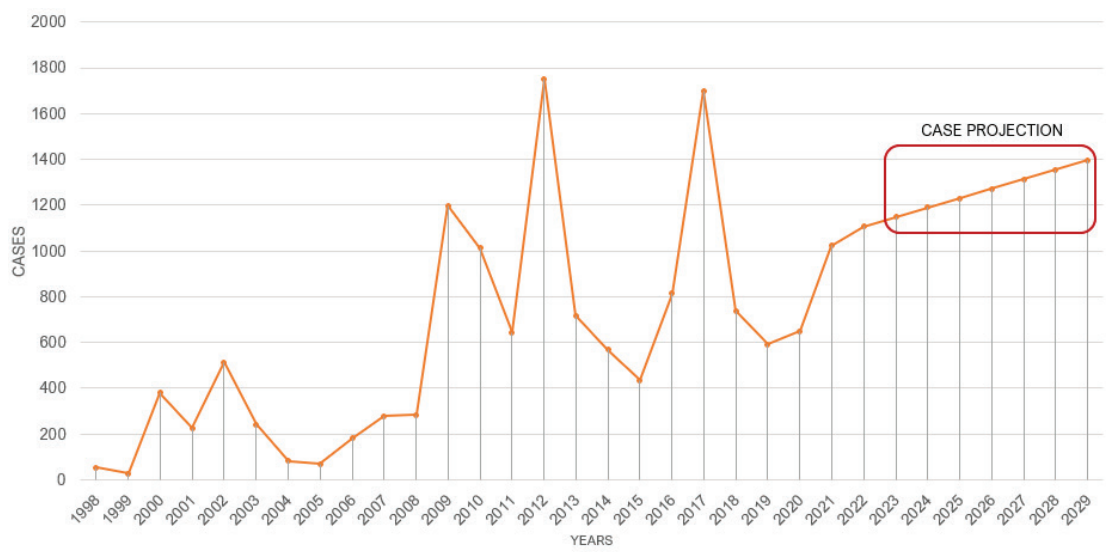


Figure 1: List of Reported Cases to MyCERT and Projection from Year 2023 Cases Onwards

CYBER INSURANCE AND RANSOMWARE ATTACKS GRAPHICAL ASSUMPTION

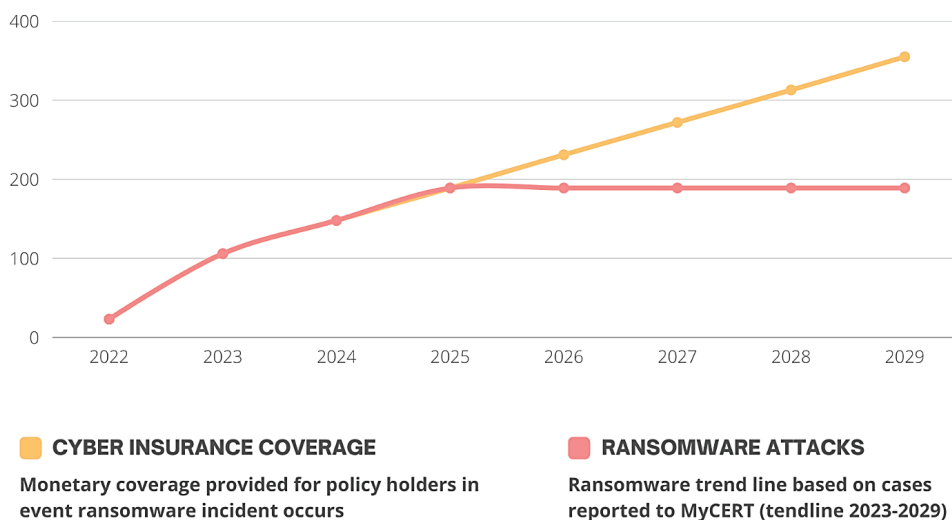


Figure 2: Possible Scenario for Cyber Insurance Model Pressured by Explosion of Ransomware Attacks

One of the pressing challenges faced by cyber insurance is the increasing threat of ransomware attacks that have become more prevalent and sophisticated resulting in significant financial losses for impacted organizations. Figure 1 depicts the reported cases for malware and similar cases to MyCERT from 1998 to January 2023. From the reported cases, a trend line projection is drawn, and the result projects a steady increase in cases from year 2023 onwards until 2029. The upward trend delete indirectly pose threat to the insurance company in supplying cyber insurance solutions.

Figure 2 shows the future challenges that cyber insurance providers may face when dealing with ransomware attacks. The trends line of ransomware attacks shows the growing gap between supply and demand of cyber insurance coverage (assuming the coverage do not change over time). Hence, mitigation works must be introduced to ensure sustainability to the cyber insurance model. Apart from that, additional challenges post further difficulties in providing a balance to the industries, among them are lack of standardized risk assessment to accurately assess the risk of ransomware attacks, increasing ransom demands for larger ransom payments, difficulty in determining payment

liability and policies not covering ransom payments, leaving organizations to foot the bill themselves. Additionally, it can also be challenging to determine whether paying the ransom is the best course of action or if it may actually encourage further attacks.

An Insight For Cybersecurity Business Opportunity

Looking towards the future, cyber insurance is expected to continue to evolve as the threat landscape changes. Insurers are likely to offer more customized policies, with specific coverage for different types of cyber-attacks. Additionally, there may be a move towards

policies that incorporate risk management and preventative measures as standard, rather than optional extras.

For cybersecurity businesses, the rise of ransomware attacks presents an opportunity to offer preventative services such as penetration testing, vulnerability assessments, and employee training. There may also be an opportunity to develop new technologies to detect and prevent ransomware attacks, as well as improve incident response and recovery. As the demand for cybersecurity services continues to grow, businesses that can demonstrate expertise and a track record of success in preventing and mitigating cyber-attacks will be well-positioned to capitalize on the growing market.

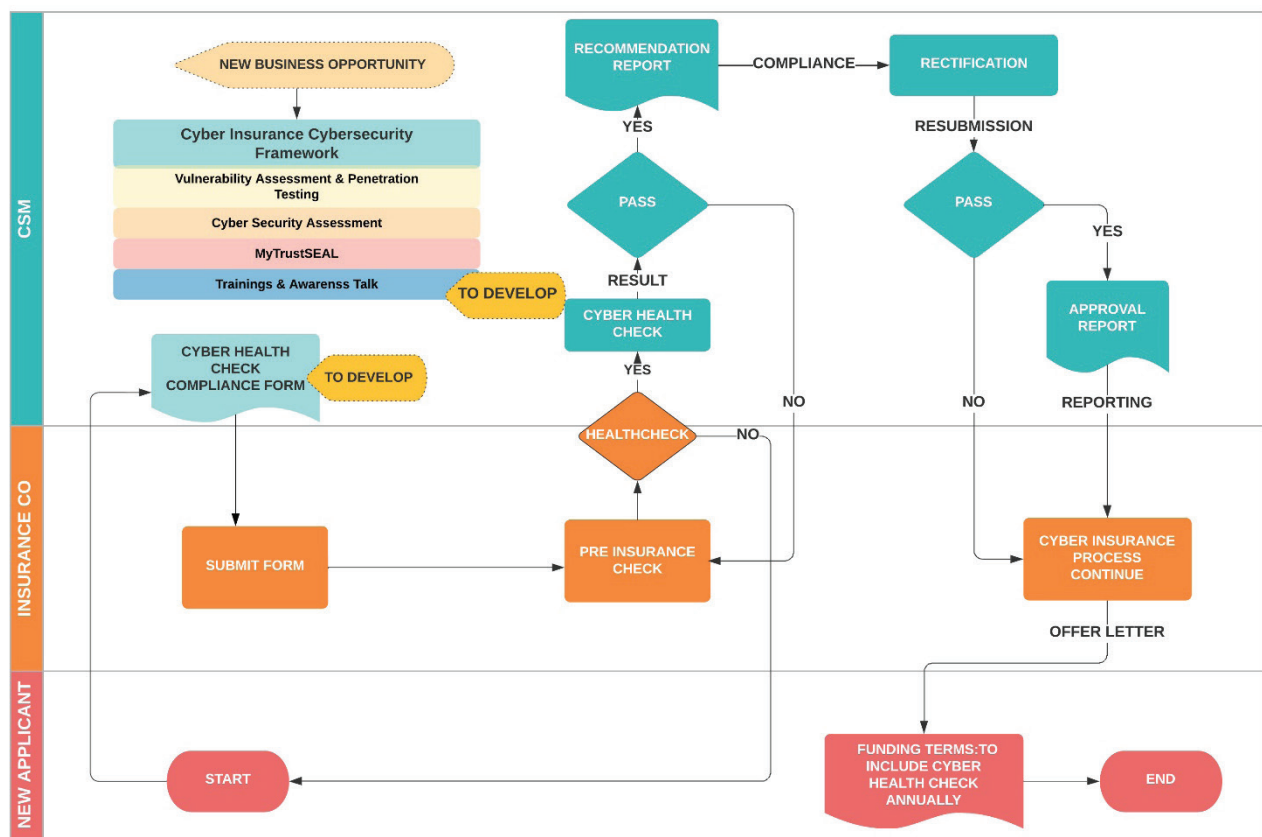


Figure 3 Possible New Business Opportunities

Figure 3 depicts a provisional process flow to prepare companies for cyber insurance enrolment with remediation step introduced early in the process. Such step is vital in ensuring the companies manage the proposed premium price. In short, high risk will yield high premium but would deem infeasible for cyber insurance. The new business opportunities in cyber insurance within the cyber security framework arise where cyber security providers prepare companies to buy insurance policy and close the gap as shown in Figure 2.

Overall, cyber insurance providers must stay ahead of the rapidly evolving threat landscape to ensure that their policies and procedures are effective in mitigating the financial impact of ransomware attacks.

References

1. Aggeliki, T., Vasiliki, D., Stefanos, G., & Costas, L. (2023). Cyber insurance: state of the art, trends and future directions. *International Journal of Information Security*.
2. Beaman, C., Barkworth, A., David Akande, T., Hakak, S., & Khurram Khan, M. (2021). *Ransomware: Recent advances, analysis, challenges and future research directions*. Elsevier, 111.
3. BERNAMA. (2022, 08 11). Malaysia records RM560m loss in cyber crime last year. Retrieved from The Malaysian Reserve: <https://themalaysianreserve.com/2022/08/11/malaysia-records-rm560m-loss-in-cyber-crime-last-year/>
4. Daniel, W., & Rainer, B. (2021). How Cyber Insurance Shapes Incident Response: A Mixed Methods Study.
5. Hayes, K. (2021, July 21). Ransomware attackers on the rampage. `UK.
6. Howden. (2021). Cyber Insurance: A hard reset. Retrieved from Howden Group: https://www.howdengroup.com/sites/g/files/mwfley566/files/inline-files/Howden%20Cyber%20Insurance%20-%20A%20Hard%20Reset%20report_1.pdf
7. Lang, M., Yuryna Connolly, L., Taylor, P., & J. Corner, P. (2022). The Evolving Menace of Ransomware: A Comparative Analysis of Pre-pandemic and Mid-pandemic Attacks. In *Digital Threats: Research and Practice*. Association for Computing Machinery.
8. Maxwell, G. (2023, 2). From cyber to captives: Exploring new ways of looking at risks. Retrieved from Allianz Global Corporate & Specialty: <https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/from-cyber-to-captives.html>
9. Mercer, W., Rascagneres, P., & Venture, V. (2020, October 6). PoetrAT: Malware targeting public and private sector in Azerbaijan evolves. Retrieved from Talos Intelligence: <https://blog.talosintelligence.com/poetrat-update/>
10. OECD Publishing. (2017). Enhancing the Role of Insurance in Cyber Risk Management. Paris. Retrieved from <http://dx.doi.org/10.1787/9789264282148-en>
11. T. Neprash, H. (2022). Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016-2021. Retrieved from <https://jamanetwork.com/journals/jama-health-forum/fullarticle/2799961>

Data Collection for Video Analytics and Its Application

By | Tajul Josalmin bin Tajul Ariffin, Mohammad Azree bin Yahaya, Muhammad Nooraiman bin Noorashid, Nor Salwani binti Ja'afar, Muhamad Zuhairi bin Abdullah & Muhammad Afrizal bin Abd Ghani

Introduction

Data collection for video analytics refers to the process of gathering and organizing large volumes of video data for analysis and interpretation. Video analytics involves the use of advanced algorithms and machine learning techniques to extract meaningful insights from video footage, such as detecting objects, identifying patterns, and recognizing human behavior.

Effective data collection is crucial for the success of video analytics, as it helps ensure that the algorithms and models used for analysis are applied on high-quality data. This involves collecting video footage from a variety of sources, such as surveillance cameras, mobile devices, and social media platforms, and then pre-process the data to remove noise and ensure consistency.

Data collection for video analytics can be challenging, as it often involves dealing with large volumes of unstructured data as well as ensuring that data is collected in a legal and ethical manner. With the right tools and techniques, organizations can leverage video analytics to gain valuable insights and improve their operations in a wide range of domains, including security, marketing, and customer service.

Data aggregation

Data aggregation involves collecting and summarizing data from multiple video sources or individual video frames to extract meaningful insights. This process may involve combining data from various sensors, cameras, or other sources as well as analyzing individual frames or sections of video footage to identify patterns or anomalies. Data aggregation is a crucial part of video analytics, as it enables analysts to extract valuable insights from large volumes of video data, enabling better decision-making and improving business outcomes.

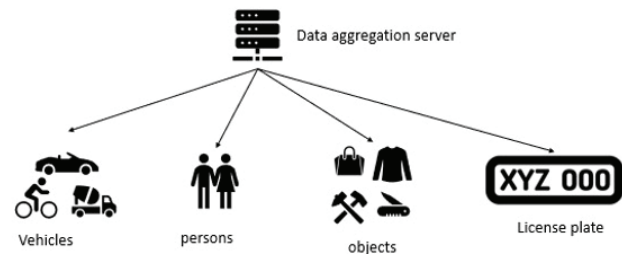


Figure 1. Type of Data

Data collection including vehicle, person, face, object and license plate

Data collection can be done in various ways and for different purposes. For instance, data collection for vehicles can be done using cameras installed in public places, toll booths, traffic signals, and parking lots. These cameras capture images of vehicles and their license plates. While passing through a particular location, the collected data can be used for traffic and parking management, law enforcement, toll collection and other purposes. Personal data can also be collected using cameras or other sensors. These include facial appearance, body measurements, and other biometric data. This data is often used for security purposes, access control, and identification.

Data collection for faces is often done through cameras or other sensors that capture facial features. This data can be used for facial recognition, security purposes, and access control. Data collection for objects can be also done through cameras, sensors, or other means. The collected data which include images, dimensions, and other characteristics of the objects can be used for inventory management, security, and other purposes.

Algorithms used in video analytics

Video analytics is the process of analyzing and interpreting video data to extract useful information, insights, and patterns.

It is a broad field that encompasses several subfields including facial recognition, deep learning, artificial intelligence (AI), person re-identification, object detection, object tracking, optical character recognition (OCR), semantic segmentation and activity recognition. Algorithms play a crucial role in each of these subfields as they enable automated processing of vast amounts of video data in real-time.

Facial recognition is a type of biometric technology that uses algorithms to identify and verify an individual's identity from a digital image or video frame. Facial recognition algorithms use machine learning to detect facial features such as eyes, nose, and mouth and then match them against a database of known faces. Deep learning is a subset of machine learning that uses artificial neural networks to perform complex tasks such as image recognition, speech recognition, and natural language processing. In video analytics, deep learning algorithms are also used to analyze large amounts of video data and extract useful information.

Artificial intelligence (AI) refers to the ability of machines to perform tasks that normally require human intelligence, such as learning, problem-solving, and decision-making. AI algorithms are used in video analytics to identify and classify objects, detect anomalies, and predict events. Deep fakes use artificial intelligence (AI) technique to create realistic and often convincing videos, images, or audio recordings that portray individuals saying or doing things they never actually did. Deep fakes are created using a machine learning technique called generative adversarial networks (GANs). GANs are a type of neural network that operates through two different models: a generator and a discriminator. The generator is responsible for creating the fake content, while the discriminator's job is to distinguish between real and fake content. The process of creating a deep fake usually involves training the GAN on a large dataset of real images or videos of the individual being impersonated. The generator then creates a synthetic image or video of the individual, while the discriminator tries to determine whether it is real or fake. The process is repeated many times until the generator is able to create a convincing deepfake.

Person re-identification is the process of identifying a specific person across different video frames or cameras. Person re-identification algorithms use a combination of facial recognition, body shape analysis, and clothing recognition to match individuals

across different videos. Object detection is the process of identifying and localizing objects within an image or video frame. Object detection algorithms use machine learning to identify objects based on their shape, texture, and colour. Object tracking is the process of following an object's movement over time in a video sequence. Object tracking algorithms use machine learning to track an object's movement across different video frames. Optical character recognition is the process of recognizing text within an image or video frame. OCR algorithms use machine learning to identify and extract text from images and videos.

Semantic segmentation is the process of dividing an image or video frame into different segments and assigning each segment a label. Semantic segmentation algorithms use machine learning to identify objects and classify them into different categories. Activity recognition is the process of identifying and classifying human activities from video data. Activity recognition algorithms use machine learning to identify and classify activities such as walking, running, or sitting.

Applications of Data Collection for Video Analytics in Smart Cities

Data collection is an important tool for smart cities. It can be used to gather insights and make informed decisions about urban planning, public safety, and resource allocation. There are many applications of data collection for video analytics including:

1. **Security:** Enhanced security by detecting suspicious behaviour, identifying unauthorized access, and tracking potential threats. This is particularly useful in high-security areas such as airports, government buildings, and financial institutions.
2. **Traffic Management:** Monitoring traffic patterns, detecting congestion, and identifying accidents or other incidents on roadways. This information can be used to optimize traffic flow, improve safety, and reduce travel times.
3. **Retail Analytics:** Tracking customer behavior, monitoring store layouts, and analyzing product placement. This information can be used to optimize store design, improve customer experience, and increase sales.

4. **Sports Analytics:** Tracking player movements, identifying patterns in gameplay, and providing insights into player performance. This information can be used to optimize team strategies, improve training programs, and enhance fan engagement.
5. **Health Monitoring:** On patient behaviour, detecting falls, and identifying potential health risks. This information can be used to improve patient care, reduce healthcare costs, and enhance patient outcomes.
6. **Manufacturing:** Monitoring production lines, identifying quality issues, and tracking inventory. This information can be used to optimize production processes, reduce waste, and increase efficiency.
7. **Agriculture:** Monitoring crop growth, detecting pests and diseases, and tracking weather patterns. This information can be used to optimize crop yields, reduce the use of pesticides, and improve farm management.
8. **Public safety:** Detecting and responding to criminal activity in real-time. For example, video cameras equipped with facial recognition technology can help law enforcement identify and track suspects.
9. **Environmental monitoring** of air quality and noise pollution. This information can be used to make informed decisions about urban planning and resource allocation.
10. **Pedestrian safety:** Detecting and responding to pedestrian safety issues such as jaywalking and pedestrian accidents. This information can be used to improve pedestrian infrastructure and reduce the risk of accidents.
11. **Emergency response:** Video analytics can also be used to provide real-time information during emergencies, such as natural disasters or terrorist attacks. This information can be used to coordinate emergency response efforts and save lives.

Data collection for video analytics has the potential to revolutionize many industries by providing valuable insights into customer behavior, production processes, and overall performance. It is also a valuable tool for smart cities, as it can help city planners and decision-makers make informed decisions about resource allocation and urban planning. By using video analytics, smart cities can improve public safety, reduce congestion, and promote sustainable development.

Conclusion

Data collection is a crucial aspect of video analytics as it provides the necessary information to train and improve the machine learning models used for video analysis. It is also important to consider data privacy and security when collecting data for video analytics. This may involve obtaining consent from individuals who are being recorded or using encryption techniques to protect sensitive information. Finally, it is essential to have a clear understanding of the data sources, collection protocols, and privacy considerations when gathering data for analysis.

References

1. Regazzoni, C. S., Cavallaro, A., Wu, Y., Konrad, J., & Hampapur, A. (2010). Video Analytics for Surveillance: Theory and Practice [From the Guest Editors. IEEE Signal Processing Magazine, 27(5), 16-17.
2. Zhou, J., & Beyerer, J. (2022). Impacts of Data Anonymization on Semantic Segmentation. 2022 IEEE Intelligent Vehicles Symposium (IV).
3. Alahakoon, D., Nawaratne, R., Xu, Y., De Silva, D., Sivarajah, U., & Gupta, B. (2020). Self-Building Artificial Intelligence and Machine Learning to Empower Big Data Analytics in Smart Cities. Information Systems Frontiers, 25(1), 221-240.
4. Aggarwal, A., Mittal, M., & Battineni, G. (2021). Generative adversarial network: An overview of theory and applications. International Journal of Information Management Data Insights, 1(1), 100004.
5. Zhang, Q., Sun, H., Wu, X., & Zhong, H. (2019). Edge Video Analytics for Public Safety: A Review. Proceedings of the IEEE, 107(8), 1675-1696.
6. Garcia-Salicetti, S. et al. (2003). BIOMET: A Multimodal Person Authentication Database Including Face, Voice, Fingerprint, Hand and Signature Modalities. In: Kittler, J., Nixon, M.S. (eds) Audio- and Video-Based Biometric Person Authentication. AVBPA 2003. Lecture Notes in Computer Science, vol 2688. Springer, Berlin, Heidelberg.
7. O'Gorman, L., Liu, X., Sarker, I., & Milanova, M. (2021). Video Analytics Gait Trend Measurement for Fall Prevention and Health Monitoring. International Conference on Pattern Recognition.

Controlling Data Storage and Interaction Using NTFS Permission Management

By | Muhammad Rasyid Redha bin Mohd Tahir, Sharifah Nurul Asyikin Syed Abdullah, Sarah Khadijah Taylor, Muhammad Iskandar Shah bin Abdul Aziz, Norhafizah binti Hashim & Akmaluraini binti Mohamed Rakof

Introduction

Digital forensics involves interpreting data from digital evidence and extracting related documents to support the hypothesis of a case. In Malaysia, the process of tendering documents requires forensic analysts to print and submit them to the prosecutor. Such procedure consumes time and financial resources. Sometimes several copies need to be printed for submission. In this article, we explore the use of flash drives to store documents that can assist prosecutors. The concern raised by practitioners is on the integrity of the data stored in flash drives, where anyone can modify its content. To solve this, we will propose an approach which controls data storing in flash drives using NTFS permission management. Next, we showcase NTFS permission management on the preparation of flash drive's file system and determine security permission selection. We then test our approach through an experiment method. The result will prove that by using our method, data in the flash drive cannot be edited and thus, enhancing the integrity of stored data for court purposes.

Overview of NTFS and Permission Management

According to Ahsan et al. (2008), a file system stores and manages information on the disks in an organized way to allow efficient retrieval while satisfying the needs of different applications. Recent Windows and Windows Server versions use the core file system NTFS, which offers a wide range of capabilities, including security descriptors, encryption, disc quotas, and rich metadata. It may be used with Cluster Shared Volumes (CSV) to offer constantly accessible volumes that can be accessed simultaneously from many failover cluster nodes. NTFS provides advanced security features such as file and folder level permissions, encryption, and access control lists (ACLs). This allows administrators to set fine-grained permissions to control who can access and modify specific files and folders.

In digital forensics, analysts need to print all extracted documents to submit them to court, which takes up a lot of time and money. They also need paper to make a hard copy of the documents. A significant advantage of NTFS permission management is maintaining document integrity since it cannot be easily altered and edited in a flash drive.

Materials and Preparations

All we need to prepare is:

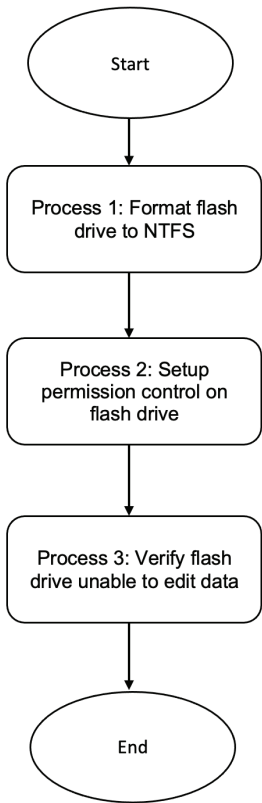
1. A computer with Windows OS (Version 7 upwards)
2. 1 flash drive (pen drive, hard disk or memory card.)

Method

The following is a brief description of the main processes of ensuring the controlled data on the flash drive via NTFS permission management work successfully. There are three key processes to be carried out:

- i. Format flash drive to NTFS,
- ii. Setup permission control on the flash drive,
- iii. Verify that flash drive is uneditable.

Kindly see the processes on the flowchart below:



Flowchart 1: The process on controlling data by NTFS Permission Management

For Process 1, we will show the steps to determine whether the file format of the flash drive is NTFS or not. Next, in Process 2, we will take steps to manage the NTFS permission on the flash drive. And lastly, we will verify all the work is yielding results in Process 3.

Process 1: Format Flash Drive to NTFS File System

Firstly, we need to check whether the flash drive is formatted to NTFS file system. The steps shown in the following table illustrates how Process 1 is done.

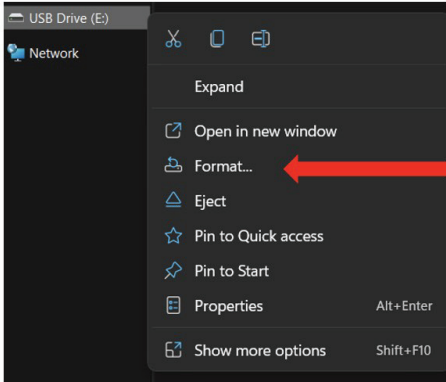
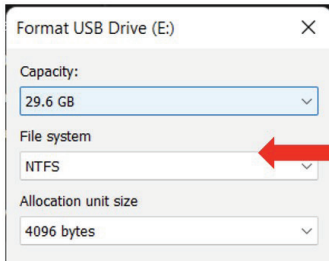
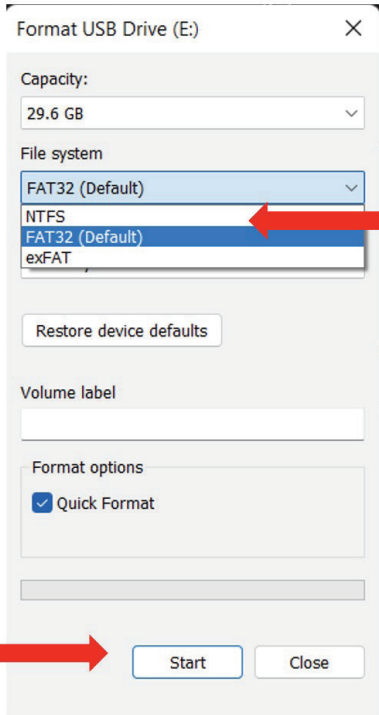
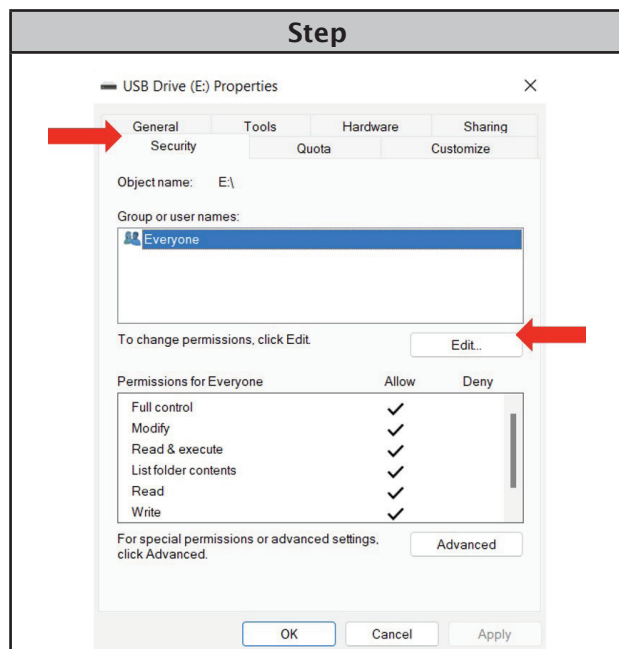
| Step |
|------------------------------------------------------------------------------------------------------------------------------------|
|  |
| At all times follow existing laws, and practice values and exercise the highest moral principles |
|  |
| Check File system on USB drive |
|  |
| If the file system is not on NTFS (FAT32 or exFAT), go to 'File system' list box and select NTFS file system. Then, click 'Start'. |

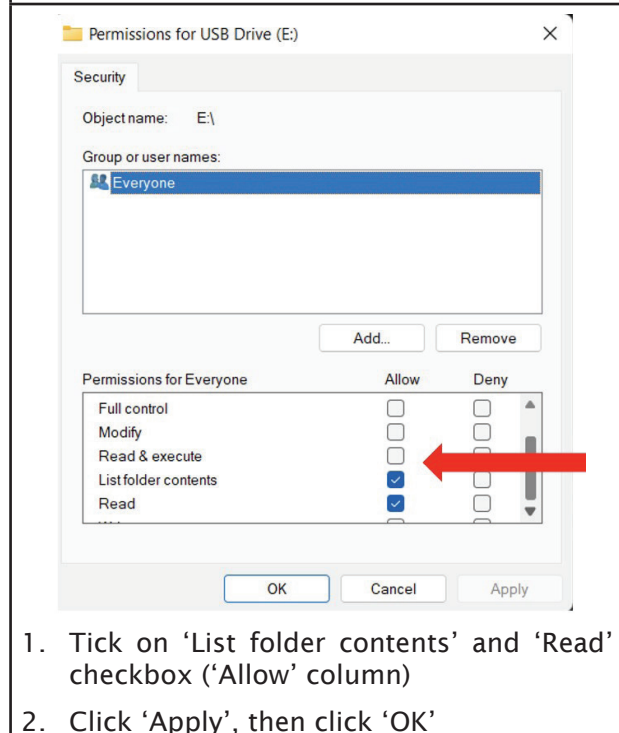
Table 1: The steps in Process 1 - Format Flash Drive to NTFS File System

Process 2: Set up Permission Control on the Flash Drive

Permission restrictions are imposed to disable complete control of data in the flash drive. The primary user takes responsibility for managing and controlling permission.



1. Right click on the flash drive folder. Then, select 'Properties'.
2. Select 'Security'. Then, select 'Edit'



1. Tick on 'List folder contents' and 'Read' checkbox ('Allow' column)
2. Click 'Apply', then click 'OK'

Table 2: The steps for Process 2 - Determination on Permission Selection

Process 3: Verify Data in Flash Drive is Uneditable

Process 3 is to make sure our approach works successfully and the end result is that editing of document is disabled or new document outside of the flash drive cannot be added. This process suggests that once the documents are inserted into the flash drive and permission control applied, restrictions are imposed to disable any control of data in the flash drive.

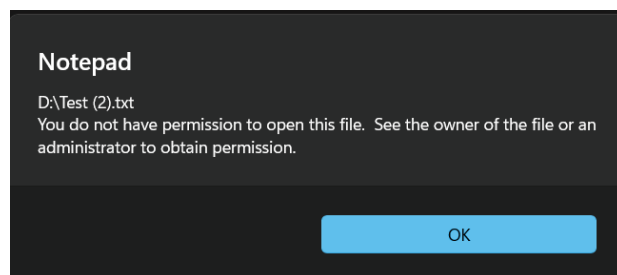


Figure 1: The pop-up shows when we try to edit the document on the flash drive

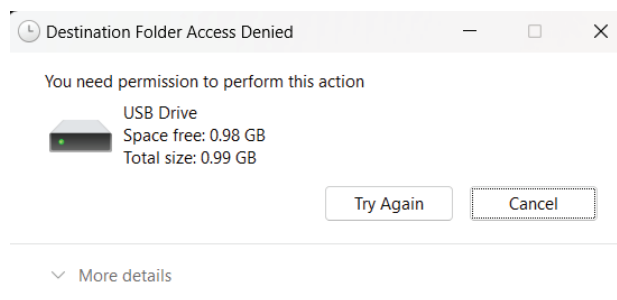


Figure 2: The pop-up message when we try to add an external document

The pictures above show the results when we try to amend the flash drives. In Figure 1, the pop-up message shows when we try to edit and save the documents on the flash drive. The result of the action is that permission has been denied to alter the documents. The same happens in Figure 2, where permission to add another document outside the flash drive is denied.

Remember that only the primary computer can handle a flash drive's permission management. It means the primary computer has complete control over the data in the flash drive. Thus, users are advised to identify the computer that is used for permission management.

Now, we compared our approach with permission management by Diskpart Command Interpreter. The comparison is shown in table 4.

| Step | Diskpart Command Interpreter | NTFS Permission Management |
|-------------------------------------------------------------------|------------------------------|----------------------------|
| Need to change to NTFS? | No | Yes |
| Can the flash drive be set into read-mode only? | Yes | Yes |
| Can the permission management changed be by non-primary computer? | Yes | No |

Table 4: The comparison between Diskpart Command Interpreter and NTFS Permission Management

Conclusion

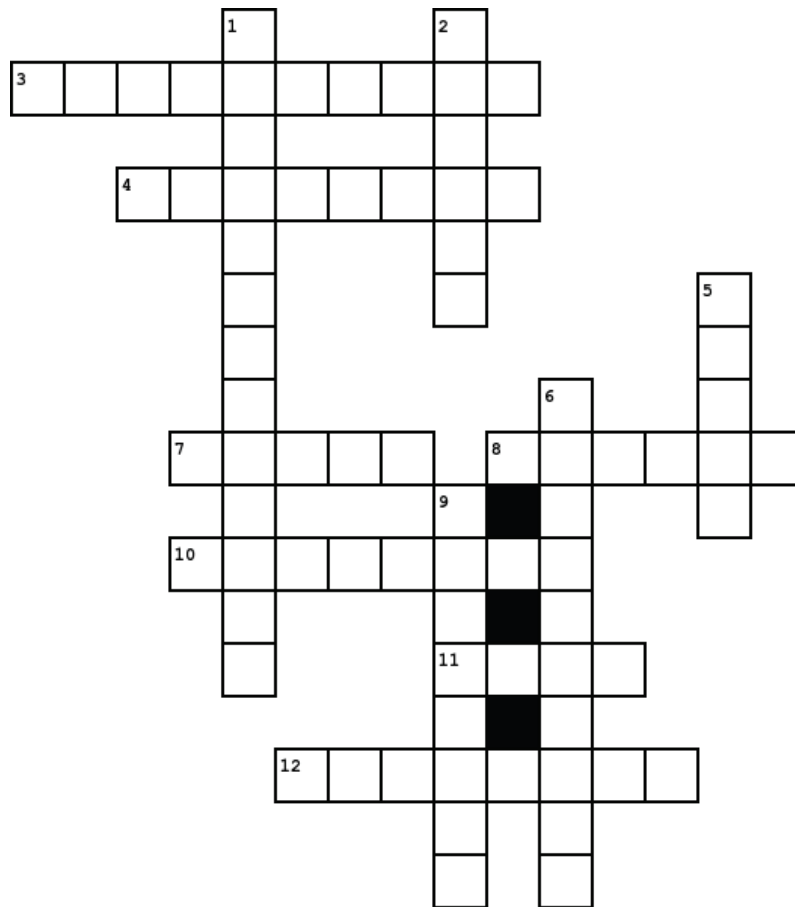
Digital forensics entails analyzing data from digital evidence and identifying pertinent documents to support a case hypothesis. The concern raised by practitioners is on integrity of the data stored in the flash drive, where anyone can possibly modify its content. To address this, we proposed an approach that controls data stored in flash drives using NTFS permission management. We showed processes on NTFS permission management including preparing the flash drive's file system, determining security permission selection and verifying whether the approach is successful. We then tested our approach using an experimental method. The result showed that by using our method, data in the flash drive cannot be edited and hence, increasing the integrity of the stored data for court purposes.

References

1. Ahsan, F., Lali, M. I., Ahmad, I., Ishaq, A., & Mohsin, S. (2008). Exploring the effect of directory depth on file access for FAT and NTFS file systems. *ISTASC*, 8, 130-135.
2. Rusbarsky, K. L., & City, K. (2012). A forensic comparison of NTFS and FAT32 file systems. *Marshall Univ*, 29.
3. Setting NTFS permissions. Setting NTFS Permissions - NTFS.com. (n.d.). Retrieved Feb 13, 2023, from <https://www.ntfs.com/ntfs-permissions-setting.htm>

Cybersecurity Crossword Puzzle

By | Yuzida Yazid



Across

3. The process of encoding sensitive data, so it can't be hacked and viewed by people or computers that it isn't intended for.
4. Video in which faces have been either swapped or digitally altered, with the help of AI.
7. The place files can be saved, so they can be accessed anywhere rather than just on one device.
8. To make a copy of data stored on a computer or server to reduce the potential impact of failure or loss
10. A type of software that defends your computer against viruses and malware. It acts as a protective shield when you're online.
11. Fraudulent business or scheme that takes money or other goods from an unsuspecting person.
12. When a hacker changes the IP address of an email so that it seems to come from a trusted source.

Down

1. A form of harassment that happens on the internet, usually through social media platforms.
2. Small files that are stored on a user's computer to help a website to recognize you and keep track of your preferences.
5. A dangerous file that can infect a computer when downloaded. It can cause harm to the computer and even steal data.
6. When someone who lacks the proper authentication follows an employee into a restricted area.
9. A string of letters, numbers and symbols that you use to access your online account.

deepfake · encryption · firewall · password
 backup · cloud · cookie · cyberbullying ·
 phishing · spoofing · scam · virus

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

Customer Service Hotline: 1 300 88 2999

www.cybersecurity.my

-  CyberSecurityMalaysia
-  cybersecuritymy
-  cybersecuritymy
-  CyberSecurity Malaysia
-  cybersecurity_my

© CyberSecurity Malaysia 2024 – All Rights Reserved



MINISTRY OF DIGITAL

ISSN 1985-1995

