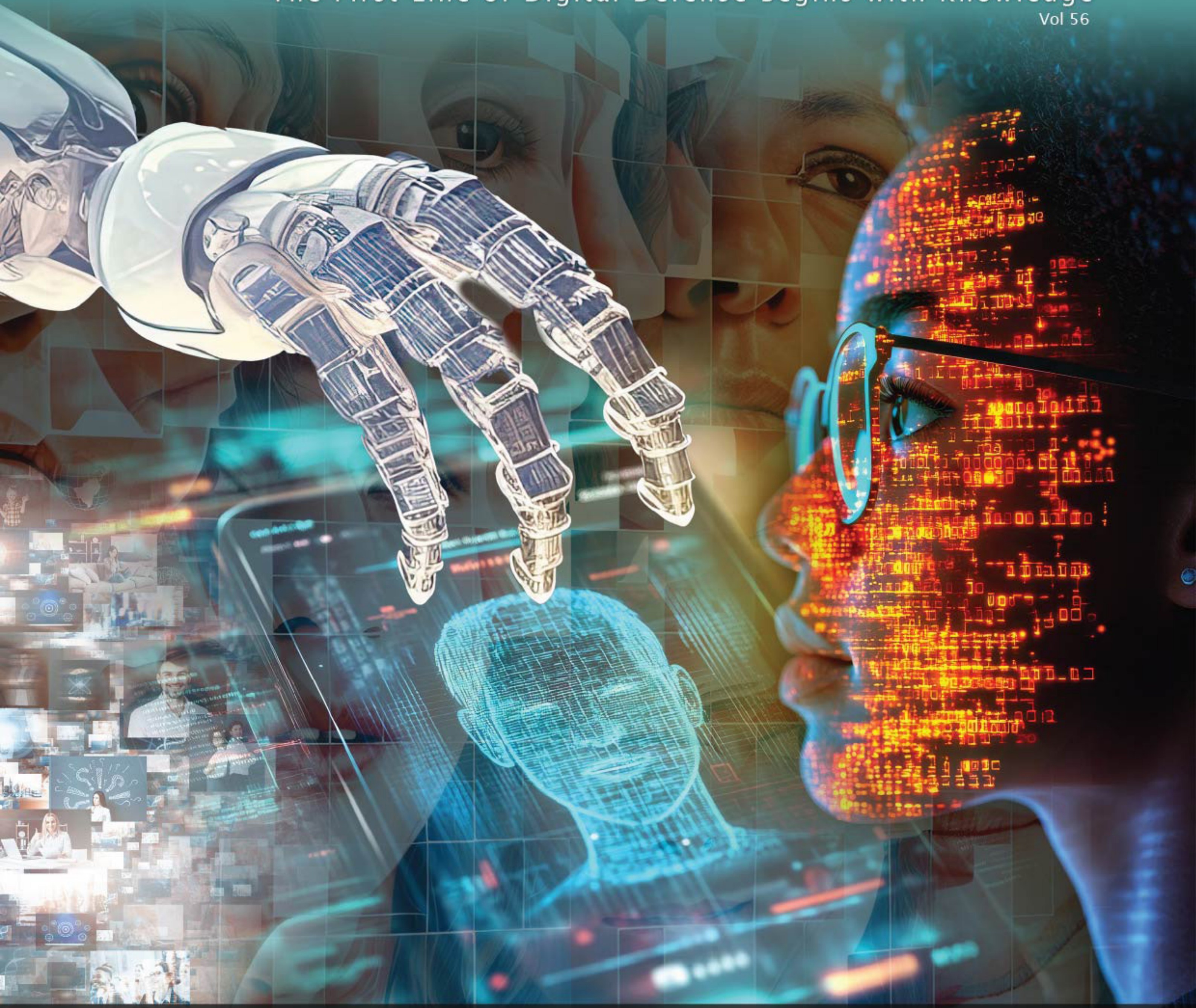
CyberSecurity MALAYSIA

www.cybersecurity.my

eSecurity

The First Line of Digital Defense Begins with Knowledge

Vol 56



Artificial Intelligence (AI) : The Helper or the Threat?

Machines On the Move: How AI And Automation Are Transforming Careers

Do's and Don'ts of Facial Recognition

"Cybersecurity is the backbone of digital transformation." ~ Satya Nadella

ISSN 1985-1995

MINISTRY OF DIGITAL

CyberSecurity MALAYSIA

CYBER RESILIENCE *for a* SAFER TOMORROW

At CyberSecurity Malaysia, safeguarding the nation's digital landscape is our top priority. As the national cybersecurity specialist and technical agency, we are committed to strengthening Malaysia's cyber resilience through innovative security solutions, expert services, and capacity-building initiatives.

Our approach is built on five core pillars:

- Cyber Security Responsive Services
- Cyber Security Proactive Services
- Outreach & Capacity Building
- Strategic Study & Engagement
- Industry & Research Development

Together, we uphold Digital Trust - *ensuring a safe, secure, and resilient cyberspace for all.*

By integrating People, Process, and Technology, we champion a sustainable and fortified digital infrastructure for the nation's future.

CyberSecurityMalaysia
cybersecuritymy
cybersecuritymy
CyberSecurity Malaysia
cybersecurity_my
cybersecuritymy

CyberSecurity Malaysia
200601006881 (726630-U)

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

T: +603 - 8800 7999 | **F:** +603 - 8008 7000
enquiry@cybersecurity.my | www.cybersecurity.my

Customer Service Hotline: 1 300 88 2999

SECURING OUR CYBERSPACE

DIGITECH BESTBRANDS AWARDS 23
CERTIFIED TO ISO/IEC 27001:2013
CERT. NO.: ISMS 00114
ACB 021
SAMM 456
MSC MALAYSIA Status Company
WSIS PRIZES 2020 WINNER www.wsis.org
THE MALAYSIA BOOK of RECORDS
Recognition of Excellence 2023 CyberSAFE by OpenGov

WELCOME MESSAGE FROM THE CEO OF CYBERSECURITY MALAYSIA

Dear Esteemed Readers,

In an era where the digital and physical worlds are becoming increasingly intertwined, the need for vigilance, innovation, and awareness in cybersecurity has never been more critical. Every click, connection, and communication carries both opportunity and risk, and it is our shared responsibility to ensure that technology continues to empower rather than endanger us.

This edition of the e-Security Bulletin brings together a compelling collection of insights that illuminate today's most pressing cybersecurity challenges and emerging frontiers. From Zero-Click Attacks and Endpoint Security to the evolving landscape of Artificial Intelligence and Post-Quantum Cryptography, each article reinforces a simple truth, the digital world demands continuous learning, adaptation, and collaboration.

As we explore topics such as Open RAN, data breach response, facial recognition ethics, and AI-driven automation, one common theme emerges: security is not merely a technical pursuit but a human one. Behind every innovation and every breach are people - creators, defenders, and users - whose actions shape the security posture of our digital ecosystem.

At CyberSecurity Malaysia, we remain steadfast in our mission to safeguard the nation's cyberspace, strengthen cyber resilience, and foster a culture of digital responsibility. Through platforms such as this bulletin, we aim to empower professionals, researchers, and citizens alike with the knowledge and foresight needed to navigate the evolving cyber landscape with confidence.

Let us continue to learn, adapt, and collaborate - ensuring that as technology advances, so too does our collective security.

Thank you for reading.

Be Smart, Be Cybersafe.

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

EDITORIAL BOARD

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

TABLE OF CONTENTS

Zero-Click Attacks: The Silent Threat Lurking In The Shadows

By | Dania Syahirah Zakry, Fatin Nabila Mohd Anuar, Siti Nur Fatihah Nor Azman

In the ever-evolving cybersecurity landscape with constantly adapting threats, the advent of "zero-click attacks" signifies a fundamental shift in the strategies used by malicious actors to penetrate and compromise digital ecosystems. Zero-click attacks function covertly by exploiting flaws in software, protocols, or infrastructure to launch covert intrusions without requiring user contact, in contrast to standard cyberattacks requiring human interaction or engagement. This article explores the complexities of zero-click attacks, elucidating their attack mechanisms, ramifications, and the corresponding proactive defence strategies.

Understanding Zero-Click Attacks

Zero-click attacks, as the name implies, require no user engagement for execution. Zero-click attacks utilise advanced methods and complex chains of exploits to exploit weaknesses in software programs, operating systems, or communication protocols. These types of attacks involve seamless and covert penetration. Exploiting these weaknesses enables malicious actors to execute harmful actions, including deploying malicious payloads, stealing confidential information, or establishing long-term access to targeted systems without leaving any evidence or raising any suspicion.

Zero-Click Attack in the News

There were reports of zero-click attacks in 2021, targeting iPhones through iMessage known as “Project Raven”. This project was UAE’s offensive cyber operations unit, comprising Emirati security officials and former US intelligence operators working as contractors. Reportedly, they used a tool known as Karma to take advantage of a flaw in iMessage. Karma used specially crafted text messages to hack into iPhones of activists, diplomats, and rival foreign leaders to obtain photos, emails, text messages, and location information.

In addition, a security incident was detected in 2019 involving a WhatsApp breach. This well-known breach was caused by a missed call, which took advantage of a vulnerability in the source code framework of WhatsApp. An undisclosed vulnerability in the system enabled the attacker to inject spyware into the data transmitted between two devices following an unanswered call. Once installed, the spyware is seamlessly integrated into the device's software framework, operating discreetly in the background.

Mechanisms and Variants

There is a wide range of techniques and methods used in zero-click attacks, each one designed to take advantage of a different weakness or vulnerability in the target setting. Key variations are:

1. **Remote Code Execution (RCE):** Remote Code Execution (RCE) is a a form of cyber-attack targeting critical cybersecurity vulnerability that allows an attacker to remotely execute any code on a target system or application, without requiring physical access to the device. These vulnerabilities frequently arise from deficiencies in software design, faults in implementation, or neglect in validating user input, which can be exploited by attackers to bypass security systems and remotely execute malicious code. RCE attacks pose a significant threat as attackers gain illicit authority over the targeted system, enabling them to carry out orders, execute malicious software, pilfer data, or even gain complete dominion over the device.
2. **Malicious Data Parsing:** Parsing refers to the procedure of analysing and interpreting structured or unstructured data based on a predetermined format or syntax. Harmful or malicious information parsing involves exploiting weaknesses in software or systems that analyse and interpret incoming data to carry out destructive operations or gain unauthorised access. Attackers use vulnerabilities in the parsing logic or implementation of

software applications to change data, causing security breaches, data corruption, or unauthorised execution of code.

In the realm of messaging apps or email clients, a zero-click attack could be executed by sending a meticulously designed message. Once the application receives and processes the message, a vulnerability is triggered, all without the user needing to open the message or interact with any links or attachments. This has the potential of trigering malicious code execution, data theft or device takeover.

3. **Wireless Exploitation:** Zero-click attacks can also target wireless communication protocols, like Bluetooth, Wi-Fi, or Near Field Communication (NFC). By exploiting vulnerabilities in these protocols, without requiring any physical or network contact from the victim. These protocols enable the transmission of data between devices without the use of physical wires, which offers convenience but also exposes them to potential exploitation if not well protected.

   For instance, BlueBorne is a notorious example of a zero-click assault that specifically targets Bluetooth devices. Discovered in 2017, BlueBorne comprised a range of weaknesses that impacted the Bluetooth systems in different devices, such as smartphones, laptops, and IoT devices. These vulnerabilities let malicious actors gain control of devices remotely without any user involvement, by merely being within the range of Bluetooth connectivity. These vulnerabilities presented a substantial threat to countless devices globally, since malicious actors could leverage them to propagate malware, steal data, or mount further attacks.

Ramifications of Zero-Click Attacks

The consequences of zero-click attack go beyond simple data breaches or system compromises and hold significant implications for individuals, organisations, and the wider digital ecosystem. Some notable consequences include:

1. **Data compromise and exfiltration:** Data compromise and exfiltration in zero-click attacks involve the illicit acquisition and extraction of sensitive or valuable data from a targeted system or network without any user engagement. During these attacks, assailants take advantage of weaknesses in software, systems, or networks to acquire data by removing and subsequently extracting it from the compromised system and transmitting it to their own servers or storage places.

   In a zero-click attack scenario, data breach and exfiltration can occur surreptitiously and autonomously, without the victim's knowledge.

2. **Disruption of critical infrastructure:** It refers to the intentional disruption or damage to essential systems and networks that are necessary for the proper operation of society, the economy, and national security. Critical infrastructure covers many industries, including energy, transportation, telecommunications, healthcare, finance, and government services. Zero-click attacks ‘zero’ in on industrial control systems or government networks with existential threats that could cause service interruptions, physical harm or, in extreme situations, even the loss of life.

   Zero-click assaults present substantial concerns for national security. It has the potential of eroding public trust, disrupting the government functions, and jeopardising classified material about the military, intelligence, and national security.

3. **Erosion of trust and confidence:** The erosion of trust and confidence is the process by which individuals, consumers, or entities gradually or suddenly lose their belief or trust on a person, organisation, product, service, or system. It happens when acts, events, or circumstances weaken the perceived trustworthiness, integrity, or ability of the subject in question.

   Zero-click attacks can undermine the trust that businesses and organisations have in their capacity to safeguard sensitive data and uphold the privacy of their users or customers. These consequences can greatly impact customer loyalty, brand reputation, and eventually, financial viability. In addition, regulatory scrutiny and enforcement actions may be triggered by the loss of trust and confidence resulting from zero-click assaults. Businesses and organisations can incur fines or other penalties if they fail to sufficiently safeguard customer data or violate privacy legislation.

Proactive Defense Strategies

To reduce the danger of zero-click attacks, it is necessary to adopt a holistic and comprehensive approach that includes proactive defence techniques, strong security controls, and constant awareness of new threats. Essential strategies for reducing or preventing negative impacts include:

1. **Continuous monitoring and threat intelligence:** Continuous monitoring and threat intelligence are essential for minimising zero-click attacks by offering proactive defence mechanisms and valuable insights into new threats.

   Constant monitoring and examination of system activity, network traffic, and user behaviour could identify irregularities or unusual patterns that may indicate a zero-click assault. Continuous monitoring systems utilise several approaches, including log analysis, network traffic analysis, endpoint detection and response (EDR), and security information and event management (SIEM), to quickly detect potential threats. Such constant surveillance could mitigate potential damage by zero-click attacks.

   Threat intelligence process encompasses gathering, examining, and distributing data on cybersecurity risks and weaknesses. In this context, threat intelligence plays a crucial role in keeping organisations updated on the most recent attack methods, different types of malware, ways to exploit vulnerabilities, and the individuals or groups responsible for harmful activities targeting their systems. Threat intelligence is gathered through exclusive research, industry publications, threat feeds, open-source intelligence (OSINT), and collaborative collaborations with relevant organisations and security communities.

2. **Vulnerability management:** Employ comprehensive vulnerability management practices to identify, prioritise, and remediate software vulnerabilities, thus reducing the attack surface and mitigating the risk of zero-click exploitation. This involves continuously monitoring and scanning systems, applications, and networks for potential vulnerabilities. Vulnerabilities stem from software bugs, misconfigurations, outdated software versions, or design flaws.

   Addressing vulnerabilities through timely patching reduces the attack surface and minimises the risk of exploitation. Once specific vulnerabilities have been identified, we need to assess their potential impact and likelihood for exploitation. Prioritisation takes into account vulnerability, severity, exploitability, and the importance of the affected systems.

   Therefore, it is a perpetual process that requires continuous monitoring and remediation to ensure that systems remain secure against zero-click attacks.

3. **User education and awareness:** User education and awareness are critical components of zero-click attack mitigation strategies. Providing users with information on the most effective computer safety methods from regularly updating software and systems, using strong and unique passwords, enabling multi-factor authentication (MFA) to avoiding interactions with suspicious links or unknown attachments, can significantly decrease the chances of becoming a target of zero-click attacks.

   Promoting a culture of cybersecurity consciousness and accountability inside an organisation motivates employees to prioritise security in their day-to-day tasks and actively contribute to safeguarding critical data and systems. In this regard, effective leadership is essential to establish a security-conscious culture by providing support and reinforcing security policies and procedures.

   By investing in user education and awareness initiatives, organizations can empower their employees to become active participants in the defense against zero-click attacks, thereby strengthening the overall security posture of the organization.

Conclusion

Zero-click attacks pose a significant and widespread risk to cybersecurity through exploitation of weaknesses in software, protocols as well as infrastructure and intrusions to systems without any user involvement or notification. As attackers constantly evolve their methods and approaches, it is crucial that organisations prioritise defensive strategies that are proactive, innovative to counter zero-click attacks effectively. By fostering collaboration, investing in robust security frameworks, and embracing a proactive security posture, individuals, organizations, and the cybersecurity community at large can successfully mitigate the invisible threat posed by zero-click attacks, safeguarding digital integrity and preserving trust in the digital ecosystem.

References

1. https://ensarseker1.medium.com/the-art-of-deception-understanding-zero-click-attacks-8bb33bbe4239

2. https://www.cpomagazine.com/cyber-security/new-pegasus-spyware-zero-click-patched-out-by-apple-in-ongoing-battle-against-commercial-zero-days/

3. https://edition.cnn.com/2019/05/14/tech/whatsapp-attack/index.html

4. https://clario.co/blog/zero-click-exploit/

5. https://thesecuritycompany.com/the-insider/zero-click-attacks-everything-you-need-to-know/

6. https://journals.ekb.eg/article_245413.html

The Next Generation Radio Access Network: Concept and Benefits of Open RAN

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

Overview

The Radio Access Network (RAN) provides an advancement in mobile network technology to connect users, including mobile phones or enterprises to the mobile network over radio waves from the base station to the upstream. RAN also acts as a bridge to access all the key applications over the Internet. Previously, RAN technology was used as a hardware and software-integrated platform in the telecommunication industry to process radio wave frequency.

Introduction

Mobile network communication is one of the emerging technologies for the current digital economy as well as the national critical infrastructure-based services. The number of users and services increases rapidly every year. However, radio spectrum is a limited resource and needs to be re-farmed to handle the proliferation of users and services. Consequently, the management and orchestration of radio resources or Radio Access Networks (RAN) evolves over each mobile generation, as both 2G and 3G use conventional methods such as inter-RAN controllers to allocate user equipment and its resources. The RAN technology experiences several technological advancement in 4G when it introduces a new interface of intra-x2 to support base station communication between core network to handle RAN resource allocation. However, the RAN architecture for existing networks is still based on monolithic building blocks while the equipment still comprises proprietary vendor-specific devices such as baseband units (BBU), radio units (RU), and antennas. Nevertheless, because many operators are able to develop unique RAN equipment, this strategy results in the renowned vendor lock-in RAN. As a result, MNOs (Mobile Network Operators) can no longer purchase mix-and-match services from RAN vendors or Network Equipment Providers (NEP).

Open RAN represents a Next Generation (NG) standard for RAN previously used for 3G and 4G technology. Open RAN defines inter-faces that support inter-operation for fronthaul between equipment and offer network flexibility at a lower cost. It integrates the advancements of network softwarization, virtualization and Artificial Intelligence (AI) to enhance the operation of RAN devices and operations. Open RAN offers new possibilities for different Network Equipment Providers (NEP) to develop their RAN solution in an open ecosystem. However, Open RAN does bring about new security and privacy challenges. This new architecture offers an entirely different RAN configuration than what existed previously, leading to severe security and privacy issues if mismanaged. Therefore, Mobile Network Operators (MNO) are taking a cautious approach in deploying Open RAN.

Concept

Open RAN heralds an exciting RAN concept, a current technology mechanism that applies to 5G network architecture. Open RAN promotes transparency and adds intelligence for RAN network elements that addresses the limitations of traditional RAN technology. These transparency features enable new players to access the RAN market with their customized products and services, while the intelligence features enhance automation and performance by optimizing the RAN elements and network resources. As a result, Mobile Network Operator (MNOs) have wider choices in RAN solutions globally. Furthermore, 5G deployment can make the operation of cellular networks less expensive and result in faster innovation of features and services, as the mechanism offers more flexibility to the network operators with many elements and intelligence.

Open Radio Access Networks (Open RAN) is a disaggregated approach in deploying mobile networks using open and interoperable protocols and interfaces, allowing for increased flexibility over traditional RAN systems. Open RAN can be implemented with vendor-neutral hardware and software-defined technology based on open interfaces and industry-developed standards.
Being a new architecture, Open RAN represents

an ongoing shift in mobile network architecture that allows networks to be built using subcomponents such as Remote Radio Unit (RRU) or Baseband Unit (BBU) from a variety of vendors (NEP).

Open RAN Architecture

Open RAN decouples hardware and software bonds in proprietary RAN equipment. This feature allows MNOs more flexibility for RAN solutions to deploy and upgrade their RAN segment based on their market plans. Such open architecture attains three key objectives:

i. **Open internal RAN interfaces**
This new interface supports various Open RAN interfaces, including interfaces defined by 3GPP.

ii. **Cloudification**
The objective is to support cloud-native RAN functions via disaggregated hardware and software components.

iii. **Intelligence and Automation**
The objective is to utilize advanced AI or ML capabilities to enable automated management and orchestration in RAN.

RAN in Open RAN architecture is disaggregated into four main building blocks. The former Baseband Unit (BBU) previously used for traditional RAN is now disaggregated into Distributed Unit (DU) and Centralized Unit (CU).

i. The Radio Unit (RU), previously known as RRU, is where the radio frequency signal is transmitted, received, amplified, and digitized before the controller. The RU is located near or integrated into the antenna with dedicated equipment for the standalone base station.

ii. The Distributed Unit (DU) is where real-time, baseband processing function resides. The DU can be centralized or located near the base station with dedicated equipment for the standalone base station.

iii. The Centralized Unit (CU) is where the less time-sensitive packet processing function typically resides with dedicated equipment for many base stations.

iv. RAN Intelligent Control (RIC) enables Open RAN to perform real-time optimization of functions and resources through data collected from the front haul (end users) and backhaul (Network Core). RIC is part of Multi Edge Computing (MEC)

Benefits of an Open RAN

i. Cost saving

Operators can build and containerize a virtualized network with each element capable of being completely broken down. This modern network can support millions of subscribers, depending on how many instances and substations of the VNFs can be run on a single platform.

ii. Multiple Operators and network sharing

Open RAN can run multiple operators using multiple VNFs concurrently on the same platform over segregated networks. The other benefit is network sharing in the future through software.

iii. Eliminate vendor lock-in

Open-RAN frees up the interface between remote radio and baseband units. Hence, operators can use multiple equipment from different vendors based on their requirements.

iv. Security

Open RAN enables operators to command full visibility and control of their network's end-to-end security. Open RAN interfaces, defined in the O-RAN technical specifications, provide enhanced independent visibility leading to a more secure system. Since the O-RAN alliance builds on 3GPP's 5G NR architecture, it benefits from 3GPP's advanced security features customised for 5G.

v. 3rd Party Testing

Open RAN will work with multiple vendors between baseband units and remote radio units defined 3GPP interface specification as every element can be independently tested. The equipment could be tested independently by a 3rd party. As a result, the radio can be produced at a lower cost and not tied to any specific system integrator.

Challenges and Considerations

While 5G Open RAN offers numerous opportunities and advantages, it also faces several challenges that need to be addressed to ensure successful deployment and widespread adoption. Some of the key challenges include:

i. **Interoperability:** Seamless interoperability between hardware and software components from different vendors is crucial for the success of Open RAN. Standardizing interfaces and protocols are essential to enable plug-and-play compatibility and avoid integration issues.

ii. **Performance and Scalability:** Open RAN architectures must deliver performance and scalability comparable to traditional RAN solutions. Optimizing network performance, especially in dense urban environments and high-traffic areas, while maintaining low latency and high throughput, remains a significant challenge.

iii. **Security:** Securing Open RAN networks against cyber threats and vulnerabilities is paramount. The disaggregated nature of Open RAN introduces additional attack surfaces, requiring robust security measures to protect network infrastructure, user data, and critical services.

iv. **Vendor Ecosystem:** Building a diverse and competitive vendor ecosystem is essential to drive innovation and prevent vendor lock-in. Encouraging new entrants and ensuring a level playing field for smaller vendors can be challenging in a market dominated by established players.

v. **Cost and Investment:** While Open RAN promises cost savings through hardware commoditization and vendor competition, initial deployment costs and ongoing operational expenses can still be significant. Operators need to carefully assess the total cost of ownership (TCO) and return on investment (ROI) when transitioning to Open RAN.

vi. **Integration Complexity:** Integrating components from multiple vendors and managing heterogeneous networks can be complex and resource intensive. Operators require robust management and orchestration tools to streamline deployment, configuration, and maintenance processes.

vii. **Regulatory and Policy Considerations:** Regulatory frameworks and government policies play a crucial role in shaping the adoption of Open RAN. Clear guidelines and incentives promoting open standards, interoperability and vendor diversity can accelerate deployment and foster innovation.

viii. **Skills and Expertise:** Building and maintaining expertise in Open RAN technologies and architectures are essential for operators and network engineers. Training programs and educational initiatives help bridge the skills gap and ensure a smooth transition to Open RAN.

Addressing the above challenges require collaboration and cooperation among industry stakeholders, including operators, vendors, regulators, and standards bodies. By overcoming these hurdles, 5G Open RAN holds the potential of revolutionizing mobile networks, driving innovation, and delivering enhanced connectivity and services to users worldwide.

User Case of 5G Open RAN implementation in real-world

Rakuten Mobile's 5G Open RAN Deployment in Japan serves as an exemplary case study in the telecommunications industry. By implementing an Open RAN architecture, Rakuten Mobile disrupted the traditional telecommunications model, offering innovative services at competitive prices; while fostering vendor diversity and interoperability. This initiative has garnered significant attention globally and has the potential to influence the future direction of telecommunications networks worldwide. Rakuten Mobile's 5G network was built on a disaggregated Open RAN architecture, comprising open interfaces and interoperable hardware and software components from multiple vendors. The approach allowed Rakuten Mobile to avoid vendor lock-in, drive innovation, and optimize network performance. Rakuten Mobile adopted a phased approach in deploying its 5G network, starting with major cities like Tokyo, Osaka, and Nagoya before expanding to rural areas. The company leveraged existing infrastructure such as rooftop sites and fiber optic backhaul, to accelerate deployment and minimize costs.

Rakuten Mobile was able to offer a range of innovative 5G services powered by its Open RAN network. These include enhanced mobile broadband (eMBB) for high-speed internet access, ultra-reliable low-latency communications (URLLC) for mission-critical applications, and massive IoT deployments for smart city initiatives and industrial automation. Rakuten Mobile continuously monitored and optimized its 5G Open RAN network to ensure optimal performance, reliability, and security. The company leveraged network analytics, artificial intelligence (AI), and machine learning (ML) algorithms to identify and address issues proactively. Rakuten Mobile's 5G Open RAN deployment serves as a model for future telecommunications networks worldwide. The company plans to expand its network coverage and capacity, introduce new services and use cases, and collaborate with partners to drive innovation and digital transformation.

Conclusion

For technical purposes, Mobile Network Operators (MNO) look to disaggregating this fronthaul of telecommunication part as such approach can increase their network agility and flexibility, increase innovation with multiple scenarios deployment based on their market area and cost savings. Contrasting this to the traditional RAN mechanism where, the Network Equipment Provider (NEP) has ‘full access monopoly’ to the entire telecommunication system for mobile operators. However, with the introduction of Open RAN, mobile operators can now choose from various options or mechanisms for their best practices. Additionally, Open RAN offers multiple RAN solutions and elements that allow network operators to be more open and flexible.

Reference

1. O.-R.S.F.G.S.O-RanAlliance,O-RANSecurityThreatModelingand Remediation Analysis, O-RAN.WG1.SFG.Threat-Model-v01.00, Tech- nical specifications (2021) 57 pages.

2. Altiostar, Security in Open RAN, White paper (2021). doi:https:// www.altiostar.com/ white- paper- security- in- open- ran/.

3. O.-R. S. F. G. S. O-Ran Alliance, O-RAN SecurityRequirementSpec-ifications,O-RAN.SFG. Security-Requirements-Specifications-v02.00 (2021) 45 pages.

4. B. Balasubramanian, E. S. Daniels, M. Hiltunen, R. Jana, K. Joshi, R. Sivaraj, T. X. Tran, C. Wang, RIC: A RAN intelligent controller plat-form for AI-enabled cellular networks, IEEE Internet Computing 25 (2) (2021) 7–17.

5. Ericsson, Security Considerations of Open-RAN, White Paper (2020). doi:https://www.ericsson.com/4a4b77/assets/local/security/ security- considerations- open- ran.pdf.

Artificial Intelligence (AI): The Helper or the Threat? A Comprehensive Guide to Understanding Artificial Intelligence and its Impact on Society

By | Nur Fazila binti Selamat, Mohd Nor A'kashah bin Mohd Kamal, Mohd Faisal bin Abdullah, Mohammad Syahir Bin Mohd Salim, Aiman Aizzat Bin Mohd Yusof & Aqilah Nabilah Binti Mohamad Jafar

What is Artificial Intelligence (AI)?

There are many ways to define AI. Some definitions describe it as a technology that makes computers and other machines capable of thinking for themselves. Another definition states that AI involves machinery that replaces human labour to increase productivity and speed. Additionally, AI is also defined as a system that can accurately process external input, learn from it, and apply insights to achieve specific objectives flexibly. Since AI can reduce workloads, it has been widely incorporated into the daily lives of many. [1]

Despite these differences in meaning, the general public often views AI as devices and software that can assist in solving problems and completing tasks more efficiently. In a nutshell, AI is human-created intelligence that is displayed by computers.

How Does AI Works?

As excitement surrounding AI starts to grow exponentially, businesses are quick to highlight how their products incorporate such technology. Often, what is referred to as AI is represented only a component of the technology, such as machine learning. While serving as a pre-requisite for AI, machine learning algorithms require specialized hardware and software for coding and training. Although there is no single programming language used exclusively for AI, developers typically favour Python, R, Java, C++, and Julia due to their versatile features. [2] [5]

AI systems typically operate by processing large amounts of labelled training data, identifying any correlations to establish mean patterns, which are then used to predict future outcomes. For example, an image recognition program can learn to identify and describe objects in photographs by analysing millions of examples. Similarly, a chatbot trained on text examples can generate realistic conversations with users. Generative AI algorithms are advancing rapidly and can now produce realistic text, images, music and other forms of media.

Programming for AI emphasizes cognitive abilities such as:

1. **Learning:** AI programming involves collecting data and designing algorithms to convert it into valuable knowledge. These algorithms provide specific instructions to computing devices on how to perform specific tasks.
2. **Reasoning:** This component of AI programming focuses on selecting the most suitable algorithm to produce the intended result.
3. **Self-correction:** AI programming continuously improves its algorithms to ensure more precise outcomes.
4. **Creativity:** AI can generate new text, images, songs, and ideas using neural networks, rules-based systems, statistical techniques and other AI tools.

Types of AI

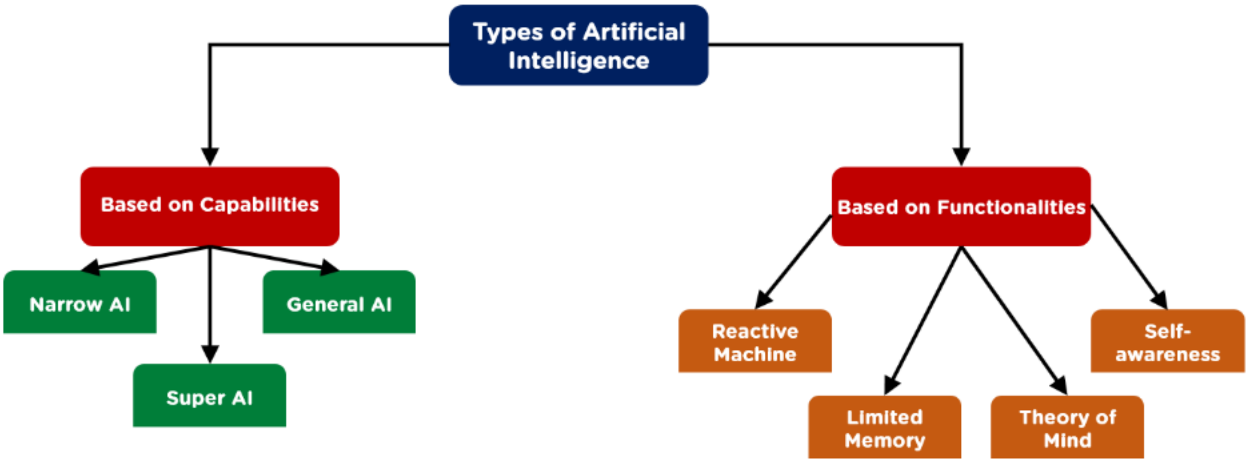


Image 1: Types of Artificial Intelligence

Based on capabilities, AI can be divided into three types [4]:

1. Narrow AI

Weak AI includes recommendation algorithms, self-driving cars, facial recognition software and virtual personal assistants like Siri or Alexa which are designed for specific tasks. This type of AI does not possess general intelligence or consciousness and operates within predefined parameters. For example, it might excel at chess or solving mathematical puzzles but its capabilities remain limited.

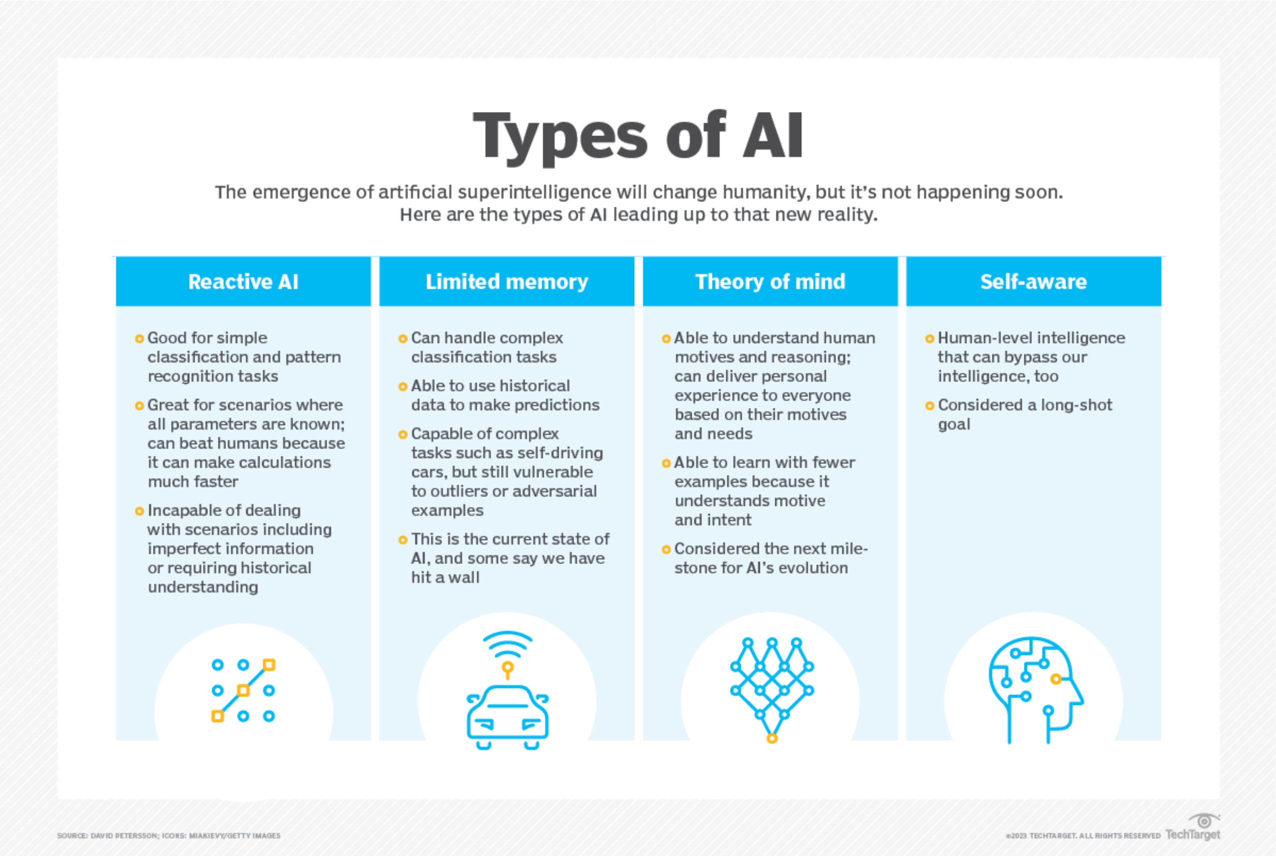
2. General AI

General AI aims to be as intelligent and conscious as humans. It enables machines to apply knowledge and skills across various scenarios. Another interpretation of AI is strong AI which suggests that it can be trained to emulate human thought process, demonstrating intelligence across different activities, and even developing perceptions, beliefs, and cognitive abilities similar to humans. However, strong AI remains theoretical and still the focus of ongoing research and discussion.

3. Super AI

Super AI is hypothetically more intelligent than humans and therefore, can handle any task. According to the theory of artificial superintelligence, AI will eventually become so advanced that it not only understands human emotions but also develops its own needs, wants, beliefs and desires. However, its existence remains speculative. Super AI must possess critical abilities including logical thinking, puzzle solving, problem-solving judgment and autonomous decision- making.

AI is also categorized according to its functions to describe the different types of AI systems. Below are the key categories [2][3][4]: -



Types of AI

The emergence of artificial superintelligence will change humanity, but it's not happening soon. Here are the types of AI leading up to that new reality.

Reactive AI	Limited memory	Theory of mind	Self-aware
Good for simple classification and pattern recognition tasks Great for scenarios where all parameters are known; can beat humans because it can make calculations much faster Incapable of dealing with scenarios including imperfect information or requiring historical understanding	Can handle complex classification tasks Able to use historical data to make predictions Capable of complex tasks such as self-driving cars, but still vulnerable to outliers or adversarial examples This is the current state of AI, and some say we have hit a wall	Able to understand human motives and reasoning; can deliver personal experience to everyone based on their motives and needs Able to learn with fewer examples because it understands motive and intent Considered the next mile-stone for AI's evolution	Human-level intelligence that can bypass our intelligence, too Considered a long-shot goal

SOURCE: DAVID PETERSSON; ICONS: MIAKIEVY/GETTY IMAGES

©2023 TECHTARGET. ALL RIGHTS RESERVED TechTarget

Image 2: Types of AI Based on Functionalities

1. Reactive Machines

The most basic type of AI, reactive machine does not retain memory or use past decisions to determine future actions. Instead, they process current data and respond accordingly. They are designed for specific tasks and cannot operate beyond their predefined functions.

2. Limited Memory

Limited memory AI can analyse past data to make future predictions by storing historical information and forecasts. However, it does not retain this information as an ongoing experience. Limited memory AI is created when a model is designed to continuously evaluate or automatically update itself. Self-driving cars utilize this technology.

3. Theory of Mind

Theory of mind AI is still conceptual and represents a more sophisticated technology class. Such AI would require a deep understanding of how objects and people interact within their environment including changes in emotions and actions. It ought to be able to comprehend people's feelings, ideas, and emotions. Although some progress has been made, this type of AI is still very much at developmental stage.

4. Self-awareness

Self-aware AI remains purely theoretical. These systems would recognize human emotions while understanding their own internal state, allowing them to operate beyond human intelligence. AI would not only be capable of sensing and responding to human emotions, but also develop its own feelings, needs, and beliefs.

Impacts of AI on Society

Similar to most technological advancements, AI has both positive and negative effects on society. [1]

Positive Impacts of AI on Society

1. **Increased Efficiency:** AI improves productivity across various industries by streamlining processes and automating repetitive tasks. This leads to cost savings and better resource management.
2. **Improved Healthcare:** AI aids in drug discovery, disease diagnosis and personalized treatment plans. It also facilitates remote patient monitoring, improving healthcare access.
3. **Enhanced Education:** AI-powered tutoring programs provide instant feedback, adapt to students' needs and offer personalized learning experiences. Language learning apps and virtual classrooms expand educational options.
4. **Safer Transportation:** Self-driving vehicles and AI assisted air traffic management can reduce congestion and accidents; while enhancing accessibility for individuals with disabilities.
5. **Advanced Research:** AI accelerates scientific research by analysing massive datasets, identifying patterns and making predictions. This is especially beneficial in fields like climate modelling and genetics.

Negative Impacts of AI on Society

1. **Job Displacement:** AI-powered automation could eliminate jobs in industries that require repetitive manual labour. Workers in these sectors need to reskill and adapt.
2. **Privacy Concerns:** AI systems process vast amounts of personal data, raising concerns about misuse or unauthorised access.
3. **Security Risks:** AI can be used maliciously to create sophisticated cyberattacks including deepfake scams and AI-generated phishing. Advanced security measures are necessary to combat these risks.
4. **Ethical Dilemmas:** AI raises ethical concerns, such as the development of autonomous weapons and the potential for disinformation campaigns.
5. **Economic Disparities:** AI investments could lead to concentration of wealth among a few, increasing the gap between the rich and poor.

Conclusion

In summary, AI is a rapidly evolving field that seeks to emulate human intelligence in machines, enabling them to perform a wide range of tasks. While Artificial General Intelligence (AGI) remains theoretical, AI has already revolutionized industries like finance, transportation and healthcare.

Despite its vast potential, AI also presents ethical, privacy and employment challenges. A balanced approach is needed to harness its benefits, while mitigating risks to ensure AI's positive impact on society.

References

1. TechyJaunt. (2023, September 12). Introduction to artificial intelligence and its impact on society.Medium: https://medium.com/@techyJaunt/introduction-to-artificial-intelligence-and-its-impact-on-society-99a18ea80722

2. Laskowski, N., & Tucci, L. (2023, November 13). artificial intelligence (AI). Enterprise AI: https://www.techtarget.com/searchenterpriseai/definition/AI-Artificial-Intelligence#:~:text=Artificial%20intelligence%20is%20the%20simulation,speech%20recognition%20and%20machine%20vision.

3. Schroer, A. (2024, February 16). What is artificial intelligence (AI)? How does AI work? https://builtin.com/artificial-intelligence

4. Biswal, A. (2023, November 6). 7 types of artificial intelligence that you should know in 2024. Simplilearn.com.: https://www.simplilearn.com/tutorials/artificial-intelligence-tutorial/types-of-artificial-intelligence

5. Frankenfield, J. (2023, December 4). Artificial intelligence (AI): What it is and how it is used. Investopedia. https://www.investopedia.com/terms/a/artificial-intelligence-ai.asp

Safeguarding Cyberspace: Enhancing Cybersecurity Awareness In Malaysia

By | Mohammad Nasrul Taufiq Bin Salleh, Shazwani Binti Salleh & Nur Syakirah Binti Shahabuddin

Figure 1: As the digital landscape evolves, so do the challenges posed by cyber threats. With cybercrimes and online scams resulting in significant financial losses, the Cyber Security Act is expected to improve the country's digital defence and cyber security posture.

Introduction

In the modern digital era, cybersecurity stands as a critical concern not only in Malaysia but globally. As our society becomes increasingly reliant on digital technologies and interconnected networks, the risk of cyber threats continues to escalate. From individual users to large corporations and government entities, the need for robust cybersecurity measures and enhanced awareness is paramount to safeguarding sensitive information, mitigating financial losses, and preserving national security. This article delves into the multifaceted cybersecurity landscape in Malaysia, highlighting the importance of education, collaboration, policy frameworks, investments in cybersecurity infrastructure, and international cooperation in bolstering cybersecurity resilience.

Cyber threats manifest in various forms, each posing unique challenges and potential cybersecurity risks. Malware, including viruses, worms, and Trojans, can infect systems and compromise data integrity. Phishing attacks leverage social engineering techniques to deceive users into divulging sensitive information, while ransomware encrypts files and demands ransom payments for decryption. Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks disrupt services by overwhelming networks with excessive traffic. Moreover, emerging threats such as cryptojacking, IoT vulnerabilities, and supply chain attacks add complexity to the cybersecurity landscape. Understanding these threats is fundamental in building a resilient cybersecurity posture.

Key Strategies for Enhancing CyberSecurity Awareness

Education plays a pivotal role in enhancing cybersecurity awareness and readiness where raising awareness begins with educating individuals about cyber risks, safe online practices, and the importance of strong passwords. Regular training programs for employees, students, and the general public are crucial. Integrating cybersecurity education into school curriculum from an early age instils a sense of digital responsibility, privacy protection, and safe online behaviours among students. Specialized training programs for professionals in cybersecurity, IT, software development, and data management are essential to equip individuals with the knowledge and skills in detecting, preventing, and responding to cyber threats effectively. Continuous education ensures that cybersecurity professionals remain updated on the latest threats, trends, and best practices, thereby enhancing overall cyber resilience.

Addressing cybersecurity challenges requires a collaborative effort involving government agencies, private sector entities, academia, and civil society organizations. By fostering partnerships and leveraging collective expertise, Malaysia can develop comprehensive cybersecurity strategies, implement defence mechanisms, and enhance information sharing and incident response capabilities. Public-private partnerships are particularly crucial in sharing threat intelligence, coordinating cybersecurity initiatives, and promoting cybersecurity awareness among businesses and individuals.

Public awareness campaigns serve as practical tools to disseminate cybersecurity knowledge, promote best practices, and empower individuals to adopt proactive cybersecurity behaviours. These campaigns leverage various communication channels such as social media, websites, workshops, seminars, and community outreach programs to reach diverse demographics across Malaysia. By engaging directly with the public, these initiatives debunk myths, raise awareness about cyber threats, emphasize the need for vigilance and responsible online behaviour, and encourage individuals to secure their digital assets and devices.

Government policies and regulations play a crucial role in promoting cybersecurity and establishing a conducive environment for cybersecurity initiatives. Malaysia should consider implementing robust data protection laws, comprehensive incident reporting mechanisms, high cybersecurity standards, and sound regulatory frameworks that align with international best practices. Additionally, sharing threat intelligence, best practices, and resources will enhance collective cybersecurity efforts. Regulatory compliance ensures that organizations adhere to cybersecurity guidelines, adopt risk management strategies, and prioritize cybersecurity investments. Additionally, fostering cybersecurity innovation and research through government funding and incentives stimulates the development of cybersecurity solutions and technologies.

Investments in cybersecurity infrastructure, technologies, and human resources is essential for building cyber resilience. Organizations must allocate resources for cybersecurity tools such as firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), encryption technologies, security analytics platforms, and endpoint security solutions. Furthermore, investing in cybersecurity talent acquisition, training, and skill development does contribute to enhancing cybersecurity capabilities and addressing skills shortages in the cybersecurity workforce. Performing regular security assessments, vulnerability scans, and penetration testing can help identify vulnerabilities, and security besides addressing weaknesses promptly.

Cultivating a cybersecurity culture within organizations and communities is crucial in fostering security-conscious mindsets and promoting cyber hygiene practices. This involves raising awareness about cybersecurity risks, establishing policies and procedures for data protection, implementing access controls and authentication mechanisms, conducting regular security audits and assessments, and promoting incident response readiness. Training programs, awareness campaigns, and cybersecurity best practices contribute to creating an inclusive culture where cybersecurity is everyone's responsibility, from senior management to frontline employees and individual users.

Why Malaysia Needs to Boost CyberSecurity Awareness?

Cybersecurity presents a critical challenge for global businesses. Although relentless focus has been placed by global IT security solutions providers to enhance security features, and improve monitoring and controls over the information systems security in mitigating the risks of cyber attacks, there is still a lot of ground to be covered.

Malaysia, as a business hub, is facing cybersecurity issues, threats, and challenges. This has made cybersecurity a top priority, compelling businesses to be more vigilant on the vulnerabilities caused by malware and other various cyber attacks.

The Government of Malaysia (GOM) launched the Malaysia Cyber Security Strategy (MCSS) 2020-2024, with a specific budget allocation of around US$434 million to enhance cybersecurity preparedness and for establishing a robust infrastructure for anti-malware solutions, as well as cybersecurity in Malaysia.

The MCSS listed five key focus areas namely improving ICT infrastructure, upgrading antivirus and anti-malware solution deployments, improving cybersecurity laws, as well as empowering cybersecurity innovation in Malaysia. Additionally, the government is keen to attract a new talent pool comprising professionals with cybersecurity backgrounds to work in Malaysian organizations.

Malaysia is turning its attention to cybersecurity strategies that leverage regional and international cooperation to protect its cyberspace. Alongside an increase in digital enablement of business operations, Malaysia also witnessed an exponential rise in cybersecurity challenges.

A report by CyberSecurity Malaysia indicates that an average of 31 cases of cyber crimes are reported daily in Malaysia. As such, there is an urgent need for businesses to ensure adequate security monitoring tools are available and used. According to CRI (Cyber Risk Index) report for the second half of 2021 for CyberSecurity Malaysia, about 87% of the organizations participating in the survey have encountered one or more cyberattacks in the last year.

The study also highlighted the type of security challenges prevalent across the cybersecurity breach in Malaysia and a need for more robust ICT infrastructure to incorporate an anti-malware system.

Cyber crimes are not constrained by borders, therefore necessitating international collaboration and information sharing to combat it effectively. Malaysia should actively engage in international cybersecurity forums, partnerships, and initiatives in order to leverage threat intelligence exchange, sharing of best practices, and promoting global cybersecurity norms and standards. Collaboration with neighbouring countries, regional organizations, and global cybersecurity bodies could also enhance cybersecurity resilience, capacity building, and incident response coordination.

Looking ahead, several trends are likely to shape the future of cybersecurity in Malaysia. These include the rise of cloud security, the adoption of Zero Trust architecture, increasing focus on supply chain security, proliferation of cybersecurity automation and orchestration tools, advancement in threat intelligence sharing platforms, and regulatory developments in data protection and privacy. Malaysia must stay agile, adaptive, and proactive in addressing emerging cybersecurity trends and challenges.

Malaysia faces a unique set of cybersecurity challenges owning to its rapid digital transformation and growing digital economy. The increasing use of cloud services, mobile devices, Internet of Things (IoT) devices, and online platforms introduces new vulnerabilities and attack vectors. Moreover, the interconnected nature of critical infrastructure sectors such as banking, healthcare, transportation, and energy amplifies the potential impact of cyber-attacks. Addressing these challenges requires a holistic approach that encompasses technical measures, policy frameworks, human resources, and international cooperation.

Effective cybersecurity risk management is essential in identifying, assessing, mitigating, and monitoring cybersecurity risks. Organizations must adopt risk-based approaches to cybersecurity, conduct regular risk assessments, prioritize critical assets and data, implement security controls based on risk levels, and develop incidence response plans. Cybersecurity risk management frameworks such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework and ISO/IEC 27001 provide clear guidelines and best practices in managing cybersecurity risks effectively.

Conclusion

Malaysia is poised to embrace the future of cybersecurity by adopting innovative technologies, robust strategies, and collaborative approaches to cyber defence.

By staying agile, adaptive, and proactive in addressing emerging cybersecurity challenges and opportunities, Malaysia can strengthen its cyber resilience, protect critical assets, foster digital trust, and navigate the evolving cybersecurity landscape confidently. With continuous investments in cybersecurity infrastructure, collaboration, international cooperation and commitment from all stakeholders, Malaysia can emerge as a strong leader in cybersecurity excellence and contribute to a safer and more secure digital future for all.

By fostering a cybersecurity-sensitive culture, promoting public awareness, implementing robust policies and regulations, investing in cybersecurity technologies and talent, and engaging in global cybersecurity initiatives, Malaysia can strengthen its cyber defences and navigate the evolving cybersecurity landscape confidently. With concerted efforts from government agencies, private sector entities, academia, civil society organizations, and individual citizens, Malaysia can build a safer and more secure digital environment for all stakeholders.

References

1. CyberSecurity Malaysia. (n.d.). Retrieved from https://www.cybersecurity.my/

2. National Cyber Security Agency (NACSA). (2023). National Cyber Security Strategy 2023-2028. Retrieved from https://www.nacsa.gov.my/

3. Lim, J. (2022). Strengthening Cybersecurity Awareness in Malaysia. The Star. Retrieved from https://www.thestar.com.my/tech/tech-news/2022/06/01/strengthening-cybersecurity-awareness-in-malaysia

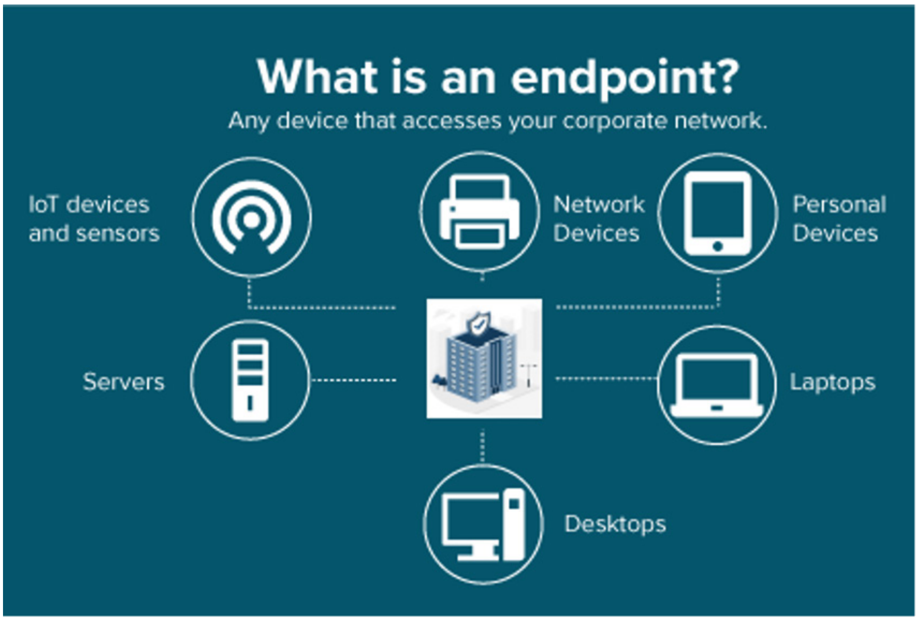
Safeguarding Digital Frontiers: The Crucial Role of Endpoint Security

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

In today's evolving digital landscape, where cyber threats are rampant, safeguarding security endpoints has become paramount for organizations striving to protect their sensitive data and critical systems. Endpoint security across laptops, desktops, smartphones, and other devices, plays a pivotal role in fortifying against an avalanche of cyber-attacks. This article delves into the significance of endpoint security, its key components, challenges, and strategies in bolstering defences.

Understanding Endpoint Security

Endpoint security encompasses a comprehensive approach to protecting endpoints from various cyber threats, including malware, ransomware, phishing attacks, and insider threats. It involves deploying a suite of security solutions and implementing robust security policies to mitigate risks and safeguard sensitive data. Key components of endpoint security include antivirus software, firewalls, intrusion detection systems, endpoint detection and response (EDR) solutions, and mobile device management (MDM) platforms. These tools work in tandem to monitor, detect, and respond to security incidents in real-time, thus minimizing the impact of potential breaches.



Challenges in Endpoint Security

Endpoint security faces several challenges that curtail its implementation and effectiveness. One significant challenge is the proliferation of endpoints in modern IT environments, including traditional devices such as PCs and laptops, as well as mobile devices and Internet of Things (IoT) devices. Managing and securing such diverse array of endpoints can be daunting, particularly for organizations with limited resources and expertise. Additionally, the rise of remote work and Bring Your Own Device (BYOD) policies has further complicated endpoint security, as employees constantly access corporate resources from outside the traditional network perimeter, increasing the risk of exposure to cyber threats.

Strategies for Strengthening Endpoint Security

To address challenges and bolster endpoint security, organizations must adopt a proactive and multi-layered approach. First and foremost, implement robust endpoint protection solutions, such as next-generation antivirus software and advanced threat detection tools, to help detect and prevent malware and other malicious activities. Regular software patching and updates are also essential to address vulnerabilities and ensure that endpoints are fortified against latest threats. Moreover, enforcing strong access controls, implementing endpoint encryption, and deploying endpoint management solutions can help mitigate the risks associated with BYOD and remote work. Finally, educating employees about cybersecurity best practices and fostering a security awareness culture can empower them to recognize and respond effectively to potential threats.

Conclusion

In conclusion, endpoint security is an indispensable component in an organization's cybersecurity strategy, serving as the frontline defence against cyber threats. By understanding the importance of endpoint security, recognizing the challenges it faces, and implementing proactive strategies to strengthen defences, organizations can safeguard their digital assets and protect against potential breaches. As cyber threats continue to evolve and proliferate, investing in robust endpoint security measures remains essential to safeguard the integrity, confidentiality, and availability of critical systems and data.

References

1. https://www.crowdstrike.com/cybersecurity-101/endpoint-security/

2. https://www.fortinet.com/resources/cyberglossary/what-is-endpoint-security

3. https://www.watchguard.com/wgrd-news/blog/4-ways-strengthen-your-endpoint-security-strategy-msp

4. https://heimdalsecurity.com/blog/endpoint-security-best-practices/

5. https://www.linkedin.com/pulse/rise-endpoint-security-risks-6-common-types-security-scorecard

The Rise Of Machines: How AI And Automation Are Set To Transform Our Lives

By | Aina Mardhiah Binti Zolkapile

Artificial intelligence (AI) refers to the fast and quick intelligence exhibited by machines. It is not biological intelligence like humans possess, but rather simulated intelligence achieved through computer programs. AI encompasses a range of techniques, from machine learning that allows machines to learn from data without straightforward programming, to deep learning that uses complex algorithms inspired by the human brain. The goal of AI is to create brilliant machines that can perform tasks typically requiring human intelligence, such as problem-solving, decision-making, and even creativity. AI is continuously evolving and impacting through various fields, from healthcare and finance to transportation and entertainment.

Nowadays, the world of work is experiencing dramatic changes. Artificial intelligence (AI) and automation, once ideas of science fiction proportion are transforming entire industries and the way we perform our jobs daily. This article delves into how this formidable combination is impacting job careers. While some jobs will disappear, others will be completely revamped, creating exciting new opportunities. AI has the potential of significantly improving our lives and solving complex challenges through innovative ways. On the other hand, we are faced with ethical challenges in the use of AI such as to deceive or manipulate, privacy compromise, biasness, and concerns about inequities. In particular, employment losses remain the greatest societal impact, as mentioned in the preceding section [1]. Nevertheless, although AI potentially has many positive effects, it produces an equally disruptive and unpredictable consequences for society, as shall be discussed in the following section.

A shadow of fear appears over the rise of artificial intelligence (AI). Experts warn of an imminent wave in automation that will sweep across factories, offices, industries and shops, displacing countless workers. The concern is fuelled by rapid developments in AI that are already transforming industries. Some paint a particularly grim picture, predicting AI will worsen income inequality. Their vision: a future where only the affluent can afford and wield the power of AI for unfair economic advantage. By leveraging, expensive AI systems and specialized skills to operate them effectively. The end result? An economic gap widens between the wealthy who leverage AI for economic dominance and the rest who struggle to compete in this new, AI-driven environment. This scenario raises serious concerns over potential social unrest and economic instability if the benefits of AI are not shared more equitably[2].

The healthcare field is also experiencing a surge in the use of robots and AI, with these technologies together to significantly impact how doctors diagnose and treat patients. While the use of robots open up exciting possibilities such as assisting in diagnoses, there is also a growing concern on its potential harm. This is especially true for robots operating with greater autonomy, such as drones and rehabilitation robots. As these robots are capable of making decisions that directly affect people's well-being, there is a need to highlight the safety concerns and ensure these technologies are implemented responsibly[3]. On other one hand, robots could do wonders. Imagine surgical robots assisting with complex procedures, improving precision, and minimizing human error. Rehabilitation robots can provide targeted physical therapy, while AI-powered diagnostic tools can analyse limitless amounts of medical data to identify patterns and potential diseases at an earlier stage. This collaboration between human expertise and machine intelligence empowers digitalized healthcare delivery, leading to more accurate diagnoses, personalized treatment plans, and eventually, improved patient care. Such immense potential enabled by technologies should be embraced while keeping in mind the associated risks. By prioritizing safety issue, fostering human-machine collaboration, and ensuring ethical implementation, we can unlock the true potential of AI and robotics to revolutionize healthcare and create a future where technology empowers medical professionals to deliver exceptional patient care.

Although AI powered machines and technology can take over tasks once done by humans, automation's has a serious downside: increased job losses. This negatively impact mental health.

Studies have shown a correlation between job loss due to factory closures and increased rates of depression, substance abuse, and even suicide[4]. In other words, the very technology that is supposed to make our lives easier might come at a cost to our emotional well-being. To mitigate such negative consequences, proactive solutions are critical. Investment in requalification programs and reskilling initiatives can help workers to survive in a changing job market. Additionally, social safety nets and mental health support systems must be strengthened to provide a buffer for those facing job displacement. Ultimately, tackling the ethical issues related to AI requires a comprehensive approach. While technological advancements offer undeniable benefits, we must prioritize the human element. By acknowledging mental health risks associated with job displacement and implementing proactive solutions, we can ensure that progress serves humanity, and not the other way.

Artificial intelligence (AI) has the potential to fundamentally change how we use technology, especially concerning information security and data privacy. One of the main worries is how AI might connect personal data in unforeseen ways, potentially making it easier for cybercriminals to access private information. While AI-powered facial recognition offers security benefits, there is also a hidden risk that criminals could hack into these systems and exploit them[5]. The development of lethal autonomous weapons controlled by AI introduces a whole new level of risk. The ease with which these systems can be manipulated is of grave concern - unauthorized access could have devastating consequences. A recent example of such potential danger is the case of "Tesla phantom braking," where a self-driving car abruptly stopped in traffic for no plausible reason, causing accidents[6]. To navigate these challenges, it is crucial for international organizations and businesses to consider the social impact of AI when developing and implementing these technologies. After all, it is public’s demand for solutions that is driving the rapid advancement of AI.

In conclusion, while Artificial Intelligence (AI) offers a future brimming with possibilities, it's path is fraught with ethical concerns and potential societal fractures. From potential job displacement and mental health concerns to privacy risks and development of autonomous weapons, careful consideration is much needed. The key lies in harnessing AI's potential for good while mitigating its negative effects. International collaboration, responsible development, and focus on the human impact are crucial in ensuring AI serves humanity, not the other way around. After all, AI is a tool, and like any powerful tool, its ultimate impact hinges on the hands that wield it. We must ensure responsible development and use of AI to create a future where the technology empowers us, improves our lives, and tackles global challenges for the betterment of all. We still have the power now to shape AI’s development and ensure it serves as a force for good. This requires a multi-pronged approach. Despite the challenges, AI holds immense potential in revolutionizing our lives for the better. Imagine AI-powered tools tackling climate change, personalizing education for every child, or collaborative problem-solving on a global scale. By approaching its development with foresight and a commitment to human well-being, we can unlock a future where AI becomes a powerful tool for progress, collaboration, and global development. The choice is ours to make now.

References

1. F. Cingano, Trends in Income Inequality and its Impact on Economic Growth, in: OECD Social, Employment and Migration Working Papers, vol. 163, OECD Publishing, 2014, https://doi.org/10.1787/5jxrjncwxv6j-en

2. G.A. Legault, C. Verch`ere, J. Patenaude, Support for the development of technological innovations: promoting responsible social uses, Sci. Eng. Ethics 24 (2018) 529–549, https://doi.org/10.1007/s11948-017-9911-5.

3. S.C. Olesen, P. Butterworth, L.S. Leach, M. Kelaher, J. Pirkis, Mental health affects future employment as job loss affects mental health: findings from a longitudinal population study, BMC Psychiatr. 13 (2013) 1–9, https://doi.org/10.1007/s11948-017-9911-5.

4. K. An, Y. Shan, S. Shi, Impact of industrial intelligence on total factor productivity, Sustainability 14 (2022), 14535, https://doi.org/10.3390/su142114535.

5. O.A. Osoba, W. Welser, The Risks of Artificial Intelligence to Security and the Future of Work, vol. 2023, RAND Corporation, Santa Monica, CA, 2017. Last accessed April 22, 2024, https://www.rand.org/pubs/perspectives/PE237.html

6. Tesla’s ‘phantom braking’ problem is now being investigated by the US government - the Verge, accessed (April 22, 2024) https://www.theverge.com/2022/2/17/22938944/tesla-phantom-braking-nhtsa-investigation-defect

Post-Quantum Cryptography

By | Nurul Amiera Sakinah Binti Abdul Jamal

Why are quantum computers a security threat?

It is said that once sufficiently powerful quantum computers become a reality, traditional asymmetric cryptographic methods for key exchange and digital signatures will be rendered obsolete. Leveraging Shor's algorithm, quantum computers will be capable of compromising the security of discrete logarithm-based schemes like Elliptic Curve Cryptography (ECC) and factorization-based schemes like RSA (Rivest-Shamir-Adleman) so much that no reasonable key size would suffice to keep data secure. ECC and RSA are currently the default algorithms used to protect everything from our bank accounts to our medical records.

Governments, researchers, and tech leaders the world over have recognized the threat of quantum computing and the difficulty in securing critical infrastructure against such attacks.

What is Post-Quantum Cryptography (PQC)?

According to the National Institute of Standards and Technology (NIST) the goal of post- quantum cryptography (PQC, also called quantum-resistant or quantum-safe) is to "develop cryptographic systems that are secure against both quantum and classical computers, and can interoperate with existing communications protocols and networks."

Not to be confused with quantum cryptography, which relies on the natural laws of physics to produce secure cryptosystems, post-quantum cryptographic algorithms use different types of cryptography to create quantum-proof security.

Types of quantum cryptography

- Lattice-based cryptography
- Multivariate cryptography
- Hash-based cryptography
- Code-based cryptography
- Isogeny-based cryptography
- Symmetric key quantum resistance

Why do we need to act now as quantum computers are still a way off?

While quantum computers which are powerful enough to break public key encryption may still be a way off, data harvesting is happening now. Malicious actors are already said to be collecting encrypted data and storing it for a time in the future when quantum computers will be capable of breaking our current encryption methods. This is known as a "harvest now, decrypt later" strategy.

Furthermore, as the shelf life of confidential or private information can span years or decades, there is a rapidly growing need to protect and future proof it from quantum attack. Additionally, many devices such as chips are saddled with a long development cycle. Given that it can take years for security testing, certification and then deployment into the existing infrastructure, the earlier the transition to Quantum Safe Cryptography begins, the better.

What progress has been made in new PQC algorithms development?

The biggest public initiative to develop and standardize new PQC algorithms was launched by the U.S. Department of Commerce's National Institute of Standards and Technology (NIST). International teams of cryptographers submitted algorithm proposals, reviewed the proposals, broke some, and gained confidence in the security of others.

On August 24th, 2023, NIST announced the first three draft standards for general-purpose Quantum Safe Cryptography. These draft standards are:

- FIPS 203 ML-KEM: Module-Lattice-Based Key Encapsulation Mechanism Standard, which is based on the previously selected CRYSTALS-Kyber mechanism
- FIPS 204 ML-DSA: Module-Lattice-Based Digital Signature Standard, which is based on the previously selected CRYSTALS- Dilithium signature scheme
- FIPS 205 SLH-DSA: Stateless Hash-Based Digital Signature Standard, which is based on the previously selected SPHINCS+ signature scheme.

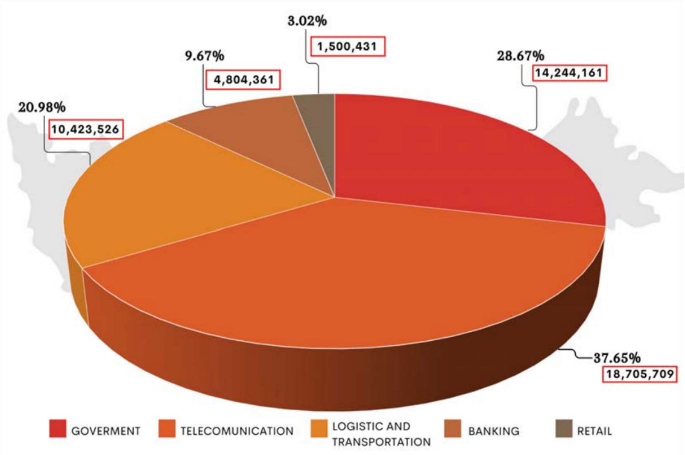
The National Security Agency (NSA) published an update to its Commercial National Security Algorithm Suite (CNSA) in September 2022, CNSA 2.0. National Security Systems (NSS) will need to fully transition to PQC algorithms by 2033 and some use cases will be required to complete the transition as early as 2030. CNSA 2.0 specifies that CRYSTALS-Kyber and CRYSTALS-Dilithium should be used as quantum-resistant algorithms, along with stateful hash-based signature schemes XMSS (eXtended Merkle Signature Scheme) and LMS (Leighton-Micali Signatures).

Navigating the Aftermath of a Data Breach: A Roadmap to Post-Failure Success

By | Mohd Rizal bin Abu Bakar, Wan Shafiuddin Zainudin, Om Nashila binti Ramli & Noor Aida binti Idris

In our modern, connected world, data breaches are bound to take place regularly. Like many countries around the world, Malaysia has experienced a rise in data breaches in recent years. Factors contributing to this increase include the growing digitalization of economy, increased connectivity, and evolving cyber threats. According to the Mid-Year Report: Threat Landscape 2023 issued by CyberSecurity Malaysia, telecommunication and government sectors in Malaysia experienced the highest number of data breaches at 37.65% and 20.98%, respectively for the period of January to June 2023. They are followed by logistic and transportation sector (20.98%) and banking sector (9.67%). These sectors are particularly vulnerable to data breaches due to the sensitive nature of data both handled and stored.

TOTAL DATA LEAKED BY SECTOR



As organizations navigate the complex landscape of information security, handling the aftermath of a data breach becomes a pivotal point for either future success or further setbacks. Success is not just about recovery but also about learning, adapting and becoming more resilient. In this article, let's explore the essential strategies to triumph after a failure, integrating compliance with ISO/IEC 22301:2019, ISO/IEC 27701:2019 extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management and leveraging Open Source Intelligence (OSINT) as a proactive tool to further securing organisations from data breaches.

Understanding the impact of data breaches

Data breaches are no longer standalone occurrences. Instead, they are significant events with widespread repercussions. The aftermath involves legal and regulatory consequences, reputation harm and financial losses.

Legal and Regulatory Consequences: Data breaches can lead to lawsuits and regulatory investigations. Organisations may be held liable for damages resulting from the breach, including compensation for affected individuals, legal fees, and court settlements. Additionally, organisations may face fines, penalties, and legal liabilities for non-compliance with data protection regulations.

Reputational Damage: Data breaches can severely damage an organisation’s reputation and erode customer trust. Clients and customers may lose confidence in the organisation's ability to protect their personal information, leading to a loss of business, negative publicity, and long-term damage to brand reputation.

Financial Impact: Data breaches can result in direct financial losses for organisations, including costs associated with investigating the breach, mitigating the effects of data breach, and compensating affected individuals and customers.

The above impact are severe, culminating in the decline in clients and customers confidence on the security of their data. Acknowledging the seriousness of these outcomes is essential for organizations to chart their path towards a successful post data breach.

Robust Response Plan

In an unpredictable world of data breaches, putting a robust response plan in place is like putting on superhero suit for your organization. Picture this: A plan that swings into action immediately, with strategic communication in place, while complying with ISO/IE 22301 Business Continuity Management System (BCMS), the international default standard. ISO/IEC 22301 BCMS isn't just a set of guidelines; it's the go-to manual for organizations, teaching them how to establish, implement, maintain, and continually improve their BCMS. It's the ultimate path to resilience, making potential disruptions, including data breaches mere ‘footnote’ in the organizational saga.

To tackle the ‘sneaky villains’ of privacy concerns, an organization also requires the Privacy by Design shield, working in concert with ISO/IEC 27701:2019. This ‘dynamic duo’ affirms ISO/IEC 27001 standard, ensuring that privacy concerns are addressed from the get-go. It is akin to activating a force field against potential risks, a ‘superhero’ shield for data integrity.

But here's the punchline: Continuous improvement isn't just a goal for an organization; it is a ‘mantra’ to navigate the complex aftermath of a data breach. In today’s data-driven world, being a ‘superhero’ organization is no longer an option – it's a necessity for survival.

Leveraging Open Source Intelligence (OSINT) for Security

Navigating the treacherous waters of data breaches is ‘no walk in the park’. Fear not with Open Source Intelligence (OSINT). OSINT is not just an average information gatherer; think of it as an organization's cyber ‘Sherlock Holmes’, complete with a magnifying glass and a deerstalker hat.

So, what is OSINT? OSINT is like instructing your own band of digital detectives to proactively seek out threat intelligence. These special agents are designed to monitor online chatter, identify potential threat actors and assess vulnerabilities like a cybersecurity ninja in the shadows.

During the post-breach analysis, OSINT transforms to become your organization's cyber detective agency by providing insights into the breach landscape. It helps enhance incident response strategies and fortify overall security measures.

OSINT is like a cyber security crystal ball, allowing cybersecuirty teams to peer into the future of potential threats. Leveraging publicly available information for threat intelligence becomes the ‘secret sauce’ of resilience against ever-evolving cybersecurity threats.

While the cyber world may be fraught with villains and virtual dark alleys, OSINT acts as a digital ‘superhero’ to your cybersecurity, always vigilant and ready to swoop in when trouble comes.

Post-breach Communications Strategies

Transparent communication is the basis to rebuild trust after a data breach. Stakeholders, including customers, employees, and regulatory bodies, need to be kept informed throughout the recovery process. Transparency goes hand-in-hand with accountability. Organizations must not only accept responsibility for the breach but also demonstrate an unwavering commitment to security moving forward.

Rebuilding trust requires more than just words. It demands tangible actions that showcase dedication in preventing future breaches. Maintaining clear communication channels for affected individuals and providing assistance are key steps. In addition, organizations should work towards regaining loyalty by initiating enhanced security features to reassure customers and rebuild their trust.

Learning from the Breach

Treat a data breach incident as an opportunity to learn rather than as setback. It's crucial to conduct a detailed analysis after an incident to ascertain its root causes and assess how well the response measures worked. The information gathered from a breach becomes a valuable tool towards ongoing improvement.

Security improvement is a direct result of learning from a breach. This could mean updating technology, strengthening access controls, or enhancing encryption protocols – all essential steps that contribute to a more robust security setup. Equally vital are employee training and awareness programs, ensuring that the human side of security is fortified to ward off future breaches.

Legal & Regulatory Compliance

Handling the legal and regulatory hoopla after a breach is like trying to untangle a slinky – complex but absolutely necessary for post-breach key learnings. Implementing ISO 22301 BCMS is crucial, not just as an assurance for business continuity but also an enforcement mechanism that organizations toe the line with legal and regulatory standards; whilst ensuring that notification requirements are met, and regulatory investigators are kept at bay. For example, BCMS activates the company's pre-established business continuity plan, adheres to legal and industry standards meticulously, handles all notification requirements, and works closely with regulatory investigators to provide the necessary documentation and information, acting as a liaison to keep the organization on the right side of the law throughout the incident response and recovery process.

Staying compliant isn't just about following the rules; it is about adapting to the legal landscape. Integrating privacy management standards, including ISO/IEC 27701:2019 is essential for maintaining compliance. This ensures the organization remains resilient under the watchful eye of regulatory scrutiny.

Rebuilding Customer Trust

Rebuilding customer trust is a delicate and ongoing process. Therefore, transparent communications and robust support mechanisms are crucial. Providing assistance for affected individuals, whether through identity protection services or direct support, underscores a firm commitment to rectify consequences of a breach.

Offering incentives for loyalty is another avenue for rebuilding trust. Enhanced security features, discounts, or special offers can go a long way in reassuring customers that the organization is not just addressing the breach but actively working towards providing a more secure environment.

Conclusion

Viewing setbacks as opportunities for improvement is essential for achieving success after a data breach. The journey towards achieving excellence in data security is an ongoing one, demanding dedication to constant improvement, a cautious approach, and proactive measures against ever-evolving threats. Following the guidelines of ISO/IEC 22301 BCMS and ISO/IEC 27701:2019 ensures a well-organized framework. The strategic deployment of OSINT further strengthens an organization's capability to proactively tackle security challenges.

In the ever-changing landscape of information security, success after a data breach isn't solely about bouncing back. It involves building resilience, promoting continuous improvement, and actively pursuing information security and data privacy excellence. By seamlessly incorporating compliance with international standards and utilizing tools like OSINT, organizations can navigate the aftermath of a data breach, transforming setbacks into stepping stones for future growth and achievement.

DO'S AND DON'TS OF FACIAL RECOGNITION

Facial recognition technology is becoming increasingly prevalent in our daily lives, raising important issues about privacy and security. This infographic offers the essential dos and don'ts to help navigate this evolving landscape wisely

Enable strong passwords and multi-factor authentication (MFA)

Be cautious when using facial recognition for payments

Take advantage of data deletion options

Review privacy settings regularly

Don't

Don't be afraid to opt out from facial identification

Don't assume facial recognition is always accurate

Don't share facial recognition data indiscriminately

Don't rely solely on facial recognition for device security

Reference
State Biometrics and Facial Recognition Legislation. (n.d.). https://leg.colorado.gov/sites/default/files/images/ncsl_biometrics_and_facial_recognition_legislation_presentation.pdf

The Human Cost Of Cyber Attacks: Stories From The Frontlines

By | Ikmal Halim Jahaya, Aliya Farhana Mohd Nasran, Amiroul Farhan Roslaini & Hasnida Zainuddin

Introduction

In the world of cybersecurity, the focus on the latest breaches and vulnerabilities is almost always about statistics and technical details. However, behind these headlines often lie stories of neglected cyberterrorism victims. The impact of cyber-attacks extends far beyond financial losses and data theft, delving into the loss of trust, invasion of privacy, and an unsettling feeling of being watched. For those at the frontline – cybersecurity professionals, employees, and individual users – this is the stark reality. They form the first-line of defense against cyber threats, relying on technology to fulfill their roles. When their systems or data are compromised, it not only disrupts vital services but also pose risks to lives. This article delves into their experiences, revealing the loss of trust and determination amidst the evolving cyber threat landscape.

Definition of Cyber Attack

According to Cisco, a cyberattack is a malicious and deliberate attempt by an individual or organization to breach the information system of another individual or organization. The attacker often seeks some type of benefit from disrupting the victim’s network. In fact, cyber-attackers frequently focus on industries such as healthcare, government, non-profit organizations, and finance companies. Cyber-attacks are not always driven by financial motives; some aim to destroy or obtain access to crucial data.

Impact of Large Scale Data Breaches

Large-scale data breaches not only affect the targeted companies, institutions, and organizations, but also cause repercussions for individuals on a personal level. Even if individuals are not directly targeted, they can suffer collateral damage if the organizations they trust with their personal information fall victim to such breaches. The consequences can be severe and long-lasting, including financial losses, reputational damage, legal action, loss of stakeholder trust, decline in business, and challenges in attracting talent. We will examine some of these negative impacts below:

- **Temporary Shut Down:** For companies, the detrimental effects of data breaches extend far beyond the instantaneous financial burdens, as they also contend with the persistent, long-term fallout
- **Financial loss:** According to industry surveys, Gartner concludes that the cost of operational downtime can be around $5,600 per minute and quickly accumulate to $300,000 per hour if breaches are not promptly resolved.
- **Reputational Damage:** Reputational damage is a major concern for companies that experience large-scale data breaches. Such damage can lead to revenue loss and long-term impact. When a company's reputation is tarnished due to a history of data breaches, people are less likely to trust it with their financial information, and they may choose to take their business elsewhere.
- **Loss of Private Data:** According to Selfkey website, hackers usually target sensitive data and intellectual property in a cyber-attack. Sensitive data, such as personal information of customers, patients, and employees, as well as private company emails which contain health history, addresses, and payment details etc. Hackers target intellectual property like designs, strategies, and blueprints, which can give competitors an edge and harm a company's competitiveness. Industries such as manufacturing and construction are especially vulnerable to these cyber threats.

Two notable real-life events illustrating the effects of cyber-attack are Sony Pictures and JP Morgan case. Both cases underscore the devasting impact a cybercrime could inflict on both businesses and individuals, therefore highlighting an urgent need for robust cybersecurity measures and vigilance in the digital age.

1. The Sony Case

In November 2014, Sony Pictures reported that an external breach has occurred in which confidential data comprising over 30,000 internal documents, 170,000 emails, social security numbers of Sony employees, personnel reviews, unreleased movies, and others were leaked. The cyber-attack disrupted all of Sony's systems, making the online stock footage database unsearchable, the telephone system non-functional, and rendering computers and servers unusable. The FBI described this attack as an "unprecedented digital assault" that would have severely impacted 90% of companies. In response, Sony had to replace many of its systems, establish an identity fraud hotline, provide psychological counseling for employees, and conduct training on data security.

Subsequent to the attacks, Sony employees received threatening emails, while their credit card information was sold on Dark Net markets, some even experienced financial disruption when their bank accounts were compromised with credit limits exceeded. A survey by the Identity Theft Resource Center revealed that victims of identity theft experienced a range of emotions including denial, frustration, rage, fear, betrayal, and helplessness. Class-action lawsuits were filed by employees, either due to Sony's failure in notifying those affected by the breach or over concerns over the potential misuse of leaked personal information. This has also led to the departure of key staff members, while Sony's diversity issues were exposed to the press via leaked emails.

2. The JP Morgan Chase Case

JP Morgan Chase, a leading bank in the United States, reported that a malicious actor obtained administrator privileges and access to multiple servers. This breach led to the theft of details such as names, phone numbers, emails, and physical addresses of some 76 million households and seven million small businesses. Just prior to the attack, JP Morgan had announced an increase of $250 million per year in their cybersecurity budget. Following the breach, the bank had to overhaul most of its IT systems, a process that was both time consuming and disruptive to its daily operations. Additionally, more than 1,000 new employees had to be hired to monitor the company's systems.

The aftermath of the cyber intrusion brought about two significant and long-term effects. Many affected customers were compelled to closely monitor their finances due to fear of fraud, such as falling prey to fake emails directing them to fraudulent websites. The second major consequence was replacement of the bank’s chief information security officer due to perceived lack of cooperation with federal authorities during the investigation aimed at containing the breach and minimizing information leakage.

Impact of Data Breaches at Personal Level

Data breaches at a personal level often stem from carelessness in the digital realm and inadequate security practices. Individuals may inadvertently disclose sensitive information on unsecured websites or become targets of phishing scams, leading to compromises to login credentials. Weak passwords and neglected software updates can also expose personal devices to hacking. Some of the negative impacts on a personal level include:

Identity Theft: Identity theft is a serious crime with devastating consequences for victims. When criminals obtain personally identifiable information like names, Social Security numbers, and birthdays, hackers can cause chaos on their financial and personal lives. Victims may have bank accounts drained, credit histories damaged, and possessions stolen. Some notable examples of identity theft including:

- On 22th June 2022, local newspaper Kosmo reported that Ang Siang Ping, 27, a carpenter at a furniture factory in Seberang Perai is now living in distress after claiming that his identity was stolen and misused by unknown parties for the past five years. The victim is said to have caused financial loss to a homeowner in the area, who had to bear a high electricity bill amounting to RM230,611.30 throughout that period until last March. He also received a civil court summons from Tenaga Nasional Berhad (TNB) for a bitcoin mining activity in Butterworth, amounting to RM234,747.50 around November last year. He suspects that his identity was stolen and misused, possibly due to the loss of his identification card, other documents, and cash in an incident back in 2017.

Personal Health Information: According to the Aura website, the theft of Personal Health Information (PHI) holds significant value on the Dark Web (as much as $1,000), often surpassing the worth of stolen credit card details by more than 200 times. Such theft leads to severe consequences, like hackers selling stolen PHI to other criminals, who can use it for various illicit purposes. For example:

- In October 2020, the largest criminal cyberattack in Finland was the case involving Vastaamo, a Finnish psychotherapy service provider, who reported a data breach where their patient database was hacked. Extortionists demanded 40 bitcoins (around 450,000 euros) ransom from Vastaamo to avoid publishing the stolen patient records. When the said ransom threat failed, they targeted clients directly, threatening to publish their sensitive data unless ransoms were paid. Roughly 30,000 victims received such ransom demands.

Financial loss: Once malicious actors acquire your personally identifiable information (PII), they can potentially use it to harm your credit rating and engage in financial fraud. A diminished credit score can create obstacles for a victim to obtain personal loans, secure mortgages and affect job opportunities. Furthermore, individuals perpetrating identity fraud can open new bank accounts in your name, deplete your existing accounts, and commit check fraud. For example:

- On 23rd April 2022, a man named Md Nor Izzudin Hamzah, posted on Facebook that he had fallen for the MyMaidKL scam after seeing a Facebook ad offering a Hari Raya Promotion for cleaning services. Upon chatting with the scammer, victims were directed to book through an Android app. Through the app, victims made payments on a fake online system, unknowingly sending their banking details to the attacker. As a result, the attackers conducted illegal transactions totaling over RM 18,000.

Impersonation on Social Media: Cybercriminals can exploit your digital identity for harmful activities, such as phishing for credentials from contacts, damaging your reputation with inappropriate online posts, and extorting you with sensitive photos or videos, causing emotional and financial harm.

- On 25th December 2022, Kosmo reported a viral social media feed whereby an anonymous parent revealed that their children’s Telegram was contacted by an individual impersonating to be a doctor, allegedly representing their school teachers for health examinations. The individual contacting students was suspected to have hacked into another Telegram account to mask his true identity and requested his victims to share pictures of their private parts for the purpose of health examinations.

Emotional and Mental Health Impact: A personal data breach can have a profound emotional and mental impact on victims, with recovery often taking a long time depending on the severity of an attack. Apart from reputational harm, victims may face extensive efforts and costs to mitigate the fallout. Victims may spend hours dealing with banks, replacing stolen documents, addressing criminal charges in their name, and etc. Failing to re-secure compromised information can also leave victims vulnerable to repeated attacks. The long-term consequences will be dire especially if the PII or PHI of the victim end up on the Dark Web. The information could be in circulation indefinitely, making them vulnerable to further harm.

Counting the Human Cost

Organizations can significantly enhance their cybersecurity posture by implementing a well-defined Information Security Management System (ISMS) and Business Continuity Management System (BCMS). An ISMS provides a systematic approach to managing information security risks, ensuring data confidentiality, integrity, and availability. A BCMS establishes a framework for recovering from disruptive events, minimizing downtime and ensuring critical business functions continue even during a cyber-attack.

Moreover, it is important to conduct regular security assessments— be it on the organization's processes, technology, or focusing on information security awareness training for employees. Periodical assessments help identify vulnerabilities and gaps in security, thus allowing for proactive measures to be taken. Security awareness training also empowers employees to recognize and avoid cyber threats, forming a human firewall against social engineering and phishing attacks.

By adopting a comprehensive approach that integrates technical safeguards, human-centric strategies, and continuous improvement, organizations can significantly bolster their defenses and build a more secure digital environment for everyone.

Conclusion

Cyber-attacks are not all just about numbers and statistics. The effects they bring on individuals and businesses can be devastating. When personal information is compromised, individuals face a myriad of challenges, from the fear of identity theft to the emotional distress of privacy intrusion. For businesses, the repercussions can be equally severe, often resulting in significant financial setbacks, damage to reputation, and loss of customer trust. Cyber-attacks come at a steep human cost, impacting individuals and communities in profound ways. Recognizing such human dimension is crucial for building a more secure and resilient digital future. By prioritizing both technical solutions and human well-being, we can work towards minimizing the devastating impact of cyber-attacks on our lives.

References

1. Australian Institute of Criminology. (2023). Cybercrime in Australia 2021. https://www.aic.gov.au/subject/cybercrime

2. The Global Cyber Alliance. (2023). Bystander Effect: The Human Cost of Cybercrime.

3. National Center for PTSD. (2023). Understanding PTSD. [https://www.ptsd.va.gov/understand/related/index.asp]

4. Cyberattacks & Data Breaches recent news. (n.d.). Dark Reading. http://www.darkreading.com/attacks-and-breaches/sony-data-breach-cleanup-to-cost-/$171-million/d/d-id/1097898

5. Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., & Upton, D. M. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. Journal of Cybersecurity, 4(1). https://doi.org/10.1093/cybsec/tyy006

6. CrowdStrike. (n.d.). Most Common Types of Cyber Attacks. Retrieved from https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/

7. Coursera. (n.d.). Types of Cyber Attacks. Retrieved from https://www.coursera.org/articles/types-of-cyber-attacks

8. Cisco. (n.d.). Common Cyber Attacks. Retrieved from https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html

9. Hern, A. (2023, April 4). TikTok fined in UK for data protection law breaches. The Guardian. https://www.theguardian.com/technology/2023/apr/04/tiktok-fined-uk-data-protection-law-breaches

10. Cimpanu, C. (n.d.). KFC, Pizza Hut owner discloses data breach after ransomware attack. BleepingComputer. https://www.bleepingcomputer.com/news/security/kfc-pizza-hut-owner-discloses-data-breach-after-ransomware-attack/

11. Atlassian. (n.d.). Cost of Downtime: How Much Does Downtime Cost Your Business? Retrieved from https://www.atlassian.com/incident-management/kpis/cost-of-downtime#:~:text=The%20average%20cost%20of%20downtime%20is%20%245%2C600%20per%20minute%2C%20according,company%20size%20and%20industry%20vertical

12. Office of Justice Programs. (n.d.). Identity Theft. Retrieved from https://www.ojp.gov/sites/g/files/xyckuh241/files/archives/factsheets/ojpfs_idtheft.html#:~:text=Identity%20theft%20has%20profound%20consequences,crimes%20they%20did%20not%20commit.

13. Albrecht, S. (2018, November 1). Understanding the Scope of Identity Theft. Fraud Magazine. https://www.fraud-magazine.com/article.aspx?id=4294978560

14. SelfKey. (n.d.). Data Breaches: Risks and Consequences. Retrieved from https://selfkey.org/data-breaches-risks-and-consequences/

15. Aura. (n.d.). The Dangers of Identity Theft: 12 Things You Should Know. Retrieved from https://www.aura.com/learn/dangers-of-identity-theft#12.-Your-personal-data-could-circle-on-the-Dark-Web-forever

16. CBS News. (n.d.). Protect against medical ID theft. Retrieved from https://www.cbsnews.com/news/protect-against-medical-id-theft/

17. Reuters. (2020, October 26). Tens of thousands' psychotherapy records hacked in Finland. The Guardian. https://www.theguardian.com/world/2020/oct/26/tens-of-thousands-psychotherapy-records-hacked-in-finland

18. Oxford Treatment Center. (n.d.). Stress and Substance Abuse. Retrieved from https://oxfordtreatment.com/substance-abuse/co-occurring-disorders/stress/

19. National Sleep Foundation. (n.d.). Stress and Insomnia. Retrieved from https://www.sleepfoundation.org/insomnia/stress-and-insomnia

20. Painted Brain. (n.d.). The Psychological Impact on the Lives of Cyber Attack Victims. Retrieved from https://paintedbrain.org/blog/the-psychological-impact-on-the-lives-of-cyber-attack-victims

21. Kosmo. (2022, December 25). Menyamar jadi doktor, minta gambar tak senonoh. https://www.kosmo.com.my/2022/12/25/menyamar-jadi-doktor-minta-gambar-tak-senonoh/

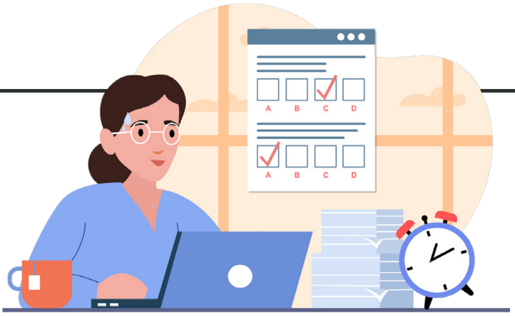
#exam development #psychometric #ISO/IEC 17024

ITEM

by:
1. Razana Md Salleh
2. Mohd Haleem Abdul Sidek
3. Ameerul Aziz Thai
4. Nur Shafiqah Nor Aztawakal

What is enemy item?

Enemy item is a psychometric term that refers to two test questions (items) which should never appear on the same test form and seen by an examinee



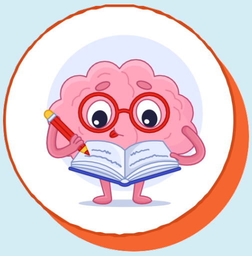
How could two items be classified as enemy item?

1. Too similar: the text of the two items are almost identical
2. One item gives away the answer to the other
3. The items are on the same topic/ answer, even if the text is different.

Why are enemy items a problem?

1. Affect content validity: Enemy items duplicate the same test scope of knowledge or competency, thereby reducing the coverage of exam content.
2. Reduced credibility: Receiving similar items may lead the examinee to be distracted and question the credibility of the examination.
3. Introduce inter-item dependency: The examinee has an increased probability of answering either correctly or incorrectly for enemy sets on the same test.
4. Reduced measurement precision: Utilizing responses to enemy items in assessing the examinee's ability could skew and affect the validity of the final scores.

Common Categories of Enemy Items



Duplicate Items

01

All item components are virtually identical. These items are true duplicates except for punctuation, notation of other trivial differences.

Duplicate Stems

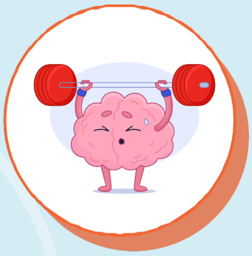
02

Items have identical stems and different options. This may\ occur when items are reproduced from item bank and not “from scratch”.

Duplicate Options

03

Items have different stems but nearly identical options. This could occur when a response option is constructed from different stems.



Duplicate Stimuli

04

Items have identical graphics, exhibits, sounds or reading passages. This could be due to making the best use of the stimuli elements.

Overlapping Content

05

Items have different phrasing of stem and/or options, but the specific concept being tested is the same. It is more difficult to detect but may not be as risky as other categories of item enemies.

Detecting Enemy Items

Enemy items are typically identified through two (2) common methods:

1 Manual

Humans review items and intentionally mark two as enemies. For example, a reviewer might identify two items covering the same concept.

2 Automated

Machine learning algorithms, such as those using natural language processing (NLP), could evaluate item similarity. However, this approach may not cover situations where items have different text but the same topic.

Summary

In summary, it is critical to identify enemy items and ensure that they do not appear together. Identifying and removing enemy items from an examination is crucial for maintaining the integrity and fairness of an assessment process.

References

1. Woo, A., & Gorham, J. (2010). Understanding the Impact of Enemy Items on Test Validity and Measurement Precision. CLEAR Exam Review, 21(1), 15-17.
2. Thompson, N. What are enemy items?. Retrieved from https://assess.com/enemy-items/

Understanding Cryptocurrency Mixing Service

By | Sarah Khadijah Taylor, Norhafizah Hashim, Akmal Suriani Bt Mohd Rakoff, Tajul Josalmin Bin Tajul Ariffin & Dharumashan A/L Bathiban

Overview

A cryptocurrency mixer refers to a service that combines a cryptocurrency fund with other cryptocurrency funds, with the intention of concealing the origin of the said fund. As a result, the process of tracing the ownership of the funds would invariably become more arduous.

Cryptocurrencies are designed to operate on logic. Since Bitcoin blockchain network is open source, anybody with the proper expertise can download it to analyze the flow of funds between wallets and potentially view the exchanges associated with any transaction. By employing mixing services, the link between wallets will be broken, making it more difficult to obtain such data and thereby erasing any relationship between the sending and receiving exchangers.

There are two types of cryptocurrencies mixers: centralized and decentralized mixers. Centralized mixers are providers that accept cryptocurrency from a user wallet and send back a different cryptocurrency for a fee. The providers usually charge 1 to 3% of fee from the total of cryptocurrency received by the user.

Decentralized mixers are peer to peer mixing service providers that pool cryptocurrencies from various users, and then send them out to the receivers. Since it is a decentralized service, it does not need a single authority to manage the service.

Users turn to mixing service to improve the secrecy and anonymity of their cryptocurrency transactions. However, the tendency of cryptocurrency mixing in masking the source and destination of transactions often links it to money laundering. Criminals also use mixing service to hide their trails from the eye of the law enforcements, particularly in the case of selling of illicit items and ransomware.

Overview Of Top 3 Cryptocurrency Mixing Services

This article delves into the top three (3) mixing services available for public use. Those are CoinJoin, Ring Signatures and CoinSwap. The following describes how each mixing service work. At the end of this section, a comparative study on the three is presented in Table 1.

CoinJoin

CoinJoin provides an extensive variety of methods for improving cryptocurrency transaction. The core idea of CoinJoin is “When you want to make a payment, find someone else who also wants to make a payment and make a joint payment instead”.

For example, as illustrated in Figure 1, there are two transactions: one is from Alice to Bob, and another is from Carlos to David. These two independent transactions can be combined into one CoinJoin transaction while inputs and outputs are unchanged. The resulting joint transaction mixes the link between inputs and outputs, so that the exact direction of data flow will be kept unknown to the other peers.

This method ensures that no node can learn about transaction linkages, while offering flawless compatibility with blockchains such as Bitcoin. CoinJoin implementations can be either centralized or decentralized depending on how the mixing process is executed. Mixing transactions in decentralized CoinJoin are created and carried out through direct user interaction. In centralized CoinJoin, the mixing process is managed by a single entity or service.

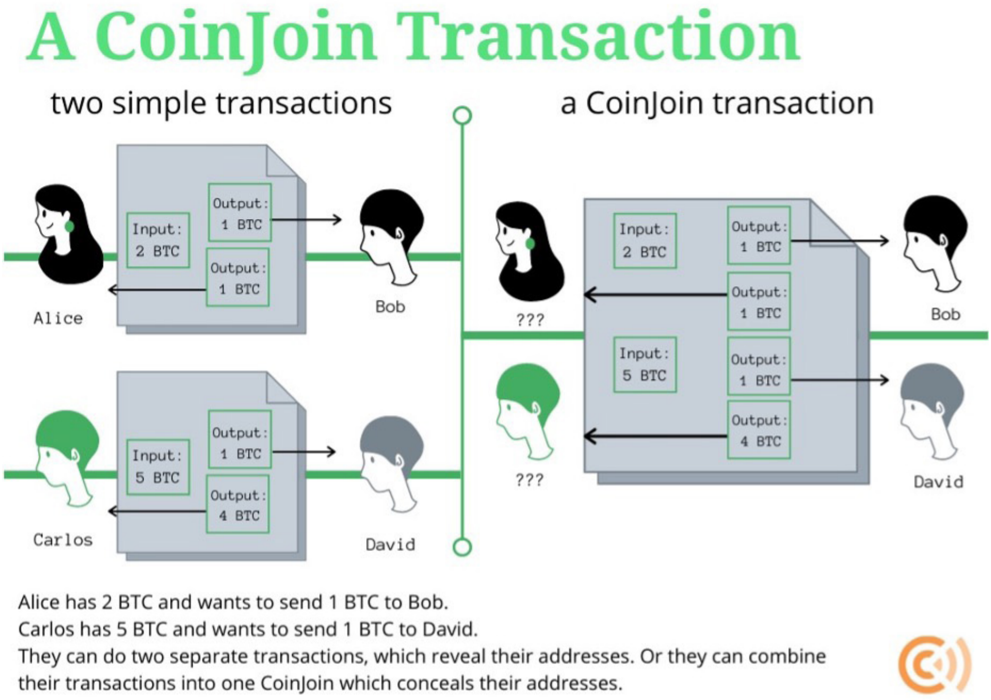

A CoinJoin Transaction
two simple transactions
a CoinJoin transaction
Input: 2 BTC
Output: 1 BTC
Output: 1 BTC
Alice
Bob
Input: 5 BTC
Output: 1 BTC
Output: 4 BTC
Carlos
David
???
???
Alice has 2 BTC and wants to send 1 BTC to Bob.
Carlos has 5 BTC and wants to send 1 BTC to David.
They can do two separate transactions, which reveal their addresses. Or they can combine their transactions into one CoinJoin which conceals their addresses.

Figure 1. CoinJoin's core idea

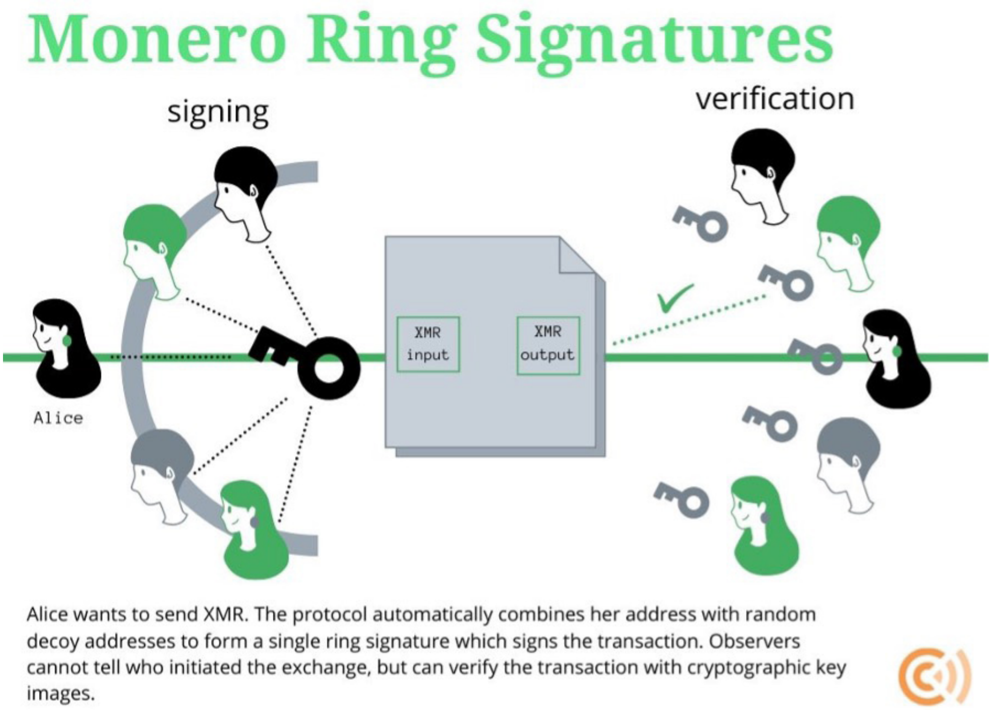
Source: https://www.coincenter.org/

Ring Signatures

Ring signatures, initially introduced by Rivest et al. in 2001, represent a cryptographic innovation aimed at preserving anonymity in digital transactions. The core concept of ring signatures revolves around the idea of allowing a user, who is part of a predetermined set, to sign a message on behalf of the entire group without revealing the identity of the actual signer.

A participant selects a set of users, including themselves, forming a ring structure. Each participant possesses a public key derived from a standard signature scheme. When a participant initiates a transaction, they sign the message using their private key along with the public keys of all participants in the ring. Consequently, the resulting signature indicates that one of the set members has signed the message, but the true signer remains unidentifiable to external observers. Figure 2 shows the core concept of ring signatures. One variant of ring signatures, known as traceable ring signatures, incorporates additional features to detect potential fraud or misuse. With traceable ring signatures, each signature carries a unique tag consisting of public keys from the participant set and a specific identifier. This enables verifiers to ascertain if multiple signatures originate from the same user, thus enhancing the traceability of transactions while preserving anonymity.

Despite their effectiveness in enhancing privacy, ring signatures pose certain limitations. Transactions utilizing ring signatures tend to be larger in size, leading to increased storage requirements for blockchain records. Additionally, the scalability of ring signatures is constrained by the direct relationship between signature size and participant count, which restricts the number of foreign outputs per transaction.



Alice wants to send XMR. The protocol automatically combines her address with random decoy addresses to form a single ring signature which signs the transaction. Observers cannot tell who initiated the exchange, but can verify the transaction with cryptographic key images.

Figure 2. The ‘operation’ of Ring Signatures

Source: https://www.coincenter.org/

CoinSwap

CoinSwap is a decentralized cryptocurrency exchange protocol designed to facilitate peer-to-peer trading without the need for intermediaries. CoinSwap is an entity that allows users to swap crypto assets for other tokens, either on the same or different blockchain. One of its most distinct features is the lack of an account opening or identification verification requirement for users. Users can simply connect their wallet, send crypto to the service, and receive converted assets back into a predetermined wallet address. For the privilege of remaining anonymous, most coin swaps charge higher commission on average than typical compliant exchanges.

The protocol operates by leveraging multi-signature schemes, specifically 2-of-2 multi-signature addresses, to enable trustless transactions between users. In a CoinSwap transaction, both parties cryptographically sign the transaction, ensuring that neither can manipulate it unilaterally. This approach enhances security and prevents fraudulent activity during the exchange process. Unlike traditional cryptocurrency exchanges or decentralized exchanges (DEXs), CoinSwap transactions occur directly between users' wallets, without relying on a central platform. This decentralized nature of CoinSwap eliminates the need for third-party custody of funds, reducing counterparty risk and enhancing user control over their assets.

One notable aspect of CoinSwap is its emphasis on privacy. The system obscures the relationship between the exchanging parties by segmenting transactions into several steps and using intermediary CoinSwap addresses. While improving anonymity, this multi-stage procedure makes it more difficult to trace transactions back to their original parties.

Feature	CoinJoin	CoinSwap	Ring Signatures
Anonymity Level	Moderate	High	High
Fees	Variable (depends on service)	Variable (depends on service)	Variable (depends on service)

Ease of Use	Moderate (requires participation in mix)	Moderate (requires coordination with counterparty)	Moderate (requires understanding of cryptography)
Supported Cryptocurrencies	Primarily Bitcoin	Primarily Bitcoin	Various (depending on implementation)
Decentralization	Can be decentralized (depends on service)	Can be decentralized (depends on implementation)	Can be decentralized (depends on implementation)
Trust Requirements	Minimal trust required in service	Minimal trust required in counterparty	Minimal trust required in protocol
Transaction Size	Larger (due to combining multiple inputs/outputs)	Like standard transactions	Standard size (with potential for larger rings)
Linkability	Potential for linkability between transactions	Low (transactions are swapped directly)	Low (signer remains anonymous within ring)
Security Features	Relies on encryption and transaction obfuscation	Relies on direct coin swap	Relies on cryptographic anonymity

Table 1. Comparison between CoinJoin, CoinSwap, and Ring Signature

Conclusion

Mixing services utilize advanced cryptographic techniques to anonymize cryptocurrency transactions for the purpose of providing users with more control over their financial security.

However, it is crucial to recognize that mixing services are subjected to abuse in criminal operations and tax evasion. At the time that this article is written, there are no explicit laws prohibiting the use of mixing services. Whether utilized by individuals seeking to protect their privacy or those navigating oppressive regimes, mixing services serve as a crucial tool for preserving financial autonomy. While acknowledging the associated risks, it is essential to view mixing services within the broader context of privacy rights and individual autonomy in the digital age.

References

1. What Is a Bitcoin Mixer? Centralized vs. Decentralized Mixers, Bitkan, Seth Rowden , https://bitkan.com/learn/what-is-a-bitcoin-mixer-centralized-vs-decentralized-mixers-10395, viewed on 22 April 2024

2. Bitcoin Mixers: Centralized Vs. Decentralized Mixers, The Cryptonomist, https://en.cryptonomist.ch/2020/08/15/bitcoin-mixers-centralized-decentralized/, viewed on 22 April 2024

3. Evaluating Tooling and Methodology when Analysing Bitcoin Mixing Services After Forensic Seizure, Edward Henry Young et al, International Conference on Data Analytics for Business and Industry, 2021

Innovations In Video Compression For Efficient Storage And Analysis

By | Mohammad Azree Bin Yahaya, Muhamad Zuhairi Bin Abdullah, Muhammad Faridzul Bin Sukarni, Ummu Ruzanna Binti Abdul Razak & Muhammad Afrizal Bin Abd Ghani

Significant innovations and technologies have been achieved in video compression for efficient storage and analysis. Innovations include novel compression algorithms and integration with processing techniques, alongside AI-powered approaches such as deep neural networks. The proposed algorithm achieves a notable compression rate of 50% compared to existing methodologies, particularly excelling in big data surveillance systems and real-time applications. Key features of the methodology encompass feature extraction, advanced encoding schemes, automated segmentation, and tailored bit allocation strategies. Results indicate substantial bit rate savings, outperformance of existing models, and high reconstruction quality, positioning the algorithm as a competitive solution for diverse multimedia applications. In conclusion, the proposed algorithm demonstrates promising advancements in video compression technology, offering efficient data handling, enhanced analysis capabilities, and significant reductions in storage requirements.

Introduction

Innovations in video compression was initiated to address the need for efficient storage and analysis of video data (Mazumdar et al., 2019). These advancements aim to improve the performance in compression algorithms and enable faster processing of compressed data. One approach is the development of novel compression algorithms that eliminate redundancies in video inputs, resulting in better compression rates. Another approach is the integration of compression methods with processing techniques, allowing for efficient analysis and visualization of compressed images and video. Additionally, artificial intelligence (AI)-powered techniques, such as deep neural networks (DNNs), have shown promising potential in enhancing the efficiency of video compression systems, particularly in preprocessing, coding, and postprocessing stages (Kumar et al., 2022). These innovations in video compression contribute to maximizing end-user quality of experience (QoE); while optimizing resource utilization and facilitating the extraction of meaningful information from video data.

The proposed algorithm made sufficient modification in the traditional run length coding algorithm by encoding the frames and removing the redundancies using texture information similarity in the surveillance video, thereby achieving a better compression rate of 50% for a huge dataset of surveillance videos over existing methodologies. An illustration on importance map is created to guide bit allocation to areas that are important for object detection and enables bit rate savings of 7% or more compared to default HEVC, at the equivalent object detection rate. Analysis of video compression based on block SVD Algorithm and can analysis to reduce the time complexity of the video compression process based on blocks SVD Algorithm. A simple and efficient video compression framework only focuses on conditional entropy model between frames that outperforms H.265 and other deep learning baselines in MS-SSIM on higher bitrate UVG video and against all video codecs on lower frame rates.

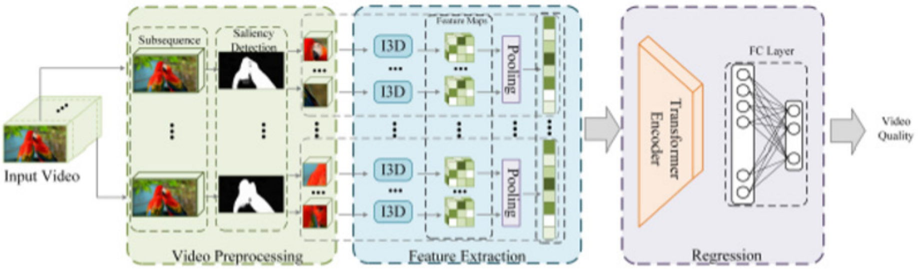


Figure1 : Illustration of the proposed pixel-level DT compression framework. (Wang et al., 2022)

Methodology

The methodology is a multi-faceted approach aimed at efficient video processing and analysis. Initially, feature information extraction techniques are employed to identify and isolate pertinent image features, thereby facilitating the elimination of redundant frames within the video file. Subsequently, frames are encoded utilizing an advanced run-length coding scheme, optimizing compression while preserving essential visual data. Algorithms are then used to reconstruct reduced image sequences from the compressed video, ensuring minimal loss of critical information (Shania Anderson, 2023).

Furthermore, automated segmentation algorithms are developed to detect highlights within the reduced images, enhancing content intelligence and retrieval. To enable object detection, a tailored bit allocation and rate control strategy is used, guided by an importance map crafted to prioritize regions crucial for object detection tasks. Finally, each frame undergoes thorough analysis to identify image features and ascertain semantic state changes, facilitating comprehensive understanding and interpretation of video content (Shania Anderson, 2023). This methodology integrates various techniques to enable efficient video processing, compression, and analysis, catering to diverse applications ranging from content delivery to object detection systems.

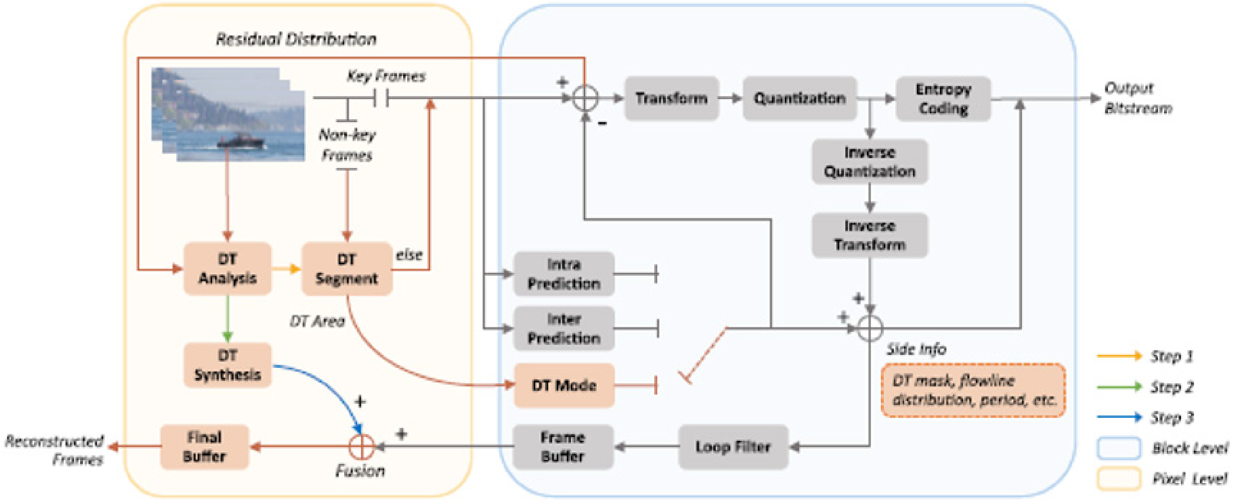


Figure 2 : The proposed STFEE Framework. (Lin et al. 2023)

Result

The results of the proposed algorithm are notable, with an impressive compression rate of 50%, indicating its efficacy in video data size reduction while preserving essential visual information (Choi & Bajic, 2017). It is particularly noteworthy that it performs better than existing models in big data surveillance systems, indicating its suitability for applications that require efficient data handling and analysis. The algorithms developed for reconstructing reduced images from compressed video showcase versatile approach across different domains. A novel compression scheme proposed for visualizing compressed 3D scalar data demonstrates its potential for multidimensional data representation. Furthermore, the 7% bit rate savings or more compared to default HEVC highlight the algorithm's efficiency in data transmission (Prakash, 2019). Equally significant is the equivalent object detection rate achieved with the proposed method, underscoring its applicability in tasks requiring accurate detection capabilities. Additionally, the video compression device's high transmission efficiency enhances its utility for real-time video streaming applications. The capability to store video data for extended periods without necessitating equipment updates indicates the algorithm's practicality in long-term data archival scenarios. In fact, the Compression Algorithm for Real-time Processing (CARP) outperforms state-of-the-art compression methods across various image types, offering high reconstruction quality and computational scalability, further affirming its potential for widespread adoption in diverse multimedia applications.

Conclusion

To sum up, the proposed algorithm stands out through a commendable 50% compression rate when benchmarked against existing methodologies, suggesting its potential for substantial data reduction across various applications. The efficacy in big data surveillance systems and real-time applications underscores its suitability for demanding scenarios requiring efficient data handling. Moreover, the algorithm enables efficient processing of compressed images and video, indicating its versatility across multimedia domains. The joint design approach integrating compression algorithms and processing methods demonstrates the possibility of significant gains in overall system performance. Most notably, the tailored bit allocation and rate control strategy geared towards object detection facilitate a 7% bit rate savings or more compared to default HEVC, highlighting its efficacy in enhancing compression efficiency for specific tasks (Lin et al., 2020). The simplicity of the architecture, coupled with modeling conditional entropy, proves competitive against other established video compression methods. Additionally, the proposed extension introduces further bitrate savings without compromising decoding speed, enhancing the algorithm's practicality in real-world applications. Impressively, the proposed compression method achieves over 96% space savings, surpassing traditional methods such as MySQL in terms of efficiency. This paper addresses the critical issue of low delay in video compression, providing a solution that aligns with contemporary demands for real-time processing. Last but not least, the comprehensive benchmarking against HEVC and V9 techniques further validates the effectiveness of the proposed approach, offering insights into its performance and potential advancements in video compression technology.

References

1. Choi, H., & Bajic, I. V. (2017). High efficiency compression for object detection. http://arxiv.org/abs/1710.11151

2. Kumar, K. S., Madhavi, P. B., & Janaki, K. (2022). An Efficient Video Compression Framework using Deep Convolutional Neural Networks (DCNN). Journal of Computer Science, 18(7), 589–598. https://doi.org/10.3844/jcssp.2022.589.598

3. Lin, W., He, X., Dai, W., See, J., Shinde, T., Xiong, H., & Duan, L. (2020). Key-Point Sequence Lossless Compression for Intelligent Video Analysis. https://doi.org/10.1109/MMUL.2020.2990863

4. Mazumdar, A., Haynes, B., Balazinska, M., Ceze, L., Cheung, A., & Oskin, M. (2019). Vignette: Perceptual Compression for Video Storage and Processing Systems. http://arxiv.org/abs/1902.01372

5. Prakash, V. R. (2019). An Enhanced Coding Algorithm for Efficient Video Coding. Journal of the

6. Institute of Electronics and Computer, 1(1), 28–38. https://doi.org/10.33969/JIEC.2019.11004

7. Shania Anderson, L. (2023). EEcient Storage and Analysis of Videos through Motion-Based Frame Removal Efficient Storage and Analysis of Videos through Motion-Based Frame Removal. https://doi.org/10.21203/rs.3.rs-3035803/v3

‘Driving’ Data: Navigating The Forensic Landscape Of Car Infotainment Systems

By | Nurul Husna Binti Mohd Nor Hazalin, Aisyah Binti Mohamad Hafizul, Sharifah Nurul Asyikin Binti Syed Abdullah, Mohd Zabri Adil Bin Talib & Fakhrul Afiq Bin Abd Aziz

Car infotainment systems have become an essential component of today’s driving experience. They offer a variety of features that cater to the diverse needs of modern drivers. Whether you are a music enthusiast looking to stream your favourite tunes, a tech-savvy individual requiring real-time traffic updates, or a family on a road trip seeking entertainment for the kids, a car infotainment system is designed to meet all of their needs.

Car infotainment systems offer both entertainment and connectivity in addition to recording and storing large amounts of data. This data includes navigation history, media preferences, and vehicle performance metrics, among other things. The collection of this information can improve future driving experience and enhance vehicle functionality. In our exploration of car infotainment, we will delve into how data is captured and its implications for privacy, security, and the future of automotive technology.

Infotainment is a combination of two key aspects that is ‘information’ and ‘entertainment,’ and refers to the sleek display (or displays) found on most modern cars’ dashboards. An infotainment system usually comprises a touchscreen or display installed on the dashboard of a car. In recent years, these systems have grown in size, with some even larger than a tablet at home.

The features in a car are directly related to the price and specifications of the car. The more expensive and luxurious models come with better processing power, digital services, and applications. However, even the most basic car models have an infotainment system that operates the radio, satellite navigation (if specified), and Bluetooth connectivity to smartphones or other device. Additionally, they provide access to essential vehicle information like service intervals and tire pressures.

As cars become more digitized, internet connectivity via onboard SIM cards will enable drivers to access live parking info, weather forecasts, and more. Even the most basic in-car entertainment systems now have a Bluetooth connection to a phone, allowing safer hands-free phone calls and streaming of media services.

Many modern car infotainment systems go beyond just simply connecting with devices. They also support **Apple CarPlay** and **Android Auto**, which opens up a whole new world in smartphone connectivity.

CarPlay seamlessly integrates an iPhone with the vehicle's infotainment system, allowing access to core iPhone functions directly through the car's built-in displays and controls.

The system mirrors a simplified iOS interface onto your car's dashboard display, providing access to key apps such as Phone, Messages, Maps/Navigation (including third-party options like Waze or Google Maps), Music, Podcasts, and more. These interfaces are optimized for in-vehicle use, with large touchscreen familiar app icons easily tapped or controlled via steering wheel buttons. Such thoughtful design minimizes distractions while driving.

To use Android Auto, one will need an Android device running Android 5.0 or higher. To get started, connect Android phone to the car's data USB port using a USB cable, and the Android Auto app should launch automatically on the phone. This is similar to using an iPhone, but with Android devices instead.

Smartphone integration systems like Android Auto and CarPlay are bridging the gap between personal tech and vehicle infotainment functions. The goal is to reduce distractions by adapting familiar mobile experiences for in-car use.

Infotainment Insights: Unveiling the Data Universe of Car Entertainment Systems

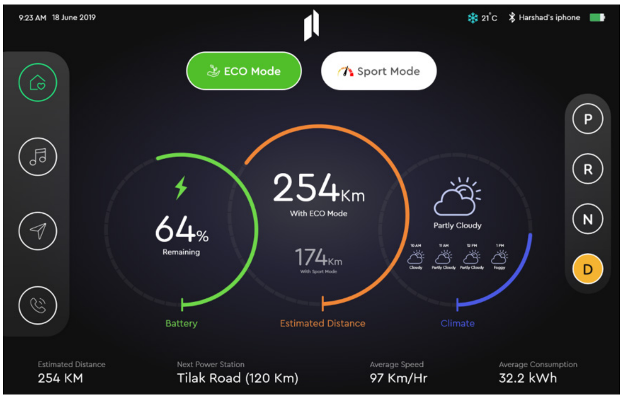
In today's world of connected vehicles, a car's infotainment system is more than just a screen for music and navigation. It's a treasure trove of data, capturing information about one's driving habits, preferences, and even vehicle's performance. From the moment engine starts to the time destination is reached, the infotainment system is silently collecting data, painting a detailed picture of the car journey.

Let's take a closer look at the types of data that a car's infotainment system could potentially extract:

1. User Interaction Data

- **Navigation History:** The infotainment system's navigation history records where one has been to, the routes taken and destinations visited.
- **Media Usage:** Music tastes and preferences are revealed through the songs, playlists, and radio stations tuned in during drives.
- **Phone Calls and Messages:** The system may log phone calls and text messages, providing insights into communication patterns.
- **Voice Commands:** Voice commands are likely being recorded and stored.

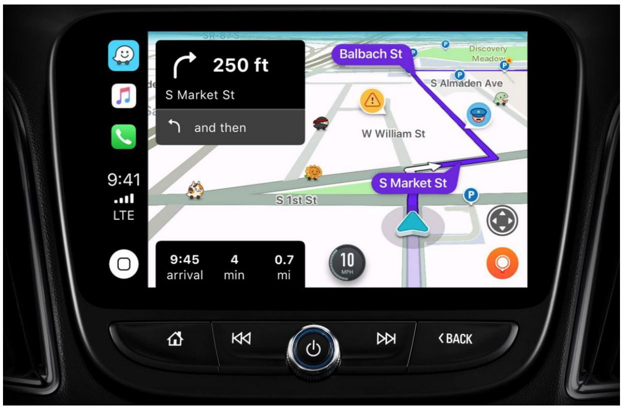
2. Vehicle Performance Data



- **Speed and RPM:** The car's infotainment system records how fast the car is going and how hard its engine has been working.
- **Fuel Consumption:** It can track the vehicle's fuel efficiency, giving drivers a glimpse into their driving habits' impact on gas mileage.

- **Maintenance Alerts:** The infotainment system can also alert when it is time for an oil change or to check tire pressure, ensuring the car stays in tip-top shape.

3. Location Data



- **GPS Coordinates:** The car's location is constantly tracked, leaving a digital 'breadcrumb' trail along the routes.
- **Geofencing:** The infotainment system can detect when one enters or leaves predefined geographical areas, such as home or workplace.

4. Entertainment Preferences

- **Favourite Stations and Playlists:** The infotainment system knows one's go-to music choices, helping it curate a personalized listening experience.
- **Customization Settings:** From display brightness to theme and language preferences, the infotainment system adapts to a driver unique tastes.

5. System Logs and Diagnostics

- **Error Codes:** A vehicle's system records will any issues or malfunctions, thereby helping mechanics diagnose and fix problems.
- **Software Updates:** The infotainment system tracks software versions and updates, thus ensuring the car's technology stays current.

6. Event Data

- **Collision Data:** In the unfortunate event of an accident, the infotainment system can capture details about impact forces, airbag deployment, and crash severity.
- **Driving Behaviour:** The acceleration, braking, and steering patterns of the vehicle are all monitored, providing insights into driving style.

7. Connectivity Data

- **Bluetooth Pairings:** The car records devices which have been paired with its infotainment system, such as smartphones and headphones.
- **Wi-Fi Networks:** The system can monitor and track the car's wireless network connections, providing insights into a driver's connectivity habits.

This list of possible information can be very helpful for personalization, diagnostics, forensics, and safety purposes. As vehicles become increasingly connected, it is essential to balance leveraging the power of data and protecting personal information.

Unlocking the Secrets of Automotive Infotainment Systems

In modern connected vehicles, infotainment systems serve as central hubs that store various data, including user preferences, multimedia files, diagnostic information, and navigation logs.

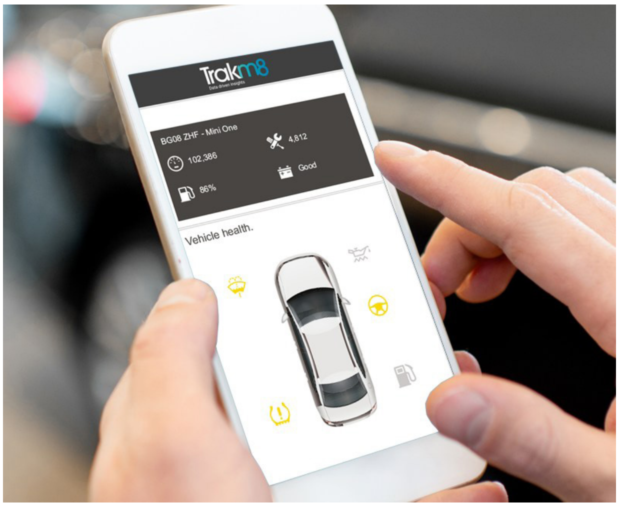
However, accessing and extracting this data can be challenging, requiring specialized tools and techniques. For automotive enthusiasts, researchers, and professionals alike, retrieving data from these systems opens up a world of possibilities, from customizing user experiences to conducting forensic investigations.

But where should one begin? Here's a closer look at some of the tools and methods available to unlock the secrets of automotive infotainment systems.

Professional Diagnostic Tools

Professional-grade diagnostic tools, such as scanners and code readers, are at the forefront of data extraction. These powerful devices communicate directly with the vehicle's onboard diagnostics (OBD) port, granting access to the infotainment system's control modules. With the right software and hardware configurations, technicians can read and clear diagnostic trouble codes and delve into a treasure trove of data parameters.

In-Vehicle App Monitoring

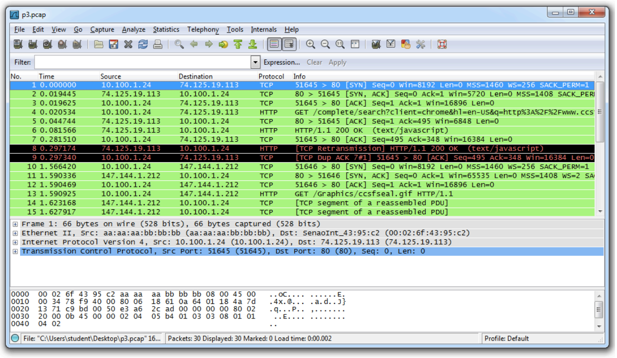


Many modern infotainment systems allow for installation of third-party applications or software monitoring tools. These specialized programs can be invaluable for monitoring and logging various data streams, including user interactions, system events, and data traffic. By capturing this information in real-time, analysts can gain valuable insights into the system's inner workings.

Forensic Data Extraction Tools

In digital forensics, specialized tools like BERLA IVE, Magnet AXIOM, XRY and UFED have become indispensable for acquiring and analyzing data from embedded devices, including automotive infotainment systems. These powerful tools often require physical access to the device or system and may employ advanced techniques such as chip-off or JTAG (Joint Test Action Group) methods to extract data.

Network Sniffing and Packet Capture


p3.pcap
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply

```
No.  Time      Source          Destination     Protocol Info
   1 0.000000  10.100.1.24     74.125.19.113   TCP      51645 > 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
   2 0.019445  74.125.19.113   10.100.1.24     TCP      80 > 51645 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1408 SACK_PERM
   3 0.019625  10.100.1.24     74.125.19.113   TCP      51645 > 80 [ACK] Seq=1 Ack=1 Win=16896 Len=0
   4 0.020534  10.100.1.24     74.125.19.113   HTTP     GET /complete/search?client=chrome&hl=en-US&q=http%3A%2F%2Fwww.ccs
   5 0.044744  74.125.19.113   10.100.1.24     TCP      80 > 51645 [ACK] Seq=1 Ack=495 Win=6848 Len=0
   6 0.081566  74.125.19.113   10.100.1.24     HTTP     HTTP/1.1 200 OK  (text/javascript)
   7 0.281510  10.100.1.24     74.125.19.113   TCP      51645 > 80 [ACK] Seq=495 Ack=348 Win=16384 Len=0
   8 0.297174  74.125.19.113   10.100.1.24     HTTP     [TCP Retransmission] HTTP/1.1 200 OK  (text/javascript)
   9 0.297340  10.100.1.24     74.125.19.113   TCP      [TCP Dup ACK 7#1] 51645 > 80 [ACK] Seq=495 Ack=348 Win=16384 Len=0
  10 1.566420  10.100.1.24     147.144.1.212   TCP      51646 > 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
  11 1.590336  147.144.1.212   10.100.1.24     TCP      80 > 51646 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1408 WS=2 SA
  12 1.590469  10.100.1.24     147.144.1.212   TCP      51646 > 80 [ACK] Seq=1 Ack=1 Win=16896 Len=0
  13 1.590925  10.100.1.24     147.144.1.212   HTTP     GET /Graphics/ccsfseal.gif HTTP/1.1
  14 1.623168  147.144.1.212   10.100.1.24     TCP      [TCP segment of a reassembled PDU]
  15 1.627917  147.144.1.212   10.100.1.24     TCP      [TCP segment of a reassembled PDU]

⊞ Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
⊞ Ethernet II, Src: aa:aa:aa:bb:bb:bb (aa:aa:aa:bb:bb:bb), Dst: SenaoInt_43:95:c2 (00:02:6f:43:95:c2)
⊞ Internet Protocol Version 4, Src: 10.100.1.24 (10.100.1.24), Dst: 74.125.19.113 (74.125.19.113)
⊞ Transmission Control Protocol, Src Port: 51645 (51645), Dst Port: 80 (80), Seq: 0, Len: 0

0000  00 02 6f 43 95 c2 aa aa  aa bb bb bb 08 00 45 00   ..oC.... ......E.
0010  00 34 78 f9 40 00 80 06  18 61 0a 64 01 18 4a 7d   .4x.@... .a.d..J}
0020  13 71 c9 bd 00 50 e3 a6  2c ad 00 00 00 00 80 02   .q...P.. ,.......
0030  20 00 0b 45 00 00 02 04  05 b4 01 03 03 08 01 01    ..E.... ........
0040  04 02                                              ..

File: "C:\Users\student\Desktop\p3.pcap" 16... | Packets: 30 Displayed: 30 Marked: 0 Load time: 0:00.002 | Profile: Default
```

Infotainment systems communicate over various in-vehicle networks, such as CAN (Controller Area Network) and Ethernet. Automotive network tools can extract and analyze valuable data by tapping into these networks and capturing network traffic using sniffing tools like Wireshark or commercial ones.

Secure Data Removal or Acquisition

For vehicles with removable storage media such as SD cards or USB drives used by the infotainment system, secure data removal or acquisition tools can be employed to copy or extract data from these media. This approach can be particularly useful when physical access to the infotainment system itself is limited.

Reverse Engineering and Decompilation

In some cases, traditional methods may not suffice, and more advanced techniques like reverse engineering and decompilation may be required. By decompiling software or firmware from the infotainment system, researchers can gain insights into data structures and extract specific data elements that would otherwise be inaccessible.

As the automotive industry continues to evolve, the importance of understanding and accessing infotainment system data will only grow. Whether it is a hobbyist seeking to customize vehicle's user experience or a professional investigating a cyber incident, having the right tools and techniques at one's disposal can help unlock a wealth of information hidden within these sophisticated systems.

References

1. Bronstein, M. (2019, May 8). Bringing you the next-generation Google Assistant. Google. https://blog.google/products/assistant/next-generation-google-assistant-io/

2. Driver Management Software System | Verizon Connect. (n.d.). Verizon Connect. https://www.verizonconnect.com/features/driver-management-software/

3. IVE Software V4.7 release – Berla.co. (n.d.). https://berla.co/ive-software-v4-7-release/

4. Leanse, A. (2024, April 10). How does Apple CarPlay work and what is it? A quick user's guide. MotorTrend. https://www.motortrend.com/features/how-apple-carplay-works/

5. Mercedes-Benz B250E W242 — Open Vehicles documentation. (n.d.). https://docs.openvehicles.com/en/latest/components/vehicle_mercedesb250e/docs/index.html

6. Stegner, B. (2021, May 18). What is Apple CarPlay? How does it work? A quick guide. MUO. https://www.makeuseof.com/tag/apple-carplay-guide/

7. Vehicle Infotainment Digital Forensics | Envista Forensics. (n.d.). https://www.envistaforensics.com/services/digital-forensics-services/vehicle-infotainment-forensics/

8. Vehicle infotainment forensics: It's about more than accidents | Envista Forensics. (n.d.). https://www.envistaforensics.com/knowledge-center/insights/articles/vehicle-infotainment-forensics-it-s-about-more-than-accidents/#:~:text=The%20data%20contained%20in%20the%20infotainment%20system%20falls,vehicle%20event%20data%2C%20navigation%20data%2C%20and%20user%20data.

Google Primary Device: The Approach To Google Email Account Preservation

By | Rasyid Redha Mohd Tahir, Muhammad Iskandar Shah Bin Abdul Aziz, Areef Aiman Bin Zainudin, Jayhanraaj A/L Jeeva & Shawn Slyvester A/L Damotharam

Google has implemented a security feature to authenticate user identity through devices. When the first responder tries to gain access and examine the Google email account on seized devices, the device will automatically send an identity verification request to all devices that are sync with that Google account, including the primary device that was used to sync with the account. It becomes an issue when the primary device is inaccessible or lost.

Introduction

It started with a situation where I had to change my mobile phone after my old one became unusable. When I tried to access my Google account, I couldn't log in because I needed to verify my identity through the old phone which was no longer usable. A solution to this problem has been obtained, but could this issue be related to digital forensics?

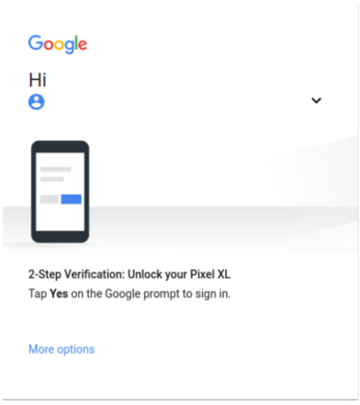
Digital forensics involves the collection, preservation, examination, and analysis of digital evidence to uncover facts for legal purposes. This could involve investigating cybercrimes, analysing digital devices for evidence in legal cases, or examining digital records for compliance purposes. According to *Ogunseyi and Adedayo (2023)*, digital forensics look for evidence on computers and other digital devices in order to assist in the investigation of a criminal activity. Email is one of the crucial digital evidence in aiding investigations into an incident or crime. Digital forensics specialists employ various tools, techniques, and methodologies to extract and analyse data while preserving its integrity to ensure its admissibility in court. Digital forensic experts may analyse email headers, metadata, attachments, and content to gather evidence relevant to a case. This could involve tracing the origin of emails, identifying senders and recipients, or examining email content for signs of tampering or forgery.

In a case study on email analysis, *Baroto and Prasetyo (2020)* stated that email metadata is very helpful for investigations as it can understand the inquiry, locate direct proof, and reveal the fraudster's objective.

According to *Altulaihan et. al (2023)*, mail security is the process of guarding email correspondence and accounts against loss, compromise, and illegal access. Regarding digital forensic practices related to email preservation, Google has established a feature that verifies user identity through a primary device. The primary device is restricted to mobile phones and tablets. Although a Google account does not have a limit on the number of devices used for logging in, the primary device is designated to authenticate a user's identity. To authenticate logins from other devices being used for the first time, an authentication email from the primary device needs to be executed.

We need to understand that the setting of the primary device is limited to only one device. Although Google offers comprehensive security features, this will result in different implications for users. If damage or loss occurs to the device, it will pose difficulties for email recovery.

In the context of digital forensics, the first responder needs to examine, maintain, and analyze emails to complete the process of an investigation. Before proceeding with such tasks, they need to log into the email account with the provided credentials. The security feature of identity verification through devices offered by Google must be taken into consideration to facilitate the investigation process.



2-Step Verification: Unlock your Pixel XL

Tap **Yes** on the Google prompt to sign in.

Picture 1. The request from google to verify the user's identity via primary phone.

There could be a situation where during a raiding operation, the device cannot be logged in because the account needs to be verified by the primary device which is not available in the vicinity of the incident. This will make it difficult for officers to conduct preservation and examination on the email account.

What needs to be done?

1. Determine the primary device

The main consideration is that officers need to identify the primary device used to verify the user's identity. If officers log in using the primary device, it will facilitate their access to the relevant email account.

2. Retrieve the device that has accessed the Google account

When officers cannot identify the primary device that verifies a user's identity, they need to first find the device that previously accessed the relevant Google account. Officers should log in with the device that has been used for login, using the same Internet network and usual location to access. This is to prevent Google from suspecting unusual activity from that account, which could lead to restrictions in access.

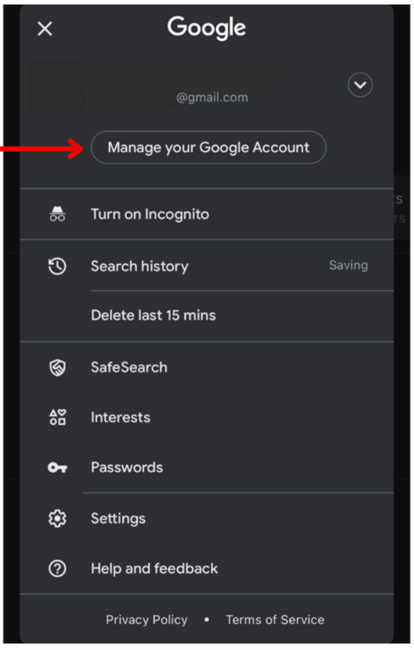
3. Log in back for a while

When officers attempt to access the email account, there is also a possibility that login attempts will be made several times and user identity verification through the primary device will be prompted. If verification notices from the primary device have been issued multiple times, officers should stop logging in again. It is recommended to log in again a week later.

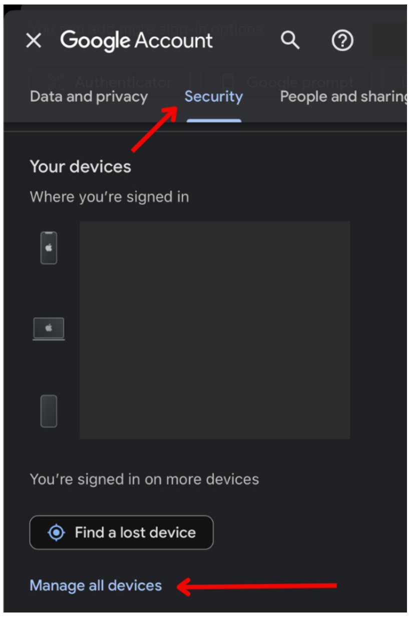
It is important to log in carefully to prevent Google from suspecting unusual activity from the account, which could lead to restrictions on accessing it.

Takeover Process of Primary Device

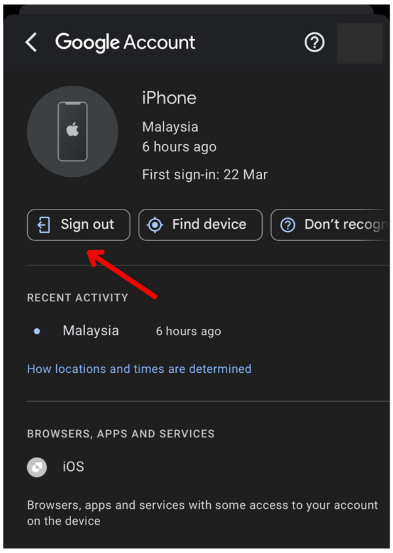
Suppose that the first responder can access the Google account and they want to change the primary device to an existing one. The first thing to do is to go to 'Manage your Google Account'.



Then, go to the 'Security' section, which will lead to 'Manage all devices'.



In this section, officers can see a list of devices used to access this Google account. Typically, these devices (which include mobile phones and tablets) are a possible primary device. It is recommended to record all these devices and remove them from the respective Google account.



iPhone

Malaysia

6 hours ago

First sign-in: 22 Mar

RECENT ACTIVITY

Malaysia 6 hours ago

How locations and times are determined

BROWSERS, APPS AND SERVICES

iOS

Browsers, apps and services with some access to your account on the device

Removing existing devices from this Google account makes it easier for officers to take over the account. Additionally, officers can use the confiscated mobile phone as the primary device since it was not initially set as the primary device. By taking over the primary device, officers can identify other devices used to access this account to assist in the investigation.

Reference

1. Altulaihan, E., Alismail, A., Hafizur Rahman, M. M., & Ibrahim, A. A. (2023). Email Security Issues, Tools, and Techniques Used in Investigation. Sustainability, 15(13), 10612.

2. Ogunseyi, T. B., & Adedayo, O. M. (2023). Cryptographic Techniques for Data Privacy in Digital Forensics. IEEE Access.

Navigating Data Breaches In Malaysian Landscape: Insights From Digital Forensics

By | Abdul Wafi bin Abdul Rahman, Nor Salwani binti Ja'afar, Hanania Aida binti Mohd Hilmi, Muhammad Nooraiman bin Noorashid & Mohd Izuan Effenddy bin Yusof

In today's technology driven world, personal data is stored across multiple locations which are exposed to data breach, posing significant risks to organizations and individuals alike. A data breach occurs when unauthorized individuals gain access to sensitive information, leading to potential theft, exposure, or misuse of data. The consequences of a data breach can be severe, ranging from financial losses and reputational damage to legal and regulatory penalties. To effectively respond to and mitigate the impact of data breaches, digital forensics plays a crucial role in uncovering facts, identifying perpetrators, and strengthening cybersecurity measures. This article examines the critical insights offered by digital forensics professionals in navigating data breaches, highlighting key strategies, best practices, and case studies to safeguard digital assets and enhance incident response capabilities.

Growing Threat of Data Breaches

In recent years, data breaches have become increasingly common and sophisticated, targeting organizations of all sizes across various industries. Based on a recent CyberSecurity Malaysia report during the first half of the year, the government sector suffered the highest number of data breaches, while telecoms industry had faced the largest amount of data leak. The telecoms industry faced the largest amount of data leaks during the first half of the year. On the volume of data compromised, a surprisingly large amount of 842.84GB was compromised, the biggest portion of which belonged to the telecommunications industry (424.92GB), followed by the banking and IT sectors (62.46GB), government sectors (291.49GB), and others (49.37GB).

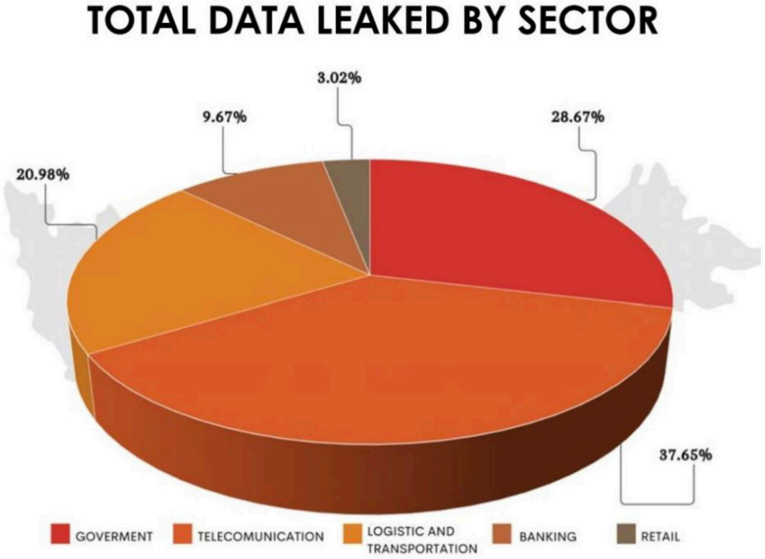


Figure 1: Total Data Leaked by Sector

The most vulnerable sectors are government, telecommunication, logistic and transportation and banking. Based on the national cybersecurity specialist agency under the Digital Ministry, these sectors are at high risk of cyber-attacks due to vulnerable software, weak access control, data exposure and other critical issues (Angelin Yeoh, 2023).

According to IBM Security's **'Cost of a Data Breach Report 2021'**, the average global cost of a data breach reached $4.24 million, which took an average of 292 days to identify and contain the breach. These statistics underscore an urgency for organizations to enhance their cybersecurity measures and adopt proactive strategies to mitigate data breach risks.

According to Malaysia Communication and Multimedia Commission (MCMC), recent ransomware attacks have grown more sophisticated as hackers leveraged artificial intelligence and machine learning tools to zero in on specific victims and avoid detection. Such attacks are especially harmful since they may cripple companies and organizations, which eventually leads to severe economic losses and reputational damage. Another emerging threat is cyber extortion where hackers demand a ransom, otherwise they threaten to reveal sensitive data that could potentially harm the victim. Such attacks will impact corporations and organizations.

Based on a report by cybersecurity firm Surfshark, Malaysia was ranked eighth most breached country in Q3 2023, with 494,699 exposed accounts. The breach rate was 144% greater in Q3 2023 than in Q2, with four Malaysian user accounts were exposed per minute.

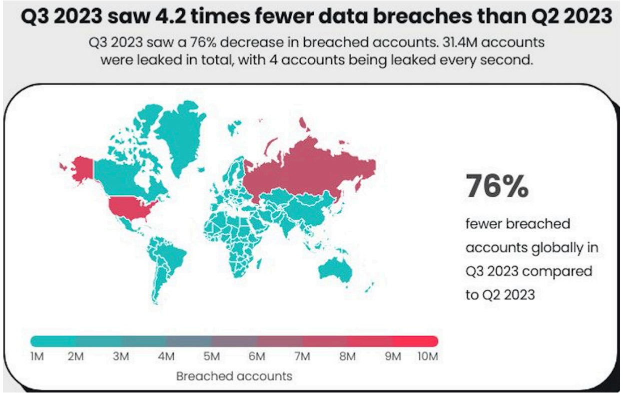
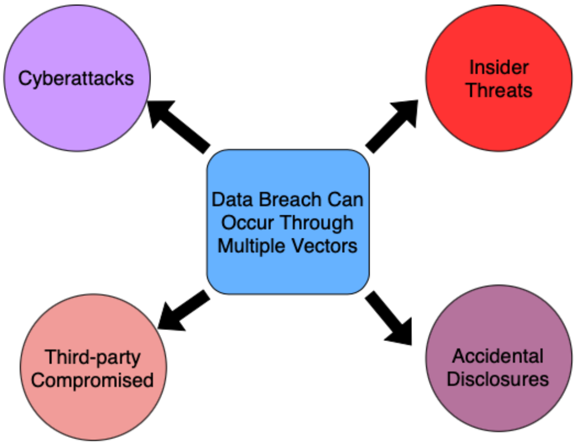

Q3 2023 saw 4.2 times fewer data breaches than Q2 2023
Q3 2023 saw a 76% decrease in breached accounts. 31.4M accounts were leaked in total, with 4 accounts being leaked every second.
76%
fewer breached accounts globally in Q3 2023 compared to Q2 2023
1M
2M
3M
4M
5M
6M
7M
8M
9M
10M
Breached accounts

Figure 2: Data Breaches in Q3 2024 by Surfshark

In our modern digital era, the security of personal and sensitive information has become more important than ever. Unfortunately, data breach can occur anytime and through various vectors. These vectors present different pathways through which unauthorized data access could occur. Understanding these vectors is therefore critical. By exploring different avenues, we can better grasp the complexity in safeguarding information within an interconnected world. Let's delve into the various vectors through which data breaches can occur and explore how we can mitigate the risks associated with one another.



The figure 3: Data Breach Vector

Data breaches can occur through multiple vectors, including:

1. Cyberattacks: Data breaches can occur through various cyberattacks, with differing levels of sophistication and impact. For instance, ransomware attacks encrypt valuable data, demanding payment for its release, while phishing campaigns trick unsuspecting users into revealing sensitive information like login credentials. Similarly, malware infections infiltrate systems, providing attackers with unauthorized access to networks and allowing them to exfiltrate data without detection.

2. Insider Threats: Data breaches can stem from malicious insiders or negligent employees within an organization who may intentionally or unintentionally compromise sensitive information. Malicious insiders could abuse their access privileges to steal data for personal gain or to sabotage the organization. On the other hand, negligent employees could inadvertently expose sensitive data through careless actions such as sharing passwords or failing to secure devices properly.

3. Third-Party Compromises: Organizations often rely on third-party vendors or partners for various services or products, and vulnerabilities within these external systems can pose significant risks. Attackers may exploit weaknesses in third-party software or supply chain processes to gain unauthorized access to an organization's networks or data repositories. Such compromises can result in the unauthorized extraction of sensitive information or the disruption of critical operations.

4. Accidental Disclosures: Human errors and oversight can also lead to data breaches, even without malicious intent. Misconfigurations in databases or cloud storage systems, for example, can leave sensitive data unintentionally exposed to the Internet. Moreover, improper handling of data, such as sending confidential information to the wrong recipient or failing to encrypt sensitive files, can result in accidental disclosures that compromise data security and privacy.

The Role of Digital Forensics in Breach Response

Digital forensics is a specialized field that encompasses a systematic preservation, collection, validation, identification, analysis and interpretation of digital evidence to understand the nature and scope of a data breach. Forensic experts leverage advanced tools and techniques to:

1. Identify a Breach: Determine the root cause and entry point of the breach, such as vulnerabilities in software, misconfigured systems, or compromised credentials. Some of the root causes why Malaysia's cybersecurity is struggling include inadequate funding and resources, insufficient personnel training, and a lack of coordination and communication between commercial and governmental institutions (Khairul Haqeem, 2023).

2. Collect Forensic Evidence: Collecting forensic evidence amounts to saving digital proof linked to the breach. It includes saving logs, data on network activity, snapshots of affected systems, and memory snapshots. These pieces of evidence help investigators understand what happened and how severe the breach was. Logs track the order of events on the system. Network data shows how information moved across networks, pointing to where the breach may have occurred. System images are like photos of the entire system, showing exactly what was on it at the time of the breach. Memory snapshots capture what was happening in the computer's memory when the breach occurred.

3. Analyze Impact and Scope: Assess the extent of data compromised, the types of information exposed like personally identifiable information, financial records and the potential impact on affected individuals or organizations.

4. Attribution and Incident Response: Trace the origin of the breach and attribute it to specific threat actors or entities, collaborating with incident response teams to contain the breach, mitigate further damage, and implement security measures to prevent future incidents.

Digital forensics professionals encounter numerous challenges during their investigations that can complicate the process of identifying the scope of breach, determining the root cause of breach and the way to mitigating and minimize the impact. Some of the challenges are summarized as below:

1. Complexity of Digital Environments: The complexity of digital systems, networks, and devices makes it challenging to investigate information leaks. Due to the vast scale of technologies and configurations that need to be reviewed, forensic investigations can become more difficult.

2. Data Encryption and Obfuscation: Investigative professionals have struggled with data that is encrypted or obscured. It becomes harder to decode and retrieve relevant proof when data is encrypted or scattered, thus slowing down the investigation.

3. Legal and Regulatory Compliance: Adhering to legal and regulatory frameworks is an essential component of forensic investigations. Professionals are required to navigate complex regulations and privacy restrictions in order to ensure that their investigation procedures comply with legal requirements. Non-compliance with these rules could affect the admissibility of digital evidence in court proceedings, thus impacting the effectiveness of an investigation.

4. Data Privacy Concerns: Digital forensic professionals must adhere to strict protocols when conducting and handling sensitive data in order to protect the privacy of individuals affected by a breach.

5. Evolving Threat Landscape: In this digital era, the tactics and techniques used by cyber threat actors are constantly evolving. It warrants digital forensic professionals to stay abreast of the latest tactics and techniques, developments, and acquire skills to adapt into their investigation methodology accordingly. Moreover, effective collaboration between forensic teams, legal experts, and regulatory authorities is essential to ensure thorough and legally sound investigations that could mitigate the impact of data breaches.

Best Practices for Data Breach Response

To effectively respond to data breaches and mitigate their impact, organizations should adopt the following best practices:

1. Implement Proactive Security Measures: Deploy robust cybersecurity protocols, including intrusion detection systems (IDS), access controls, endpoint protection, and employee training programs to prevent breaches and detect intrusions early.

2. Develop Incident Response Planning: Create and test incident response plans to quickly detect, contain, and remediate breaches, thus minimizing its impact on operations and data security.

3. Foster Collaboration and Information Sharing: Establish partnerships with law enforcement agencies, regulatory bodies, and industry peers to enhance breach response capabilities and share threat intelligence, in order to strengthen overall cybersecurity posture.

4. Conduct Regular Forensic Readiness Assessments: Proactively assess organizational readiness to respond to data breaches through forensic audits, penetration testing, and incident response drills.

5. Remediation and Recovery: Implement remediation measures by restoring affected data and system from backups. In addition, the team needs to address vulnerabilities to prevent similar incidents from occurring in the future by reviewing and updating security policies, procedures, and control.

Case Studies and Insights

Real-world case studies provide valuable insights into the effectiveness of digital forensics response, especially on how risks are mitigated and sensitive information are protected. Organizations should stay vigilant, continuously assess their security posture and tighten their security defense to address emerging threats. For example:

In a recent cyberattack on a multinational corporation, digital forensics experts were able to trace the source of the breach to a phishing campaign that exploited employee credentials. By leveraging forensic techniques, the organization managed to quickly contain the breach, mitigated further damage, and implemented enhanced security measures to prevent future incidents.

Following a data breach at a financial institution, digital forensics professionals collaborated with law enforcement agencies to identify the perpetrators and recover stolen funds. The insights gained from forensic analysis helped strengthen the institution's cybersecurity defenses and improve incident response procedures.

Conclusion

In today's digital world, Malaysia faces a growing number of cyber threats. Data breaches represent a major cybersecurity threat, necessitating proactive measures and effective incident response strategies. Digital forensics plays a pivotal role in responding to and investigating these incidents, providing critical insights that help organizations strengthen their cybersecurity posture and protect sensitive information. By embracing forensic expertise, leveraging advanced technologies, and adopting proactive security measures, organizations can effectively navigate data breaches and safeguard their digital assets in an evolving threat landscape.

This comprehensive article highlights the importance of digital forensics in navigating data breaches, offering critical insights, best practices, and real-world case studies to help organizations mitigate cybersecurity risks and protect sensitive information from unauthorized access and exposure. By prioritizing cybersecurity readiness and fostering collaboration across stakeholders, organizations can enhance their incident response capabilities and safeguard against evolving data breach threats.

References

1. https://www.thestar.com.my/tech/tech-news/2023/10/25/cybersecurity-malaysia-report-government-sectors-suffered-most-data-breaches-while-telcos-spilled-over-400gb-of-data-in-h1-2023

2. https://www.mcmc.gov.my/skmmgovmy/media/General/pdf2/MCMC-MyConvergence-Vol-22.pdf

3. https://cybersecurityasean.com/daily-news/recurring-data-breaches-malaysia-plain-ignorance-or-just-weak-enforcement

4. https://techwireasia.com/01/2024/malaysian-telco-provider-has-data-breach-again/#:~:text=According%20to%20a%20report%20by,every%20minute%20in%20Q3%202023

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: enquiry@cybersecurity.my
Customer Service Hotline: 1 300 88 2999
www.cybersecurity.my

CyberSecurityMalaysia
cybersecuritymy
cybersecuritymy
CyberSecurity Malaysia
cybersecurity_my

MINISTRY OF DIGITAL

ISSN 1985-1995

9 771985 199003

CERTIFIED TO ISO/IEC 27001:2013
CERT. NO. : ISMS 00114

ACB 021
SAMM 456

MSC MALAYSIA Status Company

Best Child Online Protection Website

WSIS PRIZES 2020 WINNER www.wsis.org

Recognition of Excellence 2023 CyberSAFE™ by OpenGov