ADMM Cybersecurity and Information Centre of Excellence

UPDATE ON

THE CYBER DOMAIN

Issue 8/24 (August)

Virtual Threats Going Physical: Cybersecurity in Autonomous and Semi-Autonomous Systems

INTRODUCTION

1. Technological advancements have propelled the development of fully autonomous and semi-autonomous systems across various facets of our lives, transforming how we live and work. As technology continues to evolve, we can anticipate even more sophisticated systems that seamlessly integrate into our daily routines, enhancing efficiency, safety, and convenience. Autonomous systems enhance efficiency and safety by performing tasks without human intervention, reducing the risk of human error and increasing productivity. Semi-autonomous systems, on the other hand, seek not to eliminate human factor entirely, but to reduce the danger to humans and enhance their performance. Both autonomous and semi-autonomous systems are projected to play an increasingly important role in tackling global concerns such as climate change, public health, transportation, energy efficiency, and generating innovation across a wide range of sectors. Therefore, understanding the cybersecurity challenges associated with their usage is key to ensuring that they are developed and deployed safely.

AUTONOMOUS AND SEMI-AUTONOMOUS SYSTEMS

2. Autonomous systems are defined as systems that operate independently without the intervention of humans. These systems use advanced technologies like artificial intelligence (AI) and machine learning (ML), enabling them to adapt to new environments, execute tasks, and make decisions effectively. Examples of autonomous systems include driverless cars and autonomous mobile robots

(AMRs). These systems utilise a combination of sensors, data processing units, and algorithms to recognise their environment, interpret data, and perform suitable actions to accomplish specific goals such as enhancing road safety, reducing traffic congestion, and lowering carbon emissions. Furthermore, autonomous systems integrated into smart city infrastructure manage a variety of functions including traffic control, public transportation, and emergency response systems. Similarly, the world of aviation has seen a steady push to increase the use of automation, such as autopilot systems for maintaining course and altitude, flight management systems for optimised routing, and automated landing systems for precision approaches, thereby seeking to reduce the number of incidents caused by human error.

3. Hence, cyberattacks on these systems can undermine their safe use, leading to potential loss of data, interruptions to daily life, or impediment of emergency services. As a result, autonomous systems with AI-powered threat detection and response capabilities are critical for reducing such risks and ensuring urban resilience.[1] These systems represent a significant advancement in technology but require rigorous cybersecurity protocols to protect against potential risks and ensure safe and reliable functioning in a variety of applications.

4. Semi-autonomous systems, on the other hand, are designed to work together with humans, requiring some degree of human intervention. These systems allow better efficiency by automating certain tasks while still enabling human operators to assume control when necessary. For example, surgical robots assist surgeons by providing precision and stability during operations. In the future, tele-operated robots will enable surgeons to perform these operations remotely over networks, allowing medical treatment to be delivered faster and in areas where medical assistance is less accessible, such as disaster zones, battlefields, or rural areas. In the automobile industry, semi-autonomous systems are critical in factories and manufacturing continuous operation and efficiency. Other examples of semi-autonomous systems also include advanced driver assistance systems (ADAS), which enhances vehicle safety and driver comfort by using sensors and software to control tasks like adaptive cruise control, blind spot detection, and parking assistance.

[1] Urban resilience refers to the ability of cities and other human settlements to resist and recover from shocks and stresses (Source: urbanresiliencehub.org)

CYBER THREAT LANDSCAPE

5. The cyber threat landscape for autonomous and semi-autonomous systems is rapidly evolving as these technologies become more integrated into critical sectors such as healthcare, military, and transportation. For example, cyberattacks on autonomous and semi-autonomous medical devices can pose direct threats to patient safety, cripple hospital operations, and compromise patient data. Researchers at the University of Washington conducted an experiment to demonstrate the risks cyber threats pose to tele-operated medical robots. Operators performed a set of prescribed tasks meant to simulate a medical surgery while a separate team performed cyberattacks. The hacking team succeeded in disrupting the robot's functions in several ways. In one case, the cyberattack forced the robot to come to an emergency stop. In another, the team successfully overrode the operator's commands entirely. The team was also able to demonstrate an attack that disrupted the operator's ability to make precise movements in real time – something that could have fatal consequences during a real surgery.

6. As these autonomous and semi-autonomous systems rely heavily on complex software, sensors, and interconnected networks to function, they present an attractive target for cyber adversaries. Such systems may also be deployed in areas where the system operator and systems are physically separated, requiring remote connectivity. This further enlarges the cyberattack surface area. Below are some examples of cybersecurity challenges for autonomous and semi-autonomous systems:

a. **Spoofing attacks** involve the manipulation of sensor inputs to deceive the autonomous system into perceiving false information or commands. For instance, GPS spoofing can trick autonomous vehicles into navigating to incorrect locations or following malicious commands.

b. **Jamming attacks** disrupt communication between autonomous systems and their command centres or operators by emitting electromagnetic signals that interfere with wireless transmissions. For example, during a military operation, an enemy could use a jamming device to block the GPS signals received by autonomous drones, causing them to lose navigation capabilities and potentially crash or become uncontrollable.

c. **Software vulnerabilities** are weaknesses or flaws in software that can be exploited to compromise the integrity, confidentiality, or availability of a system or its data. These vulnerabilities arise from errors or oversight in the design, implementation, or maintenance of the software code. In 2016, as part of research, a team from Keen Security of Tencent had successfully demonstrated a remote attack on the Tesla Model S by utilising a complex chain of vulnerabilities.

STRATEGIES TO ENHANCE CYBERSECURITY

7. Improving cybersecurity in autonomous and semi-autonomous systems entails taking a holistic approach that covers multiple layers of security. Below are some key strategies to achieve this:

a. **Implementing stronger encryption protocols and data protection procedures throughout the development cycle**. Encryption and data protection are key components of autonomous systems as it ensures that sensitive information is kept secure and accessible only to authorised individuals. Encryption refers to encoding data using cryptographic algorithms which makes it indecipherable to unauthorised users, while data protection procedures include the techniques and technology used to protect data against illegal access.

i. **Enforcing robust encryption protocols**. There are three types of encryptions: symmetric encryption, asymmetric encryption, and hash function (see Fig. 1). When being applied in autonomous systems, data transmission between autonomous vehicles and infrastructure is encrypted using protocols such as TLS (Transport Layer Security), which helps in maintaining confidentiality and integrity throughout communication. Furthermore, encrypting stored data on self-driving vehicles or cloud-based systems prevents illegal access if physical or digital security measures are compromised. This helps in mitigating cybersecurity risks and safeguarding data confidentiality.

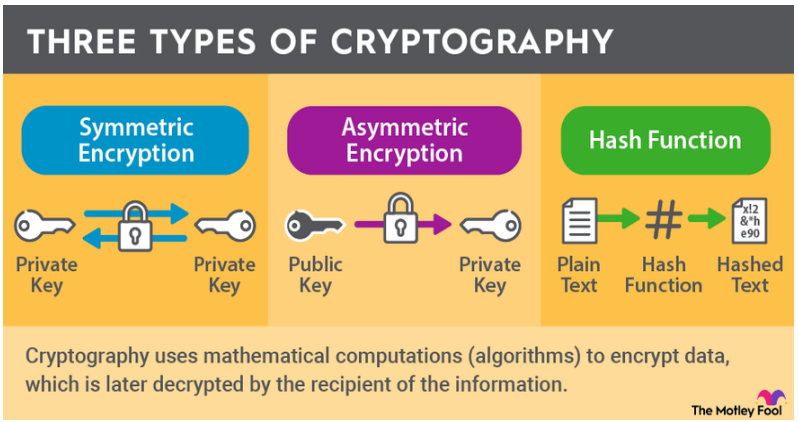

Fig. 1: Different types of cryptography to encrypt data
(Source: The MotleyFool)

ii. **Applying and adhering the procedures for data protection**. Implementing authentication measures, such as passwords and biometrics ensures only authorised users and devices have access to sensitive information. In addition, data masking and anonymisation helps to protect privacy, while individuals and businesses can use cryptographic hash functions to ensure data integrity and detect unauthorised changes. For example, Azure Key Vault helps protect cryptographic keys and secrets used by cloud apps and services, allowing individuals or businesses to have control over keys that were used to access and encrypt data (see Fig. 2). Compliance with data protection measures is critical for meeting regulatory obligations and ensuring the resilience of autonomous systems in a dynamic context.

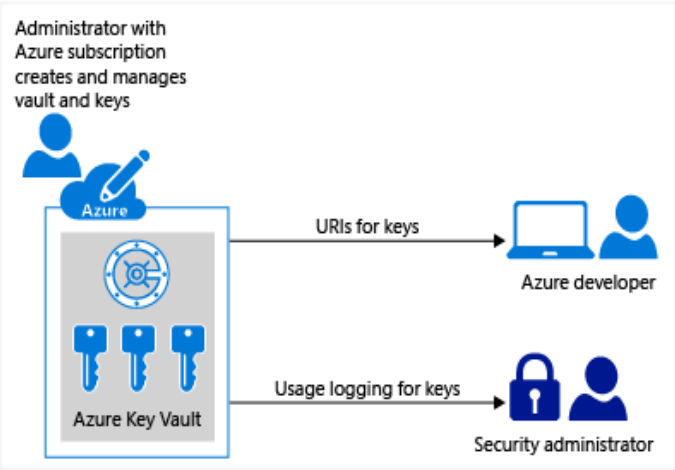

Fig. 2: Brief illustration on the usage for Azure Key Vault
(Source: Microsoft Learn)

b. **Incorporating secure design concepts into the autonomous system's development lifecycle.** Autonomous systems typically require minimum human intervention. They are primarily reliant on software, sensors, and communication networks. This reliance makes them prime candidates for cyberattacks, aiming at interrupting operations and stealing critical data. As a result, the integration of secure design concepts allows organisations to improve their cybersecurity posture, reduce risks, and ensure the safety of autonomous operations. Secure design concepts can be effectively integrated into the development lifecycle through conducting risk assessment and threat modelling and adhering secure development practices.

i. **Risk Assessment and Threat Modelling** are two approaches that serve as critical elements in integrating safe design principles into the autonomous system development life cycle. For instance, the risk assessment section would include identifying the assets and threats, followed by assessing the vulnerabilities and analysing the impact. It will also evaluate the frequency of various threats that may arise and conduct a risk prioritisation. On the other hand, threat modelling involves defining systems, determining threat scenarios, proposing mitigation strategies, and documentation (see Fig. 3). Both have complimentary functions and support businesses in preventing high risks from affecting their operations and initiatives. This strategy helps protect the system from present dangers and prepares to adapt to challenges in the future.

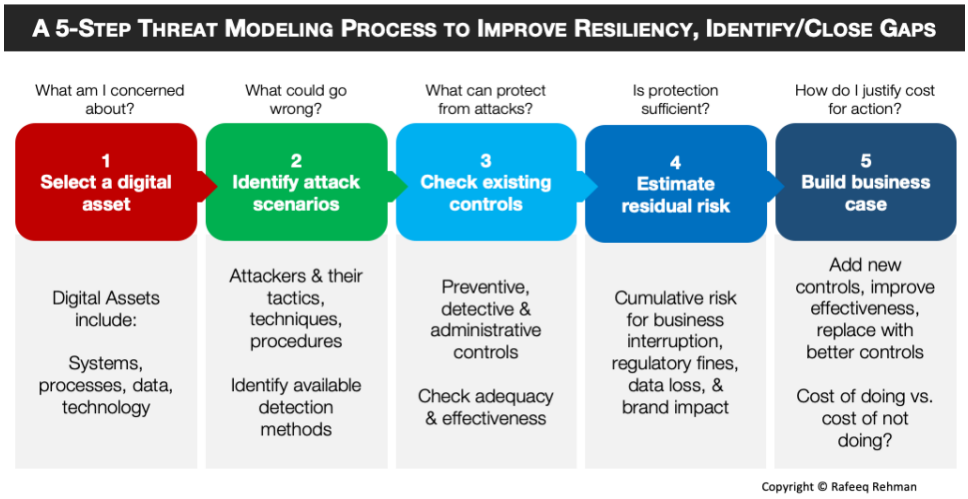

Fig. 3: An example of the threat modelling process (Source: Rafeeq Rehman)

ii. **Secure Development Practices** involve security considerations across all stages of the software development lifecycle (SDLC), ranging from initial design and coding to testing, deployment, and maintenance. There are a few approaches under secure development practices, such as following Secure Coding Standards, conducting peer code reviews, using secure development frameworks and libraries, and performing various security testing. Software security is vital as it ensures the software is protected from potential vulnerabilities and bugs. Hence, secure coding standards are an important component of such protection. Companies that adhere to safe coding standards, such as those promoted by Open Worldwide Application Security Project (OWASP) and other industry associations, will be able to ensure their autonomous systems are not only technologically proficient, but also resistant to cyber threats (see Fig. 4).

Fig. 4: Some of the best secure coding practices, which will reduce software vulnerability (Source: Taken from VPN overview)

iii. **Regulations and Legislations** play a crucial role in the autonomous system's development lifecycle by establishing safety standards, compliance requirements, and ethical guidelines that must be incorporated into the design, testing, and deployment of these technologies to ensure that they operate safely and responsibly within society. For instance, in September 2023, the US Food and Drug Administration (FDA) issued a guidance on

'Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions'. The guidance provides detailed recommendations on conducting cybersecurity risks assessments, interoperability considerations, and documents to be submitted to provide reasonable assurance that the medical device and related systems being developed are cybersecure. This new legal authority allows the US government to prosecute violations of cybersecurity requirements, ensuring that companies protect against cybersecurity risks throughout the device life cycle.

c. **Establishing private-public partnerships (PPP) to share threat intelligence within the autonomous field**. Private-public collaborations improve cybersecurity in the autonomous field by encouraging information sharing and coordinated responses to cyberattacks. Through mutual sharing of threat intelligence, stakeholders in the industry and government agencies will be able to strengthen their defences against cyber threats and provide a safer environment for autonomous technology to operate securely. Furthermore, partnerships allow industry players to collaboratively work on policies and regulatory frameworks that support cybersecurity measures in autonomous systems.

CONCLUSION

8. Autonomous technologies bring tremendous benefits to our daily routines but also pose non-trivial cybersecurity threats. These dangers place both individual safety and national security at risk by jeopardising the confidentiality and integrity of autonomous systems. Robust cybersecurity measures are important to reduce risks and vulnerabilities.

9. Proactive methods must be implemented in order to counter and mitigate such risks. Implementing secure design concepts into autonomous systems from the start can help to build a strong foundation against potential vulnerabilities. Advanced encryption algorithms and strong data protection mechanisms can also prevent classified information from being intercepted or accessed without authorisation. Furthermore, strengthening PPPs can refine the process of information exchange, threat intelligence, and coordinated efforts to build robust cybersecurity frameworks.

10. By embracing these techniques and investing in novel solutions, we can confidently navigate the complicated landscape of autonomous systems and safeguard against emerging cyber dangers.

Contact Details

All reports can be retrieved from our website at www.acice-asean.org/resource/.

For any queries and/or clarifications, please contact ACICE, at ACICE@defence.gov.sg.

Prepared by:
ADMM Cybersecurity and Information Centre of Excellence

• • • •

REFERENCES

1. Blackberry: Ultimate Guide to Autonomous Systems
https://blackberry.qnx.com/en/ultimate-guides/autonomous-systems

2. Ublox - Autonomous driving levels: from unassisted to hands-free driving
https://www.u-blox.com/en/blogs/insights/autonomous-driving-different-levels

3. World Robotics- Industrial Robots - IFR
https://ifr.org/wr-industrial-robots

4. Free Fall: Hacking Tesla from Wireless to Can Bus - BlackHat
https://www.blackhat.com/docs/us-17/thursday/us-17-Nie-Free-Fall-Hacking-Tesla-From-Wireless-To-CAN-Bus-wp.pdf

5. Risk assessment vs. threat modeling: What's the difference? – TechTarget
https://www.techtarget.com/searchsecurity/tip/Risk-assessment-vs-threat-modeling-Whats-the-difference

6. Risk management and Threat Modelling – NCSC
https://www.ncsc.gov.uk/collection/risk-management/threat-modelling

7. A Threat Modeling Process to Improve Resiliency of Cybersecurity Program – Rafeeqrehman
https://rafeeqrehman.com/2019/12/02/a-threat-modeling-process-to-improve-resiliency-of-cybersecurity-program/

8. Security Development Lifecycle (SDL) Practices – Microsoft
https://www.microsoft.com/en-us/securityengineering/sdl/practices

9. About the OWASP Foundation – OWASP
https://owasp.org/about/

10. Secure Coding Practices – OWASP
https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/stable-en/01-introduction/05-introduction

11. Secure Coding – Singapore Government Developer Portal
https://www.developer.tech.gov.sg/guidelines/standards-and-best-practices/secure-coding

12. Security Standards: What Are Secure Coding Standards? – Perforce
https://www.perforce.com/blog/qac/secure-coding-standards

13. What is Secure Coding and Why is It Important? – Vpnoverview
https://vpnoverview.com/internet-safety/business/what-is-secure-coding/

14. Define and use cryptography standards – Microsoft
https://www.microsoft.com/en-us/securityengineering/sdl/practices/cryptography

15. What is encryption? – IBM
https://www.ibm.com/topics/encryption

16. Transport Layer Security – Mdn Web Docs
https://developer.mozilla.org/en-US/docs/Web/Security/Transport_Layer_Security

17. What Is Cryptography? – The Motley Fool
https://www.fool.com/terms/c/cryptography/

18. Azure data security and encryption best practices – Microsoft Learn
https://learn.microsoft.com/en-us/azure/security/fundamentals/data-encryption-best-practices

19. Key Vault – Microsoft Azure
https://azure.microsoft.com/en-us/products/key-vault/

20. Azure Key Vault basic concepts – Microsoft Learn
https://learn.microsoft.com/en-us/azure/key-vault/general/basic-concepts

21. UW researchers hack a teleoperated surgical robot to reveal security flaws
https://www.washington.edu/news/2015/05/07/uw-researchers-hack-a-teleoperated-surgical-robot-to-reveal-security-flaws/

22. Building Resilience - Urban Resilience Hub
https://urbanresiliencehub.org/building-resilience/

23. FDA Finalizes Guidance on Medical Device Manufacturer Cybersecurity Responsibilities
https://www.ropsegray.com/en/insights/alerts/2023/10/fda-finalizes-guidance-on-medical-device-manufacturer-cybersecurity-responsibilities