ADMM Cybersecurity and Information Centre of Excellence

UPDATE ON THE CYBER DOMAIN

Issue 08/23 (August)

Internet of Things – Benefits and Challenges to Watch out for

OVERVIEW

1. The Internet of Things (IoT) has become one of the most important technological developments of the 21st century. Despite its somewhat abstract and elusive connotation, IoT devices are ubiquitous in today's society, with everyday household items such as kitchen appliances, self-driving cars and thermostats being connected to the internet. As such, the line between the physical and digital worlds are beginning to blur, and it is important for technology professionals to understand the benefits and implications of this to their respective organisations.

"IoT is no longer a mystery fad. It is a technology that has quietly gained traction and is now altering our future invisibly." **– iCert Global**

WHAT IS THE INTERNET OF THINGS?

2. IoT describes the collective network of physical objects that are embedded with sensors, software and/or other technologies to connect and exchange data with other devices over the internet or other communications networks. These devices range from common household objects like refrigerators and smart televisions, to industrial tools like assembly line sensors and tracking devices. The interconnectedness of IoT devices empowers industries by allowing industries to collect real-time data and collectivise information, thereby strengthening their ability to streamline operations.

"The number of active Internet of Things (IoT)-connected devices is estimated to be at 41.76 billion in 2023." **– Frost & Sullivan**

HOW CAN THE INTERNET OF THINGS BENEFIT ORGANISATIONS?

Supply Chain Management

3. IoT solutions can be used to enhance processes in each stage of the supply chain management for different industries. For example, car company Volvo integrates IoT sensors into its vehicles, parts and equipment used in the supply chain. These sensors provide real-time data on the location, status and condition of vehicles and components, allowing the company to more precisely track its shipments and anticipate delays, thereby being able to optimise its routes for faster delivery times. Each industry offers a wide array of openings for IoT solutions to be integrated into the supply chain network. The list below illustrates some of them:

a. Agriculture. Gathering real time data on crops or/and livestock in farming and agriculture to help increase output, decrease energy consumption and ensure profitability.

b. Manufacturing. Used to identify bottlenecks, reduce downtimes and improve production efficiency.

c. Logistics Management. Detecting deviations from recommended transportation conditions, such as temperature, as well as to optimise delivery routes.

Smart Buildings

4. A smart building uses IoT devices to enable efficient and economical use of resources to provide a safe and comfortable environment to occupants. For example, IoT ecosystems in a building can make buildings more energy-efficient by constantly monitoring and adjusting the temperature for optimum energy efficiency and comfort. The Oakland City Centre in California utilises an AI-powered advanced variable air volume (UAV) system to continually collect and evaluate temperature and humidity data. Inputs are then sent to the building's Heating, Ventilation and Air Conditioning (HVAC) system, allowing it to recalibrate itself to ensure better occupant comfort. Other applications of IoT devices in Smart Buildings include:

a. Integrated Detectors. Used to detect heat, smoke or flames and calculate the fire's potential to accurately alert occupants, building owners and emergency response units.

b. Smart security systems. This includes intelligent locks, card readers, keypads, alarms and other related devices which allow control over buildings' access and security.

Smart Energy Grids and Meters

5. Previously, energy only flowed one way along the grid: from the power generation site to the customer. Now, IoT devices can be integrated across all the energy production, distribution, supply and consumption phases, to monitor and acquire essential real time data thereby increasing efficiency. Smart energy meters installed in organisations provides real time data to help to make energy management more effective.

Logistics and Fleet Management

6. Organisations can use sensors, telematics, navigation systems and analytics to track and monitor warehouse operations. IoT solutions are also used to preserve perishable goods through storage conditions monitoring. The IoT ecosystem can also enable organisations to improve fleet operations through predictive maintenance and route optimisation. For example, Grab Food uses IoT technology to allow both the company and the user to track the status of the food ordered, from the time the order is received, to the time it is in the kitchen, and finally when it is out for delivery, and eventually delivered.

"The global internet of things market is estimated to grow from $662 billion in 2023 to over $3.3 trillion by 2030, as healthcare and industrial IoT use cases increase dramatically." – **According to Techtarget**

POTENTIAL SECURITY CHALLENGES

7. Although IoT technology has many advantages, security teams are facing challenges unique to IoT security. Listed below are some common IoT security challenges and recommendations on how to overcome them:

No Clear Visibility on Inventory

8. Organisations might lack a clear understanding of the IoT devices within their network and how to ensure their secure management. This lack of clear visibility of their inventory is potentially dangerous because organisations may lose track of the maintenance cycles of these devices, which may lead to operational inefficiencies or inaccurate data being provided. Moreover, they may fail to provide sufficient security mechanisms for the entire network of IoT devices, increasing the organisation's vulnerabilities to cyberattacks.

9. As such, organisations should employ device discovery to get visibility into the exact number of IoT devices connected to their networks and their functions. The asset list should always be updated as and when new IoT devices get connected to the network for complete visibility and oversight on the IoT devices.

IoT Devices that are Hard or Impossible to Patch

10. Traditional security solutions used by computers or smart devices do not work on IoT devices, which typically use different software. For example, medical devices approved by the US' Food and Drug Administration typically align to very stringent regulatory standards, and therefore have to follow very strict and time-consuming processes for software updates. IoT technology that is incorporated into everyday items like refrigerators or air-conditioners, for example, is almost never patched after it leaves the factory. Hence, most IoT devices are not designed to get regular security patch updates, which means that their security flaws will not be patched automatically. Therefore, it is important to ensure that all the organisation's IoT devices have a recurrent patch management and firmware upgrade strategy to ensure that the IoT devices' patches are up to date.

Diversity of IoT Devices Increases Attack Surface

11. The diversity of IoT devices increases the attack surface area by introducing a wider range of vulnerabilities and entry points for attacks. To combat this, organisations can employ Network Segmentation – this process divides a large computer network into smaller, isolated sections, allowing security teams to better control the flow of data between segments. This helps to contain breaches within specific segments, while making it more difficult for cyber hackers to exploit a single compromised device as a gateway to launch lateral attacks.

Poor Password Security Practices

12. Many IoT devices come with weak pre-programmed passwords that can be found online, allowing cyber criminals to easily launch a cyberattack on an organisation. Hence, adopting good password practices is essential in reducing the attack surface. Pre-programmed passwords should be changed to more secure and complex ones, in line with the password management policies set by the organisation's IT security and management team.

CONCLUSION

13. IoT technology has been proven to be a key enabler for many industries such as agriculture, manufacturing, utilities, retail and transportation. However, there are significant security risks arising from unpatched and unmonitored devices connected to the networks. By implementing the best security and regulatory practices, organisations can effectively mitigate these risks and safely tap on the benefits of IoT devices.

"IoT is no more a tech buzz. It has become a trendsetter for many modern businesses and a new economic driver. Moreover, its impact is expected to grow over the years, especially as part of the fourth industrial revolution or Industry 4.0." **– According to Forbes**

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

ANNEX A

News Articles

1. What is IoT (Internet of Things)?
   [Link: https://aws.amazon.com/what-is/iot/]

2. Top 12 IoT applications and examples in business
   [Link: https://www.techtarget.com/iotagenda/tip/Top-8-IoT-applications-and-examples-in-business]

3. What is IoT Security?
   [Link: https://www.paloaltonetworks.com/cyberpedia/what-is-iot-security]

4. How to Secure IoT Devices in the Enterprise
   [Link: https://www.paloaltonetworks.com/cyberpedia/how-to-secure-iot-devices-in-the-enterprise]

5. 7 Examples of Smart Buildings
   [Link: https://www.ashb.com/examples-of-smart-buildings/#:~:text=1.,responds%20to%20changes%20in%20demand.]

6. IoT in Supply Chain Management
   [Link: https://www.infosysbpm.com/blogs/supply-chain/internet-of-things-supply-chain.html#:~:text=Volvo%20uses%20IoT%20supply%20chain,the%20QR%20code%20on%20packages.]