ADMM Cybersecurity and Information Centre of Excellence

UPDATE ON

THE CYBER DOMAIN

Issue 1/25 (January)

Cybersecurity in the Home: The Oft-Overlooked Location

INTRODUCTION

1. In today's rapidly advancing digital landscape, the home – a space traditionally associated with privacy and safety – may now become a new front in the ever-expanding cyber threat landscape. This is because the home has increasingly become a hub of interconnected devices. This transformation, powered by Internet of Things (IoT) technologies, brings unmatched convenience but also raises significant cybersecurity concerns. As cyberattacks targeting households are on the rise, securing our digital sanctuaries has never been more critical.

TRANSFORMING OUR HOMES THROUGH THE INTERNET

2. From communication to commerce, internet-related services underpin most daily activities. The rapid adoption of IoT technologies is reshaping how we interact with our environments. IoT ecosystems, which consist of smart devices such as home assistants, thermostats, robotic vacuums, and smart locks, are at the forefront of creating fully automated environments. These devices collect extensive data, including location, daily routines, energy consumption, and even biometric information, to offer personalised services that enhance convenience and efficiency.

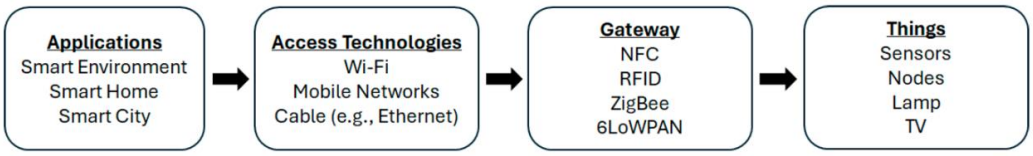

Fig. 1: Basic building blocks of IoT ecosystems

3. The scale of this transformation is evident in the explosive growth of internet-enabled devices, with a Cisco study projecting the number of IoT devices worldwide to rise from 12 billion connected devices in 2010 to a staggering 1 trillion by 2035. However, the increasing reliance on connected devices comes with its own set of challenges.

CONNECTED HOMES: POSSIBLE CYBERSECURITY RISKS

4. The rapid adoption of IoT has turned homes into microcosms of the digital world. IoT devices, such as baby monitors, smart thermostats, and robotic vacuum cleaners, often rely on internet connectivity. Devices not only communicate with their users but also with each other, creating a network of interdependencies. This interconnectedness, while offering seamless integration, also amplifies vulnerabilities – any single compromised device can jeopardise the entire network.

5. Poorly Secured Home Networks. The rise in remote work has made home networks an attractive target for ransomware attacks. The consequences of a ransomware attack can be severe: families may lose access to critical files, while businesses can suffer operational disruptions if employees use compromised home networks. Common vulnerabilities such as unsecured Wi-Fi networks using outdated encryption standards (like WEP) or default router credentials are easily exploitable by attackers. An attack could start when the victim receives a phishing email which contains a malicious attachment or link that downloads ransomware onto the home computer when opened. If the home network lacks proper segmentation, the ransomware spreads to other devices connected to the same network, such as tablets, phones, and IoT devices. If infected, the device displays a ransom note explaining that the victim's files on those devices have been encrypted; the note also provides instructions for payment, usually in cryptocurrency, for release of the data. In 2023, ransomware actors intensified their operation, with total ransomware payments surpassing the US$1 billion mark, the highest number ever observed. The challenge brought about by

ransomware attacks is further exacerbated by the limited resources and expertise available to the average homeowner to recover from such attacks without paying the ransom.

6. IoT Device Vulnerabilities. IoT devices often have weak security protocols, making them attractive targets for cybercriminals. Even devices marketed as 'secure by design' may have unknown vulnerabilities or hidden risks introduced by third-party applications integrated into IoT ecosystems. Forescout's *The Riskiest Connected Devices in 2024* report, which analysed data sourced directly from nearly 19 million devices, found that the proportion of IoT devices with vulnerabilities rose from 14% in 2023 to 33% in 2024. The most vulnerable IoT device types were wireless access points, routers, printers, and IP cameras. Cybercriminals can exploit weak security in these devices to infiltrate networks, steal personal information, or compromise physical safety. For example, hacked baby monitors have been used to eavesdrop on families or even deliver frightening messages, while compromised smart thermostats can reveal patterns indicating when a home is unoccupied.

7. Lower Levels of Protection. Unlike corporate networks that are fortified by dedicated IT teams, advanced firewalls, and regular monitoring, home environments typically have lower levels of protection such as default settings, basic antivirus software, and user self-management. In May 2024, several homeowners in the US reported incidents where hackers took control of their Ecovacs Deebot X2 Omni robotic vacuums. The compromised devices were used to chase pets and broadcast offensive language, including racial slurs, through the robot's speakers. The company attributed these breaches to a credential stuffing attacks, where attackers exploited weak or reused passwords to gain unauthorised access, highlighting the fragility of consumer-grade smart security systems in the face of determined attackers. The company responded by blocking the offending IP address and emphasised the importance of using strong, unique passwords to enhance device security. Many IoT devices are shipped with pre-set passwords or inadequate encryption protocols. Many households adopt these default settings without implementing adequate protective measures, leaving them easy targets for attackers. Compounding this issue is the lack of technical expertise among homeowners, who often struggle to recognise and mitigate these vulnerabilities.

8. Increased Connectivity. The proliferation of smart devices, including wearable health monitors, smart appliances, and interconnected entertainment systems, can exponentially expand the attack surface. Each new device introduces potential vulnerabilities, and their seamless integration within home networks creates opportunities for attackers to move laterally once a single device is compromised. In 2024, a new variant of the Mirai botnet emerged, exploiting zero-day vulnerabilities in IoT devices to conduct large-scale distributed denial of service (DDoS) attacks. At its peak, over 15,000 devices – including industrial routers, smart home hubs, and security cameras – were actively compromised and used as nodes in the botnet. These IoT device owners unknowingly contributed to the attacks, which caused significant disruptions to critical services in sectors like telecommunications, e-commerce, and financial services. This example shows that the increased connectivity of IoT devices can be used by malicious actors to target not only individuals, but also society as a whole. As connectivity grows, developing strategies to secure these complex ecosystems will become essential for protecting the digital home and safeguarding cybersecurity on a societal scale.

COMBATING THE RISE OF CYBERSECURITY RISKS AT HOME

9. The gap between rapid technological adoption and readiness to secure these advancements highlights the pressing need for practical solutions. By building awareness and adopting proactive measures, households can better navigate the challenges of living in an increasingly connected digital world.

a. Strengthen Legislation and Regulatory Frameworks. Governments must establish robust standards for IoT devices, requiring manufacturers to implement secure-by-design principles, including mandatory software updates and strong encryption. For instance, the European Union's Cyber Resilience Act establishes mandatory cybersecurity requirements for connected devices, setting a precedent for similar global initiatives. The US has also introduced frameworks like the IoT Cybersecurity Improvement Act of 2020, which mandates security standards for IoT devices procured by the federal government. The Cyber Security Agency of Singapore (CSA) has launched the Cybersecurity Labelling Scheme (CLS) for consumer smart devices, as part of efforts to improve IoT security, raise overall cyber hygiene levels and better secure Singapore's cyberspace. The CLS is the first of its kind in the Asia-Pacific region. Under the scheme, smart devices

will be rated according to their levels of cybersecurity provisions. This will enable consumers to identify products with better cybersecurity provisions and make informed decisions.

Fig. 2: Overview of Global IoT Regulations (voluntary or mandatory)

b. Awareness Campaigns. Behavioural economics principles can be leveraged to design campaigns that nudge homeowners toward better cybersecurity practices. Collaborations between tech companies and governments could lead to widespread distribution of cybersecurity toolkits, including apps that guide users through basic security configurations. For example, timely notifications prompting users to change weak passwords or gamifying security checks can encourage better habits without overwhelming less tech-savvy individuals. Practical steps that can be promoted through these campaigns include:

- **Use unique, complex passwords:** Avoid default or easily guessable passwords for all accounts and devices to deter threat actors from unauthorised access.

- **Segregate home and work networks:** Create separate networks for personal and professional activities to limit the potential spread of breaches.

- **Install reputable antivirus and anti-malware solutions:** These tools help detect and mitigate threats, ensuring a baseline level of security for home systems.

THE FUTURE: POTENTIAL CHALLENGES

10. As technological innovation accelerates, emerging risks challenge the ability of traditional cybersecurity measures to protect increasingly interconnected home environments. These risks stem from both the expanding capabilities of malicious actors and the rapid proliferation of devices that create new vulnerabilities. Understanding these future threats is critical to ensuring resilience against an evolving threat landscape.

a. AI-Powered Threats. Cybercriminals have been leveraging Artificial Intelligence (AI) to create more convincing phishing scams and to bypass traditional security measures. AI enables attackers to generate highly targeted messages, mimic legitimate communications, and adapt malicious strategies in real time. However, AI can also be a powerful defence tool, capable of identifying unusual network activity, detecting anomalies, and deploying automated responses to mitigate risks effectively. The dynamic interplay between AI as both a weapon and a shield will shape the future of cybersecurity in home environments.

b. Quantum Computing Risks. As quantum computing matures, it may render current encryption methods obsolete, exposing home systems to significant risks. Many of the encryption protocols that underpin modern cybersecurity, such as RSA and ECC, could become vulnerable to quantum attacks capable of breaking them within seconds. To counteract this threat, researchers are developing quantum-resistant cryptographic methods, which aim to ensure data security even in the era of quantum computing. Preparing for this transition will be critical to maintaining secure communications and protecting sensitive data.

CONCLUSION

11. Homes are no longer isolated from the broader cybersecurity landscape. As IoT continues to evolve, protecting our homes requires a shared responsibility. By

implementing strong regulations, fostering awareness, and adopting advanced technologies, we can ensure that digital homes remain safe havens in an interconnected digital world.

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. Cisco Annual Internet Report
https://www.cisco.com/c/en/us/solutions/executive-perspectives/annual-internet-report/index.html

2. Two out of five digital households worldwide at cyber risk, Avast reveals
https://press.avast.com/two-out-of-five-digital-households-worldwide-at-cyber-risk-avast-reveals

3. EU adopts cyber resilience act – and other cybersecurity news to know this month
https://www.weforum.org/stories/2024/10/eu-cyber-resilience-act-cybersecurity-news-october-2024/

4. Cyber Resilience Act
https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

5. Global IoT Regulations | What you need to know
https://community.checkpoint.com/t5/IoT-Protect/Global-IoT-Regulations-What-you-need-to-know/td-p/197020

6. Cybersecurity Labelling Scheme (CLS)
https://www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme

7. DrayTek routers exploited in massive ransomware campaign
https://www.forescout.com/blog/draytek-routers-exploited-in-massive-ransomware-campaign-analysis-and-recommendations/

8. Ransomware Payments Exceed $1 Billion in 2023, Hitting Record High After 2022 Decline
https://www.chainalysis.com/blog/ransomware-2024/

9. IoT Vulnerabilities Skyrocket, Becoming Key Entry Point for Attackers
https://www.infosecurity-magazine.com/news/iot-vulnerabilities-entry-point/

10. Hackers took over robovacs to chase pets and yell slurs
https://www.theverge.com/2024/10/12/24268508/hacked-ecovacs-deebot-x2-racial-slurs-chase-pets/

11. New Mirai botnet targets industrial routers with zero-day exploits
https://www.bleepingcomputer.com/news/security/new-mirai-botnet-targets-industrial-routers-with-zero-day-exploits/