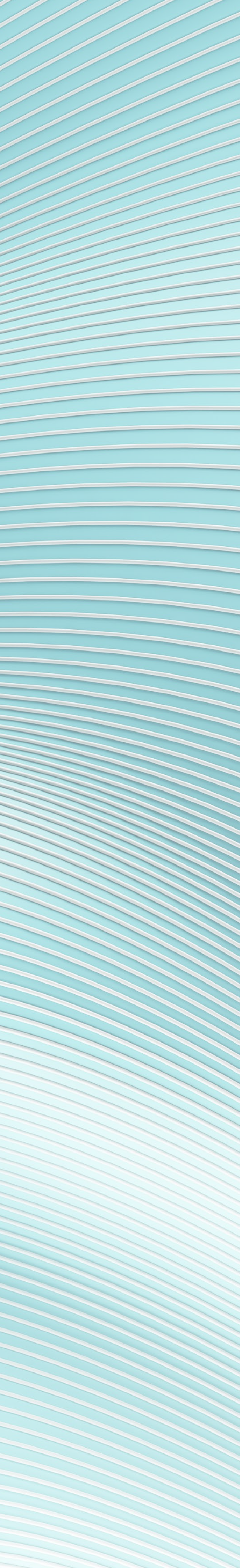
UNSW
Institute for
Cyber Security

The internet of things:

Protecting network assets and infrastructure



Introduction

The Internet of Things (IoT) is revolutionising the way we live and work, connecting everything from household appliances to critical infrastructure systems. However, the rapid proliferation of IoT devices introduces serious cyber security risks. Many devices lack basic security protections, making them vulnerable to cyber threats, including botnets, data breaches, and system takeovers.

A well-documented example is the **2016 Mirai botnet attack**, which exploited insecure IoT devices to launch a **Distributed Denial of Service (DDoS) attack**, disrupting major online services. These incidents highlight the urgent need for robust IoT security measures.

Current regulatory landscape

The Australian Government has taken steps to address IoT security, including the **Cyber Security Act 2024**, which mandates manufacturers to provide a statement of compliance outlining device security measures. However, enforcing compliance remains a challenge. Without strong enforcement mechanisms, manufacturers may prioritise cost savings over security, leaving businesses and consumers vulnerable.

A regulatory approach that balances compliance requirements with industry feasibility is essential. Instead of imposing costly and complex device-level security, an alternative approach - network-level security - offers a practical, scalable solution.

Network-level security: A feasible solution

Security experts advocate two primary approaches to IoT security:

Device-Level Security

Embeds security features into each device. While effective, this approach is expensive, difficult to implement universally, and often resisted by manufacturers due to cost and complexity.

Network-Level Security

Places security controls at the network level, enabling operators to enforce security policies without requiring changes to individual devices. This approach is lighter, more flexible, and cost-effective, as it does not require modifying device hardware or software.

A practical implementation of network-level security is the **Manufacturer Usage Description (MUD) standard (RFC8520).**

University of New South Wales

The Manufacturer Usage Description (MUD) Standard

The MUD standard, developed by the Internet Engineering Task Force (IETF), requires manufacturers to declare the expected behaviour of their devices. This allows network operators to enforce policies that limit unnecessary or potentially harmful device communications.

Key Benefits of MUD:

Locks down authorised communications by restricting devices to expected network behaviours.

Reduces attack surfaces by preventing unspecified connections.

Minimises security costs by shifting protection to network operators instead of manufacturers.

Implementation of MUD Policies:

- **For Large Organisations** (e.g., government agencies and infrastructure operators): Network administrators can configure switches and routers to enforce security policies based on known MUD profiles.

- **For Home Networks:** Internet Service Providers (ISPs) can offer managed security services, applying MUD-based protections at home network gateways.

This approach does not require modifications to devices, making it a low-cost, high-impact solution. That said, device-level protections can complement network-level approaches, further enhancing overall security.

Case study: Enhancing IoT security with MUD

IoT security is a pressing challenge that demands proactive policy measures. While device-level security is costly and difficult to enforce, network-level security offers a viable, scalable alternative. By mandating MUD adoption, the Australian Government can:

- Enhance IoT security in public and private sectors.
- Protect national infrastructure from escalating cyber threats.
- Position Australia as a global leader in cyber security policy.

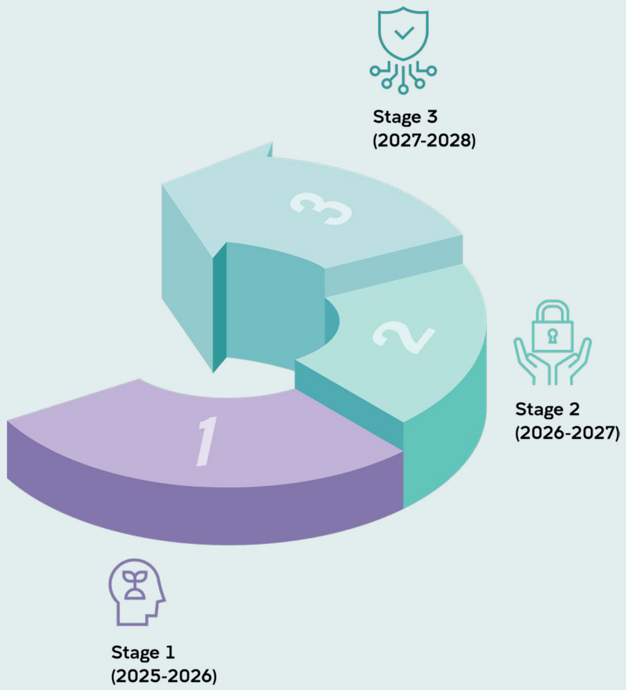
A secure IoT ecosystem will strengthen national resilience, safeguard businesses and consumers, and set a benchmark for international best practices.

Implementation and enforcement strategy

To achieve widespread adoption of network-level security, a phased enforcement strategy is recommended:

1. **Stage 1 (2025-2026):** Awareness and education for manufacturers and network operators.
2. **Stage 2 (2026-2027):** Voluntary adoption of MUD, with government incentives (e.g., procurement preferences for compliant manufacturers).
3. **Stage 3 (2027-2028):** Regulatory enforcement requiring IoT manufacturers to comply with published security expectations.

Additionally, third-party certification bodies could verify manufacturer compliance, similar to existing testing frameworks for telecommunications and mobile devices.



Conclusion

IoT security is a pressing challenge that demands proactive policy measures. While device-level security is costly and difficult to enforce, network-level security offers a viable, scalable alternative. By mandating MUD adoption, the Australian Government can:

- Enhance IoT security in public and private sectors.
- Protect national infrastructure from escalating cyber threats.
- Position Australia as a global leader in cyber security policy.

A secure IoT ecosystem will strengthen national resilience, safeguard businesses and consumers, and set a benchmark for international best practices.

Further reading

For further insight into IoT security and regulatory frameworks, we recommend the following documents:

- **Systematic Verification of IoT Device Conformance to IETF Manufacturer Usage Description Standard** – A technical overview of the MUD standard and its practical applications.

- **Submission on Australia's Cyber Security Regulations and Incentives** – Policy recommendations and regulatory insights for improving national cyber security.

- **Manufacturer Usage Description (MUD) standard (RFC8520).**

Glossary

2016 Mirai Botnet Attack

The 2016 Mirai botnet attack was a large-scale cyber attack that leveraged vulnerabilities in Internet of Things (IoT) devices to create a botnet. The botnet, known as Mirai, infected thousands of IoT devices with weak security settings, such as default passwords and open ports, and used them to launch a Distributed Denial of Service (DDoS) attack against major websites and online services. The attack disrupted services such as Twitter, Netflix, and Reddit, highlighting the risks of unsecured IoT ecosystems.

Manufacturer Usage Description (MUD) Standard

The Manufacturer Usage Description (MUD) standard is a security framework developed by the Internet Engineering Task Force (IETF) to enhance IoT device security at the network level. The MUD standard requires IoT manufacturers to publish expected device behaviour, allowing network operators to enforce policies that restrict unnecessary or unauthorized communications. By limiting a device's interactions to only essential services, MUD helps reduce attack surfaces and prevent cyber threats such as DDoS attacks and unauthorised access. The standard provides a low-cost, scalable security solution that does not require modifications to device hardware or software.

Distributed Denial of Service (DDoS) Attack

A Distributed Denial of Service (DDoS) attack is a cyber attack in which multiple compromised devices, often part of a botnet, are used to flood a target system, network, or website with excessive traffic. This overwhelms the target, rendering it inaccessible to legitimate users. DDoS attacks can disrupt businesses, government agencies, and critical infrastructure, making them a significant cyber security threat. The Mirai botnet attack is one of the most notable examples of a large-scale DDoS attack.

Australian Cyber Security Act 2024

The Australian Cyber Security Act 2024 is a legislative framework introduced to enhance the cybersecurity posture of Australian businesses and government entities. The Act mandates stricter security measures for Internet of Things (IoT) devices, requires compliance statements from manufacturers, and establishes regulatory enforcement mechanisms to ensure device security. The Act aims to mitigate cyber risks by enforcing security standards, promoting threat intelligence sharing, and enhancing national cyber security resilience.

Hassan Habibi Gharakheili is an Associate Professor at UNSW Sydney in the School of Electrical Engineering and Telecommunications and a member of UNSW's Institute for Cyber Security (IFCYBER). His research specialises in programmable computer networks, data-driven inference systems, and network security. Additionally, he teaches core courses in computer networking, focusing on technologies, protocols, performance modelling, and cyber security.

Further enquiries

UNSW Institute for Cyber Security (IFCYBER)

✉ ifcyber@unsw.edu.au

🖥 ifcyber.unsw.edu.au

CRICOS 00098G | 4602865