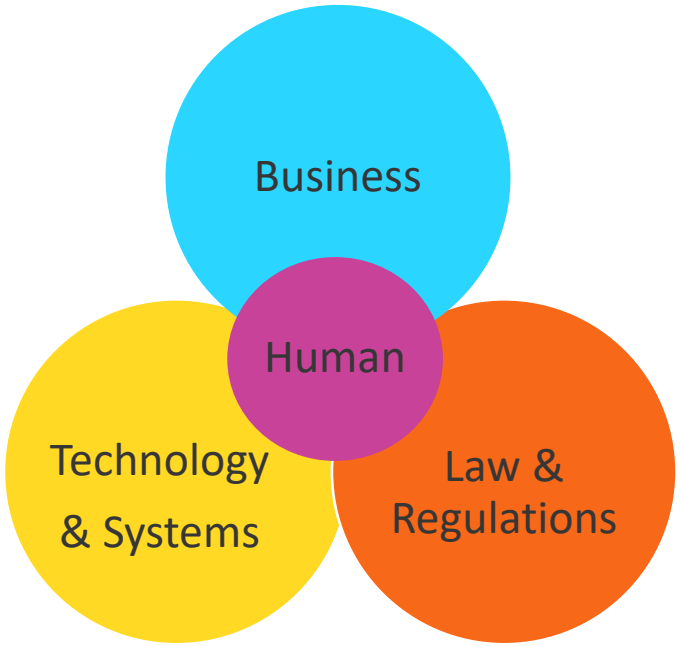
Secure IoT Platform

CSRI
CENTRE FOR CYBER SECURITY RESEARCH AND INNOVATON

DEAKIN UNIVERSITY

Professor Robin Doss
Research Director

CSRI
CENTRE FOR CYBER SECURITY RESEARCH AND INNOVATON



45 Cyber Security Researchers from 4 Faculties (Arts & Education, Business & Law, Health and Science, Engineering and Built Environment) representing a truly **multidisciplinary approach** to cyber security challenges.

~40 PhD students
6 Core Research Themes

Projects include: Development of new honeypot technologies, DDOS protection for social media systems, IoT, Blockchain, cyber security for critical infrastructure, information warfare and message propagation, human decision making in a cyber security context, cyber security capability and maturity etc…..

Solving the Cyber Security challenges of tomorrow for Australian Industry and Government in innovative and collaborative ways today.

My Research

Research Areas

- Secure protocol design & formal verification of security correctness
- Secure IoT/M2M/V2V Communications
- Applied Cryptography (Zero Knowledge proofs)
- Applied ML for Cyber Security

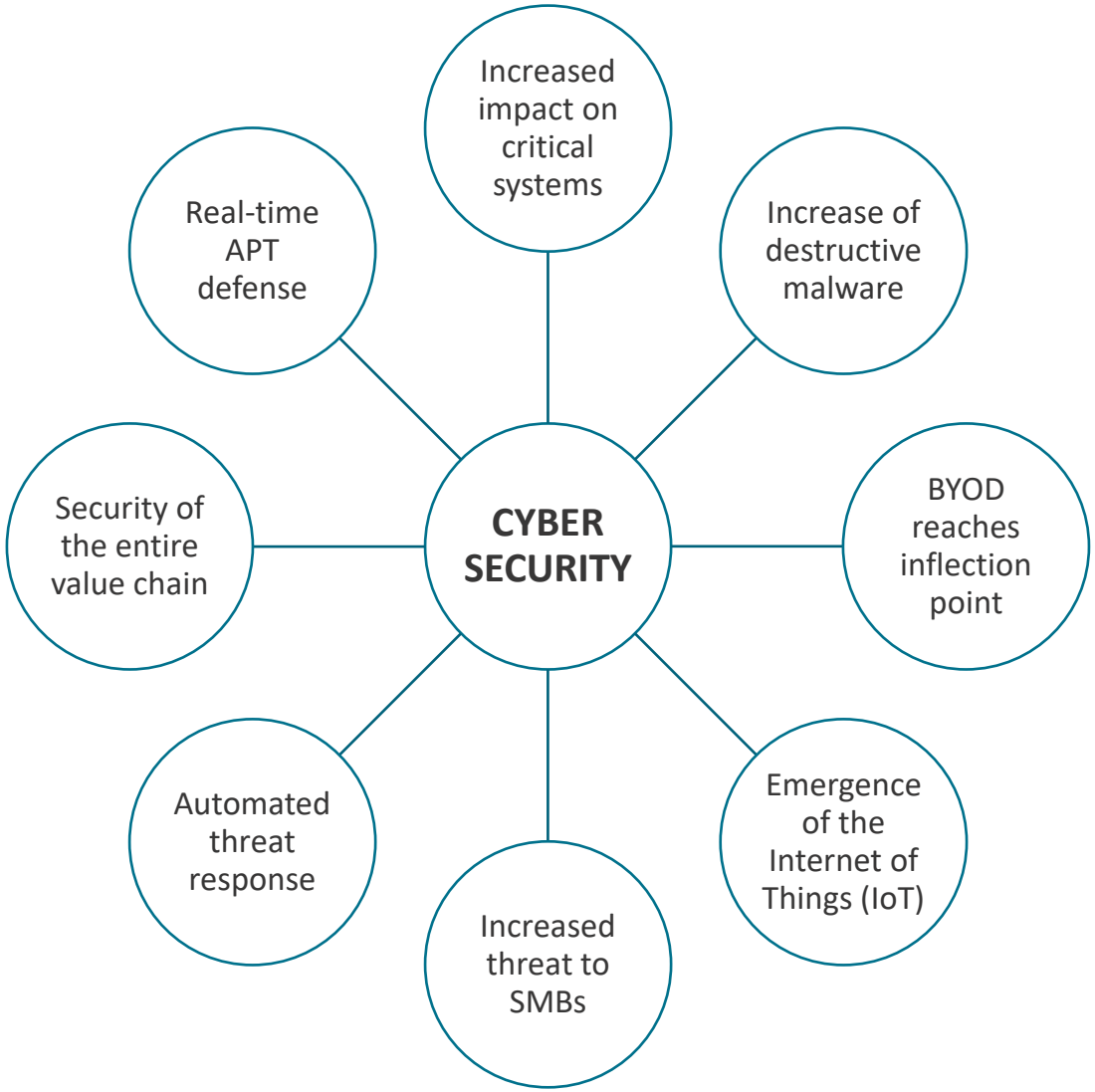
Research Partners

- Defense Signals Directorate (DSD)
- Defense Science and Technology Group (DSTG)
- IBM Research, Zürich Research Lab (Visiting Scientist)
- Department of Industry, Innovation and Science (DIIS)
- Bosch Australia
- Department of Prime Minister & Cabinet (PMC)

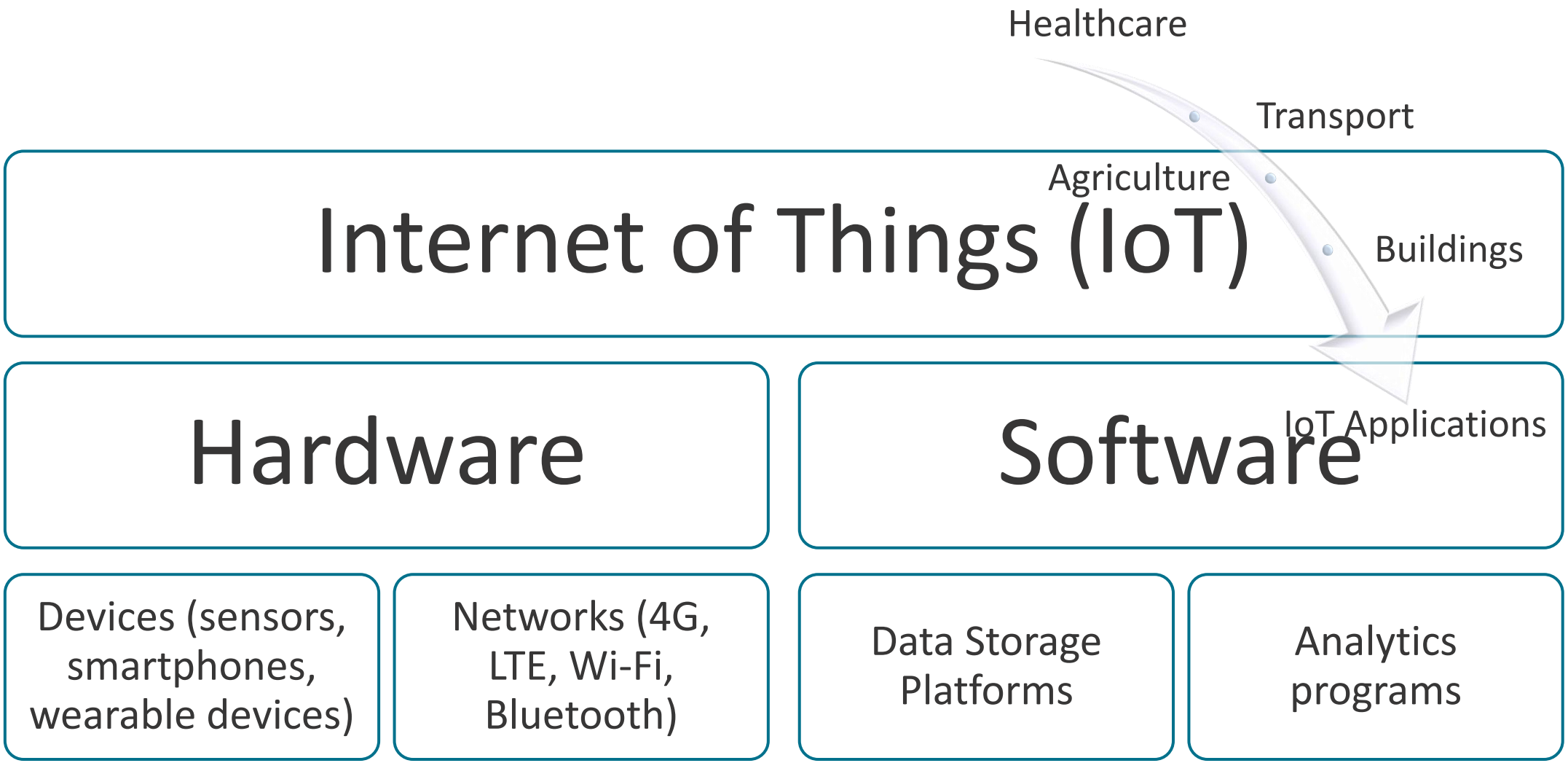
Research Outcomes

- Successful bids for the establishment of CSRI (2015) and the CSCRC (2017)
- Over $2.5M in external research income
- 100+ research publications including high impact journals such as IEEE Transactions

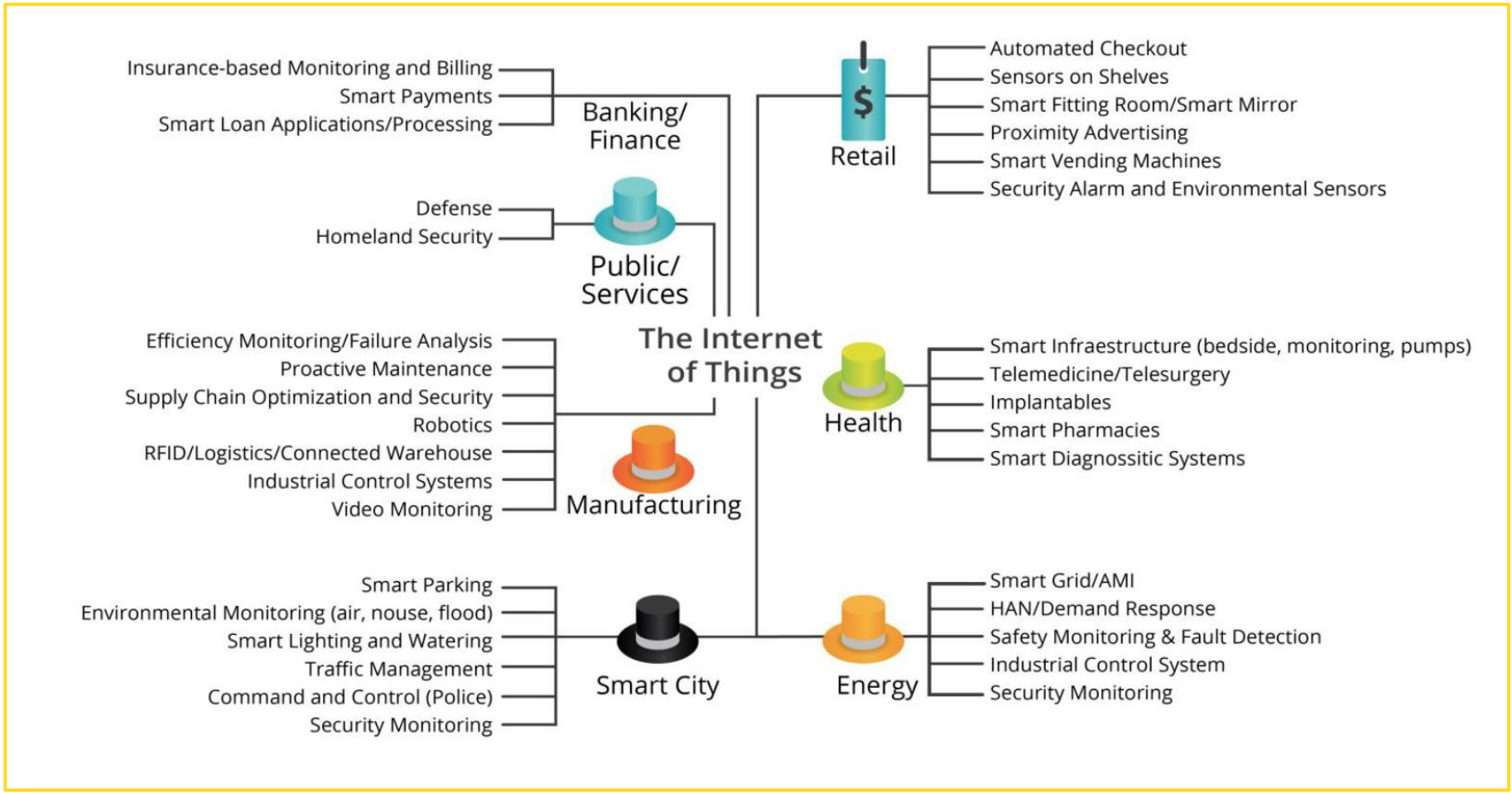
The changing cyber security landscape



What is the IoT?

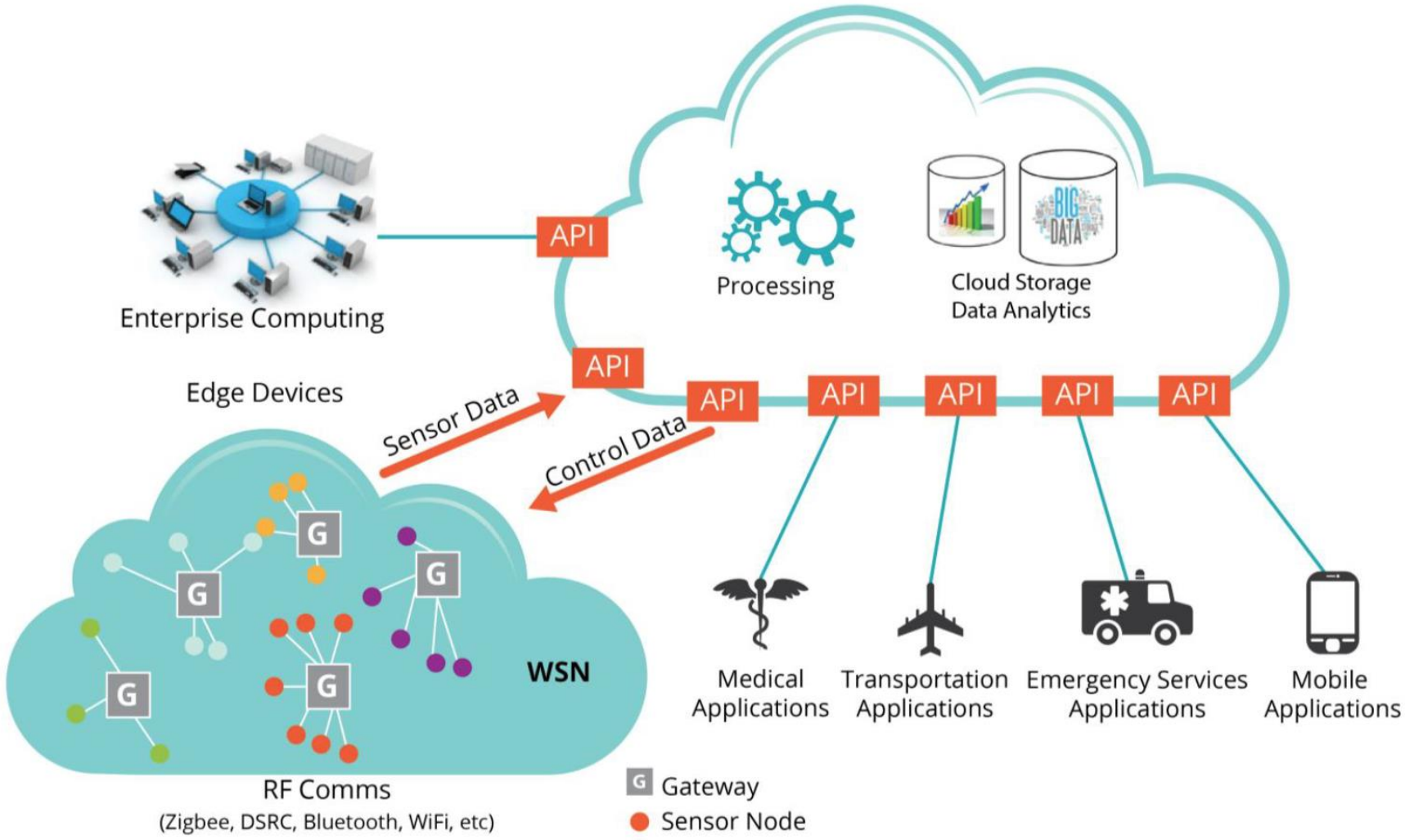


Security and Privacy Critical for IoT Application Domains



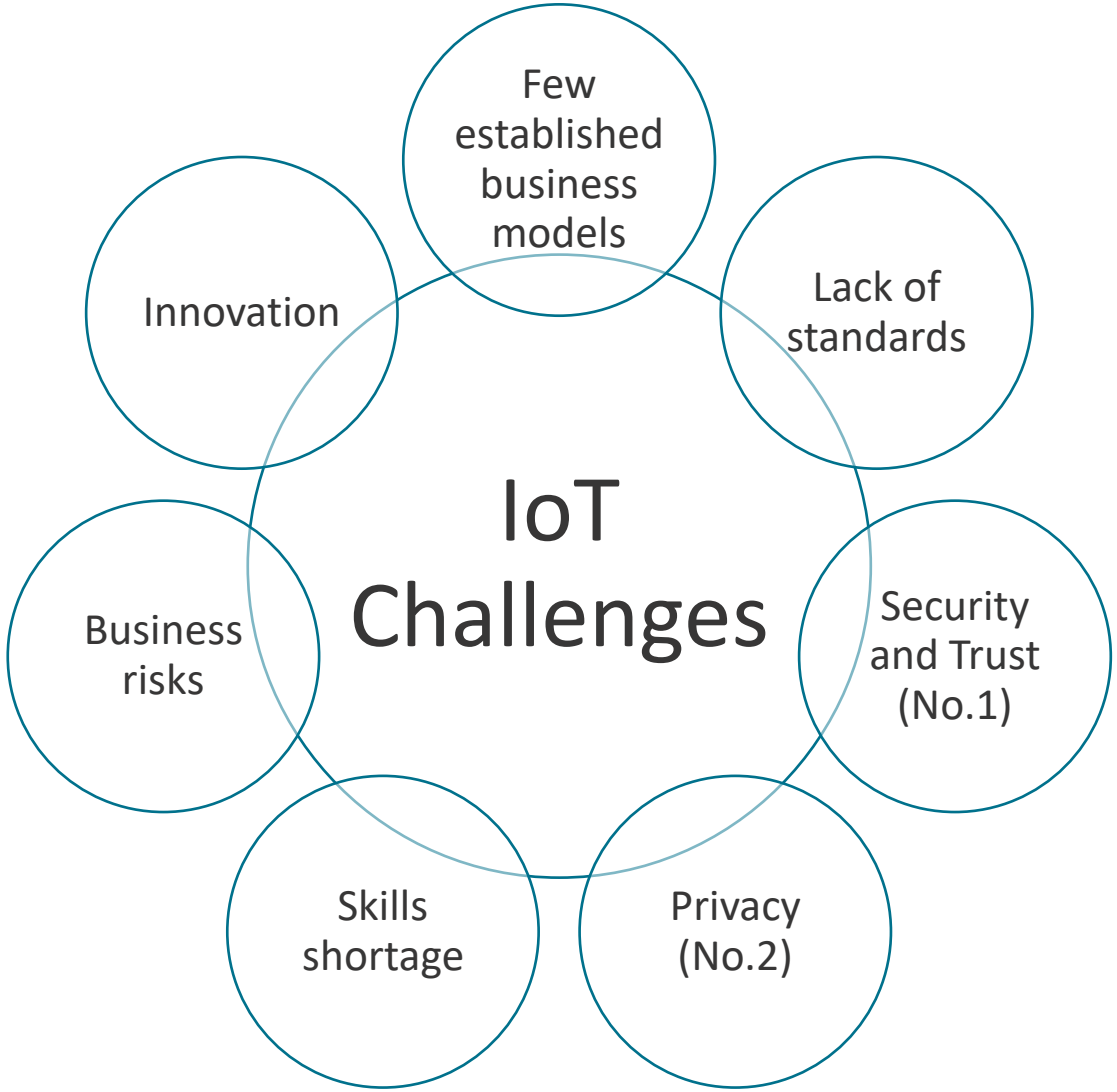
Source: CSA, 2015

The IoT System View

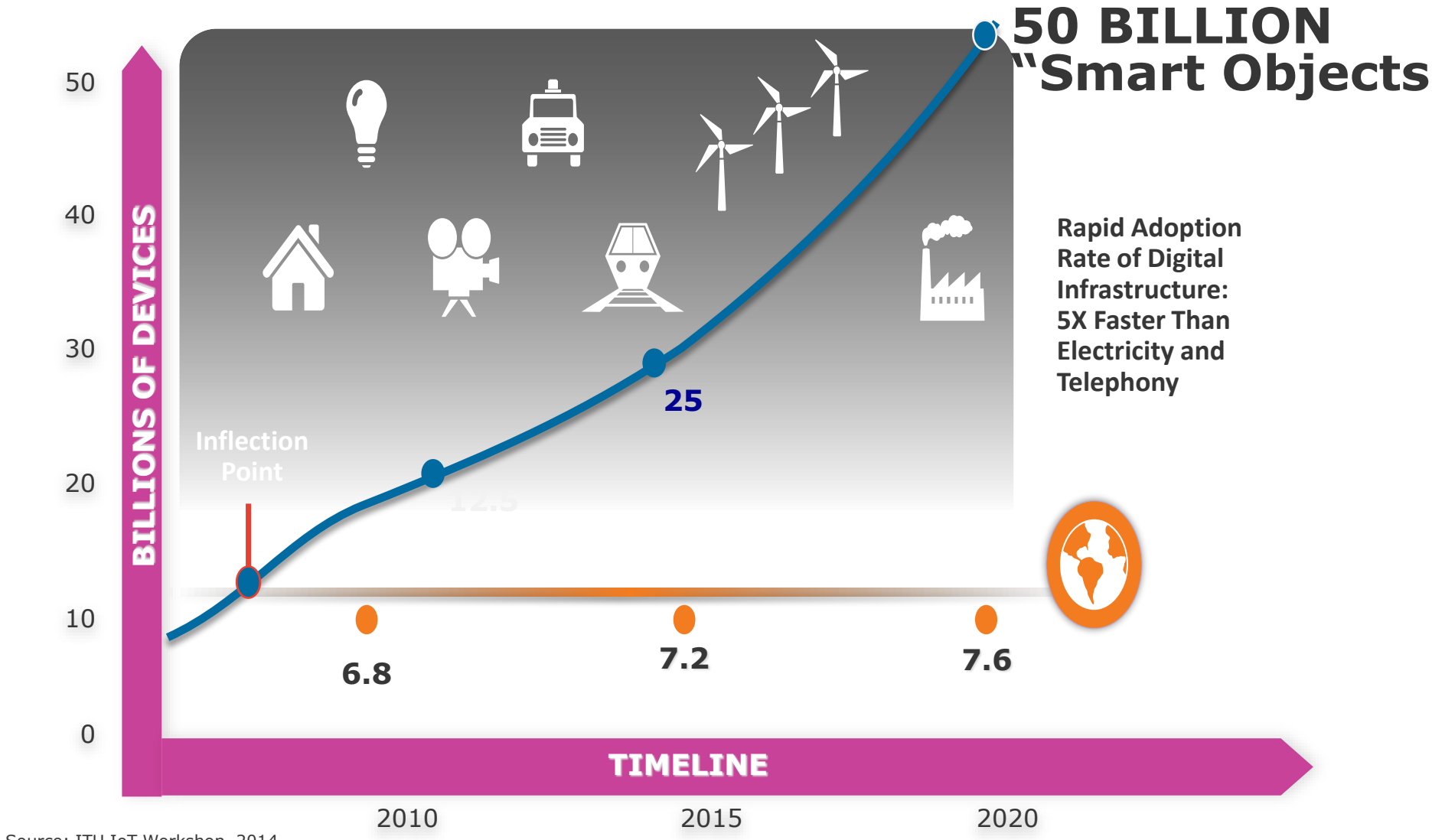


Source: CSA, 2015

IoT Challenges

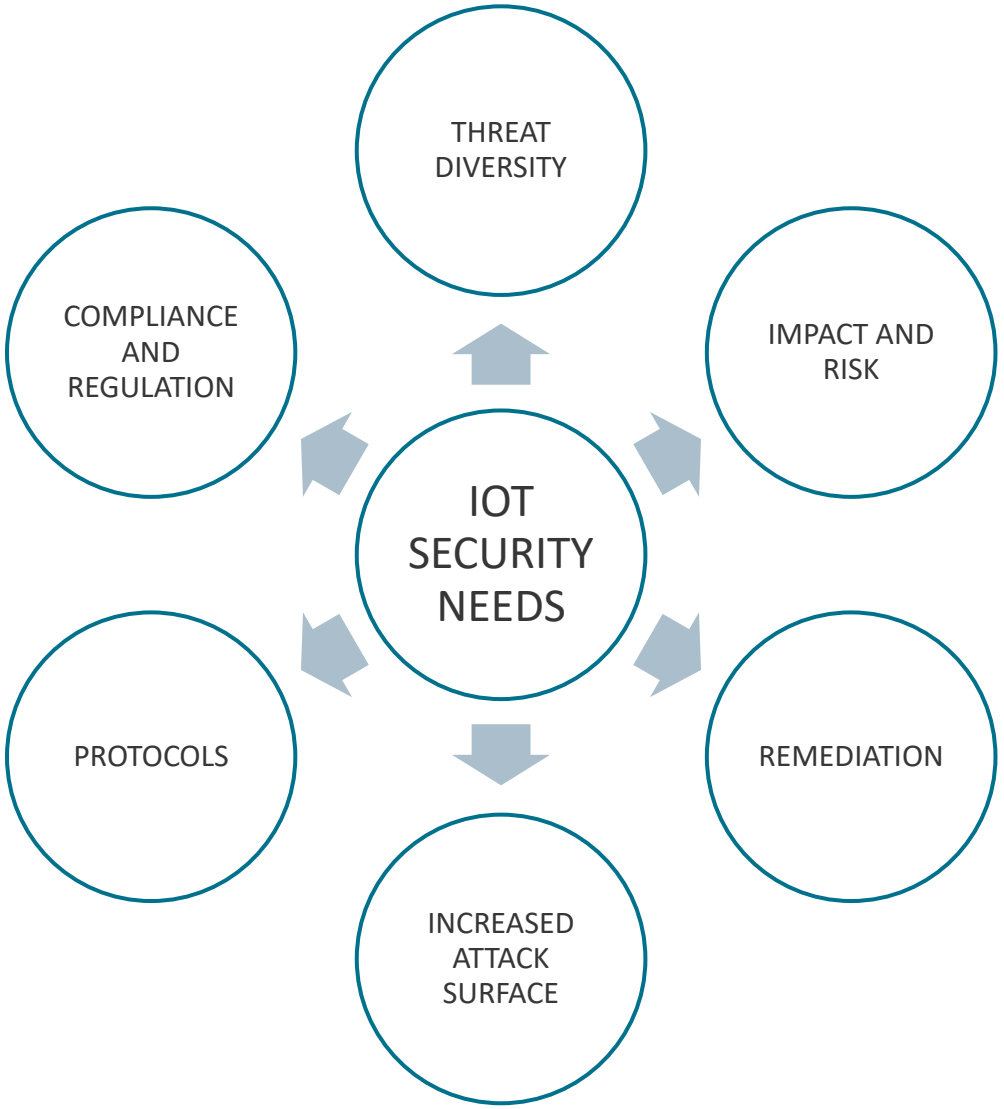


IoT is Growing Rapidly

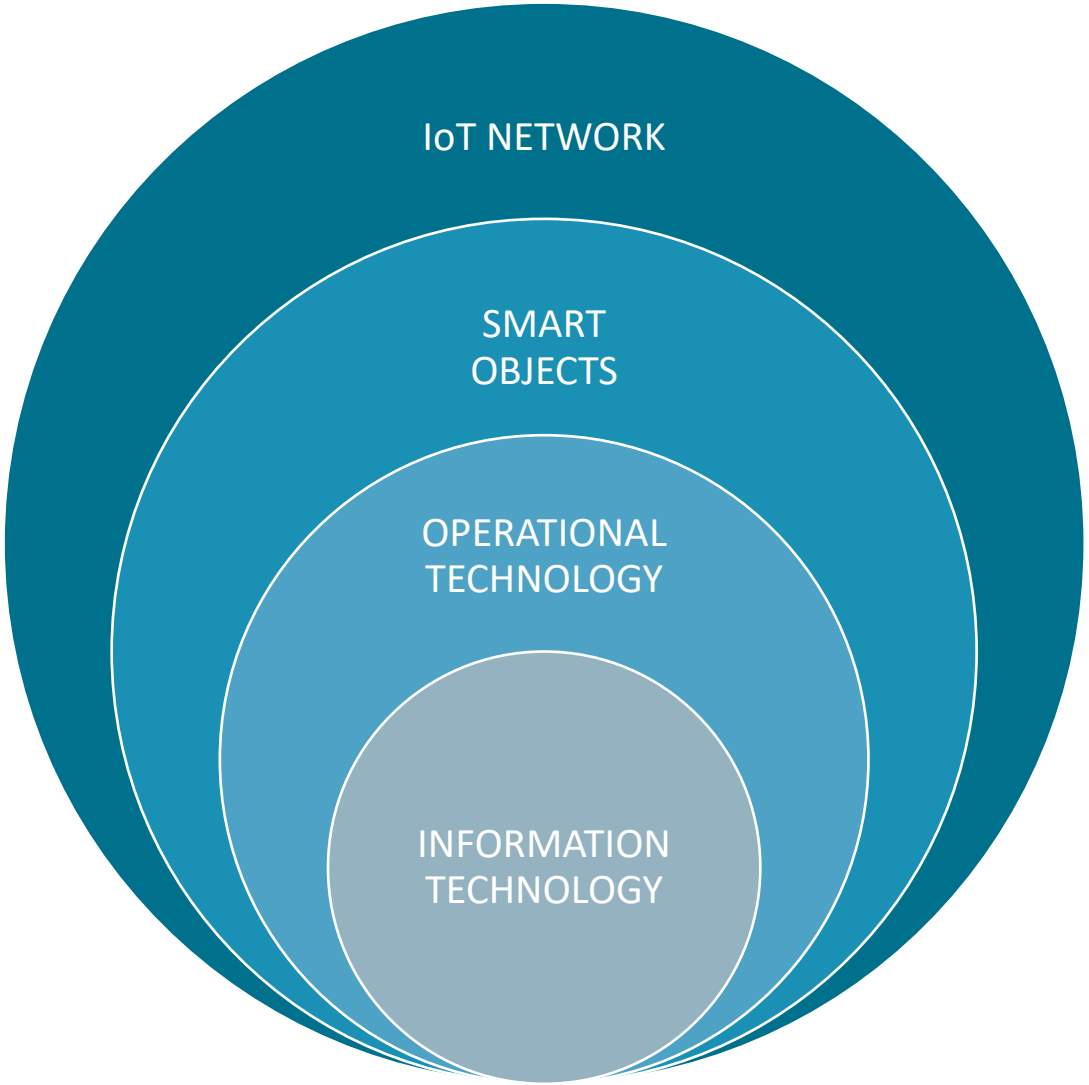


Source: ITU IoT Workshop, 2014

IoT Expands Security Needs



IoT network – more that just “IT”



OWASP Top 10 IOT SECURITY RISKS

Insecure web Interface	•Exploitability : EASY •Prevalence: COMMON •Impact: SEVERE
Insufficient Authn/z	•Exploitability : AVERAGE •Prevalence: COMMON •Impact: SEVERE
Insecure Network Services	•Exploitability : AVERAGE •Prevalence: UNCOMMON •Impact: MODERATE
Lack of Transport Encryption	•Exploitability : AVERAGE •Prevalence: COMMON •Impact: SEVERE
Privacy Concerns	•Exploitability : AVERAGE •Prevalence: COMMON •Impact: SEVERE

OWASP Top 10 IOT SECURITY RISKS

Insecure Cloud Interface	•Exploitability : AVERAGE •Prevalence: COMMON •Impact: SEVERE
Insecure Mobile Interface	•Exploitability : AVERAGE •Prevalence: COMMON •Impact: SEVERE
Insufficient Security Configurability	•Exploitability : AVERAGE •Prevalence: COMMON •Impact: MODERATE
Insecure Software/Firmware	•Exploitability : DIFFICULT •Prevalence: COMMON •Impact: SEVERE
Poor Physical Security	•Exploitability : AVERAGE •Prevalence: COMMON •Impact: SEVERE

IoT Threat Types

Spoofing Identity	• Authentication protocols, Device/identity bootstrapping, Unique identities
Tampering with Data	• Identify and implement configuration restrictions, Implement principle of least privilege
Repudiation	• Health checks on data and device functionality, Design in methods to restrict the replay of messages (e.g., sequence numbers / timestamps).
Information Disclosure	• Implement cryptography carefully (data at rest, key zeroization, TLS/DTLS)
Denial of Service	• Implement rate-limiting on APIs as needed.
Elevation of Privilege	• Design based on principle of least privilege for all user and service roles.
Bypassing Physical Security	• Debug ports should be password protected and disabled. Techniques such as tamper detection and response are advisable for IoT products designed to support critical infrastructure use cases.

Implement Authn/z and AC Features

- As a developer of IoT products you will likely hear that today's identity management, authentication and authorization protocols and systems are not optimized for IoT solutions.
- When considering authentication, authorization and access control features, you must understand how your IoT products are used and managed.
- The power of the IoT is that devices can communicate with each other, preferably in an automated manner. This means that to enable a value-added IoT ecosystem (within a home environment or a business environment), IoT devices must be able to establish trust relationships with other IoT devices.
- This device-to-device communication must be established securely or you run the risk of a bad actor taking advantage of an entry point into the network.

Recommended security controls for early adopters

- Analyze privacy impacts to stakeholder and adopt a privacy-by-design approach to IoT development and deployment
- Apply a secure systems engineering approach to architecting and deploying new IoT systems
- Implement layered security to defend IoT assets
- Implement data protection best-practices to protect sensitive information
- Define lifecycle controls for IoT devices
- Define and implement an authentication/authorization framework for IoT deployments
- Define and implement a logging/audit framework for IoT ecosystem

Thank You