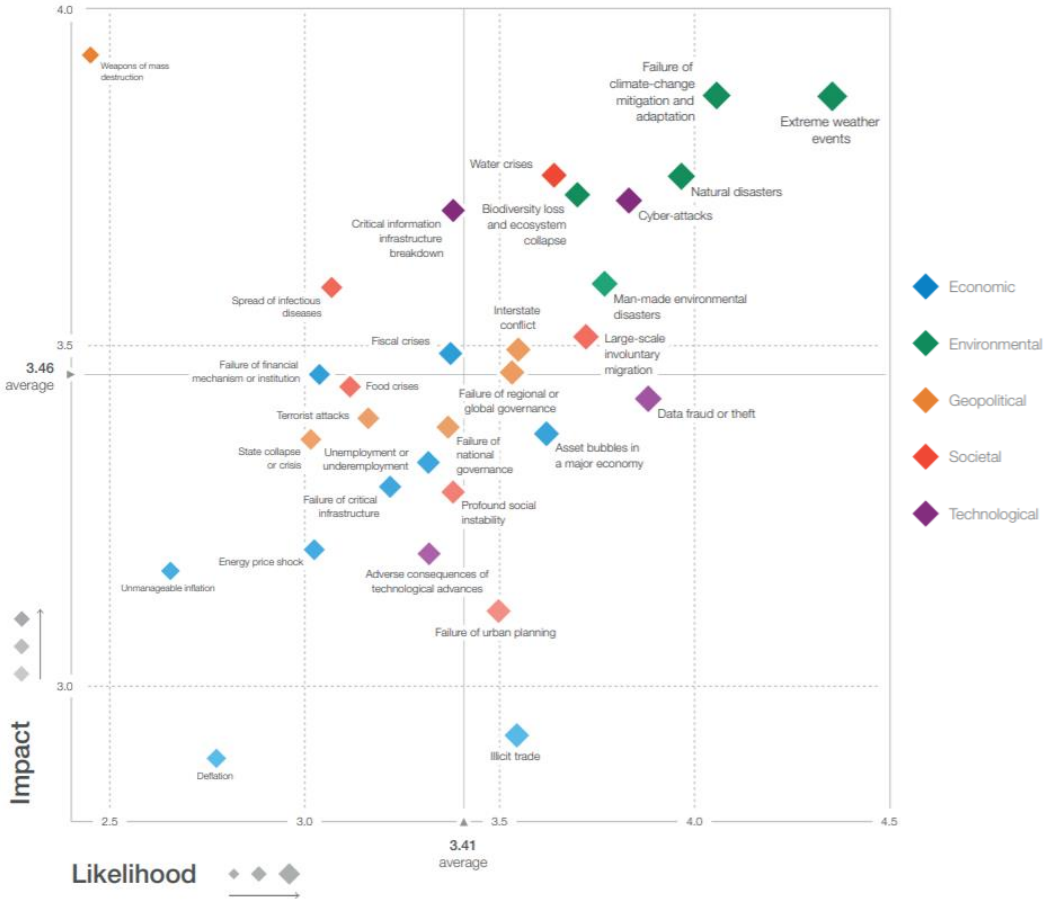
IoT Security (lecture notes)

3rd April 2019

Introduction

- Today, “smart” means “insecure”
- “If it does what I want it to do, I don’t care that it is part of a botnet”
- The IoT security problem is primarily a cultural one

Global Risk Landscape 2019



1. Extreme weather events
2. Failure of climate-change mitigation and adaptation
3. Natural disasters
4. Cyber-attacks

Source: World Economic Forum Global Risks Report 2019 - http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

Notable cybersecurity articles related to IoT

- Hackers Remotely Kill A Jeep On The Highway (2015)
  - https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
- “Internet of Things” security is hilariously broken and getting worse (2016)
  - https://arstechnica.com/information-technology/2016/01/how-to-search-the-internet-of-things-for-photos-of-sleeping-babies/
- Millions Of Private Messages Between Parents And Kids Hacked In Cloud Pets Security Breach (2017)
  - http://www.huffingtonpost.com.au/2017/02/28/millions-of-private-messages-between-parents-and-kids-hacked-in_a_21816860/
- CovertBand: Activity Information Leakage using Music | University of Washington (2017)
  - http://musicattacks.cs.washington.edu/activity-information-leakage.pdf

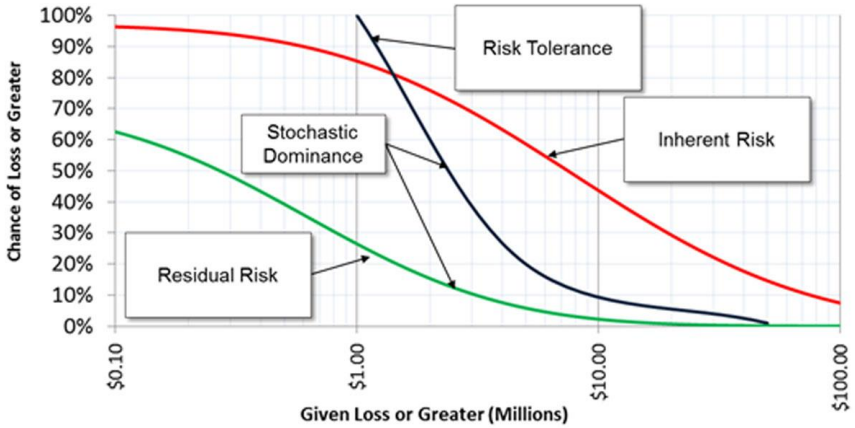
Notable cybersecurity articles related to IoT (continued)

- Burger King 'O.K. Google' Ad Doesn't Seem O.K. With Google (2017)
  - https://www.nytimes.com/2017/04/12/business/burger-king-tv-ad-google-home.html
- Hackers Found a (not-so-easy) way to make the Amazon Echo a spy bug (2018)
  - https://www.wired.com/story/hackers-turn-amazon-echo-into-spy-bug
- Amazon’s Alexa started ordering people dollhouses after hearing its name on TV (2017)
  - https://www.theverge.com/2017/1/7/14200210/amazon-alexa-tech-news-anchor-order-dollhouse
- Smart cities around the world were exposed to simple hacks (2018)
  - https://www.cnet.com/news/smart-cities-around-the-world-were-exposed-to-simple-hacks/
- McAfee Researchers Find Poor Security Exposes Medical Data to Cybercriminals (2018)
  - https://securingtomorrow.mcafee.com/mcafee-labs/mcafee-researchers-find-poor-security-exposes-medical-data-to-cybercriminals/

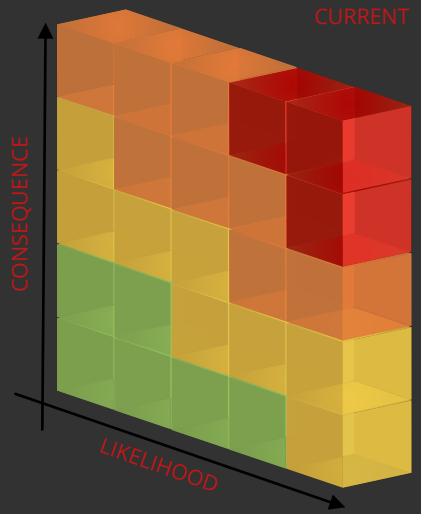
Notable cybersecurity articles related to IoT (continued)

- Hacking pacemakers, insulin pumps and patients' vital signs in real time (2018)
  - https://www.csoonline.com/article/3296633/security/hacking-pacemakers-insulin-pumps-and-patients-vital-signs-in-real-time.html
- This Guy Hacked Hundreds Of Planes From The Ground (2018)
  - https://www.forbes.com/sites/thomasbrewster/2018/08/09/this-guy-hacked-hundreds-of-planes-from-the-ground/
- New flaws in 4G, 5G allow attackers to intercept calls and track phone locations (2019)
  - https://techcrunch.com/2019/02/24/new-4g-5g-security-flaws/

Cybersecurity is ultimately a risk management exercise



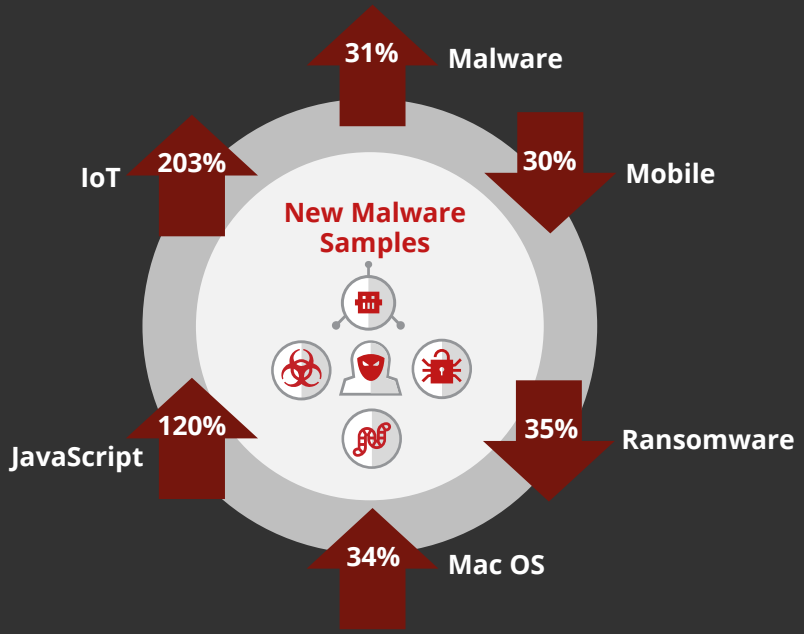
Source: How to Measure Anything in Cybersecurity Risk – Hubbard & Seiersen



McAfee Global Threat Intelligence received on average 49 billion queries per day in Q3 2018

Coin Miner Malware

We register around 8 new threat samples every second



Source: McAfee (Dec 2018)

Data breaches

87% of breaches took "minutes or less" for attackers to gain access

68% of breaches were undiscovered for one or more months

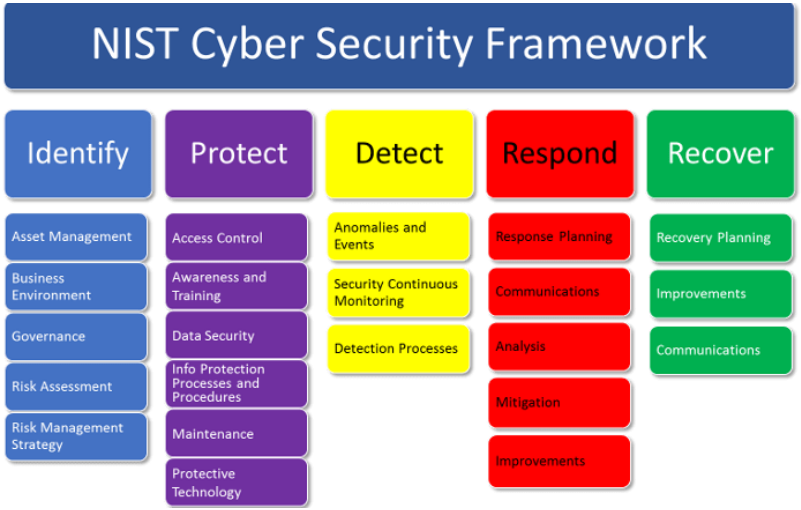
How do attackers get in?

- 48% featured hacking
- 30% included malware
- 17% involved errors
- 17% were social attacks
- 12% were nation-state-affiliated
- 50% involved organised crime
- 73% were perpetrated primarily by external parties
- 27% were perpetrated primarily by insiders

Source: Verizon Data Breach Investigations Report 2018

Top cloud security risks

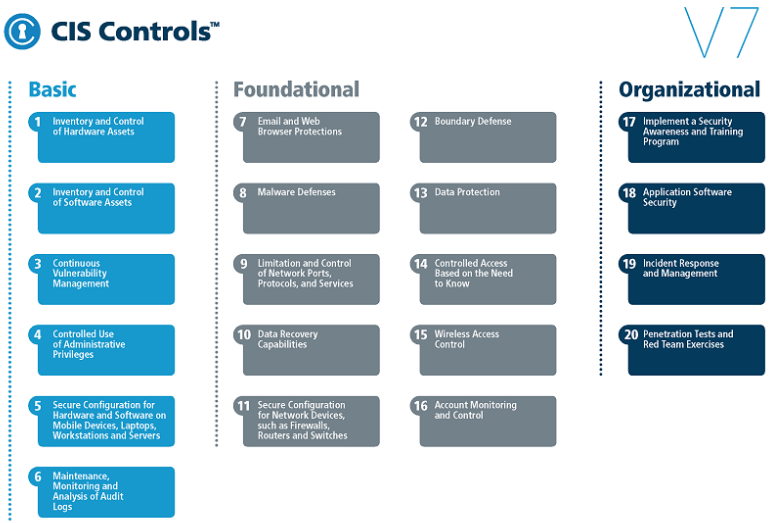
- Data Breach / Loss
- Insufficient Identity, Credential and Access Management (including Account Hijacking and Malicious Insiders)
- Cyber Threats / Abuse and Nefarious Use of Cloud Services / DoS
- Insecure Interfaces and APIs
- Insufficient Due Diligence
- System and / or Shared Technology Vulnerabilities


NIST Cyber Security Framework
Identify
Asset Management
Business Environment
Governance
Risk Assessment
Risk Management Strategy
Protect
Access Control
Awareness and Training
Data Security
Info Protection Processes and Procedures
Maintenance
Protective Technology
Detect
Anomalies and Events
Security Continuous Monitoring
Detection Processes
Respond
Response Planning
Communications
Analysis
Mitigation
Improvements
Recover
Recovery Planning
Improvements
Communications


1. Meeting Stakeholder Needs
2. Covering the Enterprise End-to-end
3. Applying a Single Integrated Framework
4. Enabling a Holistic Approach
5. Separating Governance From Management
COBIT 5 Principles


Information Security Management System
ISO
27001
Certified


PCI
Security
Standards Council


CIS Controls™
V7
Basic
1 Inventory and Control of Hardware Assets
2 Inventory and Control of Software Assets
3 Continuous Vulnerability Management
4 Controlled Use of Administrative Privileges
5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6 Maintenance, Monitoring and Analysis of Audit Logs
Foundational
7 Email and Web Browser Protections
8 Malware Defenses
9 Limitation and Control of Network Ports, Protocols, and Services
10 Data Recovery Capabilities
11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12 Boundary Defense
13 Data Protection
14 Controlled Access Based on the Need to Know
15 Wireless Access Control
16 Account Monitoring and Control
Organizational
17 Implement a Security Awareness and Training Program
18 Application Software Security
19 Incident Response and Management
20 Penetration Tests and Red Team Exercises

Australian Signals Directorate (ASD) Essential Eight

Threat: To prevent malware running	
Application whitelisting TOP 4 A whitelist only allows selected software applications to run on computers.	***Patch applications TOP 4*** A patch fixes security vulnerabilities in software applications.
Disable untrusted Microsoft Office macros Microsoft Office applications can use software known as 'macros' to automate routine tasks.	***User application hardening*** Block web browser access to Adobe Flash Player (uninstall if possible), web ads and untrusted Java code on the Internet.
Threat: To limit the extent of incidents and recover data	
Restrict administrative privileges TOP 4 Only use administrator privileges for managing systems, installing legitimate software and applying software patches. These should be restricted to only those that need them.	***Patch operating systems TOP 4*** A patch fixes security vulnerabilities in operating systems.
Multi-factor authentication This is when a user is only granted access after successfully presenting multiple, separate pieces of evidence. Typically something you know, like a passphrase; something you have, like a physical token; and/or something you are, like biometric data.	***Daily backup of important data*** Regularly back up all data and store it securely offline.

Source: https://cyber.gov.au

Key IoT security challenges

Low powered	Limited computing capabilities mean difficulty implementing security controls (e.g. encryption).
Standards and regulation	Lack of government regulation and standards mean most are not designed with security in mind.
Lifecycle management	Keeping devices up to date is not something that is currently well managed, leading to security vulnerabilities potentially remaining unpatched indefinitely.
Transport protocols	The sheer number of emerging connection protocols makes them difficult to manage and secure.
Physical access	Devices are increasingly unlikely to be located in physically secure sites, significantly increasing the opportunities for attackers to compromise their integrity.
Number of devices	IoT deployments are largely uncontrolled environments (in the context of security) where the number of devices grows exponentially, making it extremely challenging for cyber security teams to govern and manage.
Availability and continuity	Devices are often not designed without alternate options to maintain availability of both functionality and connectivity in the event of failure.

Common IoT security weaknesses

Interface
(web/cloud/mobile/physical)

Security configurability

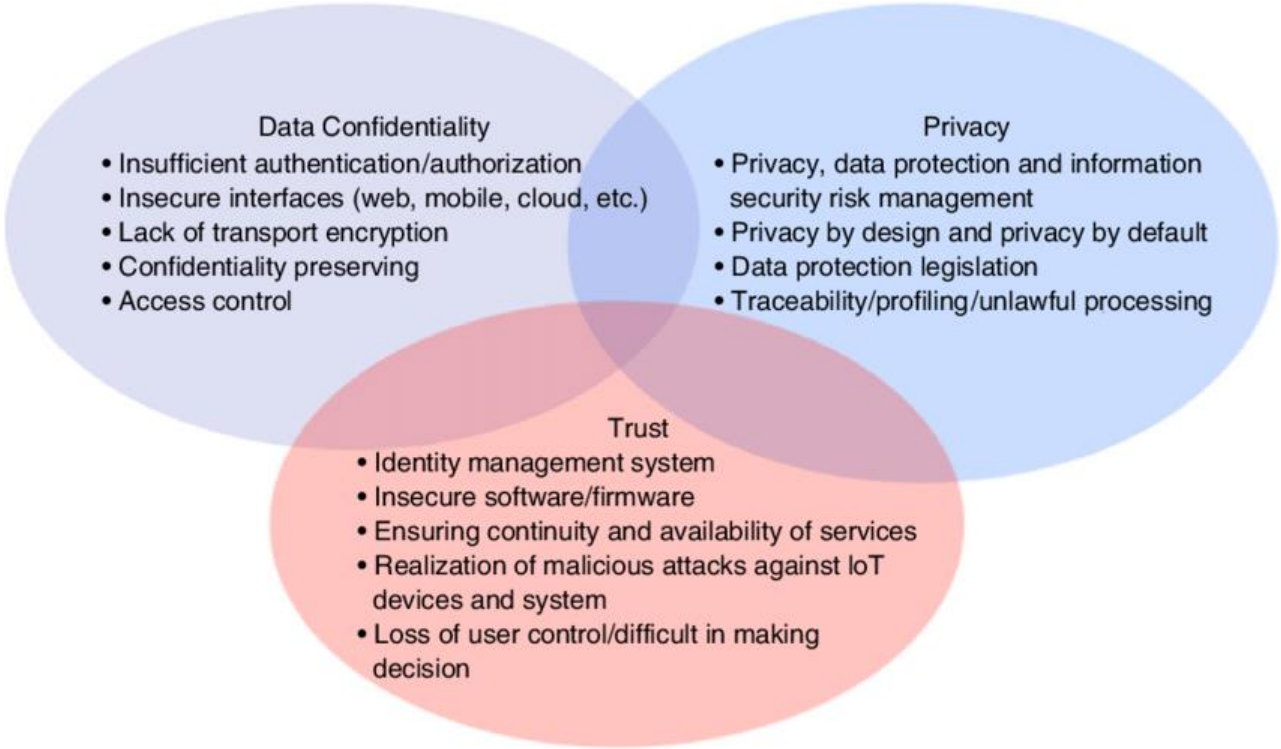
Authentication/authorisation

Network connectivity and services

Confidentiality & integrity
verification

Software & hardware (incl.
firmware, memory, sensors)

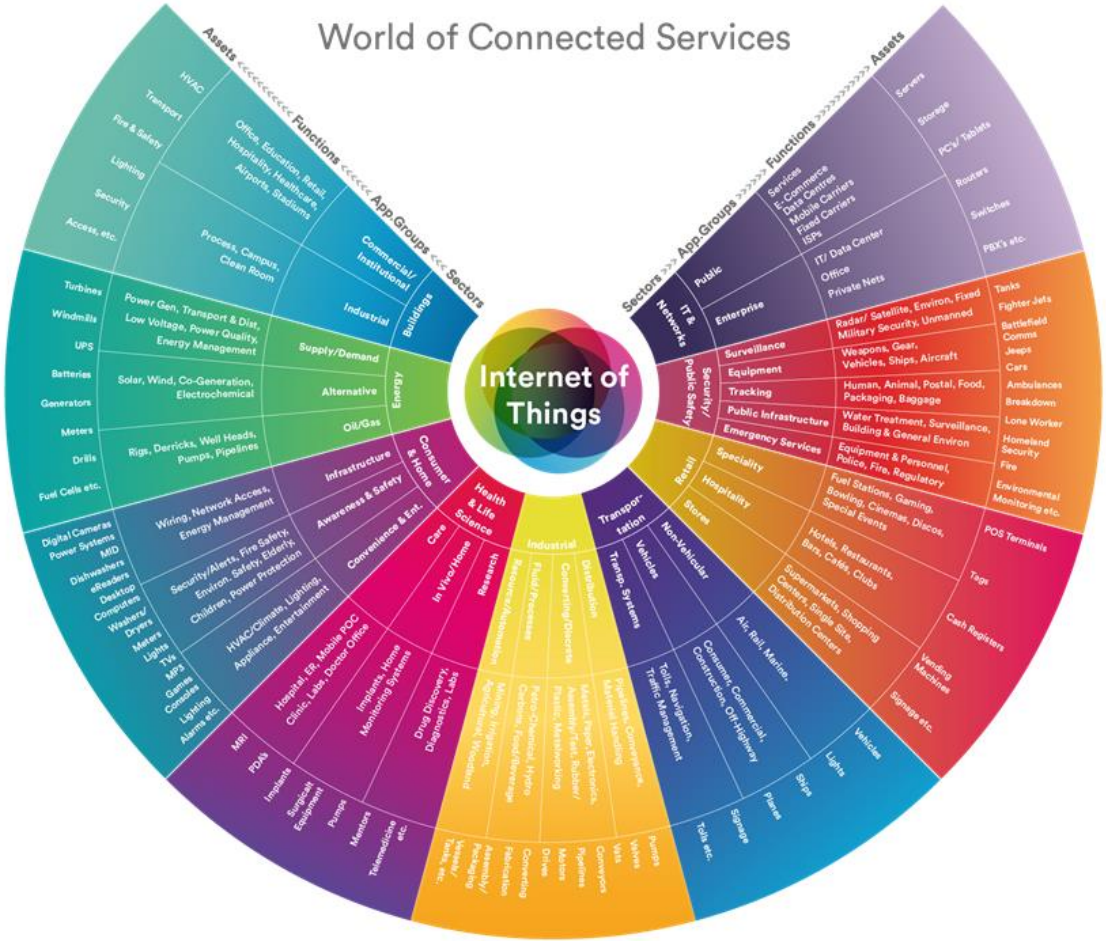
IoT data security concerns



Source: https://www.researchgate.net/figure/Security-issues-in-IoT_fig1_299421725

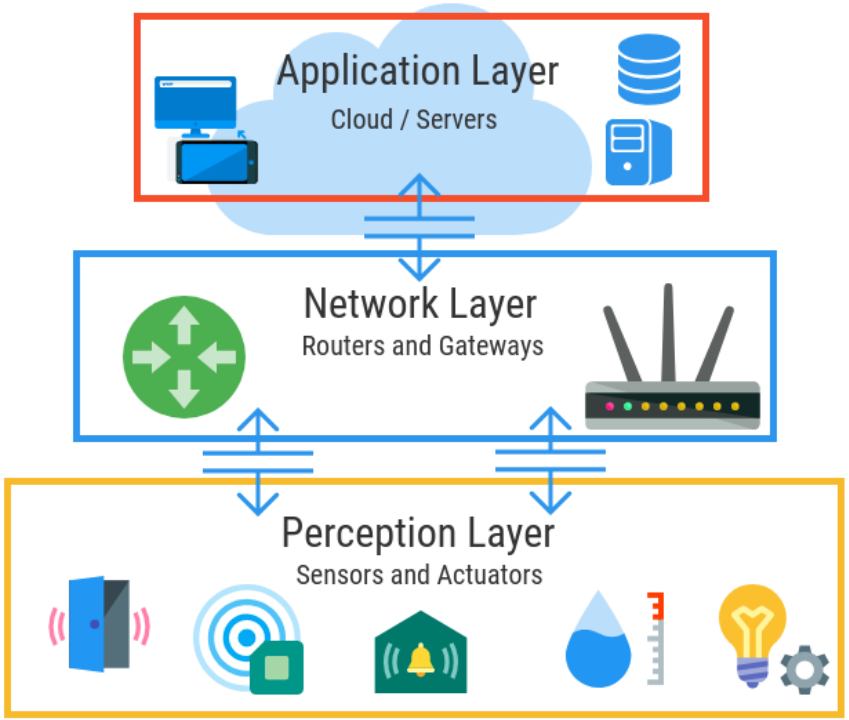
Information a hacker could obtain from an IoT device

Source: https://heimdalsecurity.com/blog/internet-of-things-security/



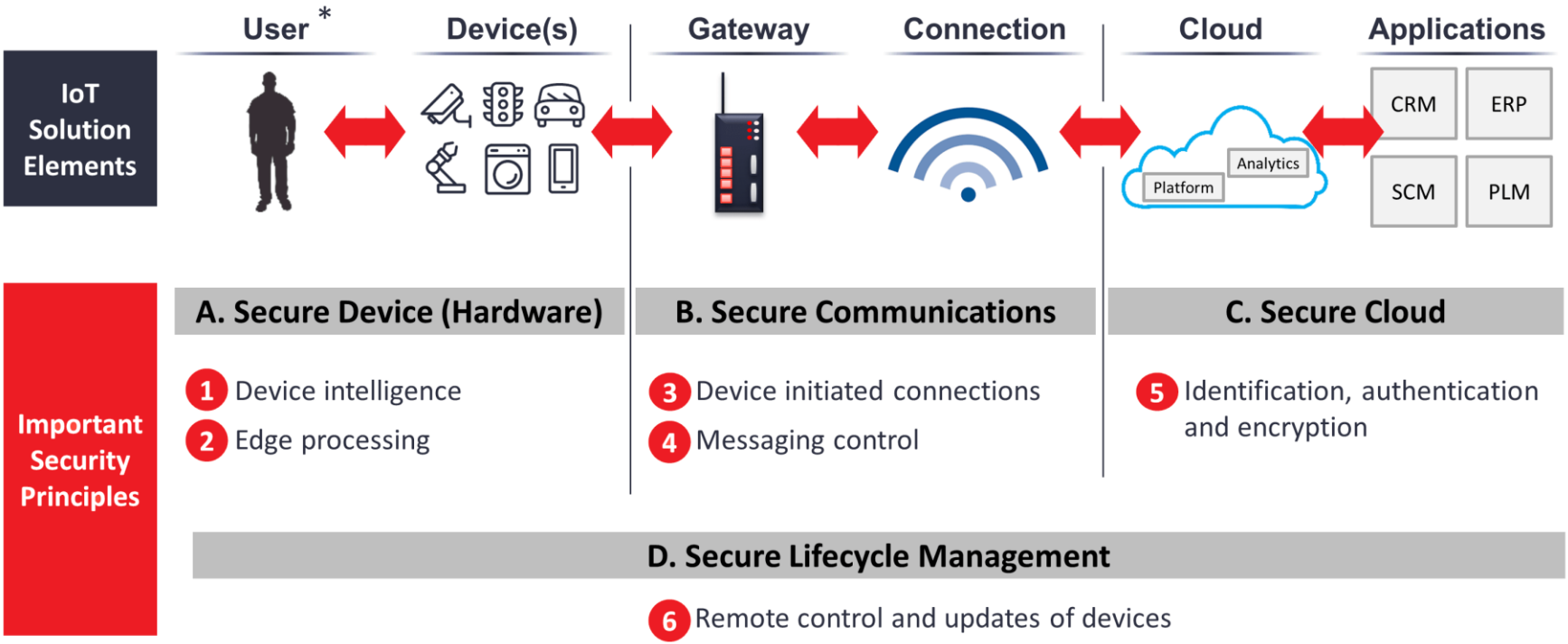
Source: https://www.beechamresearch.com/

In a nutshell...



Source: https://www.netburner.com/learn/architectural-frameworks-in-the-iot-civilization/

Six principles of IoT Security Architecture



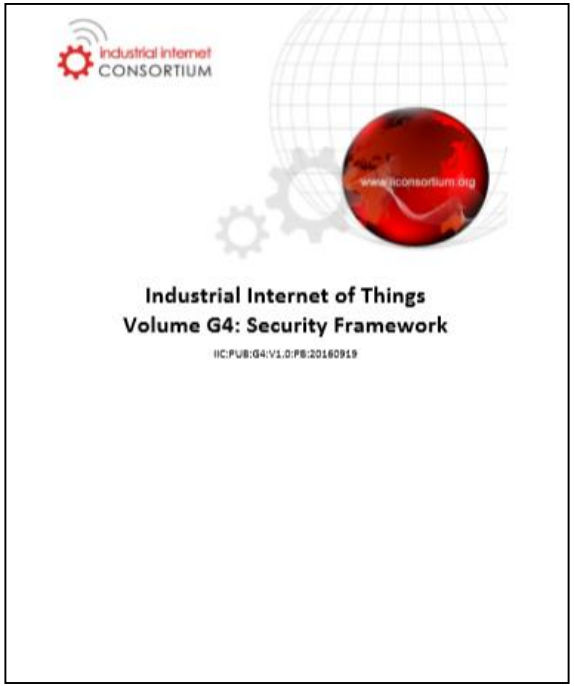
Source**: IoT Analytics* * User**: can represent a person, device, system, or application*

IoT wireless protocols

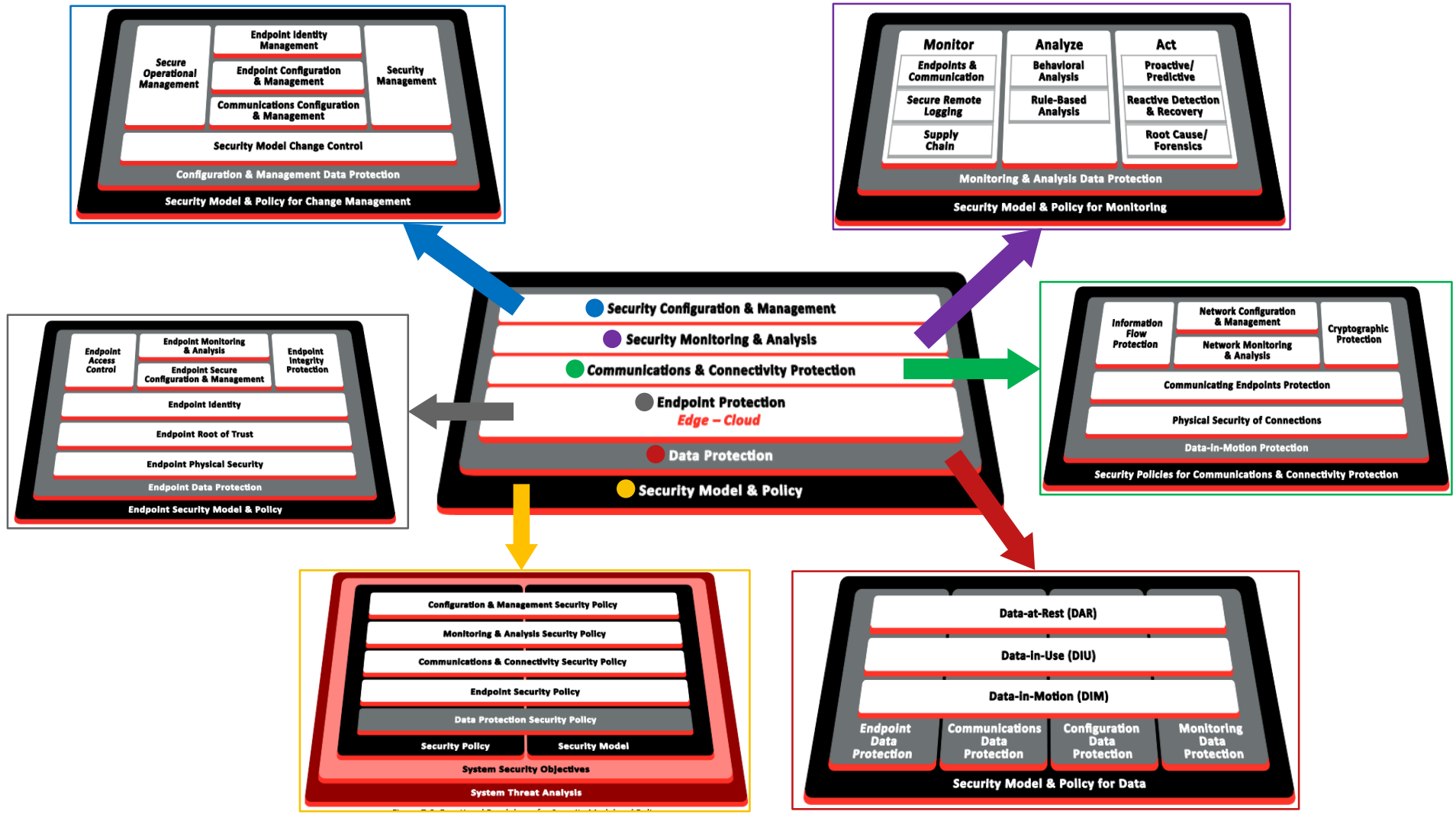
Key wireless technologies and their characteristics									
	5G	BLE	Cat-M1	LoRaWAN	LTE-A	NB-IoT	Sigfox	Wi-Fi	Zigbee
Open standards or proprietary	Open standards	Open standards	Open standards	Proprietary	Open standards	Open standards	Proprietary	Open standards	Open standards
Public or private	Public/ private	Private	Public	Public/ private	Public/ private	Public	Public	Public/ private	Private
Range	Wide	Short	Wide	Wide	Wide	Wide	Wide	Local	Short
Low or high bandwidth	High/low	Low	Low	Low	High	Low	Low	High	Low
Licensed or unlicensed spectrum	Licensed/ Unlicensed	Unlicensed	Licensed	Unlicensed	Licensed/ Unlicensed	Licensed	Unlicensed	Unlicensed	Unlicensed
Current Global Status	Not launched	Widely available	Limited availability	Limited availability	Widely available	Limited availability	Limited availability	Widely available	Widely available

Source: https://www.ihsmarkit.com

Industrial Internet of Things (IIOT)



Source: https://www.iiconsortium.org/IISF.htm


Secure Operational Management
Endpoint Identity Management
Endpoint Configuration & Management
Communications Configuration & Management
Security Management
Security Model Change Control
Configuration & Management Data Protection
Security Model & Policy for Change Management
Monitor
Endpoints & Communication
Secure Remote Logging
Supply Chain
Analyze
Behavioral Analysis
Rule-Based Analysis
Act
Proactive/ Predictive
Reactive Detection & Recovery
Root Cause/ Forensics
Monitoring & Analysis Data Protection
Security Model & Policy for Monitoring
Endpoint Access Control
Endpoint Monitoring & Analysis
Endpoint Secure Configuration & Management
Endpoint Integrity Protection
Endpoint Identity
Endpoint Root of Trust
Endpoint Physical Security
Endpoint Data Protection
Endpoint Security Model & Policy
Security Configuration & Management
Security Monitoring & Analysis
Communications & Connectivity Protection
Endpoint Protection
Edge – Cloud
Data Protection
Security Model & Policy
Information Flow Protection
Network Configuration & Management
Network Monitoring & Analysis
Cryptographic Protection
Communicating Endpoints Protection
Physical Security of Connections
Data-in-Motion Protection
Security Policies for Communications & Connectivity Protection
Configuration & Management Security Policy
Monitoring & Analysis Security Policy
Communications & Connectivity Security Policy
Endpoint Security Policy
Data Protection Security Policy
Security Policy
Security Model
System Security Objectives
System Threat Analysis
Data-at-Rest (DAR)
Data-in-Use (DIU)
Data-in-Motion (DIM)
Endpoint Data Protection
Communications Data Protection
Configuration Data Protection
Monitoring Data Protection
Security Model & Policy for Data

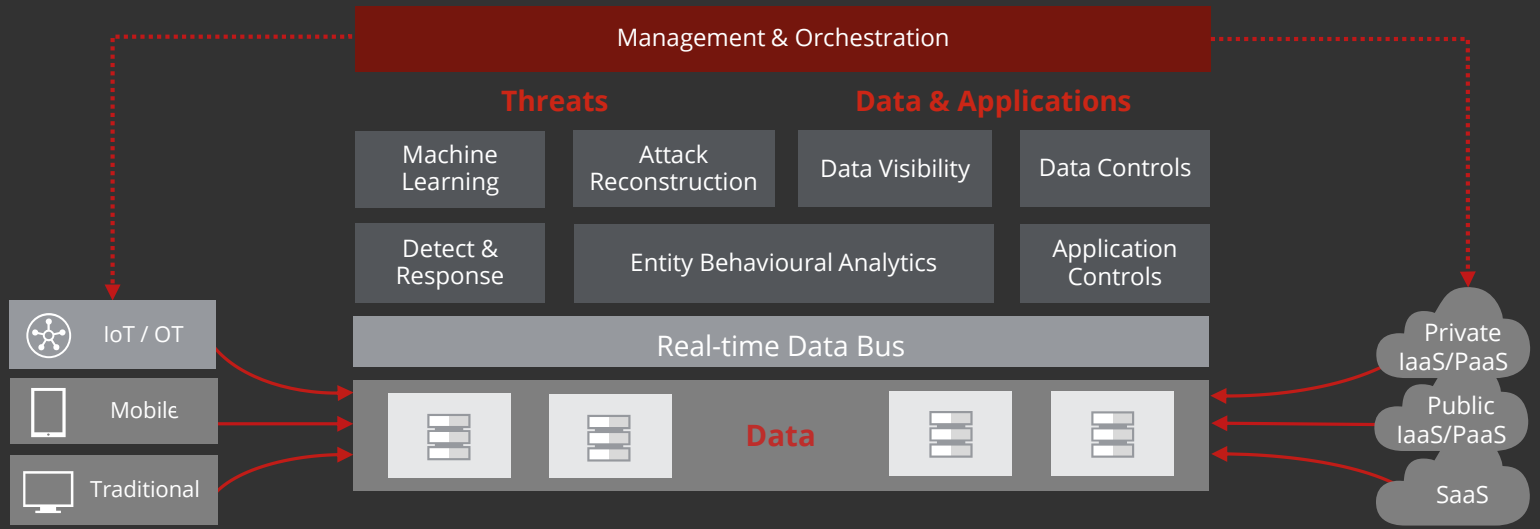
IoT Attack Surface

- I1. Weak Guessable, or Hardcoded Passwords
- I2. Insecure Network Services
- I3. Insecure Ecosystem Interfaces
- I4. Lack of Secure Update Mechanism
- I5. Use of Insecure or Outdated Components
- I6. Insufficient Privacy Protection
- I7. Insecure Data Transfer and Storage
- I8. Lack of Device Management
- I9. Insecure Default Settings
- I10. Lack of Physical Hardening

Source: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

Advanced cyber defence

Architecture



Device

- Visibility and contextual control
- Data Protection
- Threat Detection and Response

Security Operations

- System level Data Protection
- System level Threat Detection and Response
- Automation & Orchestration (Proactive / Reactive)

Cloud

- Visibility and contextual control in hybrid and multi-cloud environment
- Data and Workload Protection
- Threat Detection and Response

Advanced cyber defence

Bringing it all together

Prepare

- **Take a risk-based approach**
- Understand your data and assets
- Adopt a maturity and controls framework
- Ensure regular review and rehearsal of your incident response program

Compromise

- **Assume an adaptive trust environment**
- User awareness and education
- Proactive patching
- Whitelisting, sandboxing, encryption, access control, multi-factor authentication, limit privileged access

Maneuver

- **Implement an automated and integrated detect and response capability**
- Firewall/Proxy/IPS can block malicious and traffic
- Proactively hunt for threats and IoCs
- Use data analytics

Execute

- **Continuously monitor, remediate, and adapt**
- Track user and device identity, integrity and behaviour
- Monitor data at rest, in motion and in use
- Back up and restore files - keep a recent backup offsite and “air gapped”

How do we solve the problem and give ourselves more time for fun?

- Do not underestimate the threat; assume they are already in the system
- Cooperation and collaboration is critical; enough with protectionism
- Stop playing the hapless victim; take responsibility and be proactive

> “I’ve never found it hard to hack most people. If you listen to them, watch them, their vulnerabilities are like a neon sign screwed into their heads.” – Mr. Robot