Vision in IoT, why It's a Security Minefield and How to Navigate It

Dr. Lyndon Fawcett

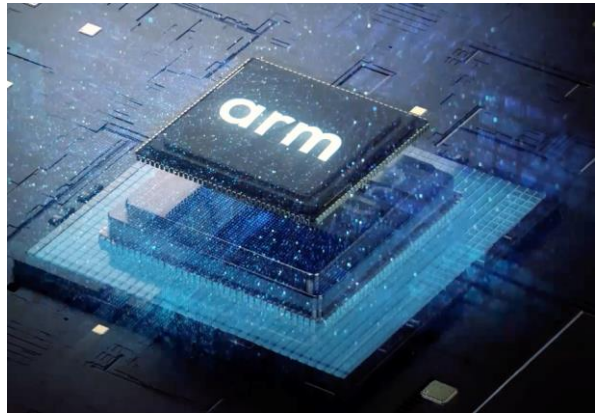
Principal Software Security Architect
Arm

arm

Company

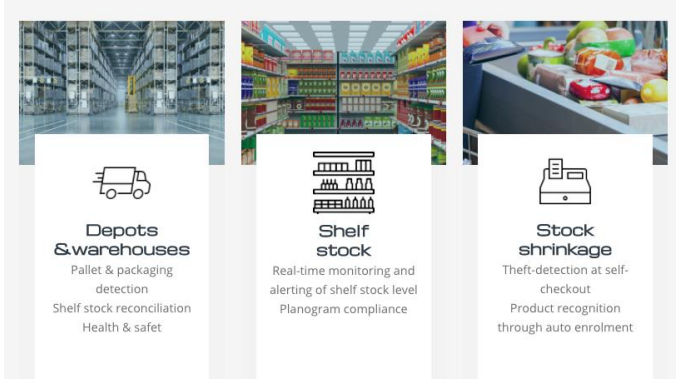
arm

Armv9



SeeChange
an arm company

SeeWare



arm

About this talk

arm

Intended audience & Objectives

Audience:

- Business decision makers (for vision in IoT)

Objectives

- Threat landscape of deploying vision in IoT
- The state of the art in guidance around security
- Recommendations for hardening

What this talk **is not**:

- A replacement for dedicated security professionals
- Holistic capture of security for your business

Vision in IoT

arm

Embedded vision use cases

Vision in critical systems:

- Autonomous cars
- Smart streets
  - CCTV
  - Water levels
- Industry 4.0
- Autonomous delivery
- Smart Homes

Critical systems

Sensitive data

93% See security as a key differentiator

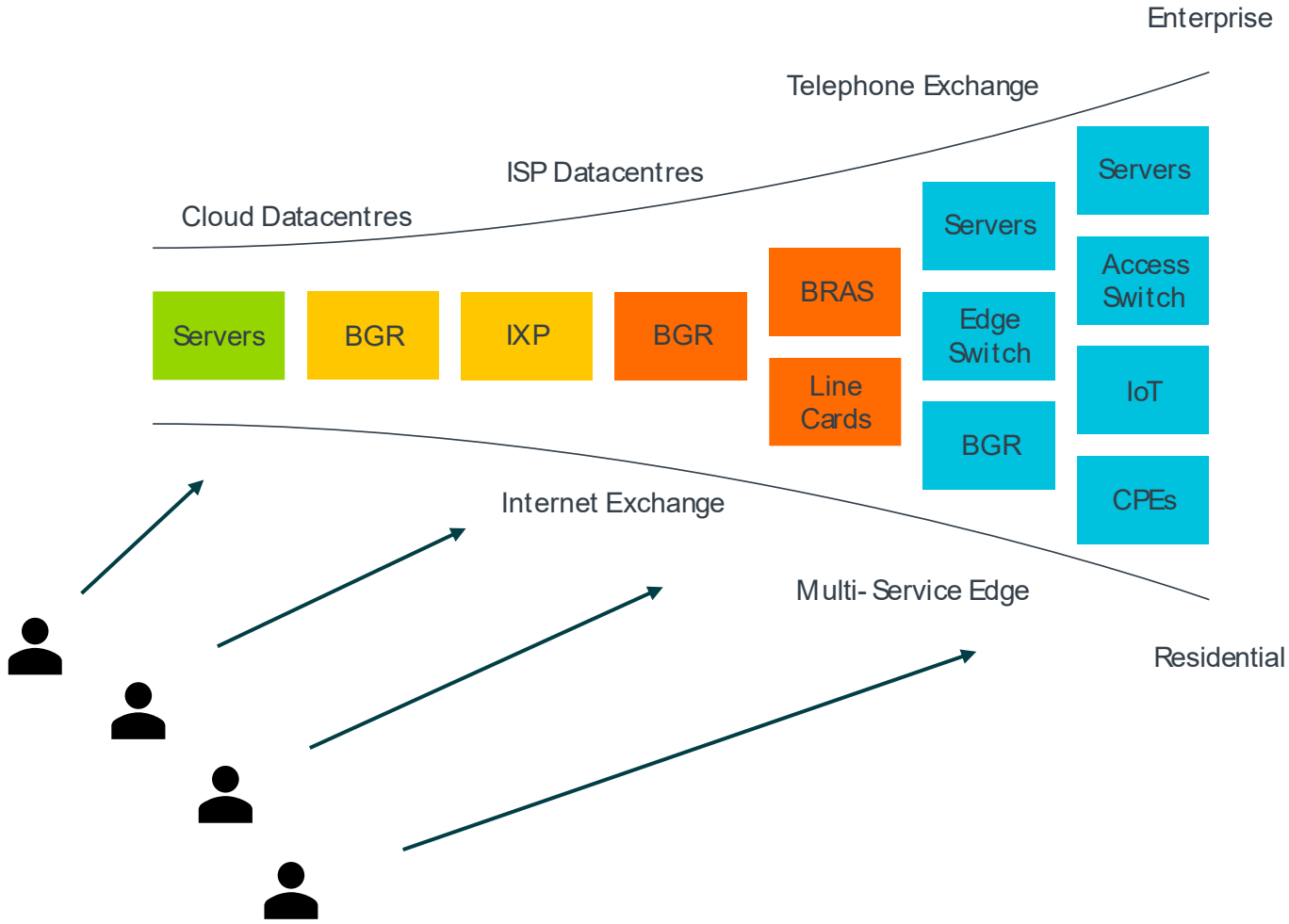
Threat Landscape

arm

Cloud to edge deployment continuum

Threat modeling

- Actors
- Context
- Heterogeneity



Vision/ML specific threats

- Adversarial attacks in computer vision
  - Sign manipulation example
  - Lane manipulation example
- Typographic attacks
  - https://openai.com/blog/multimodal-neurons/
- Knowledge distillation attacks
  - https://arxiv.org/pdf/1906.06046.pdf
  - Loss of IP

IoT threats

- Webcam/CCTV incidents
  - Smart home cameras with weak passwords
  - CCTV breach
- General IoT incidents (still applicable to vision)
  - Malicious control of car driver aids
  - Mirai Botnet

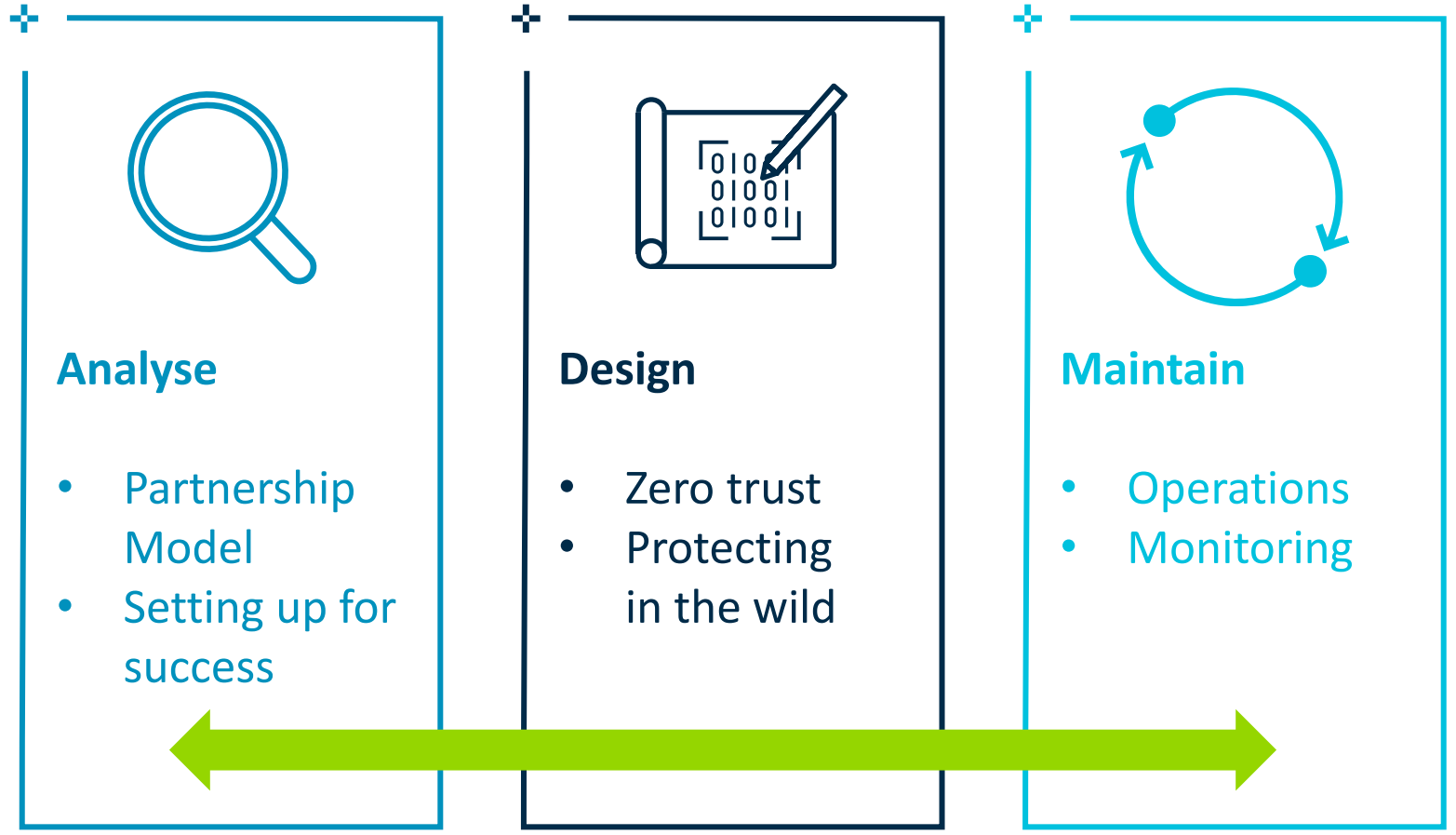
- https://www.bloomberg.com/news/articles/2021-03-09/hackers-expose-tesla-jails-in-breach-of-150-000-security-cams
- https://www.bbc.co.uk/news/technology-33650491
- https://en.wikipedia.org/wiki/Mirai_(malware)
- https://www.iotsecurityfoundation.org/iot-botnets-might-be-the-cybersecurity-industrys-next-big-worry/

arm

Navigating the minefield

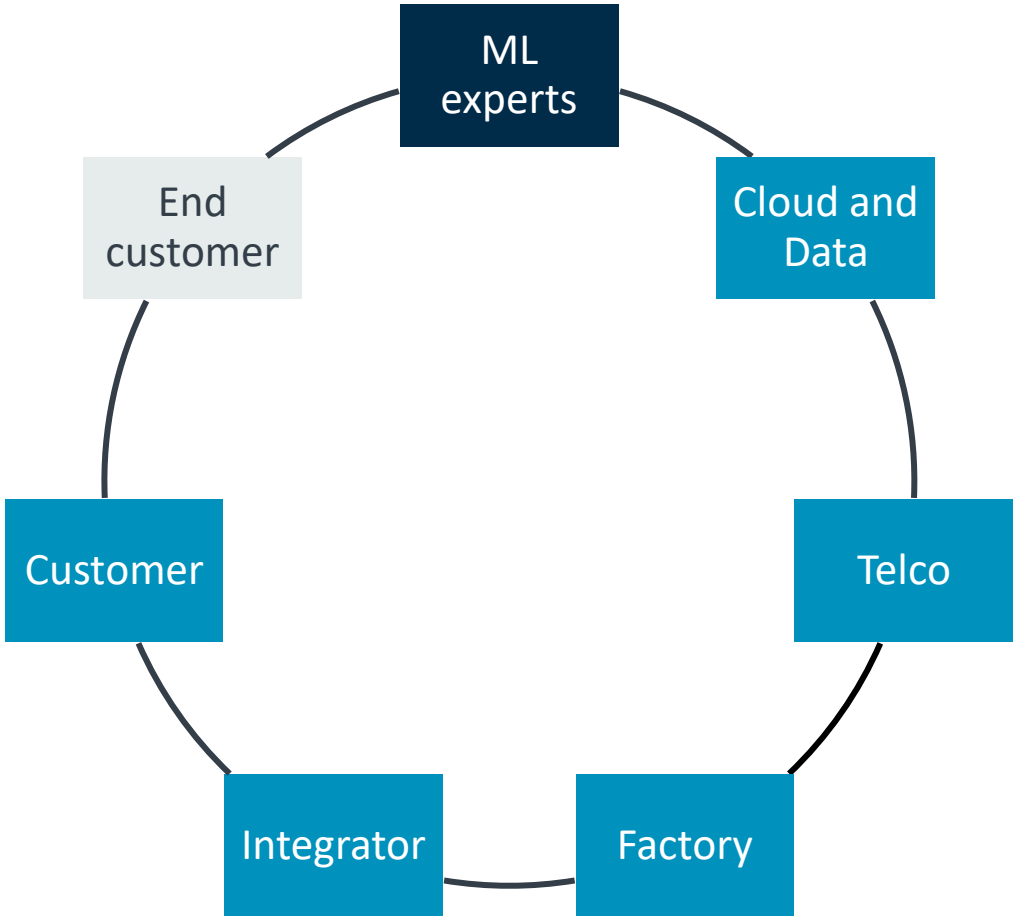
arm

Navigating the minefield: Overview



Analyse: Partner model to IoT

- Producing end solutions in Vision & IoT is difficult!
- How many components do you do in this circle?
- How many components do you directly rely on?



Analyse: setting up for success

- Perform risk analysis & threat modelling for all parts of your remit
- Understand what frameworks and standards you need to follow
  - NIST Cyber Security Framework
  - IoT Security Framework
- Validate your partners stance and implementation of security
  - Field specific standards and guidelines
    - Road vehicles -- Cyber security (**ISO/SAE FDIS 21434**)
    - IoT Security and Privacy (**ISO/IEC CD 27400.3**)
  - Pen-tests
- Selling security
  - Calculating your ROI

Design: Zero-Trust Security

- Follow and implement a ***Zero-Trust*** approach to security

Authentication & Identity

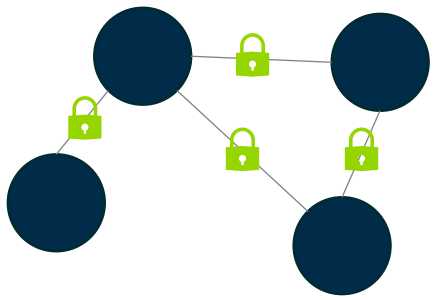
End2End Encryption

Observability & Monitoring

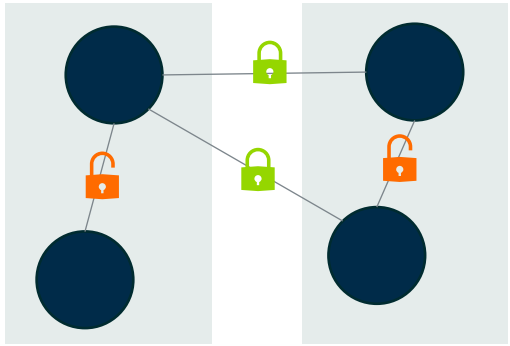
Data driven protection

Perimeter security

Zero-Trust Security



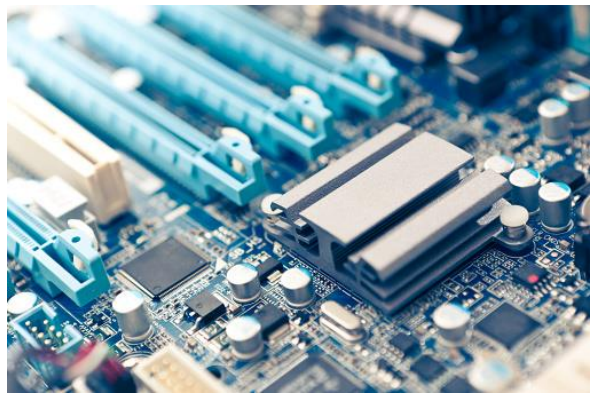
Perimeter Security



Design: Protecting IoT in the wild

Implementing security at the hardware layer

- Not using dev boards in production!
- RoT, Encrypted Storage, Secure Boot



- Tamper proofing
  - Fuses
- Device hardening
  - Removing access

- Minimizing risk potential
  - Limiting data
  - Limiting function

Maintain

- Getting certified for your field
- Operational security
  - Login detection, endpoint protection
- Using Multi-factor authentication (MFA)
- Pen-testing
- Fast Zero Day remediation

Summary & Questions

- Vision in IoT and the threat landscape
  - Vision use cases and critical systems
  - Adversarial attacks
  - IoT threats
- Navigating the minefield
  - Understanding the partnership model
  - Scoping your security
  - Standards and best practices

Parts not included

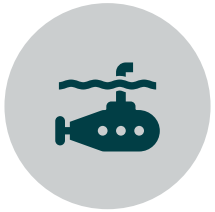
Appendix

arm

Warning: Parts not included!

SECURITY DEVELOPMENT LIFECYCLE (SDL)

INFLUENCING YOUR TEAM THAT SECURITY IS IMPORTANT



DEFENSE IN DEPTH

RELEASE CHECKPOINTS

AND MORE....

Frameworks & Specifications

- Threat Management
- Tooling & Automation
- E2E Security Process
- Operational Security

Still interested? Further reading:

Related content reading

- https://seechange.ai/privacy-and-security/
- https://seechange.ai/from-cloud-to-iot-securing-the-continuum/

General security reading

- https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.pdf
- https://www.cisco.com/c/dam/en/us/products/collateral/security/2020-outcomes-study-main-report.pdf
- https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program