SECURE TECHNOLOGY ALLIANCE

Security in the IoT Ecosystem: Trusting Data at the Edge

IoT Security Council Webinar

May 22, 2019

Who We Are

The Secure Technology Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption and widespread application of secure solutions.

We provide, in a collaborative, member-driven environment, education and information on how smart cards, embedded chip technology, and related hardware and software can be adopted across all markets in the United States.

What We Do

- Bring together stakeholders to effectively collaborate on promoting secure solutions technology and addressing industry challenges
- Publish white papers, webinars, workshops, newsletters, position papers and web content
- Create conferences and events that focus on specific markets and technology
- Offer education programs, training and industry certifications
- Provide networking opportunities for professionals to share ideas and knowledge
- Produce strong industry communications through public relations, web resources and social media

SECURE TECHNOLOGY ALLIANCE

Our Focus

- Access Control
- Authentication
- Healthcare
- Identity Management
- Internet of Things
- Mobile
- Payments
- Transportation

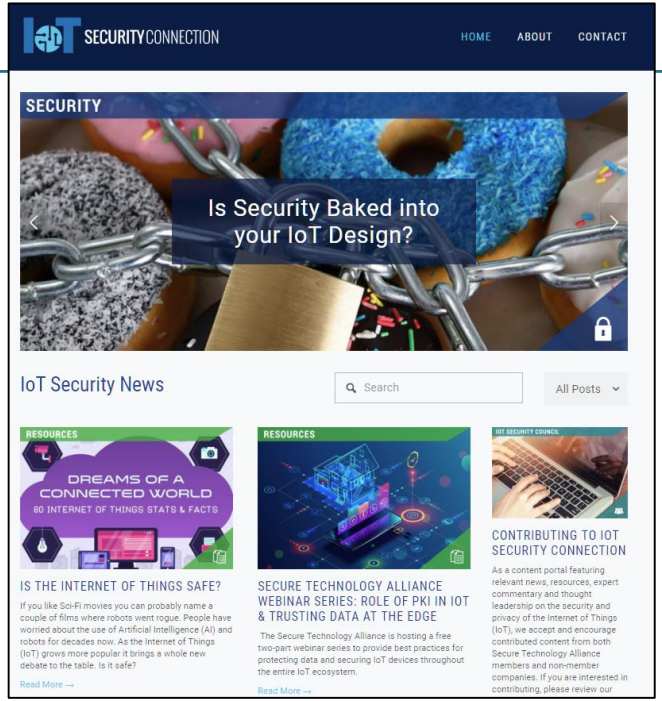
Member Benefits

- Certification
- Council Participation
- Education
- Industry Outreach
- Networking
- Technology Trends

IoT Security Council

IoT SECURITY COUNCIL PRIORITIES

- Accelerate market adoption of secure IoT architectures that incorporate embedded security and privacy
- Provide a forum for intra-industry and cross-industry collaboration on secure IoT architectures
- Provide a business-focused organization to discuss best practices and implementation of IoT architectures using embedded security and privacy
- Provide a single organization where all industry stakeholders can network, share implementation experiences, and discuss applications and security approaches
- Identify and collaborate with other industry organizations to define and promote standards for secure IoT architectures using technologies that provide embedded security and privacy



Publications – IoT

- Blockchain and Smart Card Technology
- Embedded Hardware Security for IoT Applications
- Implementation Considerations for Contactless Payment-Enabled Wearables
- IoT and Payments: Current Market Landscape

Security in the IoT Ecosystem Webinar Series

- **#1 – The Role of PKI in IoT – May 16th**
  Review of how public key infrastructure (PKI) can play a role in securing the IoT ecosystem

- **#2 – Trusting Data at the Edge – May 22nd**
  Review of the security requirements for trusting and managing data collected and/or stored at the edge of the IoT network and approaches for ensuring data integrity, privacy and authenticated access control

Introductions

- Randy Vanderhoof, Secure Technology Alliance

- Sri Ramachandran, G+D Mobile Security

SECURE TECHNOLOGY ALLIANCE

Trusting Data at the Edge

May 22, 2019

What Is the “Edge”?

- "anything that’s not a traditional data center could be the ‘edge’ to somebody.“
- "in close proximity to the last mile network.“
- Cloud Computing operates on “Big Data” while Edge Computing operates on “Instant Data” that is real-time data generated by sensors or users.
- An **edge device** is a device which provides an entry point into enterprise or service provider core networks. Examples include routers, routing switches, integrated access devices (IADs)
- **Fog computing** or **fog networking**, also known as **fogging**, is an architecture that uses edge devices to carry out a substantial amount of computation, storage, communication locally and routed over the internet backbone.

Growth of the Edge

> “Around 10% of enterprise-generated data is created and processed outside a traditional centralized data center or cloud. By 2025, Gartner predicts this figure will reach 75%”

Gartner defines edge computing as solutions that facilitate data processing at or near the source of data generation. For example, in the context of the Internet of Things (IoT), the sources of data generation are usually things with sensors or embedded devices. Edge computing serves as the decentralized extension of the campus networks, cellular networks, data center networks or the cloud.

The Many Types of “Edge”

END DEVICES

EDGE DEVICES

EDGE COMPUTING

G+D Mobile Security

Major Increase in Connected Edge Devices

IoT connections (billion)

IoT	2018	2024	CAGR
Wide-area IoT	1.1	4.5	27%
- Cellular IoT[2]	1.0	4.1	27%
Short-range IoT	7.5	17.8	15%
Total	8.6	22.3	17%

New devices

New services and use cases

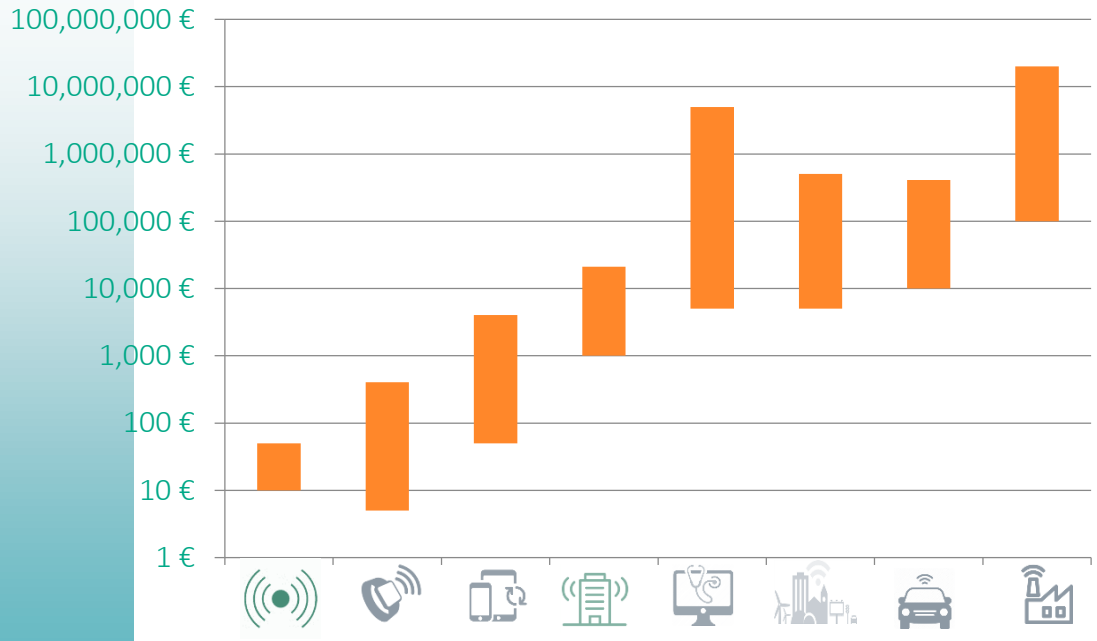
New business models

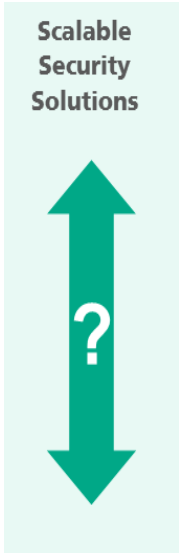
New security threats

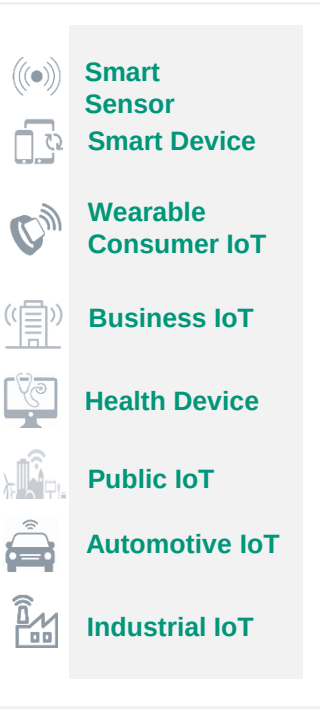
Source: Ericsson Mobility Report, November 2018

Internet of Things – Security Required for a Wide Range of Risk Profiles

IoT Device Value and Risk Taxonomy







G+D Mobile Security

IoT Industry Examples

- **Utilities**
  - Gas/water metering
  - Solar/wind/thermal sensors
  - Smart Grid (energy infrastructure monitoring)
- **Logistics**
  - Asset tracking
  - Supply chain management
- **Industrial**
  - Machinery control
  - Tank monitoring
  - Vending machines (general and data verification)
- **Smart City**
  - Parking sensors
  - Waste management
  - Smart Lighting
- **Agriculture and Environment**
  - Live stock tracking (fish, cattle, wild animal)
  - Stationary Condition tracking (soil, weather)
  - Environment monitoring (fire hydrant, chemical emission levels)
- **Consumer and Medical**
  - Wearables
  - Children and pet tracking
  - White appliances
  - Assisted living
- **Smart Buildings**
  - Smoke detectors
  - Alarm systems
  - Home automation

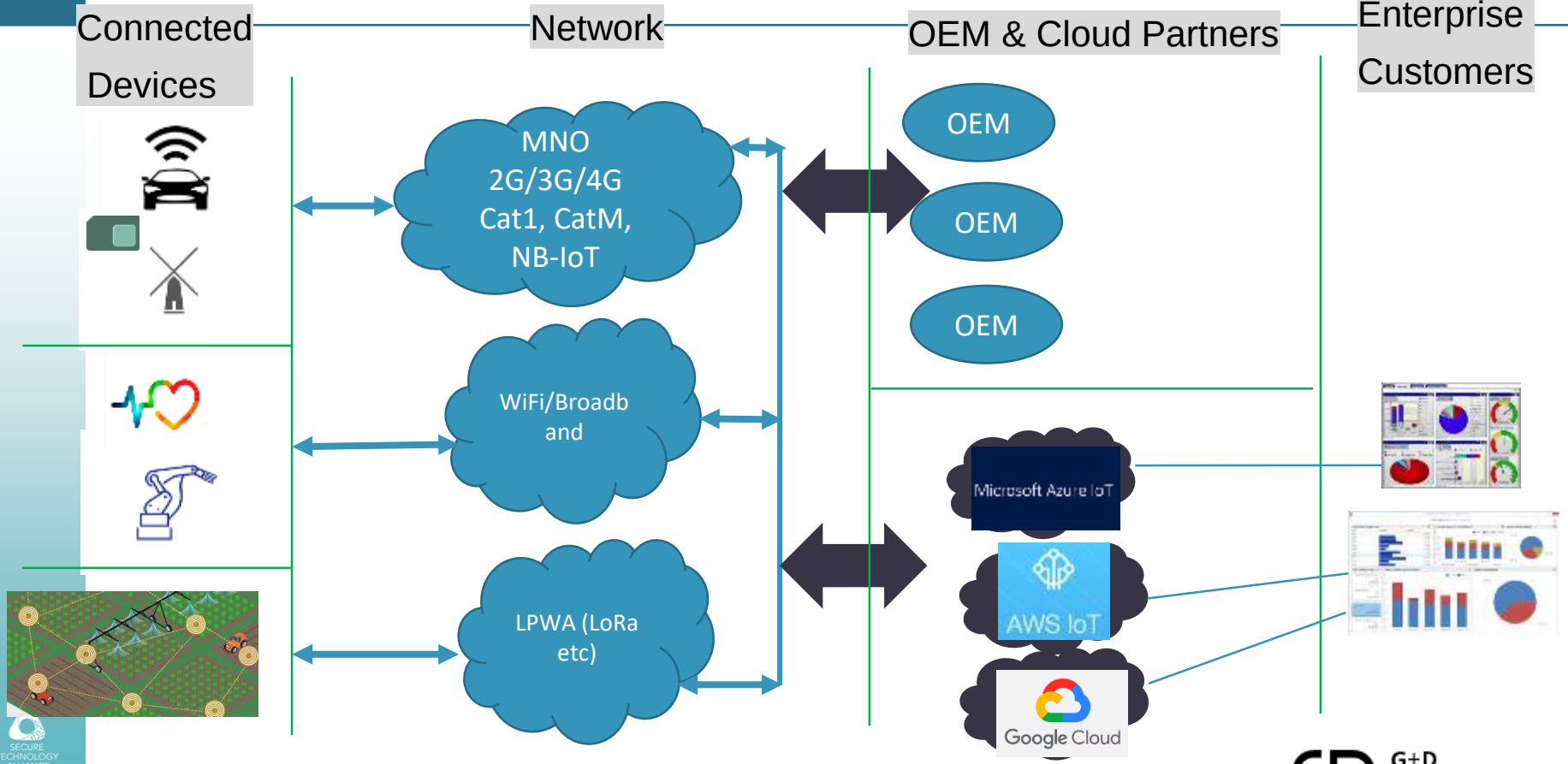
Source: GSMA 3GPP Low Power Wide Area Technologies, 2016

Polling Question

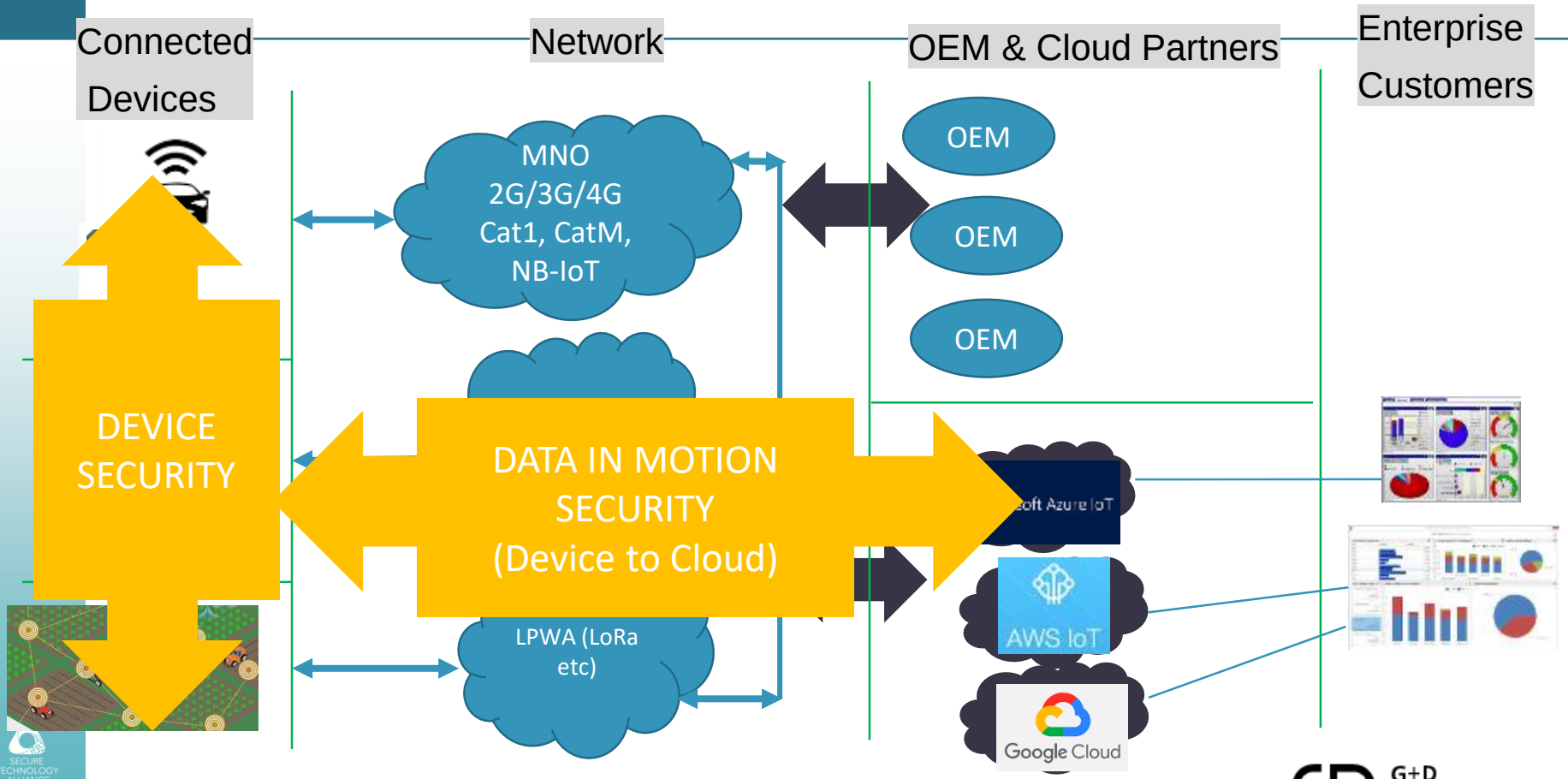
Which part of your organization do you report into?

- IT
- CTO/R&D or Product team
- Security or Risk (CFO)
- Technical Operations
- Business Operations

The IoT Is Complex



The Challenges of IoT Edge Security



Headlines Are Dire…

JUL 27, 2017 @ 05:00 PM 3,146 12 Stock

Criminals Hacked A Fish Tank To Steal Data From A Casino

DEJA VU ALL OVER AGAIN —

"RobbinHood" ransomware takes down Baltimore City government networks

A year after 911 system hit, most of city's networks are down.

SEAN GALLAGHER - 5/8/2019, 11:31 AM

Devices are Unsecured and are

A Cyberattack Hobbles Atlanta, and Security Experts Shudder

Home › Internet of Things (IoT) › Security and IoT: Most IoT D

By Dick Weisinger

80 percent of all Internet of Things (IoT) devices have security flaws and are vulnerable to an attack, according to a Ponemon study made earlier this year.

Polling Question

What's the stance of your organization regarding security threats?

- Paranoid: zero trust
- Aggressive: monitor and thwart new attacks
- Defensive: only able to protect against known threats
- Passive: best effort

The Data Journey…

Secure data collection

Secure storage

Secure communications

SECURE TECHNOLOGY ALLIANCE

G+D Mobile Security

Challenges of IoT Edge Security…

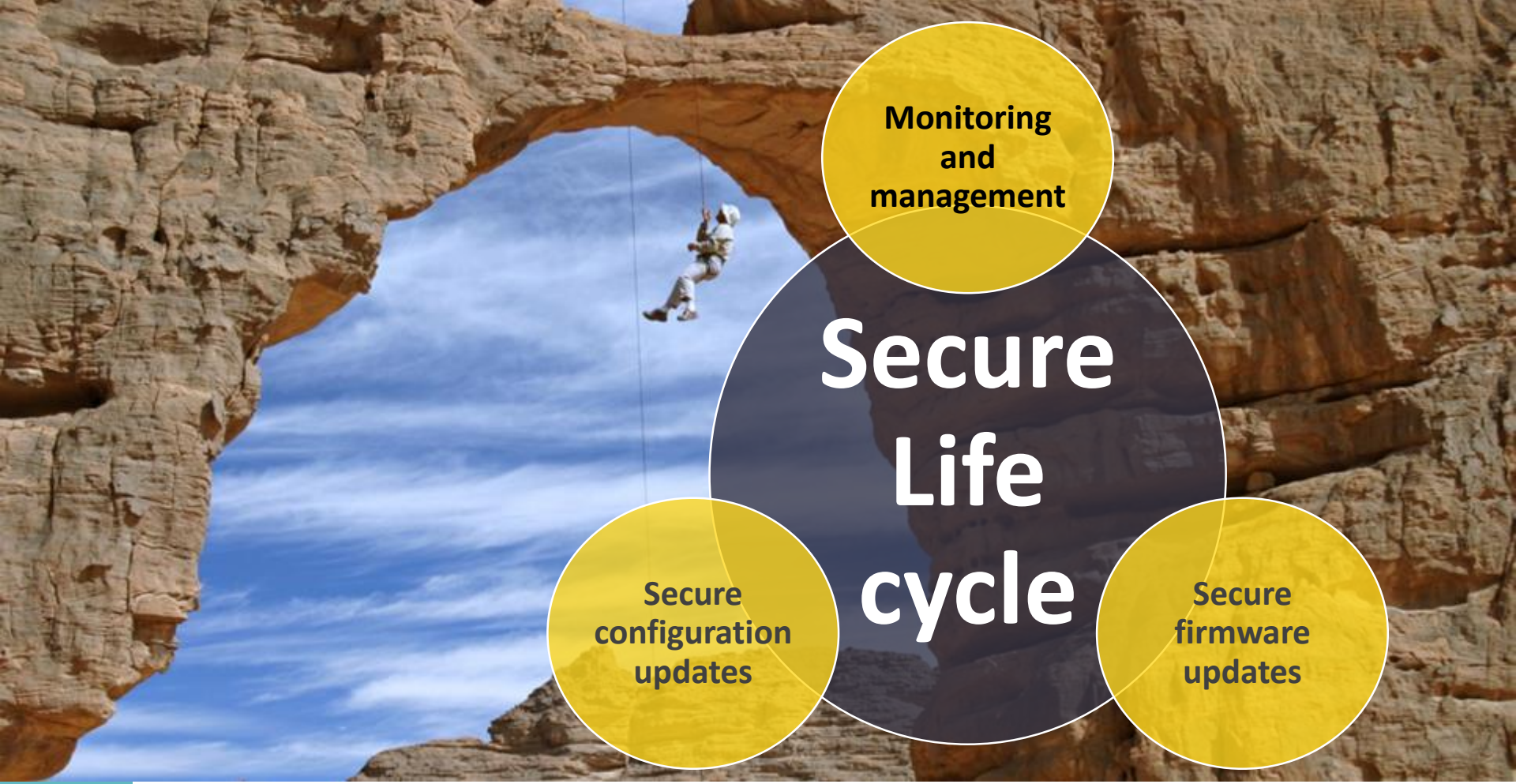
→ Identify every Device in the system
- Unique Identity
- Independent of network access

→ Device integrity
- Ensure Device is operating as planned

→ Data protection
- Data gathering as well as secure transport of data

→ Secure management and monitoring throughout life cycle
- Device is protected at all times - including secure firmware and configuration updates

→ Differential access control
- Differentiate among privileged and regular operations


Monitoring and management
Secure Life cycle
Secure configuration updates
Secure firmware updates

Patching IoT devices Is Cumbersome

99% of security problems have solutions in software/firmware. But the creation and delivery of the patches faces many hurdles:

- Release qualification takes a long time
  - Complexity of test procedures
  - Certification dependent on type of organization
- More vulnerabilities get exposed every month than patches to fix them
- Deployment of patches to all devices requires a robust OTA infrastructure and process
- The enterprise also needs compliance management to monitor and ensure devices are up to date
- Zero day vulnerabilities continue to be a challenge

IoT Security Skills Are the Hardest to Find…

1. **Security Expert**
2. Digital Marketer
3. Mobile Expert
4. Cloud Expert
5. Database admin
6. Architect
7. Project Manager
8. Big Data Analytics
9. Networking expert
10. Business Analyst
11. Software engineer
12. Integration engineer
13. QA/Test Engineer
14. Business Intelligence
15. Help Desk/Tech Support

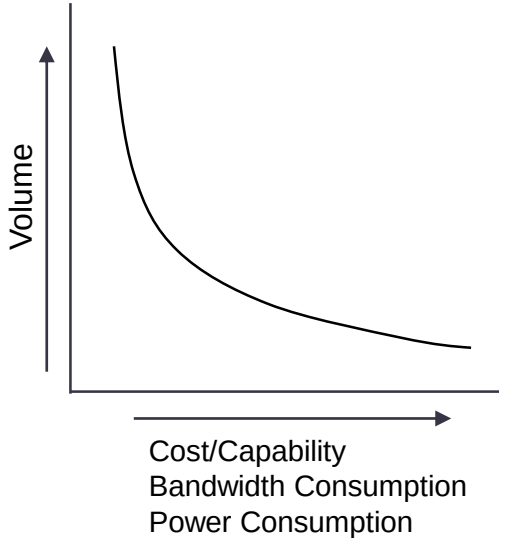
Source: IoT Institute

Compromised IoT Devices Have a Significant Operational Burden

IoT devices are, for the most part, remote and unattended.

- Devices are meant to have a long life – typically >10 years
- Data can be intercepted and go unnoticed for weeks or months.
- They can be hijacked without knowledge of the operator or enterprise (may just show as “down.”)

This can lead to high cost of ownership and significant operational burden as well as increased liability.



G+D Mobile Security

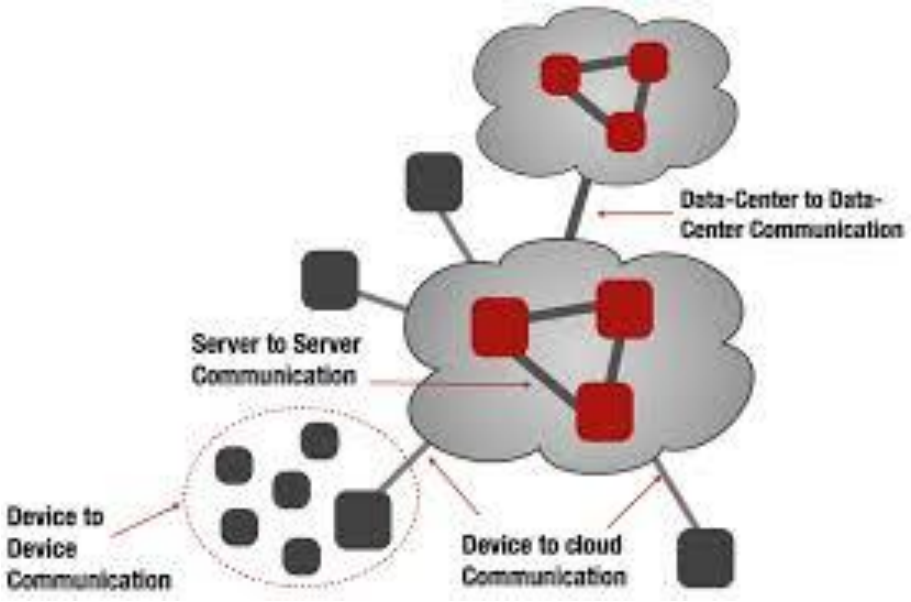
What the IoT Edge Really Needs…

- **ROOT OF TRUST**
  providing irrefutable identity management
- **ALL DATA ENCRYPTED**
  between device and cloud
- **PREVENTION**
  of malware and rogue configurations
- **RECOVERY**
  of stranded devices

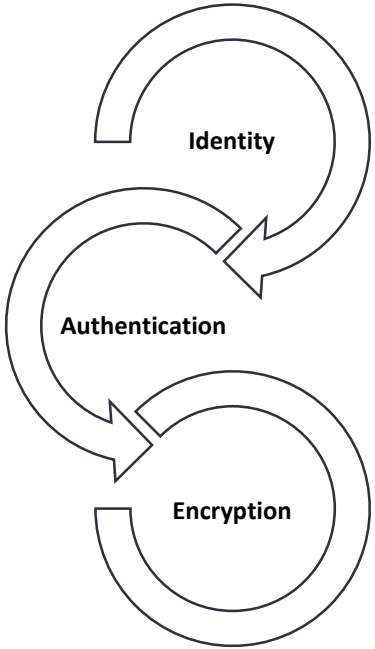
Data in Motion Security

What Is Device to Cloud?

- Cloud based applications are used to extract the business value of IoT deployments
- Cloud based applications enables rapid turn up of IoT devices
- These applications leverage the cloud infrastructure for scalable data aggregation and management
- Cloud infrastructure also future proofs IoT deployments by enabling application evolution and mash up services



The Three Problems of Device to Cloud Security



DEVICE IDENTITY

Devices tend to use network identifiers for their identity which are easily abused

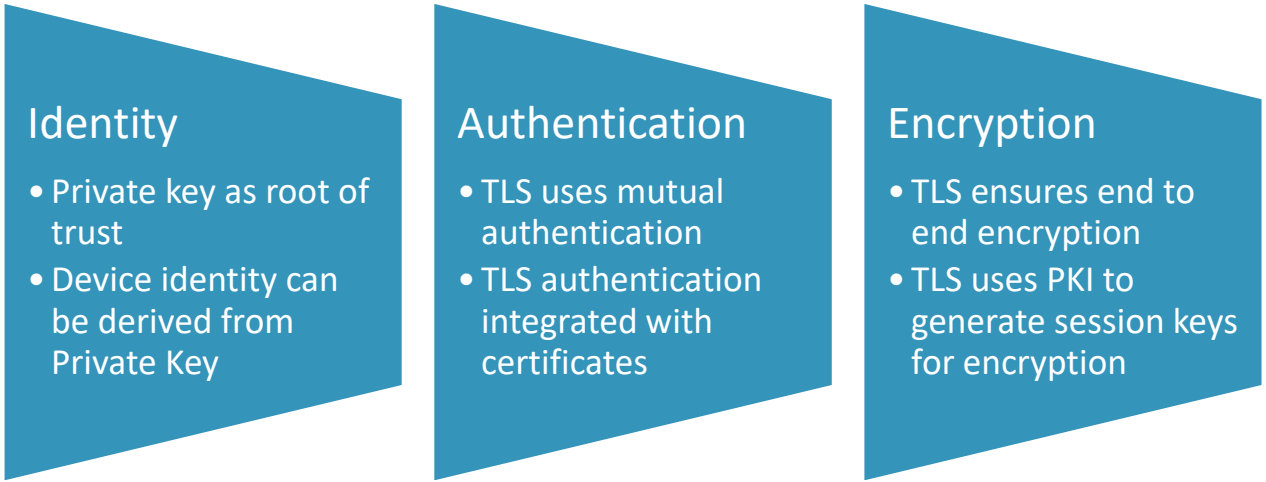
MUTUAL AUTHENTICATION

Lack of username/passwords in IoT devices make traditional authentication methods impractical

ENCRYPTION OF CHANNEL

Segment by segment encryption is not secure enough and very hard to manage

Public Key Infrastructure (PKI) and Transport Layer Security (TLS)



- *PKI provides a chain of trust*
- *Well established web infrastructure uses PKI and TLS to ensure secure transactions*

Polling Question

What's the status of your organization's plans for IOT deployment?

- No identified projects or not applicable
- Investigating, but no firm plans
- New project in next 12 months; determining security approach
- New project in next 12 months; aligned security approach
- Project deployed, looking at improving security posture

Regulations?

- Many governments and regulators are exploring IoT Security frameworks and guidelines
- “Security-by-design” is an example of that

Examples of IoT security frameworks and regulation requirements

Framework	Target
ETSI TS 103 645	Consumer IoT manufacturers
GSMA IoT Security Guidelines	Mobile operators
ENISA	The broad IoT ecosystem
IEC	Industrial IoT stakeholders
NIST IoT Security Roadmap Initiative	The broad IoT ecosystem
Open Web Application Security Project (OWASP)	IoT application developers

Regulation	Target
EU GDPR	Digital enterprises
California Bill SB-327	Internet-connected device manufacturers
UK voluntary Code of Conduct	Consumer IoT device manufacturers
EU Cyber-security Act	Digital enterprises
German IT Security Act	Digital enterprises

Source: GSMA Intelligence

Summary

- The “Edge” will comprise of mostly IoT Devices and related components
- As IoT deployments grow, the Edge plays a crucial role in generating data for enterprises for business process automation and business intelligence
- Securing the IoT Device Edge and the data is paramount
- IoT devices may be compromised in many ways
- Regulators, in the interest of consumers, are willing to propose regulations for securing the IoT.

SECURE TECHNOLOGY ALLIANCE

Q&A

IoT Security Webinar Series Assessment

- Online assessment quizzes available for both webinars in the series
- Participate in the two webinars and pass both assessments to receive a Secure Technology Alliance certificate of participation
- Assessment link: https://www.surveymonkey.com/r/IoTEdge

Selected Secure Technology Alliance Resources

- **IoT Security Council Resources**
  - https://www.securetechalliance.org/activities-councils-internet-of-things-security/
- **IoTSecurityConnection.com -** http://iotsecurityconnection.com/
- **Secure Technology Alliance Knowledge Center**
  https://www.securetechalliance.org/knowledge-center/
  - Embedded Hardware Security for IoT Applications
  - IoT and Payments: Current Market Landscape
  - IoT Security: Mitigating Security Risks in Secure Connected Environments Webinar
  - Secure Technology Alliance Response: NIST "IoT Security and Privacy Risk Considerations" Questions

SECURE TECHNOLOGY ALLIANCE

Randy Vanderhoof, rvanderhoof@securetechalliance.org

Sri Ramachandran, sri.ramachandran@gi-de.com