Security Best Practices

Key to implementing a secure IoT solution

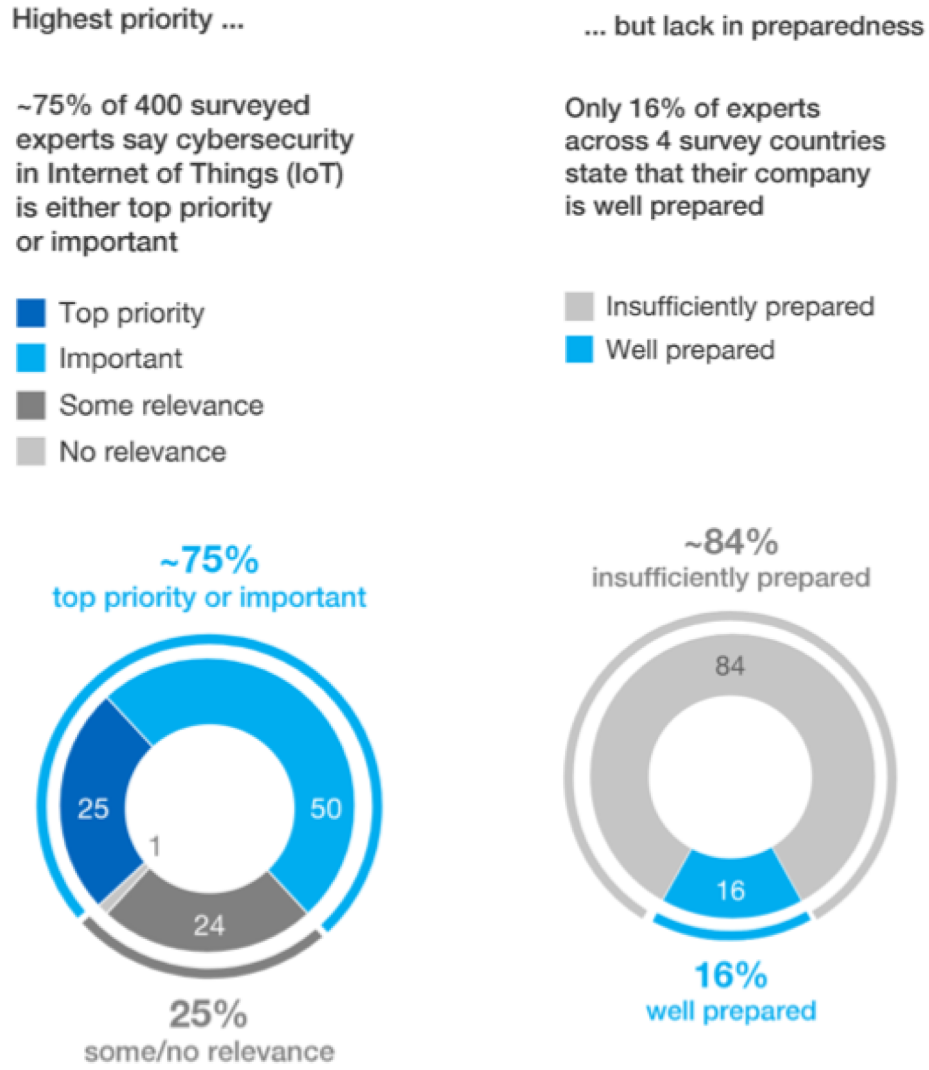
Wei Xiao

Nov, 2018

SAMSUNG ARTIK™

The Internet of Things is Dangerously Insecure

- Time to market prioritized over security
- Very little of IoT budgets have been allocated to security
- IoT and App development teams lack security skills
- Unprotected “Things” vulnerable to physical abuse
- Establishing trust between devices, gateways and cloud is difficult



Source: McKinsey global expert survey on cybersecurity in IoT, 2017

IoT Security Guidance is Maturing Rapidly

Internet of Things Cybersecurity Improvement Act

IoT: Enhanced Assessments and Guidance are Needed to Address Security Risks in DOD

Baseline Recommendations for IoT Security In the Context of Critical Infrastructure

Massive Fines €20B or 4% Global Turnover

Internet of Things Working Group

800-160 System Security Engineering
899-183 Network of Things

'WHISTL' network of security testing labs for medical devices

UL 2900-1 Cybersecurity for Network-Connectable Products
UL 2900-2-1 Healthcare
UL 2900-2-2 Industrial
UL 2900-2-3 Life signaling and safety

Internet of Things Security Framework

IoT Top 10
IoT Attack surface

IoT Security Best Practices

Secure Communication

Device Identity

Hardware Root-Of-Trust

Secure Storage

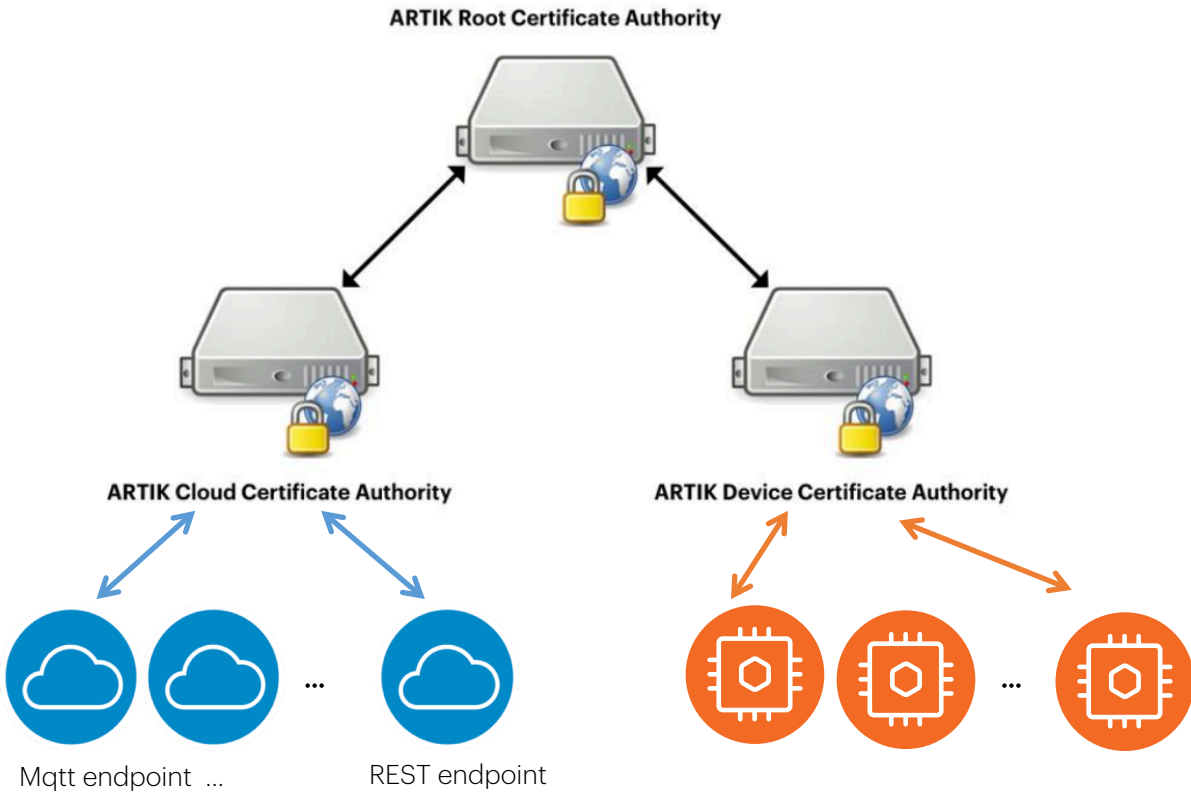
Device Integrity

Secure Update

SAMSUNG ARTIK™

Secure communications

- Ensure mutual authentication from silicon to cloud via keys and certificates using ARTIK Public Key Infrastructure (PKI) and X.509 certificates
- Ensure local node-to-node and node-to-cloud communication is secure using industry standard cryptographic techniques
- Using appropriate cryptographic protocols such as TLS for communication security



SAMSUNG ARTIK™

Device Identity

- Each device must be identified uniquely. This is implemented by injecting a unique certificate into the device at manufacturing
- Create a whitelist allowed devices for each production run
- Prevent unauthorized and counterfeit devices from accessing the network / system

SAMSUNG ARTIK™

Hardware protected secure storage

- Store sensitive keys and certificates in secure element or secure storage for confidentiality and data integrity

- Secure element conforms to security level Common Criteria EAL5+

- This ensures the data, key/certificates in the system are not accessible to malicious parties who might have physical possession of the asset

SAMSUNG ARTIK™

Hardware Root of Trust - Trust Chain

- Secure boot is enabled in hardware during manufacturing
- ROM code establishes the Root of Trust
- This prevents assets from connecting to untrusted malicious sources
- Samsung Key Management System(KMS) is provided for key management and code signing

SAMSUNG ARTIK™

Device Integrity via Secure boot and Secure OS

- Device protection and trusted code execution are central to IoT security
- Each IoT asset should include secure boot mechanism to validate the integrity of critical code
- Stop boot process if boot code verification fails
- Use Trusted Execution Environment of secure OS to further isolate secure processes in software
- Block debug ports such as JTAG in production units
- This ensures device protection even when malicious parties have physical access to the asset

SAMSUNG ARTIK™

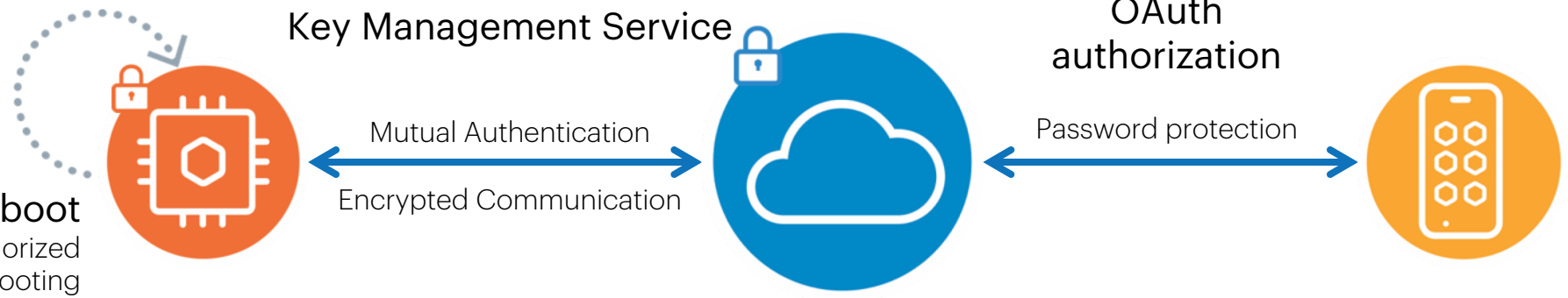
Secure field updates for assets

- Ensure device updates are coming from a trusted source using standard cryptographic techniques such as Public Key Infrastructure (PKI)
- Sign firmware image to be distributed to assets to ensure only authentic firmware updates are committed on assets
- Maintain default factory roll back image
- This ensures assets are updated to the intended firmware from intended source

SAMSUNG ARTIK™

Samsung ARTIK™ End-to-end Platform Security

Protection for you and your customers



Secure boot
Prevents unauthorized software from booting and running on device

Secure OS
Hardware-enforced secure applications

Secure storage
Data encryption

Authentication and authorization, secure OTA
Cloud services are protected

User data encryption
Protects sensitive info on mobile devices

SAMSUNG ARTIK™ Security

Q & A

SAMSUNG
ARTIK™