Security in the IoT Ecosystem: The Role of PKI in IoT

IoT Security Council Webinar
May 16, 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

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 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
- Josh Jabs, Entrust Datacard
The largest IoT opportunities require the digital transformation of our most critical environments.
What is driving digitization in industry?

**CONNECTIVITY**
- Smart connected devices
- Standards-driven connectivity
- Lower cost of measurement

**CLOUD**
- Massive data aggregation
- Data access by specialists
- Industrial application developer ecosystem

**MOBILITY**
- Pervasive, affordable communication
- Remote access
- User-driven interfaces

**ANALYTICS**
- Cognitive applications
- AI optimizing performance
- Actionable information
Growth of connected IoT devices

- 2020: Billions
- 2015: 
- 2006: 

A guide to the internet of things infographic – Source: Intel report

- 40.2% Industry
- 30.3% Healthcare
- 8.3% Retail
- 7.7% Security
- 4.1% Transportation

Entrust Datacard
Growth in IoT connected devices creates opportunity – and risk.

Companies must address the challenge on multiple levels.

By 2020, 60% of digital businesses will suffer major service failures due to the inability of IT security teams to manage digital risk.

Special Report: Cybersecurity at the Speed of Digital Business, Gartner, G00315580
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, but figuring out security approach
- New project in next 12 months, with aligned security approach
- Project already deployed, looking at improving security posture
Challenges to IoT adoption

- Cybersecurity: 46%
- Lack of standardization: 35%
- Legacy installed base: 34%
- Large upfront investments: 30%
- Lack of skilled workers: 24%
- Data integrity: 23%
- Internal systems barriers: 18%
- Liability of current technologies: 15%
- Social/political concerns: 6%
10 IoT Security Targets

**01 INDUSTRY**
Connectivity offers new risks. As cars and industrial facilities become increasingly connected to the cloud, security risks increase.

**02 CARS**
Cars are now a source of cyber-attacks. For example, a bug in the 2015 Model S caused a security breach that allowed hackers to control the car.

**03 VIDEO CAMERAS**
Video cameras can be exploited. Even video cameras, which are intended to improve security, can be hacked.

**04 CYBER-WARFARE**
Cyber-warfare is now possible and Iran now has one of the largest cyber-arms in the world.

**05 POWER GRIDS**
Power grids are vulnerable. Cybersecurity experts have been warning of the risk of hackers breaching the power grid and natural gas pipelines.

**06 BUILDINGS**
Buildings are more connected and the risk for attacks increases.

**07 CITIES**
Cities are vulnerable to cyber-attacks, and many have weak security controls in place.

**08 MEDICAL DEVICES**
Medical devices are already targets. The security of many medical devices is weak and hospitals often lag behind.

**09 AIR TRAVEL**
Air travel is vulnerable. Last year, a security breach in an FAA unit allowed hackers to break into a system.

**10 RETAIL**
Retail is also vulnerable. In 2014, hackers managed to break into Target's financial systems unit by way of an HVAC unit.

**ATTACKS LIKELY UNDER-REPORTED**
It is difficult to gauge the true risk of software breaches in the industrial and retail sectors, which tend to downplay their risk of being compromised.

**AIRPLANES CAN BE HACKED**
Software vulnerabilities have been identified in several commercial aircraft.

**CONNECTIVITY OFFERS NEW RISKS**
Connectivity offers new risks. As cars and industrial facilities become increasingly connected to the cloud, security risks increase.

**CAMS CAN BE EXPLOITED**
Even video cameras, which are intended to improve security, can be hacked.
IoT Presents New Security Challenges

- Device Disparity & High Volumes
- IoT and OT Convergence
- Immature Security Standards
- Gap in Technology Sophistication

- Operational Challenges
- Data Integrity
- Common Security Framework
- Privacy Issues

- Automation Challenges
- Encryption Capabilities
When the Worlds of IT and OT collide
Polling Question

Which part of your organization do you report into?

- IT
- CTO
- Security or Risk
- Line of Business or Product Team
- Other
Establishing Trust in the IoT

Trust is having the confidence or assurance that a person, system, or thing will behave as you expect or as intended
Device Lifecycle in IoT

**Device Manufacturers – Endpoints (OEM)**

- **Control Module (MCU / ECU)**
- **Controllable Sensing things**
- **Semi-Conductors**
  - Sensors
  - Low power MCU
  - Chip

**Operators of OEM**

- **Gateway (MQTT, AMQP, REST)**
  - Remote monitoring
  - Enterprise / OEM Cloud infrastructure
  - Connected Solutions (Apps)

**Module / Sensor Manufacturing**

- **Secure Identity**
  - Installation of Device Agent
  - Addition of Device attributes & bootstrap certificate / token
  - Key & Certificate generation
  - HSM, TPM, E-Sim, SE (Secure Element), software keystore
  - TEE

**Security**

- **Provisioning**
  - Discovery
  - Device Authentication
  - Provisioning & Authorization

**Securing Sensor / Module + Data**

- **Lifecycle Mgt**
  - Secure Data & Identity
  - Policy Updates
  - Activate / Suspend / Terminate
  - Device Update – Firmware, Cert
  - User Access

---

**System Capability**

- Low
- High
# Identity Lifecycle Management for Devices

## Manufacture
- Identity Issuance
- Scalable Device trust and Identity
- All classes of devices

## Provision
- Whitelisting the device
- Register the device
- On-Demand / Bulk

## Deploy
- Enrollment of device
- Authenticate the device
- Part of Trusted Ecosystem
- Enterprise Integration

## Monitor
- Access control
- Audit
- Block unauthorized connections
- Data extraction
- Secure Data Transmission

## Service
- Suspend device
- Activate / Re-Activate device
- Prevent unauthorized command and control

## Update
- Code Signing
- Secure Bootstrapping
- Secure Firmware update
- Secure Software Update

## Decommission
- Terminate the Device
- Blocked from the Trust zone / network

---

**Entrust Datacard**

[Identity Lifecycle Management for Devices diagram and icons]
Polling Question

What’s your familiarity with Public Key Infrastructure
- Expert
- Operate it, but not an expert
- I know about it, but don’t have hands on experience
- I think I’ve heard about certificates before
- Unfamiliar
Why PKI? What does it do?

1) How do I know who I’m talking to?
2) Are these parties allowed to communicate?
3) How do I prevent others from listening in?
4) How do I make sure what was sent was received?
5) How do I prove what was said later?

Trustworthy Interactions

Authentication
Authorization
Encryption
Integrity (signing)

Important Concepts (especially with scale)

It’s digital, so keys and crypto make it work and you need to protect them accordingly.

It starts with registration.

It’s a system and will evolve (there’s a lifecycle).

Validation is required and the concepts impact performance (when, how).
What is PKI?

What is a public-key infrastructure (PKI)?

The comprehensive set of roles, policies, and procedures required to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption. Every authorized person, device and app gets a digital certificate that proves their identity.

What does PKI do?

A PKI enables an organization to establish and maintain a trustworthy digital ecosystem (people, systems, and things) by managing keys and certificates.

For more on PKI, these sound like fun =)
PKI – A history of providing security at scale
PKI – Continues to gain traction in the IoT security community

IoT is becoming a major driver for the use of PKI

21%  28%  40%  44%

42% of IoT devices in use will use digital certificates for identification/authentication in the next two years.

IoT is the most important trend driving the deployment of applications using PKI has increased significantly from 21 percent to 44 percent.
Weighing PKI for IOT

Benefits

• Enables a unique and verifiable identity for each endpoint
• Strong Authentication without Passwords
• Sensitive information is Encrypted
• Standards based + Mature
• Non-repudiation
• Ability to manage at scale
• Automated roll-over and renewal addressing longevity requirements

Challenges

• Lack of embedded functionality within OT infrastructure
• PKI skills are not always readily available in an organization
• Traditional PKI tools were built for unconstrained environments
• Handling of Keys and certificates is crucial and often overlooked
PKI for IOT Considerations

- Supply chain considerations
- Brownfield vs Greenfield devices
- Two tier (device to cloud) vs three tier (operations) environments
- Skill-sets and organizational structure
- Device provisioning and scale (manual or automated)
- Device and service lifecycles
- Deployment preferences (on-premises, cloud, hybrid)
- Compliance requirements
- Protocol requirements
- Key generation and storage
The value of cybersecurity in IoT Ecosystems

Support Safety for Staff and Environment

Protect Corporate Image and Reputation

Ensure Business Continuity

Avoid Regulatory & SLA Penalties

Protect Critical Digital Assets (IP)

Improve Cyber Defensible Position to Threats

Protect your IoT Investment

Ensure Business Continuity

Avoid Regulatory & SLA Penalties

Protect Critical Digital Assets (IP)

Improve Cyber Defensible Position to Threats

Protect your IoT Investment

Ensure Business Continuity

Avoid Regulatory & SLA Penalties

Protect Critical Digital Assets (IP)

Improve Cyber Defensible Position to Threats
“There's no silver bullet solution with cybersecurity, a layered defense that is adequately monitored, is the only viable defense.”

- James Scott, Senior Fellow, Institute for Critical Infrastructure Technology
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/PKIinIOT
Selected Secure Technology Alliance Resources

- **IoT Security Council Resources**

- **Secure Technology Alliance Knowledge Center**
  - [https://www.securetechalliance.org/knowledge-center/](https://www.securetechalliance.org/knowledge-center/)
  - Embedded Hardware Security for IoT Applications
  - *IoT and Payments: Current Market Landscape*
  - *IoTSecurityConnection.com*
  - Secure Technology Alliance Response: NIST “IoT Security and Privacy Risk Considerations” Questions
Randy Vanderhoof, rvanderhoof@securetechalliance.org
Josh Jabs, Josh.Jabs@entrustdatacard.com