How to Future-Proof IoT Security

Nordic IT Security 2019

November 14, 2019

MARK B. COOPER

PRESIDENT & FOUNDER

MARK@PKISOLUTIONS.COM

@THEPKIGUY

The PKI Guy

- President and Founder, PKI Solutions
- Known as “The PKI Guy” since early days at Microsoft
- Leading PKI subject matter expert
- At PKI Solutions, we implement PKI solutions at enterprises
- I lead hundreds of PKI trainings from Scotland to Buffalo, Sweden to Portland
- In-person and online trainings available
- My focus is security, PKI design and implementation, identity management

PKI SOLUTIONS

What are we talking about today?

- Current Internet of Things (IoT) landscape
- IoT threats
- The IoT security problem
- Building in device security
- Future proofing
- PKI is at the core
- PKI considerations for IoT

“[A] connected device has the ability to cause more disruption, which could cause actual physical injury or even death.”

- Merritt Maxim, Forrester

Current IoT landscape

- We are surrounded by IoT: thermostats, insulin pumps, water pumps, gas pumps, smart speakers, automobile navigation, security cameras, commercial airliners
- Cross-industry: automation, automotive, utilities, manufacturing, medical, government, consumer, retail
- There will be 20.6 billion connected devices by 2020 and 5.8 billion IoT endpoints (Source: Gartner)

IoT threats

- 25% of cyber attacks will target IoT devices (Source: Aberdeen)
- Cyber attacks on IoT devices surge 300% in 2019, 2.9 billion events (Source: F-Secure)
- Almost every IoT device is vulnerable; poor security in place: poor authentication protocols, poor default credentials, lack of encryption
- Smart devices provide a gateway to break a network wide open
- IoT is soft entry point to wider networks, to steal credentials and data, hijack devices, destroy devices and networks
- IoT devices expand your company’s attack surface.
- IT often unaware of IoT devices on their networks; patching security issues nearly impossible

The IoT security problem

- IoT security is not a one-size-fits-all approach
  - Lack of platform standards
  - Form factor, energy and computational abilities are limitations
  - Command and Control needs
  - Topology variations (Hub and Spoke, Mesh, Multi-Channel)
- Grey market control, contract manufacturers, “recall” inability
- Devices need to be built to interoperate with each other
- Device may have little to no connectivity in use
- Devices have lifespan issues as iterative and evolutionary changes are made to product line
- The future….

Building in device security

- Building in device security early on to secure devices over their lifetimes
  - Manufacturing, setup and management
- The lifetime of an IoT can range from short-lived devices (thermostat) to a device with a long lifespan designed to last 100 years (water pump)
- The longevity of information and privacy, all need to be considered
  - Longevity of the identity keys
  - Product useful & supported lifetime
  - Device EOL state at expiration
  - Cross-generational support and interoperability

Future proofing

- Devices must accommodate rolling/renewing identities.
  - Firmware update, Command/Control, Manually, Software based
- Identities/Keys must be cryptographically useful for intended lifetime
  - Crypto Algorithm validity and EOL
  - Crypto-agility
- Secure firmware updates: In and out of band
- Certificate Authorities (CAs) will need to be renewed and replaced
  - Future Root of Trust updates
  - Pre-Staged Advanced Crypto Roots

Future proofing - details

- Ensure platform supports identity renewals and rekey
- RSA keys
  - 2048 for short-lived devices (present-2030)
  - 3072 for mid-long term devices (present-2030+??)
  - 4096 and higher likely computationally inefficient in many IoT platforms today
- Crypto-Agility/Post-Quantum Crypto
  - Few commercial algorithms available
  - ISARA, others are available
  - Limited to closed ecosystem for support
  - Best option is to look at agile platform future secure update

Future proofing - details

- Code Signing and Timestamping for Firmware/Updates
  - Consider distribution, crypto support for lifetime, generational issues
- PKI issued identities are limited by CA lifetimes. CAs have key limitations based on crypto as well
  - Plan Certificate Authority keys to align with crypto usefulness
  - Ensure devices can operate with generational devices with potentially different, renewed or new CA keys
  - Ensure devices can update root trusts in secure manner
  - Consider pre-staging future roots in firmware for advanced crypto/agility, chains, generational, and capacity plans

PKI is at the core

- Public Key Infrastructure is designed from the ground up for disconnected authentication
- Easily adapted to unique needs of IoT
  - Crypto agnostic/agile
  - Optional revocation checking
  - Variable key sizes to suit platforms
  - Identity, signing and encryption
- Common Options
  - On-premises/secure manufacturing
  - Cloud Integrated for Command/Control
  - Managed offerings

PKI SOLUTIONS

PKI considerations for IoT

- Cloud for Command/Control
- Long-term ownership of PKI key/identity defines your business
- Cloud providers own key – unable to move workload or PKI
- Your product/business is linked in perpetuity
- Cloud services secure keys in their environment
- Leverage neutral third party for key
  - nCipher, Thales, Utimaco, FutureX provide HSM as a Service
  - Enables you to own key, place workload in desired cloud
  - Movable workloads – even to/from on premises
- Crypto is both easier (closed ecosystem) and harder (limited compute)

Online PKI Training: Attendees Get 50% Off

- Online Microsoft PKI In-Depth Course
- 20 hours of content + labs, self-paced
- Attendees enter the code “NordicIT” for 50% off this online course, valid until November 30, 2019
- pkisolutions.com/courses

Questions? Let’s Connect!

mark@pkisolutions.com

@ThePKIGuy

@PKISolutions

www.pkisolutions.com

linkedin.com/in/thepkiguy

linkedin.com/company/pki-solutions