Summary of Breakout Sessions and Wrap-up Discussion

CREDC Industry Workshop
March 27-29, 2017
Breakout Topics

Cyber Supply Chain Provenance and Protection – Dennis Gammel, SEL
Engineering Secure EDS – Zach Tudor, Idaho National Lab
PKI in Current and Emerging EDS – Sean Smith, Dartmouth College
Supply Chain Security

CREDC Industry Workshop
March 27-29, 2017
Product Development Life Cycle Stages

- Research
- Develop
- Manufacture
- Integrate
- Service
- Monitor

- Personnel
- Complexity & Cost
- Crossover Technology
Supply Chain Risks to Consider

- Environmental
- Economic
- Poor Communication
- Unreliable Delivery
- Inconsistency
- Labor Disputes
- Political Instability
- Obsolescence

- Interdiction
- Counterfeit
- Cover Functionality
Assessing Supply Chain

- Evaluate Suppliers
  - Reputation
  - Documented Features
  - Development Process

- Assess Products
  - Product Tracking
  - Certifications

- Assess Chain of Custody
  - Supply Chain Length
  - Personnel Trust
  - Delivery Time
  - Packaging
Areas of Research

• Supplier Assurance Matrix
  • Certifications
  • Reputation
  • Process
  • Stability
  • Disclosure Process

• Diversity Versus Standardization

• Tools for the Product Life Cycle Stages including Delivery Tracking
  • Blockchain
  • Product Diagnostics
Discussion
Breakout Topics

Cyber Supply Chain Provenance and Protection – Dennis Gammel, SEL
Engineering Secure EDS – Zach Tudor, Idaho National Lab
PKI in Current and Emerging EDS – Sean Smith, Dartmouth College
Engineering Secure EDS

Zach Tudor, INL
Tim Yardley, Illinois

CREDC Industry Workshop
March 27-29, 2017
Session Summary

• Great attendance and participation

• Passionate discussions, not always involving new engineering methods

• Identifying transformational technologies or methodologies
  • (Zach comment) Does any inventor foresee the transformational nature of their invention?

• Industry needs a motivating event
Path to Session Outcomes

- Overall Themes
  - Investigate **fragility** to help re-enforce resiliency
  - Make **enabling tenets** rather than restricting requirements
  - Must consider **all-hazards** approaches
  - Some **current initiatives** are moving the ball forward
  - **Secure (resilient) systems need to evolve resiliently**

- Develop tenets
  - Ten Commandments of resilient engineering

- R&D Questions
Key Comments

• Features or convenience go against security

• Railway priorities (don’t kill anyone, keep trains running, efficiency – stay in business)
  • Efficiency goes counter to reliability and security, so how do you find a happy middle ground

• Cyber security is not an end point, it’s something that we operate in
  • It’s impossible to take every risk off the table
  • Need good recovery mechanisms

• Moving from physical to cyber is difficult to grasp. Physical world is a bit easier to understand as the inject vector is physical proximity, not varied like cyber is

• Third party connections are essential, and they often cannot be decoupled/cut off for various reasons (support, warranty, etc)
More Key Comments

- Managing vendors is increasingly difficult and giving them secure the connectivity to the system
  - There’s too much stuff out there (Zach)
- Consider the protection of the system from the operators of the system itself
- Having a methodology that allows me to evaluate a secure system in relation to its deployment in a particular domain
- Missions can conflict
- Designing a system is a separate discipline from deploying it, maybe there needs to be two approaches (and they would need to be complementary)
- Power people use power tools for planning/operations, but there aren't any “design tools” that assist you in designing the systems based on particular constraints
Major Take-Aways

• Tenets
  • Control actions should be verified based on system state before acting
  • Safety engineering constraints must be adhered to in order to have a secure EDS
  • Isolate/segment trusted and untrusted components from each other
  • The system should not be allowed to take an action that harms itself
  • You must be able to trust the sensors
  • Design systems so that unacceptable consequences are physically impossible

• Lack of appreciation for attack techniques
  • People focused on malware or known vulnerabilities rather than on the full range of techniques available to accomplish the end goal

• Tactical vs strategic thinking causes more problems down the road
Discussion
Breakout Topics

Cyber Supply Chain Provenance and Protection – Dennis Gammel, SEL

Engineering Secure EDS – Zach Tudor, Idaho National Lab

PKI in Current and Emerging EDS – Sean Smith, Dartmouth College
Breakout Session Summary:

PKI in Current and Emerging EDS

Sean Smith, Dartmouth College  
www.cs.dartmouth.edu/~sws/

Scribe: Prashant Anantharaman, Dartmouth College

CREDC Industry Workshop  
March 29, 2017
Setting the stage

• **Goals**
  • Authentication/authorization of commands (and data?)
    • sent on channels that an adversary can manipulate
    • and where manipulation has big EDS consequences
  • Potentially: non-repudiation
  • Not likely: confidentiality

• **Cryptographic tools**
  • public-key signatures seem the “obvious” solution, but
  • symmetric might work in many scenarios
  • (and in some settings, even quantum)

• **Using these tools requires things have keys and know about the others**
• “**EDS PKI**: the enabling glue”
X.509 and all that

- Trust roots
- Trust paths
- Certificates
- Revocation
- Key replacement
- The dances...

1. "I trust this CA to say truthful things about keypairs..."
2. "...and it says that Bob's CA will speak truthfully about Bob's namespace..."

Certificate $C_B$

belongs to Bob...

4. "...so I will believe that actions taken by were done by Bob"

(Smith and Marchesini, *The Craft of System Security*)
X.509 and all that

- Trust roots
- Trust paths
- Certificates
- Revocation
- Key replacement
- The dances...

**Overheads**
- **Starts to get messy**
  - when trust structure goes beyond hub-and-spoke
  - when we need more than basic identity

(Smith and Marchesini, *The Craft of System Security*)
Initial questions

• **Operation and administration**

• **Non-trivial trust paths:** Will “one CA issues certs for everyone” always work?
  • Entities shared between different organizations
  • Mobile electric cars

• **Non-trivial “identity”:** Will one identity cert tell the relying party all they need to know?
  • “I am a device of type X, but at substation Y”
  • “I have software S patched to level N”

• **Non-trivial communication patterns:** Will it always be fairly static hub-and-spoke?
  • Many-to-many
  • Things talking to things they’ve seldom talked to before.
  • Asymmetry of devices?

• **“PKI” in constrained devices**
  • Insufficient entropy to generate unique keys
  • Insufficient computational power for modular math
  • Gear that lives much longer than the crypto?

• **“PKI” in constrained environments**
  • Insufficient bandwidth for standard revocation/path discovery/etc
  • Lack of time synchronization
  • Latency requirements
Initial questions

• **Operation and administration**

• **Non-trivial trust paths:** Will “one CA issues certs for everyone” always work?
  • Entities shared between different organizations
  • Mobile entities

• **Non-trivial “I am a device of type X, but at substation Y”**

• **Non-trivial communication patterns:** Will it always be fairly static hub-and-spoke?
  • Many-to-many
  • Things talking to things they’ve seldom talked to before.
  • Asymmetry of devices?

• **Does it get much beyond one hub-spoke?**
  • “administrative domains”

• **Constraints from EDS**

• **“PKI” in constrained environments**
  • Insufficient bandwidth for standard revocation/path discovery/etc
  • Lack of time synchronization
  • Latency requirements
Lively discussion: EDS crypto issues....

• **Does it get much beyond “one hub-and-spoke”?**
  • (if so, does the EDS PKI need to handle it?)
  • One thing talking with things from more than one administrative domain
  • Many-to-many?
  • Do want the machines to be able to do what the human operators did over the phone in 2003?
  • IIoT?

• **Legacy EDS**
  • long-life energy machines (and networks)
  • ...vs. shorter-life crypto. (and vendors?)
  • separate planes
  • bump-in-the-wire?
  • design with headspace?

• **Legacy PKI**
  • can the EDS PKI truly be independent?
  • rethink legacy “best practices” for EDS
  • rethink C-I-A tradeoffs
Lively discussion: EDS “PKI” requirements

- **Who talks to whom?**
  - including rare but predictable scenarios
- **Threat model**
- **Is authorization non-trivial?**
  - If so, do the keys and certs need to carry the information?
- **Is the important stuff always behind a protected physical perimeter?**
  - Do communications from end points need to be protected?
  - Do we care about smart homes...or smart buildings?
  - What about electric cars?
    - mobile
    - potential for big consequences
  - Distributed energy resources?

- **Do we always want to roll trucks? Or do we want decentralized/remote...**
  - commission
  - software update
  - transfer of ownership
- **Economic reluctance to change IT components. (Certification costs?)**
- **Can we make relying parties smarter to reduce risk of bad messages?**
  - detect bad data from monitors
  - relays that won’t listen to crazy parameter setting commands
  - exploit physical properties----e.g., gas compresses
Towards an Industrial Key Infrastructure

• **TCIP circa 2005:** “Will you ever use the Internet?”
• **Usage scenarios**
• **Interested parties and partners: please get in touch!**

Sean Smith, sws@cs.dartmouth.edu
Discussion
Funded by the U.S. Department of Energy and the U.S. Department of Homeland Security