New thinking about security for the internet of things

Credible protection for critical infrastructure systems

4 October 2016

Neil Siegel, Ph.D.

USC Viterbi IBM Professor of Engineering Management

USC Viterbi School of Engineering

University of Southern California

Background

- Until 1 January, I was vice-president & chief technology officer for Northrop Grumman Information Systems
- I started the work described herein while I was at Northrop, and am continuing it at USC

- **Cyber protection**: primarily for the U.S. intelligence community
- **Physical protection**: primarily for large facilities in the middle east: U.S. air force bases, U.S. Army bases, ARAMCO facilities

Thinking about the "internet of things"

- Huge "upside" potential
  - Efficiency, cost reduction, "1+1=3" capabilities
- But . . . if we don't get the security and privacy right – from the very beginning – I predict that we will not be allowed to realize much of that potential
  - SCADA and cyber-enabled physical systems already today represent threats of physical damage due to hacking / etc., not just data loss.
  - Tomorrow's internet-of-things just magnifies this by many orders of magnitude

So . . . I am thinking about security in the IoT context . . .

. . . and have concluded that almost all cyber-security today is based on a ***false premise***

"Operating with the enemy inside"

- Most cyber protection is based on a ***false premise***: that we can keep bad actors outside of our critical systems
  - The "M&M" security model: "hard on the outside, software on the inside"
  - It is not surprising that systems are routinely hacked
- I have been researching the problem of how to reliably ***continue critical mission processing***, and to ***continue to protect critical data***, even ***after*** the bad guys have gotten into our systems
  - Very promising results

Could be the key differentiator for IoT

How?

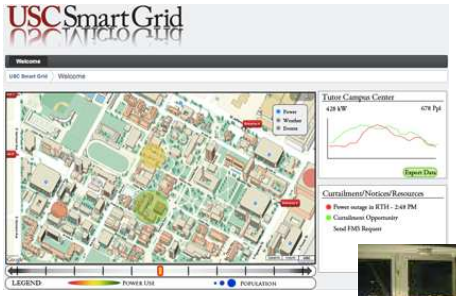
- "White-list-only" processing
- Encrypted storage of executables and data
- Temporal purging of virtual images on a frequent (ideally, execution-instance-by-execution-instance) basis, where no executables survive, and the only data that survives such purging are defined by the white-listing methodology ("proactive automatic restore")
- Methods and metrics for measuring when the design is really complete, in some cases via formal (mathematical) means
- Automatic, high-rate modulation of system configuration
- Trust-zone segmentation
- Strong identification of users and actors

Next insight: IoT is a ***cyber-physical*** system . . . so we must think about security in the context of that holistic view

Integrated cyber / physical protection

- We created a concept: that ***combining*** cyber and physical situational awareness would improve over-all understanding, and lead to better decisions, and better protection
- Funded a project with USC (with Professor Donald Paul, former CTO of Chevron), and established a lab on campus for this purpose
  - Focused initially on use-cases in the energy business
  - Lab is set up around a "smart-grid" use-case
  - Examined a number of scenarios, and showed both the technical feasibility, and the potential for value

USC cyber / physical integration lab



Control Room

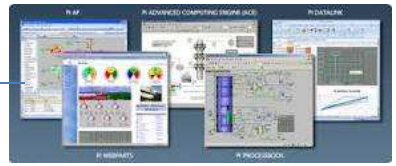
N-Dimension SCADA Anomaly Analytics via Internet

Campus LAN

Lab LAN

NG physical protection system

NG network protection system



Other protection systems

Adding integrated analysis and annunciation

SCADA Sniffer*

SCADA Sniffer*

SCADA Sniffer*

Sub-stations

HVAC

Metering

USC Viterbi School of Engineering

University of Southern California

Summary

- I believe that ***security and privacy protection*** will "make or break" large-scale internet-of-things adoption
- Most security architectures in use today – and planned for tomorrow – are ***fundamentally flawed***
  - "Operating with the enemy inside" will lead to better protection, and will also be convincing to the general public
- The internet-of-things is fundamentally a cyber-physical system, and techniques based solely in one or the other of those domains will be inadequate

Back-up information

USC Energy Institute: major ongoing programs

- Intelligent Energy Infrastructures:
  - Smart Oil and Gas Fields – CiSoft (initiated in 2003)
  - Smart Power Grids – USC Smart Grid Living Laboratory / DOE – LADWP Demonstration Program (initiated in 2009)
- Cyber-Physical Security Systems for Energy Infrastructures
  - NGC/USC Laboratory for Energy Security Systems (initiated in 2014)

Questions / discussion