The S4 Papers

Dale Peterson, Digital Bond, Inc.
peterson@digitalbond.com

SCADA Security Scientific Symposium

- Research papers presented in technical detail to a technical audience
  - Gets down to the byte, code, protocol spec, statistic, detailed math level
  - Technical papers are published in a Proceedings book
  - January in Miami Beach
  - Physical audience limited to 55 people
  - Virtual attendees around the world
  - 2009 was the 3rd year

Exploiting Field Device Ethernet Card Vulnerabilities

- Rogue firmware upload
  - No authentication of source or content
  - If you can access it, you can load your firmware
- Proof of Concept for RA ControlLogix and Koyo / Direct Logic
  - Loaded our firmware that pinged other devices and changed web pages
  - Detail of learning the load in the paper

So What?

- Paper discussed what an attacker would do
  - Delayed, staged attacks – 23:58 on New Year's Eve
  - Disgruntled insider nuisance
  - Attack platform to attack servers and workstations
    - Like printers on corporate network
  - Field device worm, botnet
  - Proof of concept worm to prove the point

Actions / Takeaway

- Does your Ethernet Card have the unauthenticated firmware upload feature?
  - Can you turn it off
  - Start asking your vendor for a solution
  - Vendors fix it!!! and we will sing your praises

- Also included vulns and ramifications of management applications
  - Cross Site Scripting, SNMP, orphaned code

Security Metrics Papers

- Estimates of 0Day Vulns in Control Systems
  - INL Paper – McQueen[2], Boyer, McBride
  - 0Day time from reporting to time of publishing
- Reviewed 491 0Days – ZDI and iDefense
- Estimate 250 0Days in control systems
  - Primarily vulns in IT components used in SCADA
  - Windows, Apache, Oracle
- Ralph Langner introduces iDay
  - Infinite Day – vendor has no plan to address

ISA 99 Security Metrics

- Dennis Holstein, OPUS Publishing
- Used Jaquith's criteria
  - Measureable, not-subjective, automated collection, etc.
- Zones and Conduits
- 7 Foundational Requirements / 10 Metrics
- Measurement over time
- Key is selecting the weights
  - Initially subjective
  - Industry sector guidance / standards

Jamming IEEE 802.15.4

- WSSC, Jake Brodsky and Anthony McConnell
- Clear Channel Assessment
  - Energy detection, then do not transmit
  - More sensitive receiver, easier to jam
  - Jam all 16 channels
  - About $70
  - Part of the IEEE spec
  - Always on in tested TI chipset

Control System Impact

- Uncertain
  - ISA 100, Wireless HART, Zigbee
  - Will impact ISA 100 “slow hopping” and “listen-before-talk” modes
  - Standard says will not affect the more typical modes
  - Will they use the IEEE 802.15.4 chipsets?
  - Will they be prevented from turning on CCA
  - Compliance testing will be key
  - Need research when ISA 100 devices are available

Design Vulns in Wireless Hardware

- Travis Goodspeed and EnerNex
- What could an attacker do if they stole or had physical access to one wireless device?
  - Very technical talk
- Bootloader timer attacks to extract firmware, keys
  - Password is Interrupt Vector Table
  - Recovered through timing attack
  - Can't be patched, vuln is in TI masked ROM
- Much more: glitching, selective jamming, bus tapping

Vulnerability Impact

- Physical access to a device and serious skills
  - Recover keys, recover firmware
  - Find an overflow, create a worm
- Hardware errors are going to be very hard to fix
  - Can't patch, replace the chip
- Architecture matters, single chip, board security
- 802.15.4 chips are cheap and readily available
  - Expect hacker community to attack
  - Small number of chips, widely used

Wireless Mesh Key Mgmt & 1st Responder

- Honeywell and Sandia paper, funded by DHS
  - Detailed description of PKI lifecycle for peer-to-peer keying in mesh network
  - Interesting . . . Ross Anderson comment on potential attack
- First Responder
  - How to you provide emergency credentials securely
  - Still very process driven, not technology
- Implemented in Honeywell OneWireless

2 Directions in Perimeter Security

- Electricite de France, Cambacedes and Sitbon
- One-way physical diode
  - True one-way, no feedback
  - Where can this be used? Between zones? Safety?
  - Fantastic Reference section and history
- Deep inspection
  - Firewall rules base on control system protocol
  - Check Point and Byres
  - Detailed example using Scapy

Application Specific IDS

- Mai Kiuchi and others from CRIEPI in Japan
- Tailor IDS rules for specific applications
- Example: HMI select limitations

- Could vendors offer a highly effective, highly customized set of application IDS signatures?

Detecting Cyber Attacks

- Digital Bond Paper
- Use Historian to aggregate and correlate security events to detect cyber attacks
  - Historians are deployed, leverage
  - OSIsoft PI Server as proof of concept
  - Dept. of Energy funded, available for low / no cost
- Expert system approach – FAIL
- Composite Approach
  - Triggers, Events, Event Class Events, Meta Events

Bonus - Keynote

- Dr. Ross Anderson, University of Cambridge
  - Author of Security Engineering
- The Economics of Control System Security
  - Adverse selection example
  - This should lead to a lot of new research
  - $ not security metrics!

Invited Talks

- Denial of Control
  - Mark Fabro, Lofty Perch and Zach Tudor, SRI
  - Different than denial of service . . . Availability
  - Denial of service . . . Integrity
  - Should we be measuring this?
- Virtualization
  - Ralph Echemendia of Terramark
  - Real world numbers are daunting!!!
  - Why isn't a vendor providing a recommended virtualized installation?

Research In Review

- Obviously Biased
- Interest is high, great audience
- Quality is high
  - Better every year
- Quantity is low
  - Struggle to find 12 strong papers
  - Showing control system protocols lack security is not research, showing IDS sigs work is not research