

# Who's Controlling YOUR Industrial Control System? (And what makes you so sure?)

An information security primer for systems professionals

October 19, 2010

International Society of Automation - Chicago Section

Todd Haverkos, Sr. Security Engineer

# Who is this guy?

- EE, CompE
- Recovering chip designer
- Application and Network Security Specialist
- 9yrs w/ IBM ISS
- Certified Ethical Hacker
- Licensed Penetration Tester
- Currently in-house infosec staff for financial trading company in Chicago focused on offensive security.

# What's offensive security?

“So it is said that if you know your enemies and know yourself, you can win a hundred battles without a single loss.

If you only know yourself, but not your opponent, you may win or may lose.

If you know neither yourself nor your enemy, you will always endanger yourself.”

--*The Art of War*, Sun Tzu

# Why do we care about security?

- Ever-increasing reliance on computer control
- Malware, Trojans, Viruses, Spyware ... no longer pranks of the slacker kid in mom's basement
- Targeted Attacks on the rise
- Industrial Espionage
- Computer crime now more lucrative than drug trade
- People can die

# Why's it so difficult?

- System complexity, attack surface
- Asymmetric threat
- Security typically an afterthought
- Developers not trained to code securely
- Developers not compensated to code securely
- Developers not reviewed on code security
- Security as a silo doesn't work
- "Lean" sourcing.

# Some Terminology

- “CIA” triad
  - Confidentiality, Integrity, Availability
- Threat - simple, generic potential for attack
- Vulnerability – specific weakness that makes something susceptible to attack (e.g buffer overflow, format string, SQLi, XSS, CSRF)
- Exploit – an attack against a specific vulnerability
- Patch/Update – remediation for the vulnerability
- Zero-day / O-day / 0-day
- Rootkit – adds the ability to hide, OS to lie

# A typical vulnerability/attack

- Our friends at Adobe produce roBUST software.
- Adobe Reader exploit du-jour (or Flash)
- Unsuspecting user visits their favorite blog site
- To find it quietly having been compromised by a Drupal or WordPress vulnerability... and
- Serving up an exploit pack that uses...
- JavaScript fingerprinting, enumerating all visitors' browser and plugins
- And... automatically redirect to exploits for the vulnerable pieces.
- Suddenly your machine has "Antivirus 2010" and you have no idea what you did wrong.

# Typical defenses (and their flaws)

- “But I have Norton Anti-Virus!”
- “But we have a firewall!”
- “I run Windows Update!”
- “I don’t surf to bad websites!”
- “No one would ever guess my l33t p4ssw0rd!”
- “I’m using WEP!”
- “That website has SSL! WCPGW?”
- “The information on my computer isn’t that sensitive.”

# Badguy (and Goodguy) Tools

- Nmap
- Nessus / OpenVAS Vulnerability Scanners
- Metasploit / CANVAS / Core Impact exploit frameworks
- Binary repackers (evade AV)
- Password crackers (John the Ripper, Rainbow crack)
- Social Engineering Toolkit (SET)
- BeEF (Browser exploitation framework)
- Kismet/AirCrack 802.11
- USB Switchblade/ USB Hacksaw (pop in and own)
- Lots of these goodies available on BackTrack Linux
- Warning: use responsibly ON SYSTEMS YOU OWN.  
The pro's don't work without a GooJF letter.

# Stuxnet

- “The Stuxnet malware is a game changer for critical information infrastructure protection, an EU security agency has warned.”
- Worm (= self propagating malware), USB keys, fileshares
- Gathering press because of its extremely advanced nature, presumed nation-state sponsorship
- 4 0-day exploits! 2 stolen crypto certs.
- Targets supervisory control and data acquisition (SCADA) systems, s7-300 and s7-400
- Targets specific Programmable Logic Controllers (PLC's) in Siemens SCADA systems
- First ever\* worm to include a PLC rootkit
- “Millions had been spent developing the malware.”

# Stuxnet (cont'd)

- Updates via peer to peer networking
- 100k infections detected
- Stuxnet parses system data blocks of PLC
- Looks for specific bytes indicating a Profibus network card
- Normal PLC programming: Step 7/Simatic software -> STL -> MC7 bytecode -> PLC
- MITM's Step7 s7otbxdx.dll and replaces with its own version
- Injects blocks of MC7 byte code into PLC's
- Real world effects still being reversed
- Props: Liam O Murchu/Symantec

# What to do??

- No easy answers!
- Defense in depth
- AV is broken, but a necessary baseline
- Application whitelisting
- Device control – removable storage, autorun settings
- Intrusion detection/prevention systems (IPS/IDS)
- SIEM Security Information and Event Management (e.g. Arcsight)
- Vulnerability Scanning/Management
- Patching (easy to say, hard to get done)
- Penetration testing
- Physical security/social engineering/least privilege
- Auditors can be your friends – help you get \$'s / buy-in

# References

- Stuxnet- infecting industrial control systems  
<http://www.slideshare.net/symantec/stuxnet>
- [http://www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/w32\\_stuxnet\\_dossier.pdf](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf) detailed white paper
- Stuxnet 'a game changer for malware defence'  
[http://www.theregister.co.uk/2010/10/09/stuxnet\\_enisa\\_response/](http://www.theregister.co.uk/2010/10/09/stuxnet_enisa_response/)
- Detecting PLC Infections  
<http://www.symantec.com/connect/de/blogs/detecting-plc-infections>

# Security Geekery

- Podcasts: pauldotcom.com, Network Security Podcast, Southern Fried Security Podcast, Exotic Liability, Eurotrash...  
podcastersmeetup.com
- Conferences: Blackhat, Defcon, Bsidies, Shmoocon, Thotcon (local), Chicagocon
- Twitter
- [www.theregister.co.uk/security](http://www.theregister.co.uk/security)  
[Darkreading.com](http://Darkreading.com)

# Thank You!

---

- Questions