

# SCADA Security Summit: Accelerating the Adoption of Security Tools That Work

October 27, 2005

PCSF

Chicago



Copyright 2005, The SANS Institute

**Alan Paller**  
Director of Research  
The SANS Institute  
[paller@sans.org](mailto:paller@sans.org)  
[www.sans.org](http://www.sans.org)

# Agenda

---

- Why it makes sense to act now
- The US House of Representatives Homeland Security Subcommittee hearing last week
- A Summit on securing control systems

# Targeted Attacks – an epidemic

- British Government disclosed the wave of successful attacks in late June  
<http://www.niscc.gov.uk/niscc/docs/ttea.pdf>
- Attackers used common vulnerabilities or spear phishing to get inside the firewall
- Anti-virus does not protect you
- Installed “collector software” that stole password files, credit cards, sensitive military data, and much more; data is being sold by brokers in the Ukraine
- NISCC: "These electronic attacks have been under way for a significant period of time, with a recent increase in sophistication,"

# Titan Rain – the new imperative

- Discovered by a Sandia National Labs Researcher
- Found a Chinese hacker group “penetrating secure computer networks at the country's most sensitive military bases, defense contractors and aerospace companies.”

# How many sites?

- “They hit hundreds of computers that night and morning alone
- “At 10:23 p.m. pacific standard time (PST), they found vulnerabilities at the U.S. Army Information Systems Engineering Command at Fort Huachuca, Arizona.
- “At 1:19 am PST, they found the same hole in computers at the military's Defense Information Systems Agency in Arlington, Virginia.
- “At 3:25 am, they hit the Naval Ocean Systems Center, a defense department installation in San Diego, California.
- “At 4:46 am PST, they struck the United States Army Space and Strategic Defense installation in Huntsville, Alabama.”

**Is anyone else targeting the US?  
Are they after anything besides  
data and money?**



# The new face of cyber crime....

**Imam Samudra,  
the “Bali Bomber” on death row in Indonesia**

**In his autobiography Samudra writes, “If hacking is successful, get ready to gain windfall income for just 3 to 6 hours of work, greater than the income a policeman earns in 6 months of work. But, please do not do that for money alone! I want to motivate the youth and Moslem men who are granted perfect mind by Allah; I want America and its cronies to be crushed in all aspects.”**

# You, the experts, know what to do

- But how do you get the buyers to buy,
- How do you get the vendors to deliver safer systems, and
- How do you do it now rather than in 15 years?

# Key opportunity areas

- Security tools that are expensive, difficult to integrate, and that disrupt operations
- Process control systems, networks and architectures that facilitate attacks
- Asset owners and operators who get conflicting advice from “experts” and are unsure what to do to protect their systems

# The House Committee on Homeland Security: Joint Hearing

- Single most important responsibility of government is to protect the public
- The threat of industrial control system compromise is immediate and proven
- No expectation of new federal money
- Regulation and legislation are a last resort
- One idea got them resonating: joint procurement power to leverage IT investment to improve security

# A Promising Approach

- Gain consensus on which problems need immediate action and what steps must be taken first (verify that they actually work)
- Create procurement language that allows buyers to be sure they are ordering the right stuff
- Consolidate sufficient buying power to persuade the vendors to act now.

# Defining the problem

AF CIO Gilligan told 200 people and the press

- “We cannot rely on the systems we deploy in wartime or the systems we use for management, and
- “It costs us more to clean up after Windows compromises than to buy the software in the first place.”

# Air Force Procurement Leadership

- \$500 million contract with Dell for Windows software
  - Consolidated 38 existing contracts
  - Saved \$100 million in initial procurement costs
  - Ensured safe configurations on every system
  - Future: Lower patch testing costs by \$100 million more
- Separate \$100+ million contract with Microsoft for support
- Testing at two Air Force bases now

# Next Steps on Security Baked In

- Air Force tests illuminate the costs of transition
- Air Force rolls out to all bases
- Air Force requires all software to be built to run on the safe configurations
- OMB extends the contract to all US government
- Vendors deliver “well behaved” applications
- Microsoft starts delivering safer systems to “all our customers”
- Same process (leveraging federal procurement) will be employed to for other operating systems, databases, applications, and appliances.

# Hypotheses

- The experts (you) know what can be done and what needs to be done to protect legacy control systems
- Consensus can be reached for specific problems/sectors
- Procurement language can be drafted
- Sufficient buying power can be consolidated

# SCADA Security Summit

- Goals:
  - to enable the asset owners of the critical infrastructure to jointly determine “what works.”
  - to develop procurement language that the operators can use
- Leadership
  - Hun Kim and Andy Purdy, National Cyber Security Division, US Department of Homeland Security
  - Karl Williams, UK National Infrastructure Security Co-ordination Centre
  - Hank Kenchington, Office of Electricity Delivery and Energy Reliability, US Department of Energy
  - Alan Paller, The SANS Institute

# Organizing Committee: Asset Owners

- \*James Cupps, BP
- \*Ian Henderson, BP
- \*Will Pelgrin, Chief Information Security Officer, State of New York and Chairman of the Multi-State ISAC
- Andrew Hildick-Smith, Massachusetts Water Resources Authority (MWRA)
- Tom Flowers, Center Point
- Tom Good, DuPont Co
- Evan Hand, Kraft Foods Inc.
- Seiki Harada, BC Hydro Canada
- Jay White, Chevron Texaco
- Tom Bowe, PJM
- Stuart Brindley, Independent Electricity System Operator, Ontario, Canada
- Gerald S. Freese, AEP

## Organizing Committee: Research Groups

- \*Mike Assante, Idaho National Laboratory
- Jennifer DePoy, Sandia National Laboratory
- Eric Byres, British Columbia Institute of Technology
- George Cybenko, Dartmouth University, I3P
- Andrew Wright, Cisco Critical Infrastructure Assurance Group

# Organizing Committee: Industry Groups

- Mike Torppey, Technical Director, Process Control Systems Forum
- Bill Rush, Gas Technology Institute
- Tom Kropp, EPRI (Electric Power Research Institute)

# How It Works

- Each session is focused on short term solutions to specific threats
- Individual solution proponents
- Discussants
- Audience composed on asset owners and operators and integrators who express their support for specific solutions

# If you want it to succeed

- Provide your recommendations of the specific solutions that can protect legacy control systems with suggested proponents
- Submit a proposed solution for presentation
- Serve as a discussant
- Point out the flaws in the strategy

# How to make suggestions

- [paller@sans.org](mailto:paller@sans.org)

**Questions?**

