Industrial Control Systems Security

Protecting the Critical Infrastructure

Seán Paul McGurk

Director, Control Systems Security

National Cyber Security Division

U.S. Department of Homeland Security

Overview

- Control Systems Overview
- Threat and Risk
- Consequences
- Mitigation
- Control Systems Security Program

Homeland
Security

Overview of Control Systems

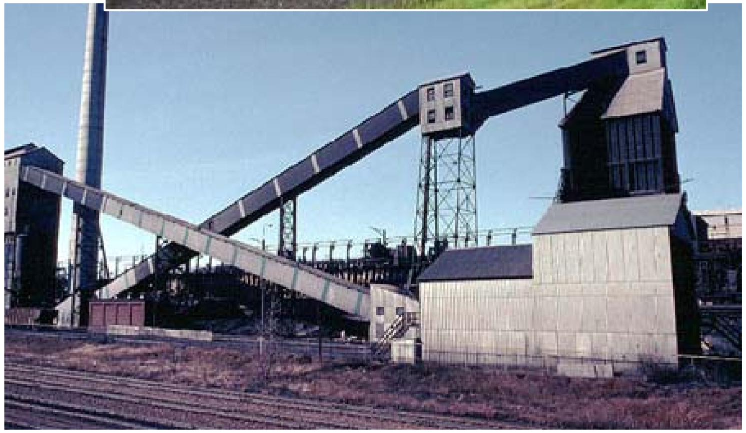
Homeland Security

Why are Control Systems unique?

- Control systems provide the means to sense a physical process and implement changes to that process to provide a product or desired result
- Modern control systems utilize communication and network components and architecture and are increasingly interconnected to business networks
- Control systems have much different life cycles, measured in decades with many communication protocols. Maintenance is also managed differently. Uptime and reliability are priority.
- Control systems have many and diverse “actors” involved including operators, vendors, integrators, and contractors over the life cycle.

What are Industrial Control Systems?

- Computer based systems (Digital to Analog)
- Connected to integrated systems
- Can control critical systems
- Usually remote operations
- Example systems
  - Railway and transit
  - Chemical processing
  - Water treatment
  - Power generation
  - Hazardous Materials storage/filtering



Homeland Security

Definition of a Industrial Control System

The term Industrial Industrial Control System (ICS) refers to a broad set of control systems, which include:

- SCADA (Supervisory Control and Data Acquisition)
- DCS (Distributed Control System)
- PCS (Process Control System)
- EMS (Energy Management System)
- AS (Automation System)
- SIS (Safety Instrumented System)
- And a number of other automated control system

Homeland Security

SCADA or DCS?

As technology advances, the terms are getting blurry. You will quite often hear the public refer to "SCADA" when they are really referring to other types of Industrial Control Systems.

- The key word in SCADA is "Supervisory." This indicates that decisions are not directly made by the system. SCADA systems are typically deployed across large geographical areas (e.g., electric grid)
- DCS provides real-time monitoring and control of a given process within a plant. All major components of the system are usually confined to one or several facilities (e.g., Nuclear power plant)

Homeland Security

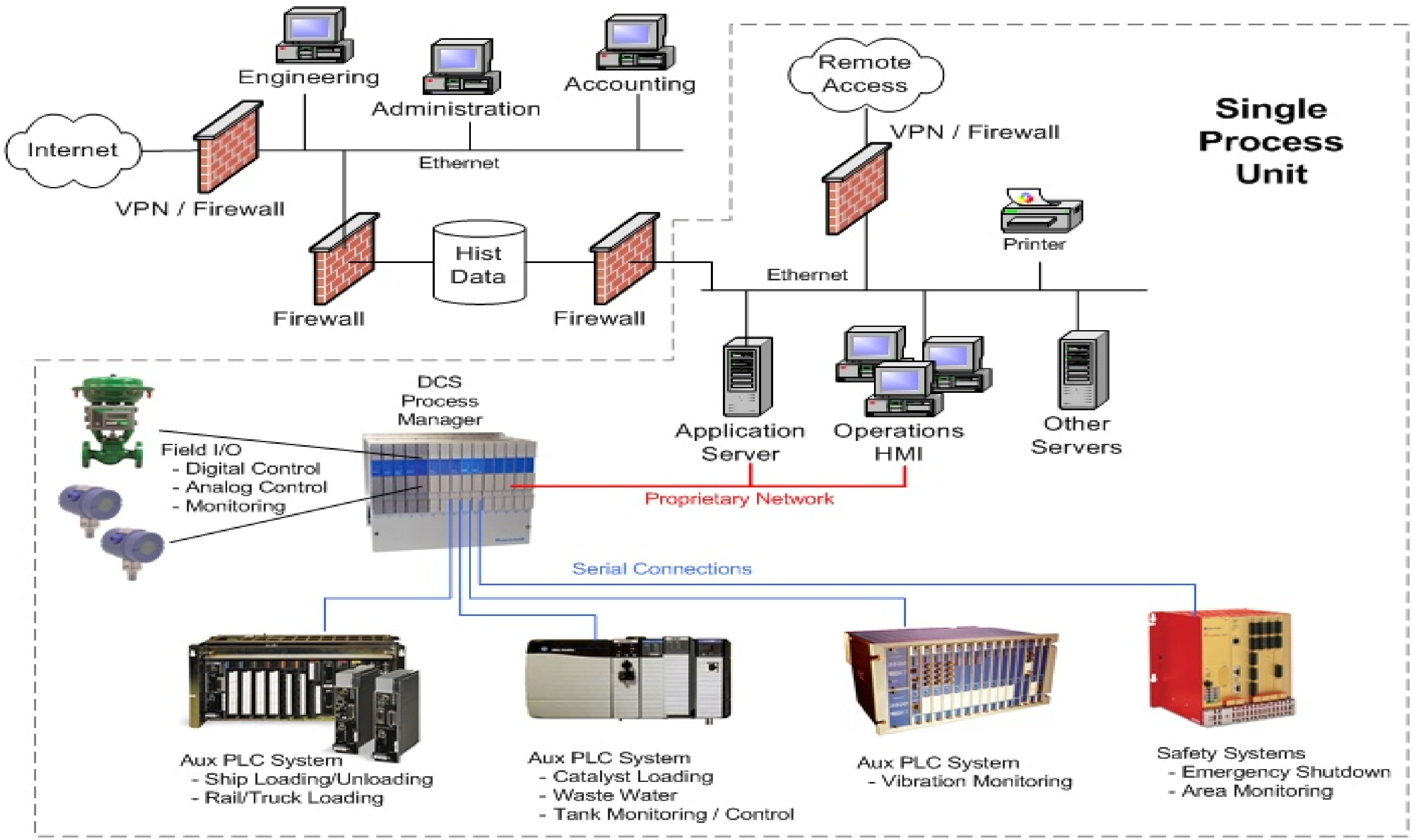
Control Systems Security Challenges

SECURITY TOPIC	INFORMATION TECHNOLOGY	CONTROL SYSTEMS
Anti-virus & Mobile Code Countermeasures	Common & widely used	Uncommon and can be difficult to deploy
Support Technology Lifetime	3-5 years	Up to 20 years
Outsourcing	Common/widely used	Rarely used (vendor only)
Application of Patches	Regular/scheduled	Slow (vendor specific)
Change Management	Regular/scheduled	Legacy based – unsuitable for modern security
Time Critical Content	Delays are usually accepted	Critical due to safety
Availability	Delays are usually accepted	24 x 7 x 365 x forever
Security Awareness	Good in both private and public sector	Generally poor regarding cyber security
Security Testing/Audit	Scheduled and mandated	Occasional testing for outages / audit for event recreation
Physical Security	Secure	Very good but often remote and unmanned

Homeland Security

© 2002 PA Knowledge Limited

Example Industrial Control System

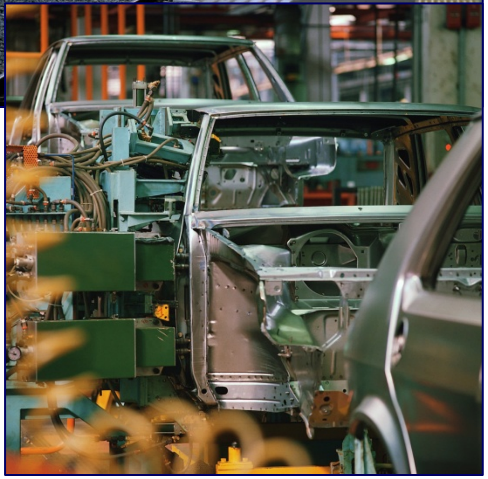


Homeland Security

18 Critical Infrastructure Sectors

Homeland Security Presidential Directive 7 (HSPD-7) along with the National Infrastructure Protection Plan (NIPP) identified and categorized U.S. critical infrastructure into the following 18 CIKR sectors

- Agriculture and Food
- Banking and Finance
- Chemical
- Commercial Facilities
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Government Facilities
- Information Technology
- National Monuments and Icons
- Nuclear Reactors, Materials, and Waste
- Postal and Shipping
- Public Health and Healthcare
- Telecommunications
- Transportation
- Water and Water Treatment



Many of the processes controlled by computerized control systems have advanced to the point that they can no longer be operated without the control system.

Homeland Security

Threat and Risk

Homeland
Security

The Risk Equation

National Infrastructure Protection Plan definition:

Risk = Threat x Vulnerability x Consequence

Threat: Any person, circumstance or event with the potential to cause loss or damage.

Vulnerability: Any weakness that can be exploited by an adversary or through accident.

Consequence: The amount of loss or damage that can be expected from a successful attack.

$$\frac{\textit{Risk} = \textit{Threat x Probability}_{(\textit{Vulnerability})} \textit{ x Consequence}}{\textit{Cost}}$$

Homeland Security

Threats to Control Systems

Crackers

Break into computers for profit or bragging rights

Insiders

Disrupt their corporate network, sometimes an accident, often for revenge

Attackers May Utilize Each Others Resources…

Terrorists

Attack systems for cause or ideology

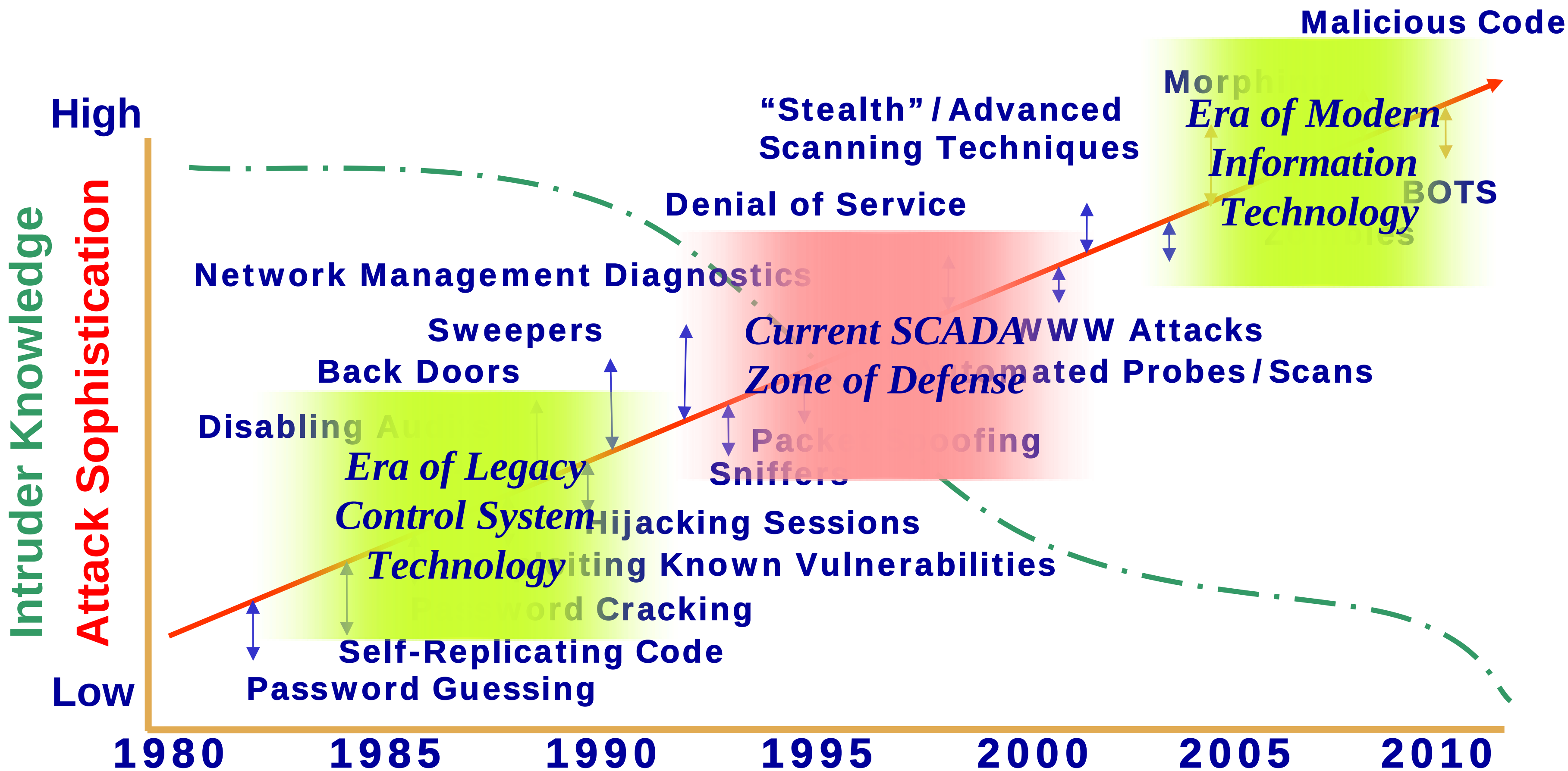
Hostile Countries

Attack enemy countries' computers

Homeland Security

Cyber Threat Trends

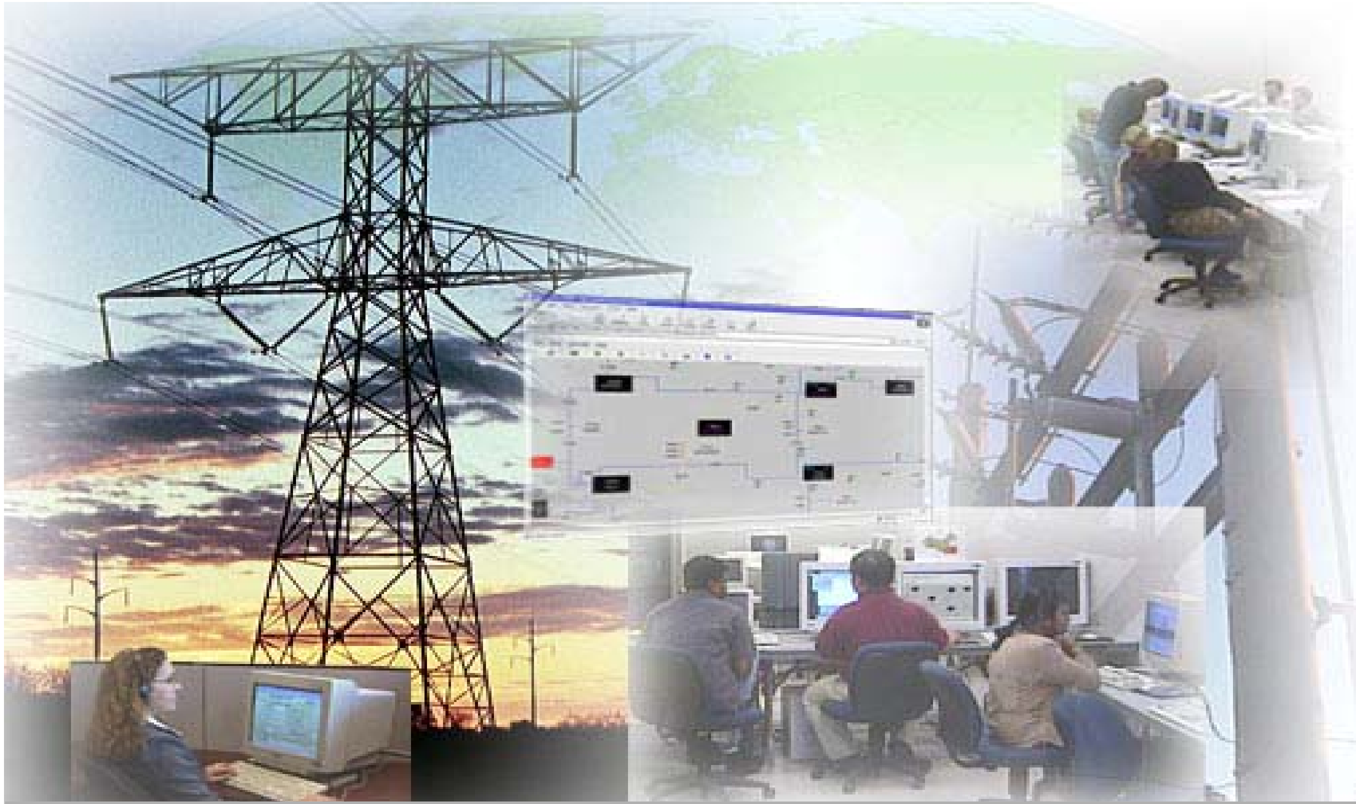
Threats become more complex as attackers proliferate



Lipson, H. F., *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues*, Special Report CMS/SEI-2002-SR-009, November 2002, page 10.

Homeland Security

Risk is Elevated in Converged & Interconnected Systems



Technology has blurred the line between the physical machine and the electronic machine driving our infrastructure.

Homeland Security

Risk Drivers: Threats

- International and domestic terrorism, and nation state cyber warfare – asymmetric warfare
- Internet increases availability of hacker tools along with information about infrastructures and control systems
- Emergence of a strong financial motive for cyber crime to exploit vulnerabilities

"We have information, from multiple regions outside the United States, of cyber intrusions into utilities, followed by extortion demands. We have information that cyber attacks have been used to disrupt power equipment in several regions outside the United States. In at least one case, the disruption caused a power outage affecting multiple cities." – CIA Senior Analyst

Risk Drivers: Vulnerabilities

- Industry pressure to streamline and automate to cut costs, resulting in connections between IT and control system networks (inheriting vulnerabilities)
- The shift from isolated, proprietary control systems to distributed systems using open protocols and standards
- Increased access and interconnectivity to remote sites through the use of modems, wireless, private, and public networks
- Numerous corporations have created shared or joint use systems for e-commerce

Risk Drivers: Vulnerabilities

- A shift towards a global environment, including multi-national companies
- Cyber attacks launched from remote locations, with very few attackers, as compared with a physical attack of similar magnitude.
- Multiple vulnerabilities exist when implementing remote access to Intelligent Electronic Devices and control systems.

Vulnerability Lifecycle

January 2008, Core Security Technologies discovers a vulnerability in the CitectSCADA product, and works with Citect and US-CERT

June 2008, Citect releases patches for affected products

Homeland Security

Vulnerability Lifecycle

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Vulnerability Notes Database

Search Vulnerability Notes

Vulnerability Notes Help Information

View Notes By
- Name
- ID Number
- CVE Name
- Date Public
- Date Published

Vulnerability Note VU#476345

Citect CitectSCADA ODBC service buffer overflow

Overview

Citect CitectSCADA contains a remotely accessible buffer overflow vulnerability which may allow a remote attacker to execute arbitrary code.

I. Description

Citect CitectSCADA is software used for monitoring and control in Supervisory Control And Data Acquisition (SCADA) systems. A buffer overflow vulnerability exists in the CitectSCADA ODBC service. The ODBC Server listens on the network (20222/tcp) for service requests from clients. An attacker could exploit this vulnerability by sending specially crafted packets to a vulnerable CitectSCADA system. According to Core Security Technologies Advisory:

> *Due to a lack of a proper length checking of the read data, a memory copy operation that uses as destination a buffer of fixed size allocated in the stack can be overflowed allowing an un-authenticated attacker to execute arbitrary code on vulnerable systems.*

Note that this vulnerability affects versions of Citect CitectSCADA and CitectFacilities. Exploit code for this vulnerability is publicly available.

June 11, 2008, US-CERT publishes Vulnerability Note regarding Citect buffer overflow

Homeland Security

Vulnerability Lifecycle

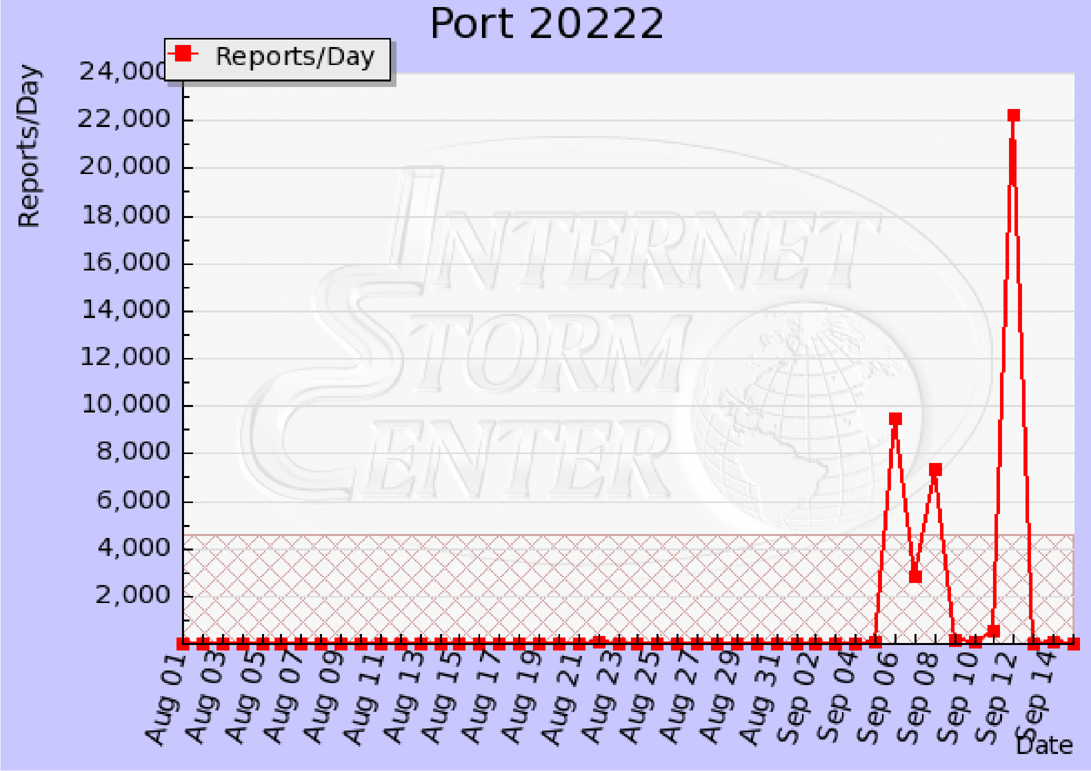
September 5, 2008, Metasploit exploit code posted

Homeland Security

Vulnerability Lifecycle

Immediately after the exploit code was posted, the SANS Internet Storm Center started recording traffic on the affected port

Port Details - Port 20222



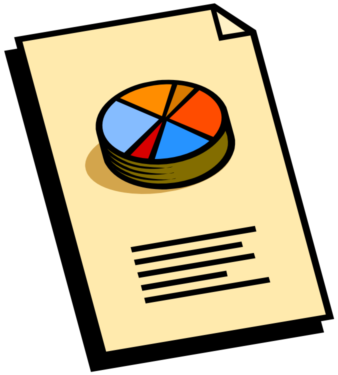
Homeland Security

General Findings

- Default vendor accounts and passwords still in use
  - Some systems unable to be changed!
- Guest accounts still available
- Unused software and services still on systems
- No security-level agreement with peer sites
- No security-level agreement with vendors
- Poor patch management (or patch programs)
- Extensive auto-logon capability

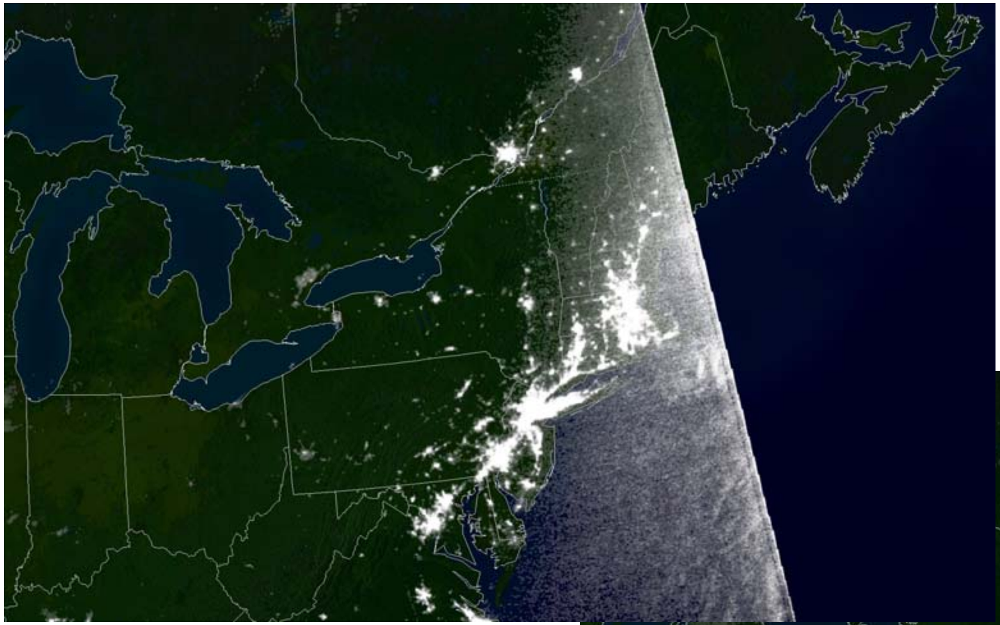
General Findings
continued

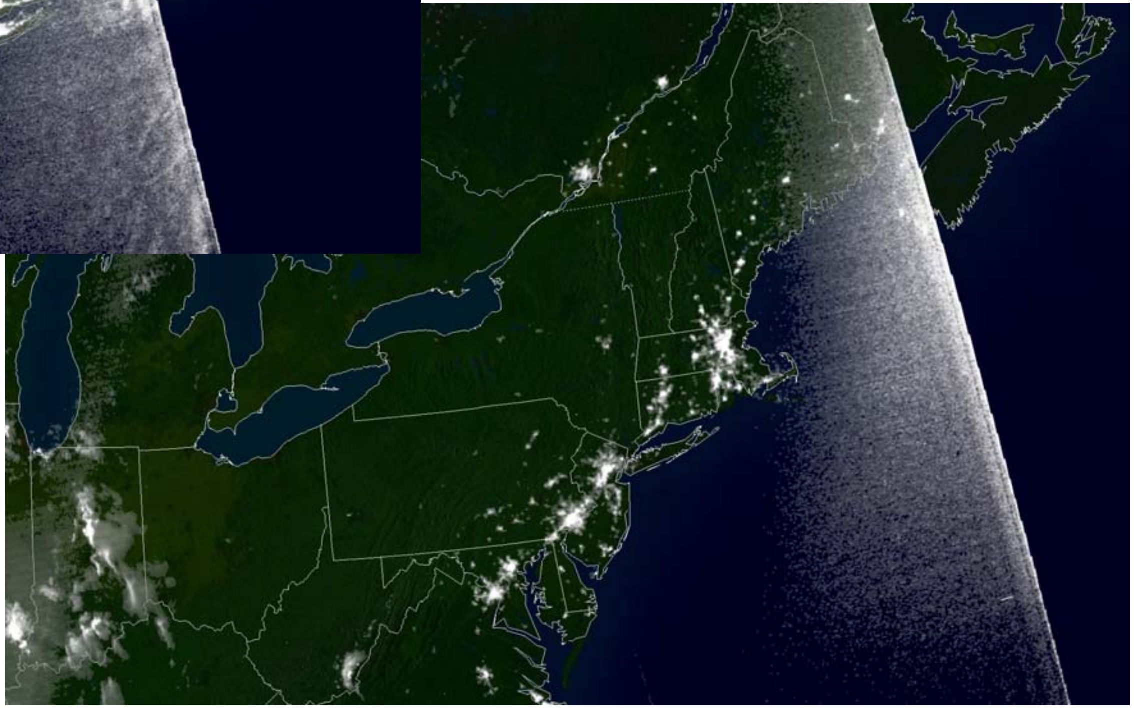
- Typical IT protections not widely used (firewalls, IDS, etc.). This has been improving in the last 6 months
- Little emphasis on reviewing security logs (Change management)
- Common use of dynamic ARP tables with no ARP monitoring
- Control system use of enterprise services (DNS, etc.)
- Shared passwords
- Writeable shares between hosts
  - User permissions allow for admin level access
- Direct VPN from offsite to control systems
- Web enabled field devices



Homeland Security

Consequences





Homeland Security

Davis Besse Nuclear Power Plant

Event: Aug 20, 2003 Slammer worm infects plant

Impact: Complete shutdown of digital portion of Safety Parameter Display System (SPDS) and Plant Process Computer (PPC)

Specifics: Worm started at contractors site

- Worm jumped from corporate to plant network and found an unpatched server
- Patch had been available for 6 months

Recovery time:

SPDS – 4hours 50 minutes

PPC – 6 hours 9 minutes

Lessons learned:

- Secure remote (trusted) access channels
- Defense-in-depth strategies, FWs & IDS
- Critical patches need to be applied

Homeland Security

Olympic Pipeline Explosion

photo by David Willoughby copyright *Bellingham Herald*

Event: 16-inch gasoline pipeline explosion and fire, exacerbated by inability of SCADA system to perform control and monitoring functions.

Impact: 3 fatalities, property damage >$45M, matching fines of $7.86M against two companies.

Specifics: Erroneous changes to live historical database caused critical slowdown in system responsiveness (evidenced by sensor scan rate changing from 3 second poll to over 6 minutes!)

- Communication link between main computer, field sensors, and controllers was a combination of leased phone lines and frame relay.

Lessons learned:

- Identify controls to Critical Assets
- Do not use administrative controls to solve system anomalies
- Do not perform database updates on live systems
- Apply appropriate security to remote access

Homeland Security

Maroochy Waste Water

Lessons learned:

- Change log-ons after terminations
- Investigate anomalous system behavior
- Use secure radio transmissions

Event: More than 750,000 gallons of untreated sewage intentionally released into parks, rivers, and hotel grounds

Impact: Loss of marine life, public health jeopardized, $200,000 in cleanup and monitoring costs

Specifics: SCADA system had 300 nodes (142 pumping stations) governing sewage and drinking water

- Used OPC ActiveX controls, DNP3, and ModBus protocols
- Used packet radio communications to RTUs
- Boden used commercially available radios and stolen SCADA software to make his laptop appear as a pumping station
- Caused as many as 46 different incidents over a 3-month period (Feb 9 to April 23)

Homeland Security

Texas City Explosion 3/23/05

The Houston Chronicle

High court frees judge to rule on BP blast plea deal

By KRISTEN HAYS Houston Chronicle Copyright 2008

July 2, 2008, 4:03PM

The U.S. Supreme Court today denied a request from victims of the 2005 explosion at BP's Texas City refinery to temporarily block a judge from accepting or rejecting a blast-related criminal plea deal.

Last week the victims filed a request that the high court order U.S. District Judge Lee Rosenthal hold off on ruling on the plea deal so they could ask the Supreme Court to review whether it should be rejected.

On the full court's behalf, Justice Antonin Scalia today rejected the request in a one-sentence order without explanation, said Paul Cassell, a professor at the University of Utah School of Law who represented the victims in the request. The order frees Rosenthal to decide whether to accept or reject the plea deal, which calls for BP's North American products division to admit to a felony violation of the Clean Air Act, pay a $50 million fine and be on probation for three years. Cassell said the victims' lawyers will meet next week and decide whether to seek a Supreme Court review the deal anyway, but those efforts could be rendered moot if Rosenthal rules.

"That was why we were asking for the stay," he said.

The high court's session ends Thursday, and justices won't meet again until the next session in October.

BP opposed the stay, and has asked Rosenthal to schedule a hearing to rule on the plea deal. The company declined comment today on the Supreme Court's denial of the stay and reiterated its support for Rosenthal to act. Don DeGabrielle, U.S. Attorney in Houston, said his office agreed with the high court's decision, the case remains before Rosenthal and "we stand ready to proceed.''

Federal prosecutors in Houston negotiated the plea deal with BP last October, and announced it publicly when an agreement was reached. But victims of the blast that killed 15 people and hurt scores more vehemently criticized the plea deal as too lenient, particularly the fine. They also accused the government of bypassing their right under the 2004 Crime Victims Rights Act to be consulted when a plea deal was in the works.

Homeland Security

Harrisburg, PA water facility

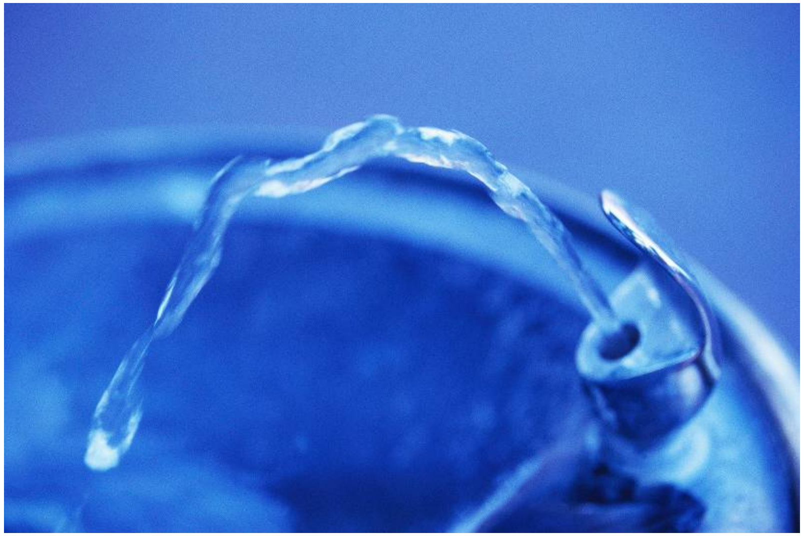
Water Tech ONLINE www.watertechonline.com

Legal Briefs - 11/1/2006 1:46:48 PM

PA water plant tapped by computer hackers

HARRISBURG, PA – The FBI is investigating a security breach in which hackers gained access to the computer system at a Harrisburg drinking water treatment plant, according to a November 1 report on InfoWorld.

The breach, which was discovered earlier this month, occurred after a laptop used by a plant employee was accessed by hackers via the Internet and used to install a computer virus and "spyware" on the plant's computer system, the article noted.



Homeland Security

Polish Trains

Telegraph.co.uk

Schoolboy hacks into city's tram system

By Graeme Baker
Last Updated: 2:48am GMT 11/01/2008

A teenage boy who hacked into a Polish tram system used it like "a giant train set", causing chaos and derailing four vehicles.

The 14-year-old, described by his teachers as a model pupil and an electronics "genius", adapted a television remote control so it could change track points in the city of Lodz.

The boy, described as a 'genius' and some of the equipment he used

Twelve people were injured in one derailment, and the boy is suspected of having been involved in several similar incidents.

The teenager, who was not named by police, told them he had changed the points for a prank.

A police statement said he had trespassed at tram depots in the city to gather information and the equipment needed to build the infra-red device.

Homeland Security

Insider Threat

2 deny hacking into L.A.'s traffic light system

Two accused of hacking into L.A.'s traffic light system plead not guilty. They allegedly chose intersections they knew would cause major jams.

By Sharon Bernstein and Andrew Blankstein, Times Staff Writers - January 9, 2007

2 Los Angeles traffic engineers admit hacking

Hours before a 2006 job action by their union, the pair sent computer commands that disconnected four signal control boxes at critical intersections.

By Andrew Blankstein
4:37 PM PST, November 5, 2008

Two Los Angeles traffic engineers admitted today to hacking into a computer system that controls traffic lights before a job action related to contract negotiations with the city, prosecutors said.

Gabriel Murillo, 39, and Kartik Patel, 36, who worked with the city's Automated Traffic Surveillance Center, each pleaded guilty to a single felony count of illegally accessing a city computer connected to the center.

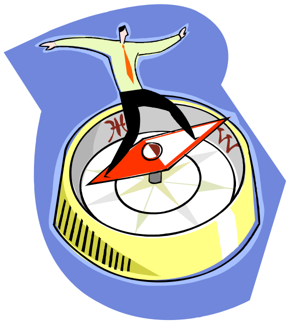
Los Angeles Times

Homeland Security

An Example -

Homeland Security

Highlights



- Control system security can no longer hide behind proprietary configurations and special training (Security by Obscurity)
- Control systems are no longer isolated systems that require special skills; open systems and protocols
- Control systems are no longer isolated from corporate and other networks
- Hackers are smart, and the prevalence of information available via the Internet makes attacking control systems easier
- Control systems are migrating away from their traditional shared and unrestricted configurations to more secure ones

CSSP Strategic Overview

CSSP Objectives
– Culture of Security
– Provide Value
– Cross Sector Focus
– Leadership

Major Activities
– Risk Reduction
– Analysis
– Technology Assessment
– Situational Awareness
– Education

Measure Progress Against Objectives

Homeland Security

Functional Areas

- ICS Analysis and informational products
- Training – Instructor and web base
- Subject Matter Expertise support
- Standards support
- ICS Assessments
  - On site / Control Systems Analysis Center (CSAC)
  - Interviewing control system operators, engineers, and IT staff on configuration and use
  - “Table top” review of network and security (firewalls, IDS/IPS, etc.)
- R&D gap analysis
- Sector Agency Support
  - Government Coordinating Council
  - Sector Coordinating Council

Homeland Security

ICS - CERT

- CSAC analysis shared across all sectors through products and trainings
  - Mitigate vulnerability in partnership with vendors
  - Vulnerabilities patched by vendors
- CSSP web site links US-CERT control systems *“Vulnerability Notes”*
- Vulnerability reports submitted via US-CERT web site and entered into National Vulnerability Database (NVD)
- PCII is an information-protection tool that facilitates private sector information sharing with the government

Homeland Security

Control Systems Cyber Security Self-Assessment Tool – CS^{2}SAT

- Based on industry standards
- Capability:
  - Creates baseline security posture
  - Provides recommended solutions to improve security posture
  - Standards specific reports (e.g. NERC CIP, DOD 8500.2, NIST SP800-53)
- Availability:
  - To industry through licensed distributors
  - To government agencies through DHS

Homeland Security

Cyber Security Vulnerability Assessment CSVA

- Assessment Covers Policy, Plans and Procedures in 10 Categories, for example:
  - Access Control
  - Monitoring and Incident Response
  - Configuration Management
  - Awareness & Training
  - Personnel Security
- Leverages Industry Standards, Guidance and Methodologies
  - NIST 800 Series
  - ISO 27001
  - Does not validate compliance Standards

Homeland Security

Comparison: CSVA to CS2SAT

CSVA

- IT and Business System Focus
- High-Level Management Overview
- Designed for Quick First-Pass Assessment
- Generates Summary-Level Management Reports

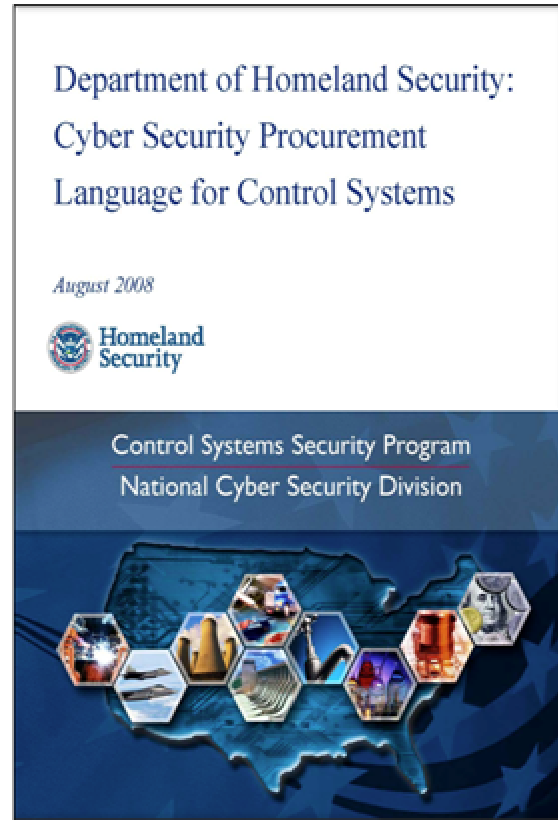
CS²SAT

- Control Systems Focus
- Detailed Standards Compliance Analysis
- Designed for Detailed Self-Assessments and Comparisons Over Time
- Generates Detailed Reports of Compliance Gaps

Cyber Security Procurement Language for Control Systems

<u>**Building Security into Control Systems**</u>

- Provides sample or recommended language
  for control systems security requirements
  - New SCADA / control systems
  - Legacy systems
  - Maintenance contracts

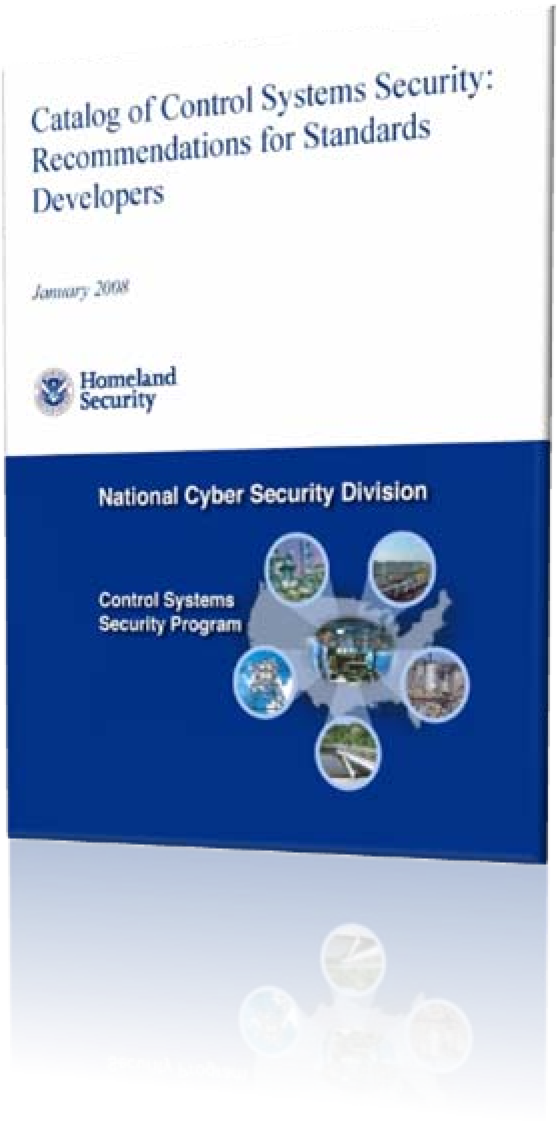


Homeland Security

Catalog of Control Systems Security: Recommendations for Standards Developers

Supporting Standards Development

- Provide guidance for cyber security requirements specific to control systems
- Enable a common security language across all industry sectors
- Support standards bodies and industry associations to implement sound security practices in current standards



Homeland Security

Education & Training

Web Based Training

- Cyber Security for Control Systems Engineers and Operators
- OPSEC for Control Systems*

Instructor Led Courses

- Cyber Security Who Needs It?
- Control Systems Security for Managers
- Solutions for Process Control Security
- Introduction to Control Systems Security for the IT Professional
- Intermediate Control Systems Security
- Cyber Security Advanced Training and Workshop

Homeland Security

*IOSS first place award

Develop Partnerships – Academia

Curriculum Development

- Critical Infrastructure and Control System Security Curriculum:
  - Masters level course on policy & management.
  - Technical courses on control system security.

- Working with leading universities and organization to develop tools and material to influence future control systems engineering concepts.

Cyber Security is a Shared Responsibility

- Report cyber incidents & vulnerabilities at www.us-cert.gov, soc@us-cert.gov, 703-235-5110, or 888-282-0870
- Sign up for cyber alerts at www.us-cert.gov
- Learn more about CSSP at www.us-cert.gov/control_systems or email: cssp@dhs.gov

Contact information:

Seán P. McGurk

Director, Control Systems Security

National Cyber Security Division

Sean.McGurk@dhs.gov

Homeland Security

U.S. DEPARTMENT OF HOMELAND SECURITY

Homeland Security