control system vulnerabilities
> analysis of 5 years of field data

jonathan pollet, CISSP, CAP, PCIP

[on behalf of the DHS CSSP program - INL contract #240704]
outline

- background on the project
- review of ISA99 architecture model
- source for data used in the analysis
- interesting results
  - avg. # of days between vulnerability disclosure and discovery
  - where in the architecture are most vulns being discovered
  - does the type of vulnerabilities change throughout the architecture
  - workstation HMI vulnerabilities ranked by OS
  - network vs. host/application vulns throughout the architecture
  - interesting security findings on control system networks
- Q & A ...and video clip of new control system defense prototype
**project background**

- Over 38,000 control system vulnerabilities collected over 5 years from mid-2002 to 2008 [plantdata and industrial defender]

- Over 100 security assessments performed on critical infrastructure facilities such as electric power generation plants, transmission energy control centers, chemical plants, water plants, and oil/gas production, refining, and pipeline systems

- Vulnerability analysis and classification conducted under research project facilitated by INL and funded through the DHS Control Systems Security Program contract #240704

- ISA99 architecture model used to classify where the vulnerabilities were discovered in the systems
data source - what was collected?

- From mid-2002 to 2008, vulnerability data was stripped of any client information and the raw vulnerabilities were captured in a database
  - Vulnerability ID (auto-numbered from entry number 1)
  - Vulnerability Title (title for the vulnerability)
  - Security Zone or Location (location based on the ISA99 model where the vulnerability was located)
  - Disclosure Date (date when vulnerability was disclosed)
  - Discovery Date (date when vulnerability was discovered by the team and entered into the database)
  - Days Between Disclosure and Discovery (time between disclosure and detection)
  - Vulnerability Detailed Description
  - Vulnerability Suggested Remediation Steps
interesting results

- avg. # of days between vulnerability disclosure and discovery
  - all field data was exported from the database to an excel spreadsheet containing over 38,000 rows, and much of the analysis had to be performed manually
  - since we captured when the vulnerability was disclosed in the public, and also captured when the vulnerability was discovered and entered into the database, we were able to perform a simple diff against these two fields
  - vulnerabilities that were never disclosed in the public were thrown out of this particular exercise since negative or zero entries would throw off the calculations
  - the maximum number of days between when a vulnerability was disclosed in the public and when it was found during an assessment was over 3 years!
  - the average was 331 days, or close to 1 year. this means that on average most SCADA and process control environments contained latent vulnerabilities, probably with compiled exploits, and were not discovered until almost a year later, and would not have been discovered had not the asset owner funded the assessment.
where are the vulnerabilities being discovered?

Vulnerabilities by Location in Architecture

- Level 5 - Internet DMZ zone: 0.3%
- Level 4 - Enterprise LAN zone: 0.0%
- Level 3 - Operations DMZ: 16.9%
- Level 2 - Supervisory HMI LAN: 24.7%
- Level 1 - Controller LAN: 46.3%
- Level 0 - Instrumentations bus network: 11.8%
does the type of vulnerabilities change throughout the architecture?

- classified each vulnerability by the system that was impacted and where the vulnerability was found in the architecture

- The data set emerged a common set of system types at each network zone or segment:
  - Email Server Applications
  - Web Server Platforms (Apache and IIS)
  - Business Applications
  - Shopping Cart Applications
  - Applications written on PHP platform
  - Applications written on ASP or .NET platform
  - Database Servers (MS SQL, mySQL, and Oracle)
  - FTP Servers
  - Portal Servers (Blogs, Forums, etc...)
  - Workstation (client) vulnerabilities
systems impacted at the Internet DMZ zone

Internet DMZ Vulnerabilities

- Email Server Applications
- Web Server Platforms (Apache and IIS)
- Business Applications
- Shopping Chart Applications
- Applications written on PHP platform
- Applications written on ASP or .NET platform
- Database Servers (MS SQL, mySQL, and Oracle)
- FTP Servers
- Portal Servers (Blogs and Forums)
- Workstation (client) vulnerabilities
systems impacted at the Enterprise LAN zone

Enterprise LAN Vulnerabilities

- Email Server Applications
- Web Server Platforms (Apache and IIS)
- Business Applications
- Shopping Chart Applications
- Applications written on PHP platform
- Applications written on ASP or .NET platform
- Database Servers (MS SQL, mySQL, and Oracle)
- FTP Servers
- Portal Servers (Blogs and Forums)
- Workstation (client) vulnerabilities
systems impacted at the Operations DMZ zone

Operations DMZ Vulnerabilities

- Email Server Applications
- Web Server Platforms (Apache and IIS)
- Business Applications
- Shopping Chart Applications
- Applications written on PHP platform
- Applications written on ASP or .NET platform
- Database Servers (MS SQL, mySQL, and Oracle)
- FTP Servers
- Portal Servers (Blogs and Forums)
- Workstation (client) vulnerabilities
workstation HMI vulnerabilities ranked by OS

- Microsoft-based Operating System or Applications: 62.2%
- Red Hat Linux Operating System or Applications: 11.5%
- Tru64 Operating System or Applications: 4.4%
- HPUX Operating System or Applications: 2.4%
- IBM AIX Operating System or Applications: 8.3%
- FreeBSD Operating System or Applications: 6.7%
- SCO UNIX Operating System or Applications: 2.2%
- Sun Solaris Operating System or Applications: 0.9%
- SuSE Linux Operating System or Applications: 0.9%
only logged 105 controller LAN vulnerabilities, but QnX showed up as the most typical source
network vs. host/application vulns throughout the architecture
interesting security findings on control system networks

- VOIP (Voice over IP) Systems
- Network Video Recording Devices
- Network Surveillance Equipment and Software
- Adult Video Directory Scripts
- Online Dating Service Databases
- Advanced Forensics Format (AFF) archives
- Gaming Software Servers
  - aGSM - a freeware game server info monitoring utility
  - Alien Arena 2006 Gold Edition
  - Counter Strike
  - Brood Wars
  - Battlefield 1942 Server and Clients
  - Quake 2 and Quake 3 Game Servers found in Supervisor HMI LAN
  - Soldier of Fortune II
- Software license cracking executables (CD-key generators)
- Torrent client software on Supervisor HMI LAN
- Paging Software Server (i.e. Air Messenger Server connected to both the SCADA and Internet for SMTP relay out)
- America Online Clients
- MP3 Music and Video Playing Software including iTunes
- Streaming Music and Radio software with vulnerabilities
- BitTorrent Clients (for peer-to-peer file sharing)
- MSN and other IM chat clients
- Anonymous FTP Servers running waiting for connections
but wait...there’s more

- Apache Web Servers and Linux hosts un-patched for over 2 years
- APC Battery Backup UPS systems with vulnerable Web Interface
- Several web blog site engines running in control system DMZ
- Office grade Linksys, Belkin, and D-Link WiFi devices on Supervisory HMI LAN
- IM clients found installed and contained vulnerabilities on Supervisory HMI LAN
- Windows 95 found installed on hosts in Supervisory HMI LAN (no longer supported by MS)
- Windows NT found installed on hosts in Supervisory HMI LAN (no longer supported by MS)
- Windows Vista found used as OS for operator consoles in Supervisory HMI LAN
- IRC Chat Servers found installed on hosts in the Operational DMZ LAN
- Nintendo Entertainment System (NES) Game Simulator
- Netscape Browser vulnerabilities detected in Supervisor HMI LAN
- Multi-function Printer/Fax/Scanner device vulnerabilities
summary / take away points

- vulnerability classification is difficult, time consuming, and manual if the correct fields are not captured up front > is there benefit in a common format?

- 331 = the average time in days between when a vulnerability was disclosed in the public versus when it was discovered in an industrial control systems assessment

- the intermediate Operations DMZ network that sites between the Enterprise network and the industrial control systems had the most vulnerabilities attributed to its zone

- web server and back-end database vulnerability findings comprised the largest number of vulnerabilities found in these Operations DMZ network - we need more web app testing!

- network devices are better managed in the Internet DMZ and Enterprise LAN networks where the IT or IS department has clear ownership of managing the network devices

- number of client workstation vulnerabilities also increased deeper into the real-time operations networks, thus proving we still have a patch problem in our industry

- vulnerabilities with Windows operating systems or Windows applications also accounted for the overwhelming majority of vulnerabilities for systems in the Supervisory HMI LAN
new prototype for a control system
security defense system