

CSC

# Measuring the Security of Industrial Control Systems in the Age of Stuxnet



Doron Becker CISSP  
Associate Fellow, CSC

Ryan Dickover, PhD  
Deputy CIO for Information Assurance  
Naval Facilities Engineering Command  
25 October 2011



**The views expressed here are strictly the views of the authors and do not necessarily reflect the views of CSC, NAVFAC, the US Navy or DoD**

## Purpose and Goals

- Many experts counseled increased focus on physical, developmental and configuration management practices
- Very little said on measurement
  - “Establish standard certification metrics for ICS processes, systems, personnel and cyber security” – Joe Weiss (2008)
  - “Perform technical audits of SCADA devices and networks, and any other connected networks, to identify security concerns” – President’s CIP Board (2007)
- Suggest some security metrics that should be collected and analyzed for infrastructures containing industrial control systems
- Show how these metrics can fit into existing and future security standards
- Divide metrics into two categories
  - Standard measures associated with configuration management
  - Measures that reflect detailed knowledge of ICS elements and the software controlling them

## Stuxnet Changed the Rules of the Game

- National Security Preparedness Group Report on 10<sup>th</sup> Anniversary of 9/11

Another way that terrorists can attack without ever physically crossing our borders is through a cyber attack. Successive DNIs have warned that the cyber threat to critical infrastructure systems – to electrical, financial, water, energy, food supply, military, and telecommunications networks – is grave. **Earlier this month, senior DHS officials described a “nightmare scenario” of a terrorist group hacking into U.S. computer systems and disrupting our electric grid**, shutting down power to large swathes of the country, perhaps for a period as long as several weeks. As the current crisis in Japan demonstrates, disruption of power grids and basic infrastructure can have devastating effects on society.

- A Stuxnet-like attack could be accidental or intentional
- Be prepared to respond to attacks by Stuxnet offshoots or descendants

## Operating Systems Affected by Stuxnet

- Windows 95
- Windows Me
- Windows 98
- Windows 2000
- Windows Server 2003
- Windows XP
- Windows Vista

- Windows Vulnerabilities Exploited

- MS 10-046 (LNK)
- MS 08-067 (Server Service)
- MS 10-061 (Print Spooler)
- MS 10-073 (Keyboard Privilege Escalation)

Falliere, Murchu and Chen, W32.Stuxnet Dossier Version 1.4,  
[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)

## Proposed Metrics

- Number and Frequency of DLL Files Loaded by Infrastructure/SCADA Applications
- How Often is the Presence or Absence of Security Products Checked by an Application
- Control of autorun.inf
- Frequency of Accessing Critical Dates or Timestamps
- Frequency of Read, Write and Locate Commands
- Frequency of Registry Entries

- **Some of these metrics can be collected using currently available development tools**
- **Collecting these metrics during production can help make us proactive**

## Metric 1 – Number and Frequency of DLL Files Loaded by Infrastructure/SCADA Applications

- DLLs Hooked by Stuxnet to Exploit Windows LNK Vulnerability

Kernel32.dll	Ntdll.dll
FindFirstFilew	NtQueryDirectoryFile
FindNextFilew	ZwQueryDirectoryFile
FindFirstFileExW	

- Ntdll.dll Functions Used by Stuxnet

- ZwMapViewOfSection
- ZwCreateSection
- ZwOpenFile
- ZwCloseFile
- ZwQueryAttributesFile
- ZwQuerySection

• How often are these functions normally called?

• How often are they called during application execution?

• Expand to Specific DLLs

• Expand to Timestamps, Hash Values, File Sizes

## Metric 2 – How Often is Presence or Absence of a Security Product Checked by an Application

- Security Products Whose Presence or Absence Checked by Stuxnet

Vendor Name	Executable Name
Kaspersky	avp.exe
McAfee	mcsshield.exe
AntiVir	avguard.exe
BitDefender	bdagent.exe
Etrust	umxcfg.exe
F-Secure	fsdfwd.exe
Symantec	rtvscan.exe
Symantec Common Client	ccsvchst.exe
Eset NODew	ekrn.exe
Trend Pc-Cillin	tmproxy.exe

How often would a legitimate application perform this check?

## Metric 3 – Control of Autorun.INF

- Used to automatically start an application running on a removable drive
- Many organizations now disable it
- When parsing an Autorun file, characters that are not understood are skipped
- Therefore, if such files are executed, collect:
  - Number of skipped characters
  - Frequency of skipped characters
- Alert when found

**Stuxnet took advantage of skipped, unreadable characters**

## Metric 4 – Frequency of Accessing Critical Dates or Timestamps

- MS 08-067 (Server Service) exploited by Stuxnet whenever
  - Current date is before 1 January 2030, and
  - Certain antivirus products have definitions dated prior to 1 January 2009, and
  - Kernel32.dll and Netapi32.dll have timestamps later than 12 October 2008

- When does an application have “need to know” a timestamp or critical date?
- How frequently would a legitimate application access the timestamps of critical DLLs or antivirus executable files?



## Metric 6 – Frequency of Registry Entries

- When are registry entries normally created or modified?
  - When the application is installed
  - When the application is patched
  - When the underlying operating system or database is patched
- What Stuxnet did
  - Created mrxnet.sys and mrxcls.sys (driver files)
  - Created registry entries to ensure driver files automatically started whenever Windows OS started
  - Adjusted integrity levels of SetSecurityDescriptorDacl or SetSecurityDescriptorSacl (Windows XP vs. Windows Vista or later)

- **Registry Entries are Not Generally Modified During Execution**
- **Integrity Levels of Security Objects are Not Generally Modified During Execution**

# Measuring ICS in the Age of Stuxnet

**CSC**

## Mapping Metrics to Various Existing and Future Standards



# Federal Energy Regulatory Commission Standard CIP-007-1

## Standard Requirements

- R3.1 – Security Patch Management
- R4.1 – Anti-Virus and Malware Prevention
- R5.1 – Access Permissions and Need-to-Know
- R5.2 – Scope of Administrator Account Privileges
- R6.1 – Processes for Monitoring Security Events
- R6.2 – Automated or Manual Events when Incident Occurs
- R6.3 – Logs of Events to Support Incident Response

## Map Requirements to Metrics

Description	Requirement in FERC Standard CIP-007-4
Number and Frequency of DLL Files Loaded by Infrastructure/SCADA Applications	R4.1, R5.1, R5.2, R6.1, R6.2, R6.3
How Often is the Presence or Absence of Security Products Checked by an Application	R5.1, R5.2, R6.1, R6.2, R6.3
Control of autorun.inf	R3.1
Frequency of Accessing Critical Dates or Timestamps	R5.1, R5.2, R6.1, R6.2, R6.3
Frequency of Read, Write and Locate Commands	R5.1, R5.2, R6.1, R6.2, R6.3
Frequency of Registry Entries	R5.1, R5.2

# NIST Special Practice 800-55

## Performance Measurement Guide for Information Security

- Measure 3 – Access Control
  - Goal – Restrict information, system and component access to individuals and machines that are identifiable, known, credible and authorized
  - Measure – Percentage of remote access points used to gain unauthorized access
- Measure 5 – Audit and Accountability
  - Goal – Create, protect and retain audit records to enable monitoring, analysis, investigation and reporting of unlawful, unauthorized or inappropriate activity
  - Measure – Average frequency of audit records review and analysis for inappropriate activity

**All six metrics can trace into one or both of the NIST SP 800-55 metrics listed above**

## DHS Cross-Sector Roadmap for Cybersecurity of Control Systems

- Goal 1 – Measure and Assess Security Posture
  - Cyber Security Evaluation Tool?
  - Near-Term development of automated tools, risk assessments and standards
- Goal 3 – Detect Intrusion and Implement Response Strategies
  - Near-Term development of asset owner/operator/vendor partnerships to develop intrusion detection software for sector use

**All six metrics can support one or both of the above goals**

## Moving Forward

- Check if Existing Tools Can Collect Some of These Metrics Now
  - Monitoring Registry Changes – RegMon, WinExpose Registry, DeviceLock Active Registry Monitor
  - Some debugger tools might check calls to specific DLLs, executable modules or read/write commands
- Cost Considerations
  - Focus on systems having single point-of-failure and high mission value critical infrastructure

**We must become more knowledgeable about the internals of both our applications and their associated operating systems and databases and be ready to detect anomalies deep in the weeds and in almost real-time**

# Measuring the Security of ICS in the Age of Stuxnet

CSC

THANK YOU



Doron Becker  
[dbecker21@csc.com](mailto:dbecker21@csc.com)  
[doron.becker.ctr@navy.mil](mailto:doron.becker.ctr@navy.mil)  
202-548-4189/202-685-9392

Ryan Dickover  
[ryan.dickover@navy.mil](mailto:ryan.dickover@navy.mil)  
202-685-0480



BUSINESS SOLUTIONS  
TECHNOLOGY  
OUTSOURCING