What is Stuxnet?
The Stuxnet Worm

- **July, 2010:** Stuxnet worm was discovered attacking Siemens PCS7, S7 PLC and WIN-CC systems around the world
- Infected 100,000 computers
- Infected *at least* 22 manufacturing sites
- Appears to have impacted its possible target, Iran’s nuclear enrichment program
Great - We Weren’t the Target…

• Stuxnet infected a large US manufacturing plant
  • Started with two USB keys
  • Spread over the network to 100 WinCC HMIs communicating with about 60 OPs and about 45 S7 PLCs
  • Virus would modify project communication configuration for the PLC’s Ethernet ports

• Impact:
  • Major resource drain to disinfect project files
  • Plant continued to experience symptoms on PLCs one month later
How Stuxnet Spreads
Isn’t a Nuclear Materials System Air-Gapped?

• How could Stuxnet migrate from the Internet to an isolated industrial control system?
• Could the next worm do the same to a different victim?
A Trivial Scenario

• **Scenario:**
  1. Joe finds a USB flash drive in the parking lot and brings it into the control room
  2. Joe plugs it into the PLC programming station
  3. PLC programming station infects PLCs

• **Solution:**
  1. Ban all USB flash drives in the control room

NOT Realistic!
Gap Analysis Methodology

• **Goal:** Understanding the routes that a directed worm takes as it targets an ICS

• **Premise:** Start with an industrial site that exactly follows the security best practices defined in vendor documents

• **Model:** Map ways that Stuxnet could make its way through the defenses to cause physical damage
Core SIMATIC PCS 7 Control System Components

- Engineering System (ES) Client
- Operator System (OS) Client
- Automation System (AS) S7 PLC
PCS 7 High Security Architecture

Enterprise Control Network

Manufacturing Operations Network

Process Control Network

Control System Network

Perimeter Control Network

WinCC
PCS7
Historian
Remote Access
General Purpose

© Byres Security Inc.
PCS 7 High Security Architecture

Identical Firewalls Here

No Firewall Between CSN and PCN

WinCC  
PCS7  
Historian  
Remote Access  
Remote Access  
General Purpose
Stuxnet Phases

Penetration

Infection

Propagation

Detection Avoidance

Target Identification

Target Modification

Process Impact
Penetration (aka Handoff to Target Organization)

- Stuxnet handoffs were highly focused
- June 2009 to May 2010 10 infiltration events
- Handoffs were made to at least five separate target organizations
Penetration Possibilities

- Employee given infected USB flash drive
- Employee given infected project files from contractor
- Employee is transmitted email with “dropper”
- Employees laptop infected offsite

- Many possibilities for attackers
Core Propagation Methods

- Via Infected Removable Drives
  - USB flash drives
  - Portable hard disks
- Via Local Area Networks
  - Administrative and IPC Shares
  - Shared network drives
  - Print spooler services
  - SQL Connections
- Via infected Siemens project files
  - WinCC files
  - STEP 7 files

A very simplified view …
Penetrating Perimeter Network Firewalls

- Many paths through firewalls:
  - Network printer and file shares
  - WinCC SQL Server database
  - RPC between PCS 7 systems
- Piggybacked on core PCS 7 protocols, making it impossible to block at the firewall
Stuxnet Had Many Paths to its Victim PLCs

© Byres Security Inc.
Red highlights more direct paths which bypass existing security controls.

Green highlights infection path described in paper.
Some Lessons Learned

• A modern ICS or SCADA system is highly complex and interconnected
• Multiple potential pathways exist from the outside world to the process controllers
• Assuming an air-gap between ICS and corporate networks is unrealistic
• Focusing security efforts on a few obvious pathways (such as USB storage drives or the Enterprise/ICS firewall) is a flawed defense
The Death of
“Security by Obscurity”
A Typical Month for ICS/SCADA Vulnerabilities

• March 15 Moscow-based Gleg Ltd. released their Agora SCADA+ exploit pack for Canvas, which included 11 0-days (now at 54 exploits)
• On March 21, a security researcher from Italy “publically disclosed” 34 vulnerabilities on 4 different ICS platforms
• On March 22-23, vulnerabilities were disclosed for 2 additional ICS platforms
Control Systems Security Program (CSSP)

Control Systems Advisories and Reports Archive

- ICS-CERT has released an Alert titled "ICS-ALERT-11-256-01 - Multiple Vulnerabilities in Progea Movicon"
- ICS-CERT ALERT "ICS-ALERT-11-255-01 - SCADATEC SCADAPhone ModbusTagServer"
- ICS-CERT Advisory "ICSA-11-215-01 - Scadatec Limited Procyon Telnet Buffer Overflow"
- ICS-CERT Advisory "ICSA-11-244-01 - Siemens WinCC Flexible Runtime Heap Overflow"
- ICS-CERT Alert "ICS-ALERT-11-245-01 - Multiple ActiveX Vulnerabilities in Advantech BroadWin WebAccess"
- ICS-CERT updated Alert "ICS-ALERT-11-233-01A - Sunway ForceControl SCADA SEH"
- ICS-CERT Alert "ICS-ALERT-11-238-01 - Sunway ForceControl SCADA SEH"
- ICS-CERT Advisory "ICSA-11-173-01 - ClearSCADA Remote Authentication Bypass"
- ICS-CERT updated Advisory "ICSA-11-223-01A - (UPDATE) Siemens SIMATIC PLCs Reported Issues Summary"
- ICS-CERT Advisory "ICSA-11-231-01 - Inductive Automation Ignition Information Disclosure Vulnerability"
- ICS-CERT Newsletter, the "ICS-CERT Monthly Monitor"
- ICS-CERT ALERT "ICS-ALERT-11-230-01 - AGORA SCADA+ Update 1.4"
- ICS-CERT Advisory "ICSA-11-103-01A - (UPDATE) Honeywell ScanServer ActiveX Control"
- ICS-CERT Advisory "ICSA-11-223-01 - Siemens SIMATIC PLCs Reported Issues Summary"
- ICS-CERT UPDATE ALERT "ICS-ALERT-11-204-01B - (UPDATE) S7-300 Hardcoded Credentials"
- ICS-CERT ALERT "ICS-ALERT-11-204-01A - (UPDATE) S7-300 Hardcoded Credentials"
- ICS-CERT Announcement, "Cross-Vendor Working Group"
- ICS-CERT ALERT "ICS-ALERT-11-204-01 S7-300, S7-400 Hardcoded Credentials"
ICS-CERT Advisory "ICSA-11-195-01 - Invensys Wonderware Information Server"
ICS-CERT Advisory "ICSA-11-189-01 - 7-Technologies IGSS Remote Memory Corruption"
ICS-ALERT-11-186-01 "Password Protection Vulnerability in Siemens SIMATIC Controllers S7-200, S7-300, S7-400 and S7-1200"
ICS-CERT Advisory "ICSA-11-175-02 - Siemens WinCC Exploitable Crashes"
ICS-CERT Advisory "ICSA-11-182-01 - ICONICS TrustedZone Vulnerability"
ICS-CERT Advisory "ICSA-11-182-02 - ICONICS Login ActiveX Vulnerability"
ICS-CERT Advisory "ICSA-11-122-01 - AzeoTech DAQFactory Networking Vulnerabilities"
ICS-CERT updated Advisory "ICSA-11-168-01A - Indusoft ISSymbol ActiveX Control Buffer Overflows"
ICS-CERT Advisory "ICSA-11-175-01 - Rockwell FactoryTalk Diag Viewer Memory"
ICS-CERT Advisory "ICSA-11-168-01 - Indusoft ISSymbol ActiveX Control Buffer Overflows"
ICS-CERT Advisory "ICSA-11-167-01 - Heap overflow vulnerabilities in Sunway ForceControl and pNetPower"
ICS-CERT Newsletter, the "ICS-CERT Monthly Monitor"
ICS-CERT has released an updated Advisory "ICSA-11-056-01A - (UPDATE) Progea Movicon TCPUploadServer"
ICS-CERT Advisory "ICSA-11-161-01 Rockwell RSLinx Classic EDS Wizard buffer overflow"
ICS-CERT ALERT "ICSA-ALERT-11-161-01 Siemens S7-1200 PLC"
ICS-CERT Updated Advisory "ICSA-11-069-01B - (UPDATE) Samsung Data Management Server"
ICS-CERT Advisory "ICSA-11-132-01A - (UPDATE) 7-Technologies IGSS DoS"
ICS-CERT updated Advisory "ICSA-11-147-01B - (UPDATE) Ecava IntegraXor DLL Hijacking"
ICS-CERT Advisory "ICSA-11-147-02 - Ecava IntegraXor X55"
ICS-CERT report "Common Cybersecurity Vulnerabilities in Industrial Control Systems"
ICS-CERT newsletter, the "ICS-CERT Monthly Monitor"
ICS-CERT Advisory "ICSA-11-132-01 - 7-Technologies IGSS DoS"
ICS-CERT Advisory "ICSA-11-147-01A - Ecava IntegraXor DLL Hijacking"
ICS-CERT Advisory "ICSA-11-131-01-ICONICS GENESIS32 and BizViz ActiveX Stack Overflow"
ICS-CERT Alert "ICS-ALERT-11-131-01 - Advantech Studio ISSymbol ActiveX Control Buffer Overflow Vulnerabilities"
ICS-CERT Alert "ICSA-ALERT-11-129-01 - Samsung Data Management Server Root Access"
ICS-CERT Update Advisory "ICSA-11-069-01A - (UPDATED) Samsung Data Management Server"
ICS-CERT Advisory "ICSA-11-125-01 - 7-Technologies IGSS Stack Overflows and Directory Traversal"
OSAMA BIN LADEN – THEMED PHISHING ATTEMPTS
ICSA-11-119-01 - 7-Technologies IGSS Remote Stack Overflow
ICS-CERT Alert "ICSA-ALERT-11-111-01 - Agora Plus Update 1.1"
ICS-CERT Advisory "ICSA-11-110-01 - RealFlex RealWin Multiple Vulnerabilities"
ICS-CERT Advisory "ICSA-11-108-01 - ICONICS GENESIS Multiple Vulnerabilities"
ICS-CERT Advisory "ICSA-11-103-01 - Honeywell ScanServer ActiveX Control"
ICS-CERT Advisory "ICSA-11-094-01 - Wonderware InBatch Client ActiveX Buffer Overflow"
"NCCIC Advisory Targeted Phishing Attacks"
ICS-CERT newsletter "ICS-CERT Monthly Monitor"
Advisory "ICSA-11-096-01 - Agora SCADA+"
Advisory Update "ICSA-11-091-01A - [UPDATE]" Multiple Vulnerabilities in Siemens Tecnomatix FactoryLink
Advisory "ICSA-11-094-02 - Broadcom (Advantech) WebAccess RPC"
Advisory "ICSA-11-051-01 - Multiple Vulnerabilities in Siemens Tecnomatix FactoryLink"
"US-CERT EWIN 11-077-01A - Malicious Indicators Update"
Advisory "ICSA-11-084-01 - Solar Magnetic Storm Control Systems Impact"
Advisory "ICS-Advisory -11-082-01 - Ecava IntegraXor Unauthenticated SQL vulnerability"
Alert "ICS-ALERT-11-081-01 - BroadWin WebAccess"
ICS-CERT Alert "ICSA-ALERT-11-080-01 - Multiple Vulnerabilities in Siemens Tecnomatix FactoryLink"
ICS-CERT Alert "ICSA-ALERT-11-080-02 - Multiple Vulnerabilities in Iconics Genesis"
ICS-CERT Alert "ICSA-ALERT-11-080-03 - Multiple Vulnerabilities in 7-Technologies IGSS"
ICS-CERT Alert "ICSA-ALERT-11-080-04 - Multiple Vulnerabilities in RealFlex ReaWin"
Advisory "ICSA-11-056-01 - Progea Movicon TCPUploadServer"
Advisory "ICSA-11-074-01 - WellinTech KingView 6.53 KVWebSrv ActiveX"
Alert "ICSA-ALERT-11-066-01 - ActiveX Vulnerability in WellinTech KingView 6.53"
UPDATED Advisory "ICSA-10-248-01A - Wonderware InBatch Buffer Overflow"
UPDATED Advisory "ICSA-10-314-01A - Multiple Vulnerabilities in ClearSCADA Software"
UPDATED Advisory "ICSA-11-041-01A - McAfee Night Dragon"
Advisory "ICSA-11-041-01 - McAfee Night Dragon"
Advisory "ICSA-11-018-02 - IGSS 8 ODBC Server Remote Heap Corruption"
Report "ICS-CERT 2010 Year in Review"
Advisory "ICSA-10-314-01 - Multiple Vulnerabilities in ClearSCADA Software"
ICSA-11-025-01 - Federal Aviation Administration OPS Testing
Alert ICS-ALERT-11-024-01 - Federal Aviation Administration GPS Advisories
Advisory ICSA-11-018-01 - AGO SCADA Viewer OPC Buffer Overflow Vulnerability
Advisory ICSA-10-322-02A - Automated Solutions OPC Server
Advisory ICSA-11-017-01 - WellinTech KingView
Advisory ICSA-11-017-02 - Sielco Sistemi Winlog Stack Overflow
Alert ICS-Alert-11-011-01 WellinTech KingView Buffer Overflow
Advisory ICS-CERT 10-337-01 - Advantech Studio Test Web Server Buffer Overflow
Alert ICS-CERT ALERT-10-302-01 - Ecava IntegraXor
- Advisory ICS-CERT 10-362-01 - Ecava IntegraXor Directory Traversal
- Advisory ICS-CERT 10-355-01 - Ecava IntegraXor
- Advisory ICS-CERT has released Update A to ICSA-10-316-01A - Intellicom Netbiter WebSCADA Multiple Vulnerabilities
- Advisory ICSA-10-322-01 - Ecava IntegraXor Buffer Overflow
- Advisory ICSA-10-348-01 - Wonderware InBACnet and I/A Series BACnet Buffer Overflow
- Advisory ICSA-10-322-02 - Automated Solutions OPC Server Vulnerability
- Advisory ICSA-10-316-01 - Intellicom Netbiter WebSCADA Multiple Vulnerabilities
- Advisory ICSA-10-301-01A - MOXA Device Manager Buffer Overflow
- Advisory ICSA-10-313-01 - RealWin Buffer Overflow
- Alert ICS-Alert-10-305-01 - RealWin Buffer Overflows
- Advisory ICSA-10-301-01 - Moxa Device Manager Buffer Overflow
- Alert ICS-Alert-10-301-01 - Control System Internet Accessibility
- Alert ICS-Alert-10-293-02 - Vulnerability in Moxa Device Manager
- Alert ICS-Alert-10-293-01 - Multiple vulnerabilities in intellicom’s Netbiter® WebSCADA
- ICSA-10-272-01 - Primary Stuxnet Indicators
- ICSA-10-264-01 - Scada Engine BACnet OPC Client Buffer Overflow Vulnerability
- Alert ICS-Alert-10-260-01 - Scada Engine BACnet OPC Client Buffer Overflow Vulnerability
- Alert ICS-Alert-10-239-01 - Dynamic Library Loading Vulnerability in Microsoft-Based Applications
- ICSA-10-238-01B - Stuxnet Malware Mitigation
- ICSA-10-238-01A - Stuxnet Malware Mitigation
- ICSA-10-238-01 - Stuxnet Malware Mitigation
- ICSA-10-228-01 - Vendor Admin Accounts Warning
- ICSA-10-214-01 - Vxworks Vulnerabilities
- Alert ICS-Alert-10-211-01 - Microsoft Announces Out-of-Band Update
- ICSA-10-201-01C - USB Malware Targeting Siemens Control Software
- ICSA-10-201-01B - USB Malware Targeting Siemens Control Software
- ICSA-10-201-01A - USB Malware Targeting Siemens Control Software
- ICSA-10-201-01 - USB Malware Targeting Siemens Control Software
- Alert ICS-ALERT-10-194-01 - Open UDP Port in Rockwell 1756-ENBT Interface
- ICSA-10-147-01 - Cisco Network Building Mediator
- ICS-CERT Advisory ICSA-10-090-01 Mariposa Botnet
- ICS-CERT Advisory ICSA-10-070-02-Rockwell-PLC5
- ICS-CERT Advisory ICSA-10-070-01A-RSlinx-UPDATE
- ICS-CERT Advisory ICSA-10-070-01-RSLinx
The Life Cycle of a ICS Exploit

• ICS platforms are becoming an obvious target for attacks
• “Security Researchers” focusing on SCADA/ICS because it is easy money/fame (little malicious intent)
• Actors with intent have access to the weapons:
  • Download exploits for free (Italian list)
  • Purchase tool kits (Gleg)
  • Directed where to look for more vulnerabilities
Incident Types from RISI Database

- **Internal**
  - Intentional: 20%
  - Unintentional: 80%

- **External**
  - Hacker: 53%
  - IT Dept, Technician: 14%
  - Malware: 38%
  - N/A: 0%

- **Unintentional**
  - Insider: 6%
  - Outsider: 47%
  - N/A: 48%
Stuxnet’s Legacy

• Model for simple, destructive SCADA worms
• Exploits inherent PLC design issues
• Applicable to almost all industrial controllers
• There are no possible “patches” to the PLC
Some Lessons Learned

- SCADA and ICS are now targets of interest
- Most systems have many exploit opportunities
- Patching is an issue for many companies
  - Patch deployment requires plant downtime
  - Vendor only patches most current version
  - Patch releases are slow
  - Upgrading to latest version may not be an option
Protecting Against the Son-of-Stuxnet

- The Good and The Ugly
- Models for Effective CIP Security
The Ugly: The US Electrical Industry Security Model

- NERC CIP 002 - 009 defines security compliance requirements for organizations who are involved with the bulk electrical network in North America
- Industry has focused on **compliance** rather than **security**
- The standard focus on **boundary protection**, not **defense in depth**.
- Yet in 2009 NERC listed their #2 vulnerability in control systems as:
  
  "Inadequately designed control system networks that lack sufficient defense-in-depth mechanisms"
The Bastion Model of Security

• Installing a single firewall between business and the control system is known as the **Bastion Model** since it depends on a single point of security

• Other examples of the bastion model:
  • The Great Wall of China
  • The Maginot Line
A Perimeter Defense is Not Enough

- We can’t just install a boundary firewall and forget about security
  - The bad guys will eventually get in
  - Many problems originate inside the control network
- We must harden the ENTIRE system
- We need Defense in Depth

*Crunchy on the Outside - Soft in the Middle*
ANSI/ISA-99: Dividing Up The Control System

• A core concept in the ANSI/ISA-99 (now IEC 62443.02.01) security standard is “Zones and Conduits”
• Offers a level of segmentation and traffic control inside the control system.
• Control networks divided into layers or zones based on control function
• Multiple separated zones manage that “defense in depth” strategy
Using Zones: An Example Oil Refinery
Specifying the Zones
Defining the Conduits
Protecting the Conduits with Firewalls

Corporate Firewall
Industrial Firewall
Look At All Possible Pathways

• Don’t focus on a single pathway such as USB keys
• Consider all possible infection pathways:
  • Removable Media (CDs, DVDs, USB Drives)
  • File Transfer (Database, PDFs, PLC Project Files)
  • Portable Equipment (Laptops, Storage Units, Config Tools)
  • Internal Network Connections (Business, Lab, QA, Support)
  • External Connections (Support, Contractor, Customer)
  • Wireless (802.11, 802.15, Licensed-band, Cellular, Wireless HART, ISA-100a, Bluetooth, USB tethering)
  • Other Interfaces (Serial, Data Highways)
• Have strategies for discovering/mitigating ALL pathways
The Attack/Consequence Funnel

- External Corporate
- Internal Enterprise Assets
- Process DMZ
- HMI/Supervisory Systems
- Primary Control Systems
- Safety Systems
- Process

Attack Quantity ➔ Available Pathways ➔ Consequences ➔ Exploit Opportunities

© Byres Security Inc.
Securing Last-line-of-Defense CIP Systems

- Focus on monitoring and securing SIS Boundary
  - Limited Pathways
  - High Consequence
SCADA/ICS-Appropriate Technologies

• Need ICS-appropriate detection technologies to raise an alarm when equipment is compromised or at risk of compromise
• Deploy ICS-appropriate security technologies
• Look beyond traditional network layer firewalls, towards firewalls that are capable of deep packet inspection of key SCADA and ICS protocols
Example:
Honeywell Safety System Firewall

- Honeywell needed a firewall to protect critical their safety instrumented systems (SIS)
- Wanted NO user configuration
- Security Requirements:
  - Allow data to be read from system but not written (Read-only Firewall)
  - Must provide “sanity check” SCADA application protocols
- Configuration is locked to SIS- appropriate rule set

Honeywell Modbus Read-only Firewall for SIS
Making Security Simple

• "Certainly controls engineers and operators need to be security aware, but they should not all need to be security experts."

• "We have to make this [security] something a plant superintendent, engineer, or senior operator can do in their spare time, or it will flop."

  Two Major End Users to ISA99 Committee
Some Closing Thoughts…

- Stuxnet has changed the threat landscape
- ICS/SCADA is the target of sophisticated attacks
- ICS/SCADA is the focus for vulnerability discovery
- Industry must accept that the complete prevention of ICS infection is impossible
- Improved defense-in-depth strategies for industrial control systems are needed urgently
- Waiting for the next worm may be too late
References

Siemens Automation
• Security concept PCS 7 and WinCC - Basic document

Tofino Security White Papers and Application Notes
• http://www.tofinosecurity.com/stuxnet-central
• Analysis of the Siemens PCS7 “Stuxnet” Malware for Industrial Control System Professionals:
  http://www.tofinosecurity.com/professional/siemens-pcs7-wincc-malware
• Using Tofino to Control the Spread of the Stuxnet Malware - Application Note:
  http://www.tofinosecurity.com/professional/using-tofino-control-stuxnet
• Stuxnet Mitigation Matrix - Application Note:
  http://www.tofinosecurity.com/professional/stuxnet-mitigation-matrix

Other White Papers and Documents
• http://www.langner.com/en/