Attacking critical infrastructures

Behind the scenes

Maarten Oosterink
maarten.oosterink@capgemini.com
m00st on Twitter
Allow me to introduce myself

Maarten Oosterink
IT security consultant at Capgemini
Expert / advisor at CPNI.NL (cybersecurity and process control security)
maarten.oosterink@capgemini.com or @m00st

Raised alongside computers, started using them in the pre-PC era and used modems when autodial was a feature. Exploring the boundaries of technology ever since..

2000: IT manager at Vuurwerk Internet (largest Dutch hosting provider at the time)
2001: BOFH and later interception specialist at Netherlands Forensic Institute
2005: Consultant at Capgemini
2008: Process Control Security at oil major
Now: Expert / Advisor for Dutch Centre for Protection of National Infrastructure
How does all this work?

PROCESS CONTROL INTRODUCTION
Teh interwebs

Typical office network

Factory network

Local unit network

In the field network
How does this work?

- Programmable Logic Controllers communicate with sensors, actuators via discrete channels or specific networks (Profibus, Fieldbus, WirelessHART)
- PLCs communicate with Human Machine Interface (HMI) and DCS servers for providing status and control
- Servers ‘control’ a complex process interfacing with one or more PLCs and interface (in)directly with IT systems (e.g. ERP, SAP, optimisation tools)
- Interface between IT systems and process control mostly via historian (Pi, PHD, Wonderware)
- Safety Integrity Systems operate separate from the control systems, with fixed boundaries. Engineered to bring process to a safe state (Fukishima)
What does it do?
What does it do?
What does it do?
What does it do?
What’s the situation

TIME FOR A QUIZ..
So what’s the situation?

System lifecycle is:

A. 25 years
B. 10 years
C. 5 years
D. All of the above
So what’s the situation?

We use Windows systems because:

A. They are cheap
B. They have open standards
C. We know them from home
D. All of the above
So what’s the situation?

Our systems run:

A. Windows 2000 workstation
B. Windows XP
C. Windows Vista Home Premium
D. All of the above
So what’s the situation?

Systems are patched:

A. During install, FAT, SAT and commissioning
B. Following plant maintenance cycles (every 1, 2 or 4 years)
C. Every 2nd Tuesday of the month
D. Never
So what’s the situation?

Applications are patched:

A. As soon as vendor notification is received
B. Following plant maintenance cycles (every 1, 2 or 4 years)
C. Never
D. When the sales guy calls about upgrades
So what’s the situation?

IT Systems are maintained by:
A. The IT department
B. Your local engineer/operator
C. The vendor
D. None of the above
The process control landscape

(UN)COMMON TECHNOLOGY
(Un)common mitigations

Hardening
- Limit physical access
- Application whitelisting
- No CD-Rom drive
- Only essential OS parts
- Choose correct PC model

Awareness
- Security training
- Purdue model
- Staging (Citrix)

Patching
- MBSA tool
- Microsoft WSUS
- Vendor maintenance contracts
- Follow local permit to work system

Malware Protection
- Anti-virus
- Host based firewall / IDS
- Disable USB ports

Network Architecture
- Intrusion Detection System
- Two-factor authentication
- Security Operations Centre
- Firewalls
- Network segregation
- Application aware firewalls
- Limit physical access
- Centralised security team
- SIEM
- Application aware firewalls

Incident Detection & Response
- Staging (Citrix)
- Microsoft WSUS
- Vendor maintenance contracts
- Follow local permit to work system
- Centralised security team
- SIEM
- Two-factor authentication
Peeling the layers

DISMANTLING STUXNET
Stuxnet’s journey to success

Infection
- Removable media (first Autorun, later .LNK vulnerability MS10-046, only infects three systems, stops after June 23rd 2012)
- Driver signed with stolen certificates (Jmicron: June 18th 2009 and Realtek: July 16th 2010)
- Command & Control functionality via HTTP (checks connectivity and dumps system info: multiple NICs)

Propagation
- Fileshares (enumerates current and system users, abuses WMI, uses task scheduler)
- Printspooler (MS10-061, RPC) and Server Service/SMB vulnerability (MS08-067, Conficker!)
- Two 0-days for privilege elevation: Keyboard layout: MS10-073 and Task Scheduler: MS10-092
- WinCC (.MCP) and Step7 project files (S7P) and fixed password for WinCC SQL database
- RPC service for peer-to-peer updates

Payload
- The Step7 system that programs the PLCs (Siemens 315-2 and $17 models) ONLY when certain code blocks exist and uses rootkit like functionality to keep the operators and engineers blind
- One set of code to manipulate the safeguarding system (the 417 PLC)
- Two sets of code for manipulating specific Profibus devices (Vacon or Fararo Paya VFDs) in specific configurations (the 315-2 PLCs)

Generic malware attack
Tailor-made solutions
State-of-the-art engineering
Day 0

Internet
Corporate Network
Datacenter
Engineer's Office PC
DMZ
Process Control Network
Citrix server
Control Bus

Control Bus #1

Controller
Foundation Fieldbus
Flowmeter
Temperature transmitter
Positioner

Controller
HART

Controller
Profibus

DCS server (database)

Operator Station
HMI

L3 switch/router
Firewall
OPC server
Webserver

Engineering Workstation

DCS server (database)

Historian server e.g. Wonderware, OsiSoft PI, Honeywell PHD

Control Bus #2

Controller

DCS server (database)

WinCC

Engineering Workstation

Level 5

Level 4

Level 3

Level 2

Level 1

Uranium enrichment centrifuge (IR-2)
Infection
Propagation

Level 5

Level 4

Level 3

Level 2

Level 1

Uranium enrichment centrifuge (IR-2)
Stuxnet Conclusions

The Good

• 4x 0-day for relevant systems (Windows XP and Vista)

• Designed for industrial environment: USB and S7P propagation to jump air-gap and RPC to jump L3 to L2

• Code is better than the code being abused

The Bad

• Initial hand-off got out of hand (AtomStroyExport)

• Did the four star general really want all this attention?
This presentation was about attacking critical infrastructure?

**ATTACK VECTORS**
Attack vectors

Human Factor

- Night shifts and remote locations
- Computers like home
- Cold and noisy auxiliary rooms
- Poor IT skills
- Third party engineers / vendor maintenance
Attack vectors

Procedural

• Low patch frequency
• Manual patching
• Backups on removable drives
• Company IT policy doesn’t fit
Attack vectors

Technological

• 90s networking (design and technology)
• Badly configured and maintained firewalls, ACLs
• IDS maturity (signatures), no security monitoring
• Control bus (Level 2) uses custom high-availability protocols. ‘Not so robust’ Windows driver implementation
  • Yokogawa Vnet/IP
  • Honeywell FTE
  • Invensys Nodebus
• OSI layers 5 to 7 (as researchers get better access)
Are you done?

WRAP UP
Take-aways

Pretty common technology (together with some ancient stuff)

The industry has a hard time taking on the other chores than come with modern IT

Attacks move up the OSI stack, but proprietary network protocols are of interest..