Stuxnet: Dawn of a new era

...about the hype & consequences of Stuxnet

Dr. Stefan Lüders (CERN Computer Security Officer)
ICALEPCS2011
Grenoble (France), October 11th 2011
Disclaimer:
This presentation is based on info from (trusted) third parties. Nobody who was involved ever commented on this.
Natanz, we have a problem.
Microsoft is investigating reports of a Trojan spreading through USB devices, malware appears to be targeting the use of industrial control systems.

IDG News Service - Siemens confirmed Tuesday that one of its customers has been hit by a new worm designed to steal secrets from industrial control systems.

To date, the company has been notified of one attack, on a German manufacturer that Siemens declined to identify. “We were informed by one of our system integrators, who developed a project for a customer in process industries,” said Siemens Industry spokesman Wieland Simon in an e-mail message. The company is trying to determine whether the attack caused damage, he said.

The worm, called Stuxnet, was first spotted last month, when it infected systems at an unidentified Iranian organization, according to Sergey Ulasen, the head of the antivirus kernel department at VirusBlokAda, in Minsk, Belarus. The unidentified victim, which does not own the type of SCADA (supervisory control and data acquisition) systems targeted by the worm, “told us their workstations serially rebooted without any reason,” Ulasen said in an e-mail message Tuesday.
“Stuxnet: Dawn of a new era” — Dr. Stefan Lüders — ICALEPCS2011 — October 11th 2011

Natanz, we have a problem.
Natanz, we have a problem.

"Stuxnet: Dawn of a new era" — Dr. Stefan Lüders — ICALEPCS2011 — October 11th 2011

Microsoft Investigating Windows Security Zero-Day Targeted by Trojan

Siemens: German customer hit by industrial worm

Stuxnet Virus Opens New Era of Cyber War

The Mossad, Israel’s foreign intelligence agency, attacked the Iranian nuclear program with a highly sophisticated computer virus called Stuxnet. The first digital weapon of geopolitical importance, it could change the way wars are fought — and it will not be the last attack of its kind.
Natanz, we have a problem.

"Stuxnet: Dawn of a new era" — Dr. Stefan Lüders — ICALEPCS2011 — October 11th 2011

Microsoft Investigating Windows Security Zero-Day Targeted by Trojan

Siemens: German customer hit by industrial worm

Stuxnet Virus Opens New Era of Cyber War

Cyberwar

The meaning of Stuxnet

A sophisticated "cyber-missile" highlights the potential—and limitations—of cyberwar
The Workings of Stuxnet (I)

“Stuxnet: Dawn of a new era” — Dr. Stefan Lüders — ICALEPCS2011 — October 11th 2011

Siemens STEP7 (Windows XP)

Siemens 315-2 & 417 CPU

Gas centrifuges for uranium enrichment

Rotational speed

monitor
configure
test

control
An infected USB stick was infiltrated into the plant either by malicious act or through social engineering.

Once inserted into a Windows PC, the stick tried to compromise the O/S with up to 4(!) zero-day exploits (worth >$100k).

There were 4-5 evolutions starting 6/2009.

Infected 100,000 PCs (60% Iran, 10% Indonesia).

Using “rootkit” technologies and two stolen certificates, it hid from being detected.

It tried to infect other hosts and establish a P2P connection “home”.

Gas centrifuges for uranium enrichment
An infected USB stick was infiltrated into the plant either by malicious act or through social engineering.

Once inserted into a Windows PC, the stick tried to compromise the O/S with up to 4(!) zero-day exploits (worth >$100k).

There were 4-5 evolutions starting 6/2009.

Infected 100.000 PCs (60% Iran, 10% Indonesia).

Using “rootkit” technologies and two stolen certificates, it hid from being detected.

It tried to infect other hosts and establish a P2P connection “home”.

So far, nothing new: A standard, but expensive virus!
Stuxnet then checked the local configuration looking for the presence of Siemens PCS7/STEP7/WINCC SCADA software.

If so, it copied itself into the local STEP7 project folder (to propagate further).

It replaced the S7 communication libraries (DLLs) used for exchanging data with a PLC.

Stuxnet can now manipulate values to be send to the PLC or displayed by the SCADA.

If not, Stuxnet got idle and would expire on 2012/06/24.

Stuxnet is now the “Man in the Middle” controlling the communication between SCADA & PLC.
Next, Stuxnet was “fingerprinting” connected PLCs.
If right PLC configuration, it downloaded/replaced code between 17 and 32 FBs & DBs.
The Workings of Stuxnet (III)

Next, Stuxnet was “fingerprinting” connected PLCs.

If right PLC configuration, it downloaded/replaced code between 17 and 32 FBs & DBs.

This code varied the rotational speed of the centrifuges over months wearing them out and inhibiting uranium enrichment.

The “Man in the Middle” made everything looked fine at the SCADA level...
Next, Stuxnet was “fingerprinting” connected PLCs. If right PLC configuration, it downloaded/replaced code between 17 and 32 FBs & DBs. This code varied the rotational speed of the centrifuges over months wearing them out and inhibiting uranium enrichment.

The “Man in the Middle” made everything looked fine at the SCADA level…
 Déjà vu?

Controls under Attack!

- 20 devices from 6 different manufacturers (35 tests in total)
- All devices fully configured but running idle

Crashed
32%

Passed
68%

Crashed
21%

Failed
18%

Passed
61%

...PLCs under load seem to fail even more frequently !!!
...results improve with more recent firmware versions 😊
In January 1982, President Ronald Reagan approved a CIA plan to sabotage the economy of the Soviet Union through covert transfers of technology that contained hidden malfunctions, including software that later triggered a huge explosion in a Siberian natural gas pipeline, according to a new memoir by a Reagan White House official.
Protective Measures (I)

- Deploy a **Defense-in-Depth** protection
- Establish security cells on your network
- **Forbid usage of USB keys** or use Epoxy 😊; restrict usage of CDs, open shares & DFS
- Teach your experts about “Social Engineering”
- **Screen your experts:** alcohol/drugs, financial, psychological/social/family, ...
- Patch, patch, patch…
  ...and **run up-to-date antivirus software** (wouldn’t have helped here 😞)
Deploy a **Defense-in-Depth** protection

Establish security cells on your network

- **Forbid usage of USB keys** or use Epoxy 😊; restrict usage of CDs, open shares & DFS

- **Teach your experts about “Social Engineering”**

- **Screen your experts: alcohol/drugs, financial, psychological/social/family, ...**

- **Patch, patch, patch...**
  - ...and run up-to-date antivirus software
  - (wouldn’t have helped here 😞)

**Apply Defense-in-Depth!!!**

...and follow a standard.
Protective Measures (II)

► Scan you PLCs on vulnerabilities & robustness

► Lock down the PLC configuration:
  Enable firewall, disable unneeded services

► Enable PLC intrusion detection

Talk to your vendor!
Accept the residual risk.
(My personal) Conclusions

Stuxnet was the wake-up call... but for whom 😞?

- Attackers and researchers are now poking around control system security
- The media is creating a hype and call out the “Era of Cyber-War”
- Security companies enter in the belief knowing control systems well

Vendors are now open to act and users to demand 😊

- Note: this was not against Siemens, they just happened to be involved

Control System Cyber-Security is now / must now be taken seriously. Defense-in-Depth is the key!!!

Choose a standard and follow it. Get all stakeholders involved: controls experts, IT/security experts, vendors.
Merci beaucoup!!!

“Stuxnet: Dawn of a new era” — Dr. Stefan Lüders — ICALEPCS2011 — October 11th 2011

Protect your computers

Any unprotected computer connected to the Internet is likely to be infected within minutes!

Be careful with e-mail & Web

Cybercriminals are trying to trick you!