The Stuxnet Worm

Babak Yadegari and Paul Mueller

CSc 566: Computer Security

April 25, 2012

Presentation Outline

- Background & Overview
- Stuxnet's Purpose
- How Stuxnet Spread
- Possible Attack Scenarios
- Infection
- RPC Server
- Attack
- Methods of Concealment
- Effects & Conclusion

What is Stuxnet?

- A sophisticated worm designed to target only specific Siemens SCADA systems
- Uses four zero-day vulnerabilities
- Uses two stolen digital signatures
- Uses rootkits on Windows and the PLCs it targeted
- Discovered in June 2010, but an early version first appeared a year earlier
- Widely suspected of targeting Iran's uranium enrichment program
- Was somewhat effective: may have destroyed 1,000 centrifuges, reduced output, sowed chaos
- The US and Israel were likely behind it

Tensions Between Iran and the West

- Iran started its nuclear program in the 1950s
- Iran's revolution delayed the program
- A few years later, the new leaders continued it
- In 2002, it turned out that Iran had developed two undeclared nuclear facilities
- Iran suspended uranium enrichment in 2003 and resumed it in 2006
- Iran: no nuclear weapons
- IAEA: Iran does not comply with safeguard agreements

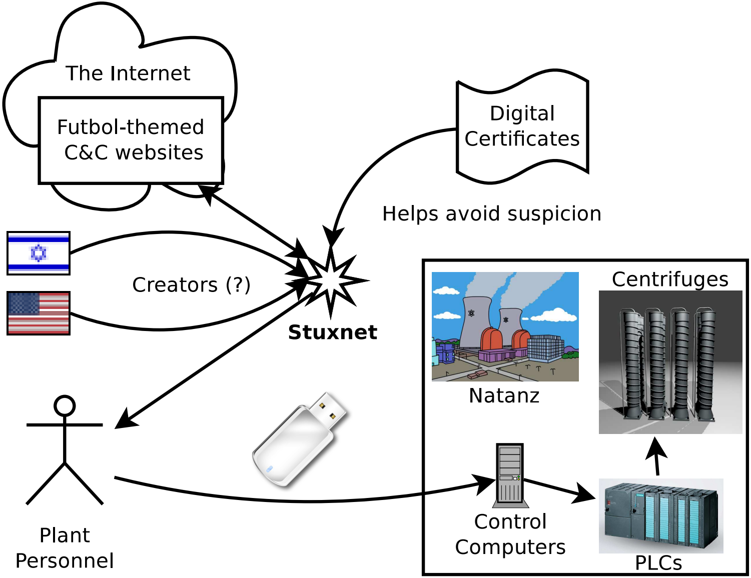
Obligatory Nuclear Bomb Explosion Photo

Figure: What's at stake. (Photo: sciencecabin.com)

Who Created Stuxnet?

- Israel
  - Israel expects they have 3 years before Iran completes a nuclear weapon
  - Has confirmed that it will use cyberwarfare to defend itself
  - Israeli officials smiled when asked if Israel had created the attack
- United States
  - American officials said the attack was not created in the US
  - Leaked cable stating that the US ambassador to Germany was told a Stuxnet-type attack could be more effective than a military attack
  - Prior to Stuxnet being discovered, John Bumgarner wrote about a possible way of using malicious code to destroy centrifuges; Stuxnet happened soon after!

Overview


The Internet
Futbol-themed C&C websites
Digital Certificates
Helps avoid suspicion
Creators (?)
Stuxnet
Centrifuges
Natanz
Plant Personnel
Control Computers
PLCs

Siemens PLC

Figure: A Siemens SIMATIC S7-300 PLC, the type of PLC Stuxnet targeted (Photo: alibaba.com)

What was Stuxnet's Purpose?

- Disrupt Iran's nuclear bomb program
- Provide plausible deniability to its creator(s).

It only attacks plants with certain (Natanz-like) configurations:

- Only certain centrifuge cascade setups will be attacked
- Centrifuge rotor frequencies- Sequence A gives the nominal frequency of its target centrifuges as 1064 Hz, which is reportedly exactly the IR-1's nominal frequency
- Likewise, the maximum speed Stuxnet speeds the rotors up to (1,410 Hz) is at the maximum range the IR-1 rotors can withstand- spinning them at this speed will likely destroy them
- Looks for Finnish and Iranian centrifuges

Infection Statistics by Country

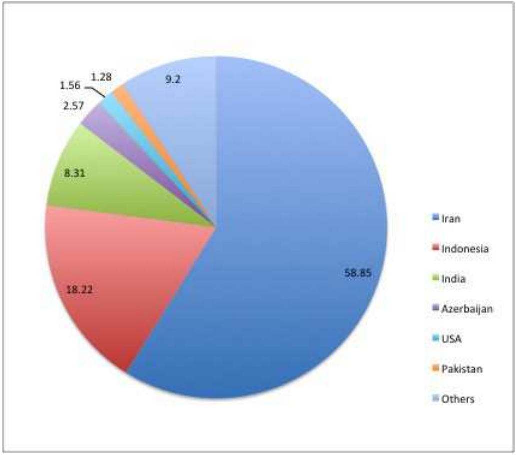


Figure: Percentage of Infected Hosts by Country

Cascade Configuration Revealed

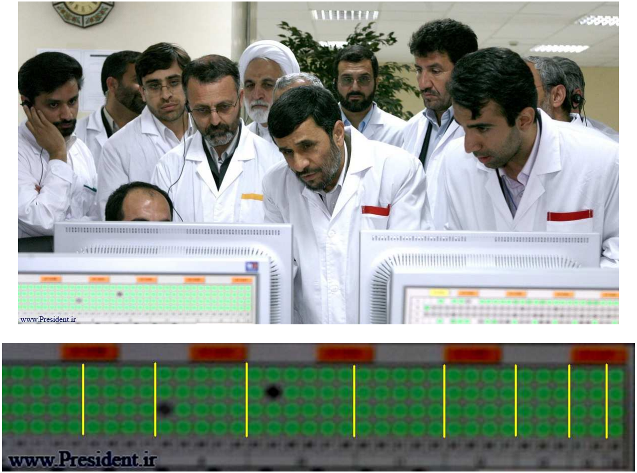
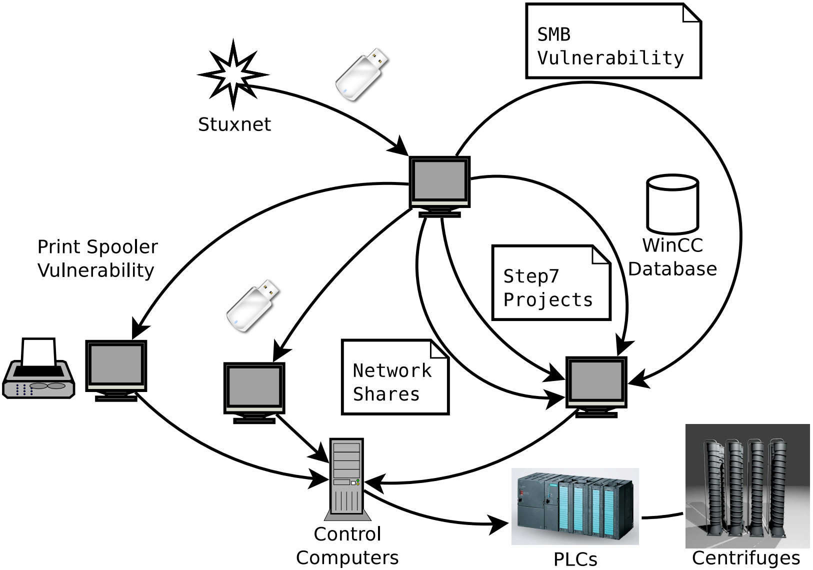


Figure: Iran's president revealed the cascade structure at Natanz: from right to left- 4, 8, 12, 16, 20, 24, 20, 16. (Photo: Office of the Presidency of the Islamic Republic of Iran)

How Stuxnet Spread



Windows Print Spooler Vulnerability

- Monitors print requests
- `http://www.youtube.com/watch?v=ExgMb5WbCrE`

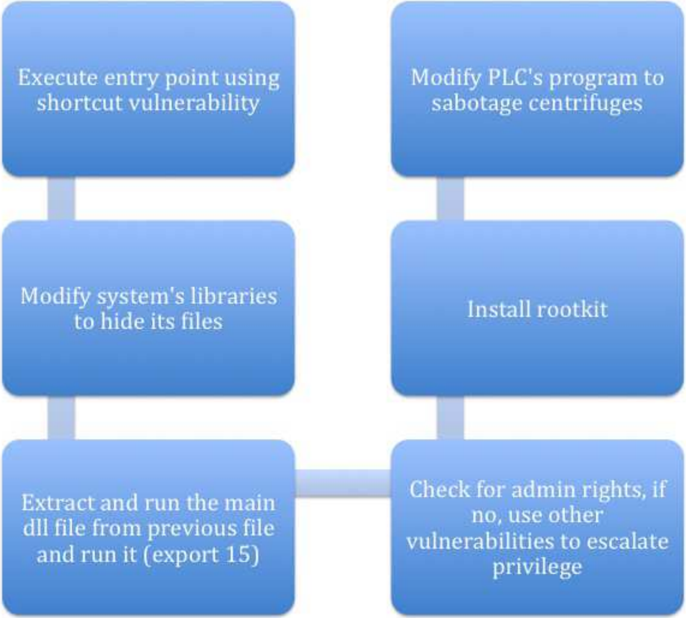
Windows Server Service Vulnerability (SMB)

- The service handles RPC calls between Windows machines
- This vulnerability can be exploited by creating specially crafted packets
- A buffer overflow occurs when the receiving side tries to process the request
- It allows arbitrary code execution on the remote machine

Possible Attack Scenarios

- Attackers should know about the design of the target system
  - Might be stolen by an insider
  - Collected by a previous malware and delivered to attackers
- Same story for the digital certificates
- Malware should somehow be delivered to the target's environment
  - Again by an insider
  - By infecting a third party contractor
  - Or delivered by email

Stuxnet Flow Graph



Execute entry point using shortcut vulnerability

Modify system's libraries to hide its files

Extract and run the main dll file from previous file and run it (export 15)

Check for admin rights, if no, use other vulnerabilities to escalate privilege

Install rootkit

Modify PLC's program to sabotage centrifuges

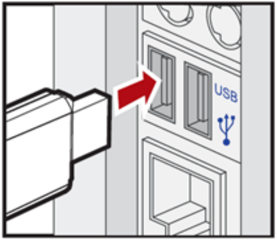
Windows Shortcut Vulnerability

- http://www.youtube.com/watch?v=eFLNG5zHaVA

Initial Stage I

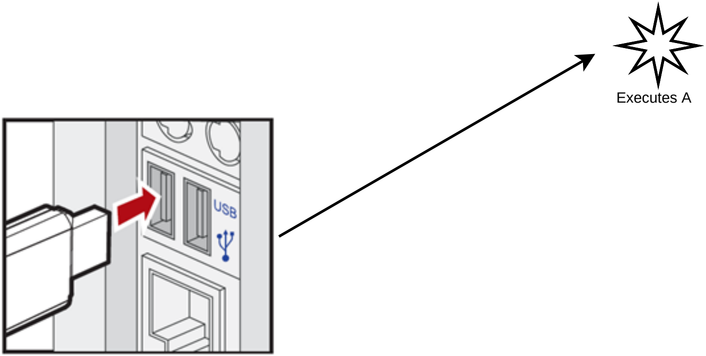
- The malware first loads and runs WTR4411.TMP file from USB stick, exploiting Windows shortcut vulnerability
- Crafted shortcut points to WTR4411.TMP file which leads the file to be loaded and executed!
- Extracts another file (WTR4132.TMP) from previously loaded file and passes control to it

Initial Stage II



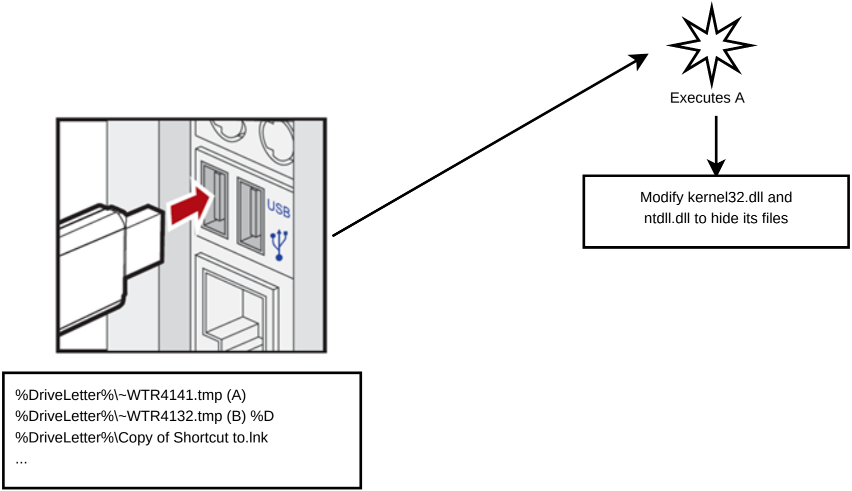
%DriveLetter%\~WTR4141.tmp (A)
%DriveLetter%\~WTR4132.tmp (B) %D
%DriveLetter%\Copy of Shortcut to.lnk
...

Initial Stage II



```
%DriveLetter%\~WTR4141.tmp (A)
%DriveLetter%\~WTR4132.tmp (B) %D
%DriveLetter%\Copy of Shortcut to.lnk
...
```

Initial Stage II

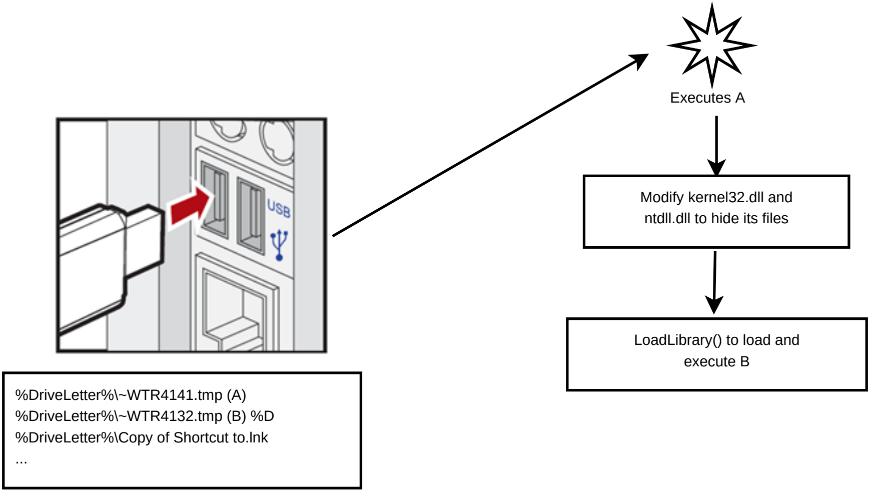


Executes A

Modify kernel32.dll and ntdll.dll to hide its files

%DriveLetter%\~WTR4141.tmp (A)
%DriveLetter%\~WTR4132.tmp (B) %D
%DriveLetter%\Copy of Shortcut to.lnk
...

Initial Stage II



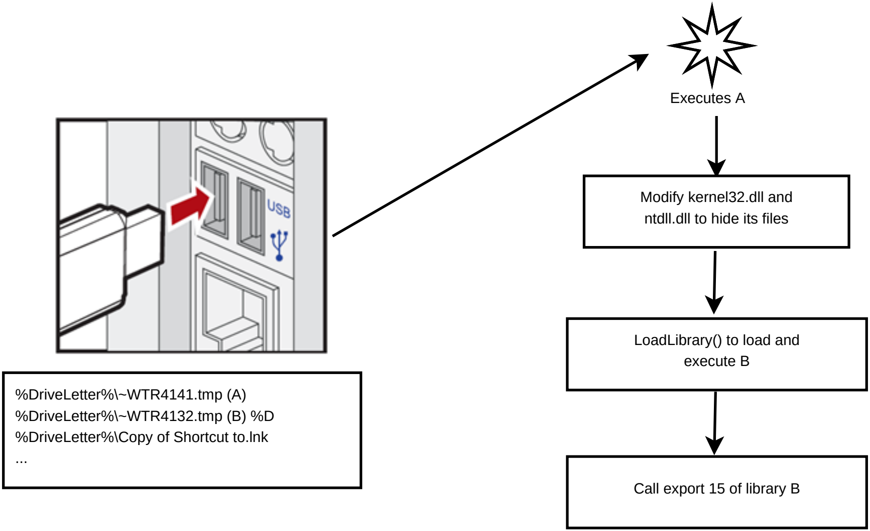
%DriveLetter%\~WTR4141.tmp (A)
%DriveLetter%\~WTR4132.tmp (B) %D
%DriveLetter%\Copy of Shortcut to.lnk
...

Executes A

Modify kernel32.dll and ntdll.dll to hide its files

LoadLibrary() to load and execute B

Initial Stage II



%DriveLetter%\~WTR4141.tmp (A)
%DriveLetter%\~WTR4132.tmp (B) %D
%DriveLetter%\Copy of Shortcut to.lnk
...

Executes A

Modify kernel32.dll and ntdll.dll to hide its files

LoadLibrary() to load and execute B

Call export 15 of library B

Attack I

After finding an appropriate target:

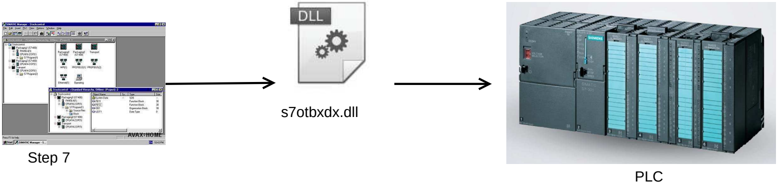
- Replaces s7otbxdx.dll library used to communicate between PLC and Step7 software
- Injects malicious code into PLC
- Runs periodic attacks against centrifuge by changing its rotor speed
- Sabotages the centrifuge!

Attack II

After finding an appropriate target:

- `http://www.youtube.com/watch?v=cf0jlzVCyOI#t=83s`

Taking Control of PLCs



Step 7

s7otbxdx.dll

PLC

Figure: The Step7 software uses a library to communicate with its PLCs

Taking Control of PLCs

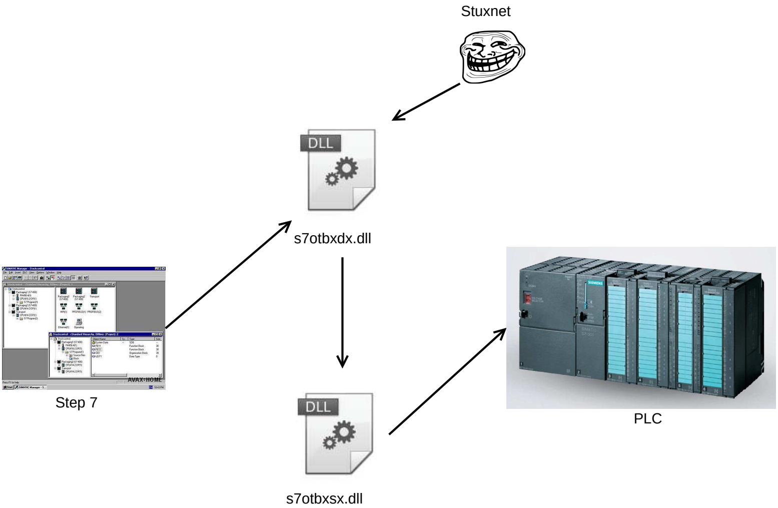


Figure: Stuxnet wraps the library used to communicate with the PLCs

Taking Control of PLCs

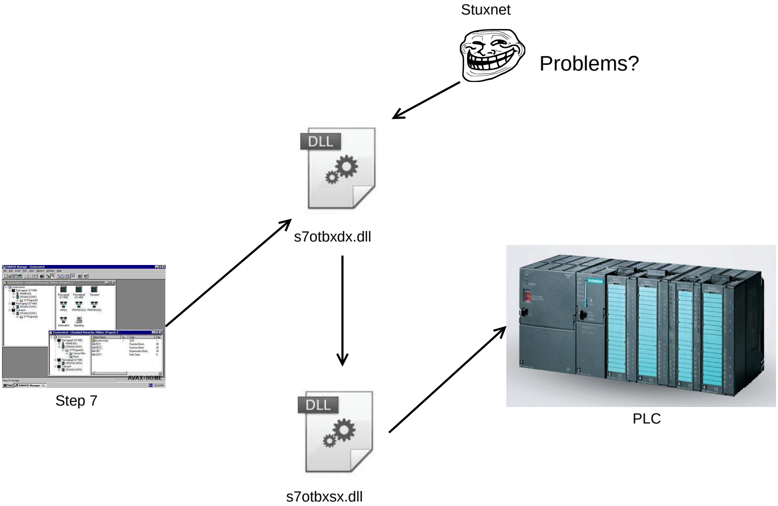


Figure: Stuxnet wraps the library used to communicate with the PLCs

Attack Sequences

Stuxnet contains three attack sequences, named A, B, and C by Symantec. A and B are very similar, and do basically the same thing. C is more sophisticated but unfinished; it contains debug code, has missing sections, etc.

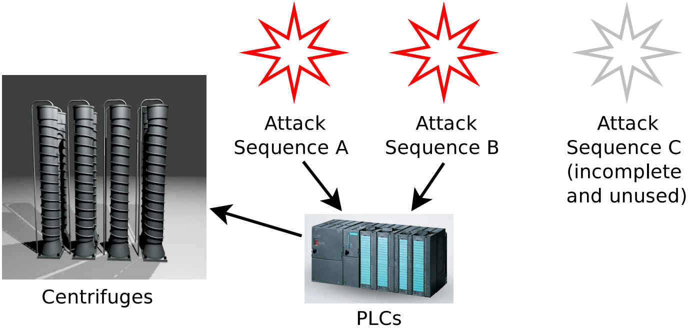


Figure: Stuxnet's attack sequences.

Centrifuges are Neat!

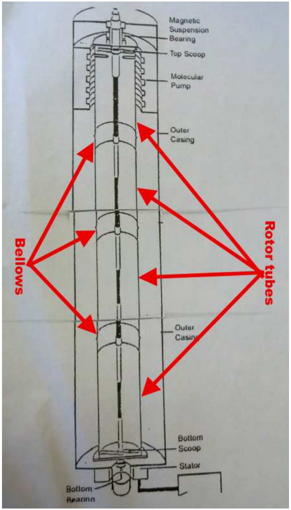


Figure: Diagram of a P-1 centrifuge. The Natanz centrifuges are based on the P-1. (Diagram: Institute for Science and International Security)

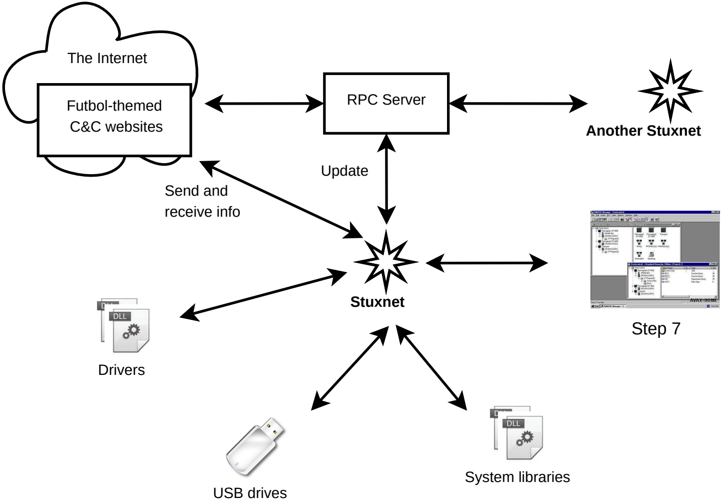
Centrifuges are Neat! (Part II)

Figure: Iran's president tours centrifuges at Natanz. (Photo: Office of the Presidency of the Islamic Republic of Iran)

Components I

- User-Mode
  - Choose a process and inject the code
  - Check to see if running on an appropriate platform (Windows XP, Vista, ...)
  - Privilege escalation
  - Checking for updates
- Kernel-Mode
  - `Mrxcls.sys`: A startup driver which allows Stuxnet to survive rebooting
  - `Mrxnet.sys`: Acts as a rootkit, intercepts requests to system device objects

Components II



The Internet

Futbol-themed C&C websites

RPC Server

Another Stuxnet

Update

Send and receive info

Stuxnet

Step 7

Drivers

USB drives

System libraries

Figure: Stuxnet Components

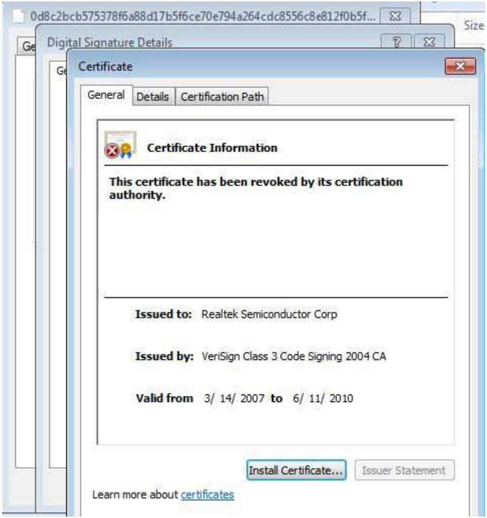
Stuxnet's Very Own RPC Server

- Has its own RPC server to communicate with and get updates from C&C servers
- Communicates with other instances over the network and gets updates from them
- Makes it possible to be updated even if there is no direct access to the Internet

Methods of Concealment

- Uses signed drivers with digital certificates stolen from two Taiwanese companies, Realtek and JMicron
- Uses Windows and PLC rootkits to avoid detection. These make it difficult to find the files it places on USB drives for propagation, and on the PLCs to do the actual attacks, respectively
- The attack sequences try to prevent plant operators from learning of the changes in rotor speed by commanding the controllers to disable their safeties and warnings, and by reporting recorded, nominal data

Stolen Digital Certificates



Certificate Information

This certificate has been revoked by its certification authority.

Issued to: Realtek Semiconductor Corp

Issued by: VeriSign Class 3 Code Signing 2004 CA

Valid from 3/ 14/ 2007 **to** 6/ 11/ 2010

Learn more about certificates

Figure: The stolen Realtek signature

Effects of Stuxnet (Intended)

Mostly, to destroy centrifuges.

- Attack sequences A and B speed the centrifuges' rotational speed up toward 1,410 Hz for 15 minutes; then, 27 days later, it slows them down for 50 minutes, during which time their speed may be reduced by as much as 200 Hz. Another 27 days later, the sequence repeats.
- The high speed is enough to probably destroy the centrifuges, and the low speed would result in inefficient processing of uranium, thereby wasting resources and slowing LEU production.

Effects of Stuxnet (Intended) (Continued)

- Unnerve the Iranians- Stuxnet's creators may also have hoped to slow Iran's nuclear program by creating doubt and confusion
- In fact, the Iranians halted uranium processing on a significant number of centrifuges
- The creators of Stuxnet probably thought Stuxnet wouldn't be uncovered as quickly as it was. If it hadn't been, the damage it did would have been greater.
- This is supported by the slow pace of the attacks- waiting 27 days between attacks, possibly to be more stealthy

Effects of Stuxnet (Unintended)

Stuxnet also had unintended effects.

- Infected 100,000 computers around the world (as of Sept 29, 2010), including in the US
- Probably didn't do any serious damage outside Iran's nuclear program, though, since Stuxnet was so highly targeted
- Others may use Stuxnet's code as a base to attack SCADA or other systems in the US, Israel, or their friendly countries
- Stuxnet set a precedent for attacking industrial systems, even nuclear ones

Conclusion

- Stuxnet was very sophisticated- probably created by Israel and/or the US
- It delayed Iran's nuclear weapons program, but wasn't a decisive blow
- Iran appears to have cleaned their systems of Stuxnet
- Israel may attack Iran- this would probably have lots of bad consequences
- Stuxnet may result in malicious entities being more likely to attack industrial systems in the future
- On the other hand, industry officials and security professionals are now more aware of the vulnerability of such systems

Sources (Part I)

- http://en.wikipedia.org/wiki/Simatic_S5_PLC/
- http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf
- go.eset.com/us/resources/white-papers/Stuxnet_Under_the_Microscope.pdf
- http://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf
- http://isis-online.org/uploads/isis-reports/documents/stuxnet_update_15Feb2011.pdf
- http://www.langner.com/en/2011/12/07/the-prez-shows-his-cascade-shape/
- http://www.langner.com/en/blog/
- http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/all/1

Sources (Part II)

- http://www.csmonitor.com/USA/2012/0106/Stuxnet-cyberweapon-looks-to-be-one-on-a-production-line-researchers-say
- http://blogs.technet.com/b/markrussinovich/archive/2011/03/30/3416253.aspx
- http://www.symantec.com/connect/w32_duqu_precursor_next_stuxnet
- http://www.reuters.com/article/2012/02/14/us-iran-usa-stuxnet-idUSTRE81D24Q20120214
- http://www.nti.org/country-profiles/iran/nuclear/
- http://en.wikipedia.org/wiki/Stuxnet
- http://www.telegraph.co.uk/technology/news/8326274/Israeli-security-chief-celebrates-Stuxnet-cyber-attack.html

Credits for Images Used in the Figures

- The US and Israel flag images come from the game Freeciv, and are licensed under the GPL (version 2).
- The nuclear power plant image is from The Simpsons, via http://images.wikia.com/simpsons/images/9/90/Snpp-1-.gif. (And yes, we know Natanz isn't actually a nuclear power plant).
- The PLC image is from alibaba.com
- The USB flash drive image is from psdgraphics.com
- The centrifuge image is from http://www.turbosquid.com/3d-models/blender-nuclear-centrifuge/663104