STUXNET AND THE IMPACT ON ACCELERATOR CONTROL SYSTEMS

S. Lüders, CERN, Geneva, Switzerland

Abstract

2010 has seen wide news coverage of a new kind of computer attack, named "Stuxnet", targeting control systems. Due to its level of sophistication, it is widely acknowledged that this attack marks the very first case of a cyber-war of one country against the industrial infrastructure of another, although there is still much speculation about the details. Worse yet, experts recognize that Stuxnet might just be the beginning and that similar attacks, eventually with much less sophistication, but with much more collateral damage, can be expected in the years to come. Stuxnet was targeting a special model of the Siemens 400 PLC series. Similar modules are also deployed for accelerator controls like the LHC cryogenics or vacuum systems as well as the detector control systems in LHC experiments. Therefore, the aim of this presentation is to give an insight into what this new attack does and why it is deemed to be special. In particular, the potential impact on accelerator and experiment control systems will be discussed, and means will be presented on how to properly protect against similar attacks.

DAWN OF A NEW ERA

In June 2010, repeated reports of a major wave of infected Windows PCs in Iran hit the news. Initially triggered by a report of a Belarus security company called VirusBlokAda on a new Windows zero-day exploit*, a deeper analysis by Symantec, another security company, revealed that this exploit targeted specifically the SCADA (Supervisory Control And Data Acquisition) systems manufactured by Siemens.

Such SCADA systems have been deployed in thousands of instances worldwide, e.g. in the car manufacturing industry, in facility management, oil & gas industries as well as for accelerator control systems. However, in this particular instance, it seemed that this exploit targets the control system of the nuclear facility of Natanz in Iran. This plant is used for the enrichment of uranium. For Siemens, it was an unfortunate coincidence, that their systems were used there.

Named "Stuxnet", as derived from some keywords buried in the exploit code, this is the first documented exploit which deliberately attacks control systems. Due to its level of sophistication, there was much speculation whether this is a case of cyber-war of a particular country against the industrial infrastructure of another, namely the U.S. and Israel against the Natanz nuclear facilities in Iran [1]. Indeed, the sophistication of Stuxnet is very impressive, and this level of sophistication and complexity makes it most unlikely that Stuxnet was produced by an average attacker, but instead required significant investments, engineering skills and intelligence gathering. However, due to the nature of the attack, it is impossible to obtain confirmed information.

The media quickly labelled Stuxnet as "a new kind of cyber-attack" [2], but it was not. In the 1980's, the U.S. CIA provided a Russian energy provider with manipulated valves which eventually led to the explosion of a Siberian natural gas pipeline [3]. Also, the inherent weaknesses exploited by Stuxnet have been reported before, like the CERN TOCSSiC tests conducted in 2005 and later which found 39% of 35 tested devices being susceptible to malicious packages [4] and that many of these devices lack basic access protection allowing them to be manipulated and/or stopped easily. It took five more years for an ultimate proof.

THE INNER WORKINGS

The Stuxnet attack proceeds in two steps: in a first step Stuxnet infects random Windows PCs, in a second it attacks the controls process. A general overview of the different phases is given in Figure 1.

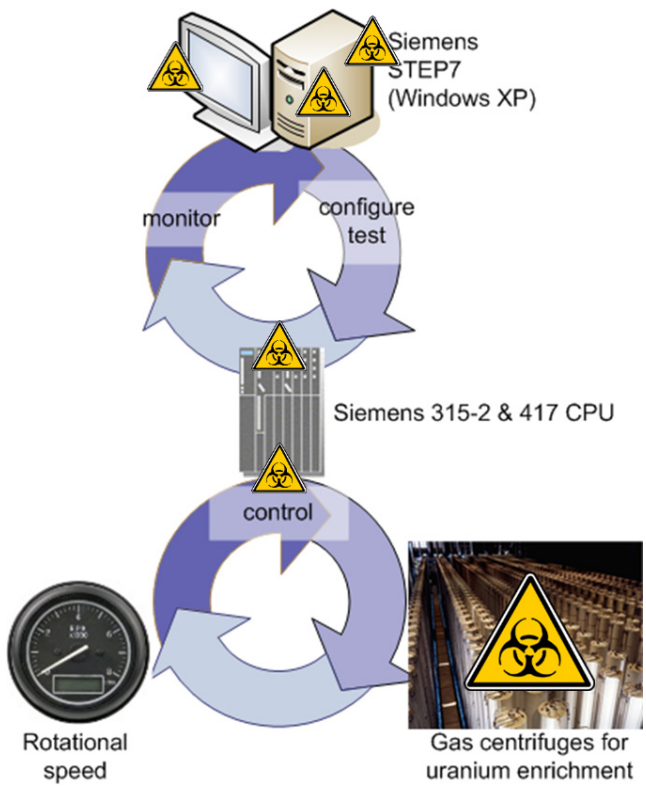

Figure 1: Sketch of a possible control system. Components which were attacked and compromised by Stuxet have been marked explicitly.

* A "zero-day exploit" is an exploit targeting a currently unknown vulnerability. Hence, no fix or patch exists.

Phase 1: Infect a SCADA PC

The PC attack was taking advantage of four (4!) initially unknown vulnerabilities in the Windows operating system. These vulnerabilities are quite valuable since they might be traded on the black market for more than $100 000 each [5]. Most likely, Stuxnet has been introduced via an infected USB stick by either a malicious insider, a saboteur or by means of social engineering luring an employee to insert the stick into a PC.

Once having successfully infiltrated the PC, Stuxnet hides itself using so-called root-kit functionality. This functionality takes benefits of two certificates stolen by the adversaries from a Taiwanese company. This gave the root-kit the air of legitimacy. This makes it neither visible to any local user who browses the infected program folders nor to any local anti-virus software. It then scans the local network and tries to infect further hosts. Using peer-to-peer functionality, all nodes are kept up-to-date and in contact with two remote command and control servers, one in Denmark, the second in Malaysia.

So far, Stuxnet behaves like a sophisticated and expensive worm harvesting compromised PCs and waiting for a command to unleash its malicious power. Up to five different versions with different functionalities have been identified, the oldest dating back to June 2009. In the end, Stuxnet has infected approximately 100.000 PCs worldwide (60% in Iran, 18% in Indonesia, 5% in India) [6].

Phase 2: Compromize the Control Process

But Stuxnet is special. Once established on a PC, it checks for the presence of the Siemens "STEP7", "WINCC" or "PCS7" software suites [7][8][9]. The STEP7 software is essential to program the control system in so-called programmable logic controllers or PLCs. The control system software consists of a series of software "blocks", e.g. "Function Blocks" (FB/FC), "Operational Blocks" (OB), or "Data Blocks" (DB) which are combined into a "project". WINCC and PCS7 are two types of Siemens SCADA applications displaying information relayed from the PLC and allowing values to be changed interactively in the PLC.

If one of these software suites is present, Stuxnet plants a copy of itself into any STEP7 project which can be found on the PC. This will open a further vector of propagation, should the project is copied and transferred to another PC by the corresponding system expert.

In addition, Stuxnet replaces the so-called S7 communication libraries (DLLs) such that it can fully control any data exchange between the SCADA PC and the PLC (see Figure 2). It acts now as a "Man-in-the-Middle" which can hide certain information from the operator looking at the SCADA display like out-of-bound values or alarms, and inhibit commands issued by an operator to the PLC.

Next, Stuxnet scans for PLCs which are reachable from that SCADA PC and "fingerprints" those PLCs: The PLC hardware must be of a certain type of hardware module and the software must contain a number of user-defined blocks with a certain byte-pattern and length. If the fingerprint does not match certain criteria, the worm stays idle and would expire on June 24th 2012.

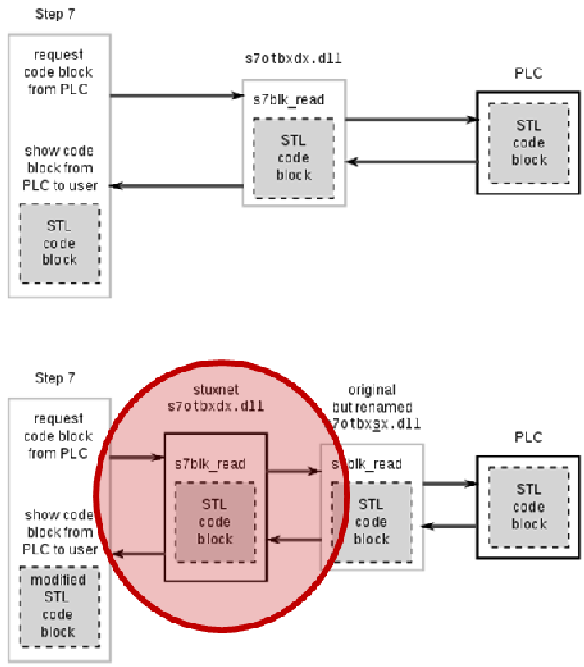

Figure 2: The Siemens S7 communication before (above) and after (below) Stuxnet has inserted its malicious libraries [10].

Phase 3: Game Over

Finally, if the control process matches what Stuxnet is looking for, Stuxnet downloads 17 to 32 additional software blocks to the PLC (depending on the PLC type). This new software blocks change the local control process such that, over the course of several months, the rotational speed of the gas centrifuges deviate from their nominal 1400Hz up to 1410Hz or down to a few hundred hertz [10]. Due to this, the uranium enrichment process was hampered, and the centrifuges wear out more quickly.

Due to the "Man-in-the-Middle" controlling the data flow from and to the SCADA system, operators in front of their SCADA displays will not have noticed anything. Thus, the production of highly enriched uranium became spoiled, and hence delayed.

PROTECTIVE MEANS

Stuxnet is targeting only one particular control system allegedly located in Iran. Therefore, given the aforementioned fingerprinting, it is very unlikely that accelerator or experiment control processes match these patterns. But in the course of the attack, Stuxnet also infects Windows (SCADA) PCs, which are employed in accelerator or experiment control processes, too.

However, not being affected *this* time should not imply that taking no action is an option. On the contrary, Stuxnet

should be considered as a wake-up call to raise the barriers, if not done yet, and deploy measures for properly protecting controls systems.

Protecting a Siemens PLC

While not broadly discussed in the media nor explicitly publicized by Siemens, their PLC come with two basic protection means: a local firewall and an intrusion detection system.

Sophisticated Siemens PLCs, as well as PLCs from other manufacturers, too, come with rudimentary firewall functionality based on IP access protection lists. For proper protection, only IP addresses of remote devices (PLCs, PCs) with a need to communicate with that particular PLC should be permitted by this firewall. All other connections should be dropped[†].

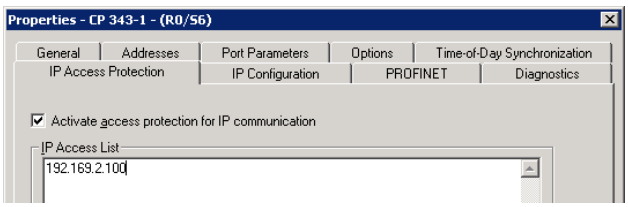

Figure 3: Configuration window of a Siemens S7-343 communication processor. The "IP Access Protection" tab allows configuring a local firewall based on IP addresses.

Special to Siemens STEP7 software is the provisioning of a so-called "Checksums" functionality which can be used as a simple intrusion detection system. Checksums are quasi-unique numbers ("hashes") which change drastically once a bit of the PLC's software blocks or its hardware is modified[‡]: STEP7 allows calculating such a hash over all software blocks, i.e. FB/FC/SFB/SFC/DB/OB, of a STEP7 project. A second hash is calculated over the hardware configuration. These values can be compared to those computed directly on-line by the PLC's CPU (see Figure 4).

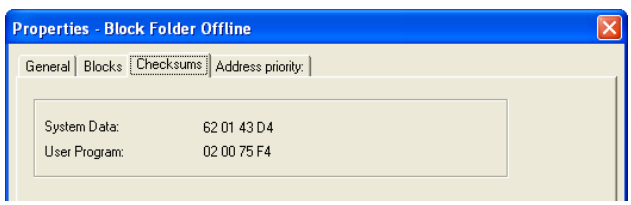

Figure 4: Information box giving the checksum values of a STEP7 project.

Mismatches indicate that software blocks in the PLC or its hardware has been altered. In such cases, the PLC or an attached display can raise an alarm (alarm e-mail, alarm sound, warning message). Important is, however, that the display can and is not compromised through a "Man-in-the-Middle" attack as the SCADA PC was[§].

Defence-in-Depth

The general strategy for the protection of control systems (as for any other computer system) must follow a "Defence-in-Depth" approach. This implies that protective measures have to be deployed on every level of the hardware and software stack[**]:

- On the network level by proper network segregation and compartmentalization of the controls network into security cells;
- On the hardware level by increasing the robustness and resilience of the device itself. Physical outlets like USB ports or CD drives should be disabled if not essential for operation;
- On the level of network services by disabling those services which are not essential for operation. A device should not be susceptible nor fail to a simple network scan issued by e.g. Nessus [11] or nmap [12];
- On the firmware and operating system level by applying software upgrades and patches in a timely manner. If possible, the device should run anti-virus software with up-to-date virus signature files. All default passwords must be changed and not disclosed to any other third party;
- On the application level by removing all applications which are no essential for operation. All remaining applications must be kept up-to-date and patched in a timely manner;
- On the social level by providing appropriate training to the system experts and operators. Particular focus should be put on awareness raising and the risks of social engineering[††].

More details on any "Defence-in-Depth" approach can be found in the "Good Practise Guidelines" of the U.K. CPNI [13] or in the ISA SP99 series of documents [14]. Other good standards are [15][16][17][18]. Usually, it is sufficient to choose any one standard or guideline and cross check later with a second one.

For example, long before Stuxnet, CERN set up a working group on the protection of control systems [19]. Since then, all control systems at CERN must adhere to the "Computer and Network Infrastructure for Controls (CNIC) Security Policy for Controls" [20] and to the

[†] However, since the Stuxnet comprimized PC was directly linked to the PLC, a local firewall wouldn't have prevented Stuxnet from connecting to that PLC.

[‡] Since this checksum is only four bytes long, there is a residual risk for finding collisions, i.e. the same checksums for a completely different set of software blocks or hardware configuration. However, to the author's knowledge, Stuxnet has not been designed to produce such a collision.

[§] There is still the risk of a "race-condition" where the malicious block downloaded to a PLC competes with the regular execution of the calculation of checksums. Depending on the exact time the malicious block gets enabled on the PLC, it might be able to inhibit raising an checksum alert.

[**] Admittedly, not all those measures would have helped to protect against Stuxnet. In particular, Stuxnet's zero-day exploits were not patchable at that time. Also, Stuxnet's sophistication bypassed the installed anti-virus software.

[††] Other good practices would require regular screening of experts and operators with view of their financial, social, family, and psychological situation, and whether they are addicted to drugs, gambling or alcohol. However, in the academic environment of high energy physics, this would be impossible.

"CERN Security Baselines" [21] which both give basic recommendations on how to protect control systems as well as computing services at CERN.

Whilst following a standard is definitively a good practise, it also must be stressed that any investment in cyber-security must be balanced. Consciously accepting the risk is a valid alternative, too.

CONCLUSIONS

Stuxnet should have been the wake-up call for all those who never believed that control system could and would be attacked. Indeed, the media was quickly interested and created an unprecedented hype about the protection of the critical infrastructure which strongly relies on control systems. They called out the new "Era of Cyber-War" [1]. In parallel, attackers as well as security researchers became interested in analysing control system hardware. Standard IT security companies joined and now provide technical solutions for protecting control systems, even if their technical knowledge in control systems might be limited.

Most importantly, vendors are also concerned. Siemens, for example, has started an elaborative initiative on securing their control systems [22]. This should, however, not serve as an argument to users not to take any action. On the contrary, users should review the security protections put in place. Deploying a "Defense-in-Depth" approach is mandatory and corresponds to good practise. Continuing to ignore control system cyber-security is grossly negligent.

A new era has begun. Stay tuned.

REFERENCES

[1] Spiegel Online, "Stuxnet Virus Opens New Era of Cyber War", August 8, 2011; http://www.spiegel.de/international/world/0,1518,778912,00.html.

[2] The Economist, "The meaning of Stuxnet", September 30, 2010; http://www.economist.com/node/17147862.

[3] The Washington Post, "CIA slipped bug to Soviets", February 27, 2004.

[4] S. Lüders, "Control Systems Under Attack?", ICALEPCS, Geneva, October 2005.

[5] C. Miller, "The Legitimate Vulnerability Market", May 6, 2007; http://weis2007.econinfosec.org/papers/29.pdf.

[6] Symantec Corporation, "W32.Stuxnet Dossier", February 2011; http://www.symantec.com/en/ca/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

[7] Siemens AG; http://www.automation.siemens.com/mcms/simatic-controller-software/en/step7/pages/default.aspx.

[8] Siemens AG; http://www.automation.siemens.com/mcms/human-machine-interface/en/visualization-software/scada/Pages/Default.aspx.

[9] Siemens AG; http://www.automation.siemens.com/mcms/process-control-systems/en/distributed-control-system-simatic-pcs-7/pages/distributed-control-system-simatic-pcs-7.aspx.

[10] Wikipedia,org; http://en.wikipedia.org/wiki/Stuxnet.

[11] Tenable Network Security, "Nessus Open Source Vulnerability Scanner Project"; http://www.tenable.com/products/nessus.

[12] Fyodor Vaskovich, "nmap — Free Security Scanner for Network Exploration and Security Audits"; http://nmap.org.

[13] U.K. Centre for the Protection of the National Infrastructure (CPNI), "Process control and SCADA security - good practice guidelines"; http://www.cpni.gov.uk/advice/infosec/business-systems/scada/

[14] The International Society of Automation (ISA), "Manufacturing and Control Systems Security", ANSI/ISA SP99 TR99.00.01-04 http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821.

[15] U.S. Department of Homeland Security (DHS), "Cyber Security Procurement Language for Control Systems", 2009; http://www.us-cert.gov/control_systems/pdf/FINAL-Procurement_Language_Rev4_100809.pdf.

[16] U.S. National Institute of Standards and Technology (NIST), "Guide to SCADA and Industrial Control Systems Security", NIST SP800-82; http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf. .

[17] U.S. Federal Energy Regulatory Commission (FERC), "Critical Infrastructure Protection CIP-002 to CIP-009"; http://www.nerc.com/page.php?cid=2%7C20.

[18] International Organization for Standardization (ISO), "Information Technology — Security Techniques", ISO/IEC 27001:2005 and following.

[19] U. Epting et al., "Computing and Network Infrastructure for Controls", ICALEPCS, Geneva, October 2005.

[20] S. Lüders et al., "CNIC Security Policy for Controls", 2011; https://edms.cern.ch/document/584092.

[21] S. Lüders et al., "CERN Security Baselines"; http://cern.ch/security/rules/en/baselines.shtml.

[22] ARC Advisory Group, "Risk Drives Industrial Control System Cyber Security Investment", May 2011; http://www.industry.siemens.com/topics/global/en/industrial-security/Documents/ARC-Siemens-CyberSecurity-2011-v1.pdf.