CONTROL SYSTEMS UNDER ATTACK ?

S. Lüders [1]
[1]CERN, Geneva, Switzerland

ABSTRACT

The enormous growth of the Internet during the last decade offers new means to share and distribute both information and data. In Industry, this results in a rapprochement of the production facilities, i.e. their Process Control and Automation Systems, and the data warehouses. At CERN, the Internet opens the possibility to monitor and even control (parts of) the LHC and its four experiments remotely from anywhere in the world. However, the adoption of standard IT technologies to Distributed Process Control and Automation Systems exposes inherent vulnerabilities to the world. The Teststand On Control System Security at CERN (TOCSSiC) is dedicated to explore the vulnerabilities of arbitrary Commercial-Of-The-Shelf hardware devices connected to standard Ethernet. As such, TOCSSiC should discover their vulnerabilities, point out areas of lack of security, and address areas of improvement which can then be confidentially communicated to manufacturers.

This paper points out risks of accessing the Control and Automation Systems in an unprotected manner over the standard Ethernet, presents the TOCSSiC and its findings, and finally discusses methods for protective measures.

INTRODUCTION

The enormous growth of the worldwide interconnectivity of computer devices (the "Internet") during the last decade offers the User new means to share and distribute information and data. In Industry this results in an adaptation of modern Information Technologies (IT) to their plants and, subsequently, in a rapprochement of the production facilities, i.e. their Process Control and Automation Systems, and the data warehouses. Thus information from the fabric floor is now directly available at the management level ("From Top-Floor to Shop-Floor"). At CERN, the Internet opens the possibility to control (parts of) the LHC particle collider and the four LHC experiments remotely from any place in the world. This is much appreciated, since thousands of experts are working worldwide on the collider and experiments and can not be permanently present locally in the corresponding control room. However, their knowledge is needed to maintain, tune, improve or repair the systems. In addition the subsystems of the LHC collider and the LHC experiments are heavily exchanging data which necessitates a high degree of interconnectivity between them. This data must also be available outside CERN's boundaries to a much broader physics community.

Unfortunately the adoption of standard modern Information Technologies to distributed Process Control and Automation Systems also exposes their inherent vulnerabilities to the world. Furthermore, this world is by far more hostile then a local private control network as the number and power of worms and viruses increase and hackers start to get interested in Control Systems. Partial protection can be obtained through the usage of properly configured firewalls and through well-defined network architectures. However, some other means of security incorporated into standard IT equipment can not be directly applied to DCS equipment since both differ in hardware but also in the concepts of availability and manageability.

The Teststand On Control System Security at CERN ("TOCSSiC") is dedicated to exploit vulnerabilities of arbitrary Commercial-Of-The-Shelf hardware devices (COTS) connected to the standard Ethernet. These devices include Programmable Logic Controller (PLC), Ethernet connected power supplies, SCADA systems, etc. As such, TOCSSiC should discover their inherent vulnerabilities and point out areas of lack of security. These areas of improvement can then be confidentially addressed to vendors and manufacturers.

The next section will discuss the upcoming threats to Distributed Process Control Systems and Automations Systems (here commonly termed "Control Systems"). Afterwards, the TOCSSiC will be described and its findings presented. Finally, proposals for first steps in mitigation will be given and this paper will be concluded.

CONTROL SYSTEMS UNDER ATTACK ?

Ten years ago Control Systems were restricted to dedicated processes with sparse interconnectivity to other systems, if at all. The corresponding hardware was based on legacy technologies and proprietary protocols coming from on one or a few vendors. As such, they were completely (or mostly) separated from the rest of the world and only reachable by means of a few dial-up modems.

From the security point of view, these Control Systems were safe ("Security through Obscurity") since only a few experts had knowledge in the protocols and methods used and the outside connectivity was low. Major threats were insiders (e.g. disgruntled employees) who were targeting the Control System in order to archive personal gain or Users who badly configured the system. A recent analysis reports that today this dominance of internal fraud is rapidly changing to threats created externally [1].

In fact, parallel to Control Networks, modern Information Technology developed its own standards based on Ethernet and the TCP/IP protocol during the end of the last century. Due to its openness and ease to use, these IT networks rapidly spread around the world and became standard for office and business networks as well as for the use at home. But with this openness, and due to the fact that no software and operating system (O/S) is free of flaws, also the dark side entered the scene in form of "war dialing", "back doors", password sniffing and cracking and hijacking user sessions during the early 90's. These threats continued in sophistication since the hackers accumulated their knowledge leading to a new breadth of viruses and worms automating the attacks. Today, IT is faced with IRC (Internet Relay Chat) based intrusions, Denial-of-Service (DoS) attacks, "BotNets" and Zombie machines which are able to strike a synchronized attack with hundreds of machines around the world.

However, many Control Systems are undergoing a change towards modern IT based solutions. More and more common IT standards are also applied to Control Systems and Networks. Proprietary field busses are being replaced by Ethernet and use TCP/IP. Common IT protocols such as SNMP, SMTP, FTP, telnet and HTTP are being used to share data from the Control Systems with data warehouses and the upper management levels ("From Top-Floor to Shop-Floor"). More and more sensors, actuators and other field devices are being directly connected to this network. Even modifications to the TCP/IP protocol in order to incorporate "real-time" capabilities are now being considered and investigated [2].

Furthermore, COTS IT hardware now allow for VPN access from remote locations (e.g. from home) and for the use of wireless communication. On the User interface side, operator consoles and SCADA (Supervisory Control And Data Acquisition) systems are being ported to the Microsoft® Windows® platform. Notebooks and USB sticks become new means to monitor and configure Control Systems. Based on Microsoft's DCOM (Distributed Component Object Model) standard, the OPC Foundation [3] developed the widely used OPC protocol (OLE for Process Control, where OLE stands for Object Link and Embedding) to exchange data between Control Systems of different manufacturers.

But with the rise of modern IT in Control Systems and Networks, also drawbacks appear. The large interconnectivity between business and office network enables viruses and worms to spread more easily to the Control Systems. VPN, wireless access, notebooks and USB sticks offer new possibilities for a virus or worms to enter the Controls Network. Not to speak of hackers and terrorists which might be interested to target Control Machines in order to shutdown the system. Since Microsoft's Windows O/S is now the de-facto platform for SCADA applications, the corresponding Control PCs inherit the same vulnerabilities that office PCs have. But Control Systems can not be patched and updated as fast as office PCs. Some Control PCs might even lack anti-virus software because of interferences with the control processes. Even if these PCs are secured, zero-day exploits might enter before the proper patch and virus signature file is available or applied. Furthermore, OPC runs on the port number 135 which is heavily used under the Windows O/S and can not easily be blocked by means of firewalls.

Users and Operators of Control Systems become the second weak link. On one hand, they might carry infected notebooks into the plant or connect their infected home-PC via VPN to the Controls Network. On the other hand, in the era of legacy Control Systems, passwords were known to many people. Due to human nature, these passwords might be weak in the sense that they consist of a few letters only or can be found in a dictionary. For convenience, many applications still use the default password or might miss it at all. In the past, sufficient traceability was guaranteed due to the restricted group of people having access to the Control System, but with the new interconnectivity, password sniffing and guessing can now be done automatically and remotely…

Last but not least, COTS Automation Systems such as PLCs, power supplies and other field devices have no security integrated into their designs. Even worse, manufacturers include more and more IT functionality (like e-mailing and web servers) into their devices and, thus, reduce security still more. In order to test these Automation Devices on cyber vulnerabilities, a Teststand on Control System Security has been created at CERN.

THE TESTSTAND ON CONTROL SYSTEM SECURTY AT CERN (TOCSSIC)

The TOCSSiC hardware and software is based on standard IT equipment, which is commonly used for vulnerability tests. The core consists of three PCs: The "vulnerability tester" conducting the vulnerability scans, break-ins and Denial-of-Service (DoS) attacks; the "configurator" allowing for the configuration of the target device; and the "traffic analyzer" used to sniff the communication between target device and configuration PC. Figure 1 gives an overview on the architecture.

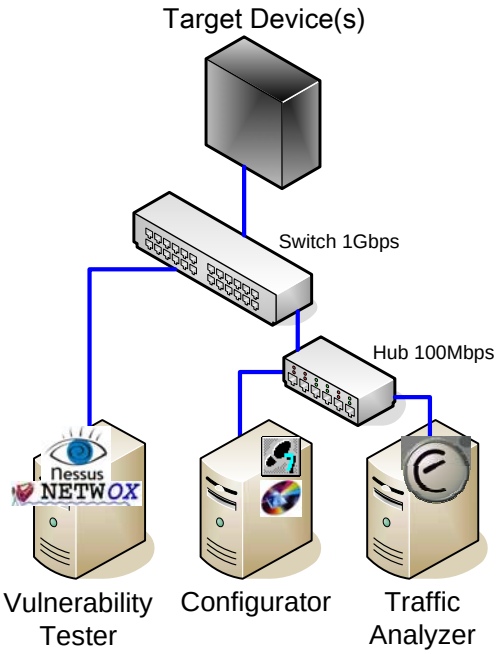

Figure 1: Hardware & software configuration of the TOCSSiC.

The vulnerability tests are performed with two freely available tools "Nessus" [4] and "Netwox" [5]. Nessus is a powerful and easy to use remote security scanner commonly used in IT auditing. It is based on "nmap" [6] and consists of about 9000 different plug-ins probing a multitude of flaws. For the TOCSSiC, all plug-ins are used. However, it should be notated, that most of these plug-ins are dedicated to IT COTS hardware (PCs, switches, servers) and the application of Nessus on Automation Devices might not reveal all vulnerabilities and/or result in false positives.

Netwox is a "network toolbox" wrapping many different network tools under one interface. For the TOCSSiC only the tool numbered "74" is used. It produces continuously a stream of random fragmented packets in order to perform a DoS attack on the target device. Details on the TOCSSiC procedures can be found in [7].

The TOCSSiC Tests

Twenty different devices (PLCs and power supplies) from six different manufacturers have been tested with the TOCSSiC. Including different firmware versions, 35 tests were made in total. All of the tested devices were configured to a minimum, e.g. fixing the IP address and changing default account names and passwords to random strings.

After the Netwox DoS attack, 68% of the devices were able to respond to an ICMP "ping" request, while the other 32% did not respond anymore and had to be restarted by power-cycling the device. The full Nessus scan was successfully completed by 61% of the devices. Only a few minor security problems were found which are also frequently present on up-to-date and properly patched PCs. In 21% of the Nessus tests, the device crashed during the scan. After power-cycling the device, the scan was repeated without the corresponding plug-in. In the remaining 18%, Nessus reported significant security holes which are described below. Figure 2 gives an overview on the results.

In addition, a few tests have been conducted with fully configured devices in production mode (i.e. with permanent communication between each other). The preliminary results point to the conclusion that devices are more likely to crash under these circumstances then when running in idle mode.

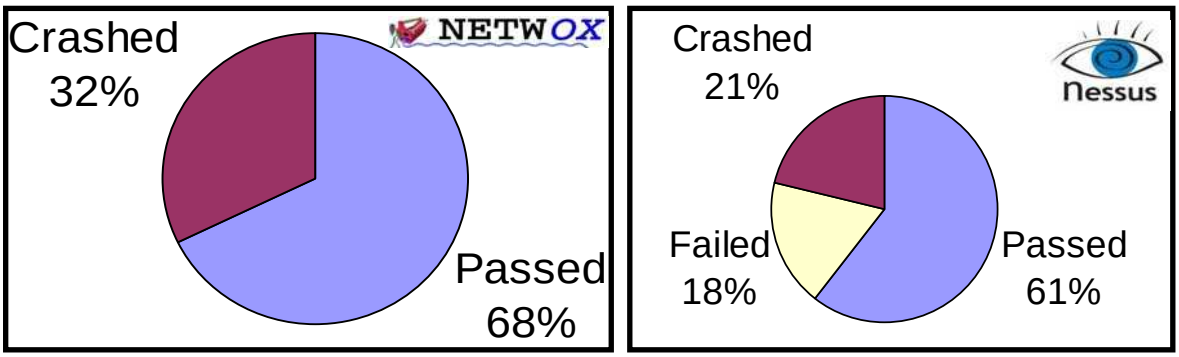

Figure 2: Statistics on the TOCSSiC results.

The TOCSSiC Findings

Security holes are generally reported when the firmware inside the device crashes. The crash might be restricted to parts of the firmware, e.g. servers such as FTP, Telnet or Modbus, which have been included in recent Automation Devices, or to the whole device. For example, devices crashed completely after sending

- special crafted IP packet fragments which cause the TCP/IP fragmentation re-assembly code to improperly handle overlapping IP fragments (the so-called "Nestea" attack) or which cause the re-assembly code to loose network connectivity (Linux "zero-length fragmentation" bug);
- a continuous stream of extremely large and incorrect fragmented IP packets which lead to the consumption of all CPU resources ("jolt2" attack);
- special malformed packets ("oshare" attack).

These findings obviously show a violation of the general TCP/IP standards in the firmware implementations. In addition, many devices responded to SNMP (Simple Network Management Protocol) request, but do not allow changing the default community names "public" and "private" which offer the only "protection" in SNMP (if this can be considered to be protective at all).

Concerning FTP, Nessus was able to crash FTP servers by sending too long arguments or passwords to the device. In a particular instance, the FTP server allowed the User to connect to a third party host which offers the possibility to create an attacker platform on this server. In addition, several FTP servers accepted anonymous logons. The same holds for the Telnet protocol, where Nessus crashed the Telnet server after flooding it with "^D" characters or sending a too long user name to it. A Modbus server crashed during the scan of its port 502. The latter is considered to be very serious, since the Modbus protocol is very well documented. Since neither of the protocols offers the possibility of encrypted data transmission, they should be discarded.

Following their customers' needs, the more fancy Automation Devices include web servers in order to display HTML pages or offer e-mailing functionality. However, the TOCSSiC results show, that this demand brings new vulnerabilities: Nessus crashed some of these web servers by requesting URLs with too many characters (e.g. "http://<IP address>/jsp/aaa....aaa", with 1000×"a", or "http://<IP address>/cgi-bin/aaa....aaa", with 8000×"a"). In addition, crashes occurred after too many pages were

requested and all resources of the device were used up ("WWW infinite request" attack). Some device even offered the full directory listing through an "http://<IP address>/../.." request. Again, this raises the question, why IT standards (i.e. those valid for web servers) can not be applied to automation devices ? Furthermore, manufacturers should implement methods to disable unwanted or unneeded services.

Finally, the network traffic between the target device and the configuration PC has been recorded using Ethereal [8]. Its analysis pointed out some more drawbacks on the firmware implementations: Generally, none of the protocols used for the configuration is either password protected or encrypted. Since most of these protocols are well documented, it was able to stop any PLC by sending a specially crafted TCP/IP packet. Even if these devices offer password protection, this protection has not been applied to start/stop commands. Thus, a bit of "googling" the Internet offers the potential for an intruder to gain control over Automation Devices.

FIRST STEPS FOR MITIGATION

The results of the TOCSSiC vulnerability scans have shown that an inherent security of automation devices is a chimera even if some manufactures recently became aware of this issue and now offer the possibility of IP address filtering and separate Control System firewalls. In order to follow up with the TOCSSiC results, all concerned manufacturers have received a copy of the corresponding reports and have been made aware of the vulnerabilities of their products. Since the disclosure of this information bears some risk, the TOCSSiC results have also been passed to the British National Infrastructure Security Co-ordination Centre (NISCC) [9] which deals with critical infrastructures (petroleum industry, power industry, to name a few) and their protection within the U.K. Their European SCADA and Control Systems Information Exchange allows discussing efforts on how further to approach the manufacturers and how to enforce security into their products. On the technical side, the TOCSSiC is collaborating with the British Columbia Institute of Technology (BCIT, Canada) Internet Engineering Lab [10], which is also performing vulnerability tests on Automation Devices and which maintains an "Industrial Security Incident Database" collecting security breaches related to Control Systems.

From the expertise of the NISCC, the BCIT and from the results of the TOCSSiC, a few general base rules can be deduced. Every Control System should to be protected by a "Defence-in-Depth" approach. This contains a clear separation of business network and Controls Network with defined interfaces between them. Furthermore, the Controls Network should be segregated into smaller entities and Automation and SCADA Systems should be protected by firewalls and anti-virus software where possible. In addition, a proper security policy must be developed which enforces rules

- how to connect devices to the Controls Network (esp. notebooks), how to manage them, and how to intervene in the case of an security incident;
- how to access to the Controls Network from the outside (e.g. via application gateways) taking also VPN and wireless connections into consideration;
- how to install, manage, patch and update SCADA systems, and how to ensure prompt patches and virus signature files;
- how to restrict the use of generic accounts and easy-to-guess passwords, and how to enforce traceability of usage;
- how to raise awareness in the User community.

At CERN, the Computing and Network Infrastructure for Controls (CNIC) has produced such a policy document in order to refine the usage of Control Systems at CERN [11].

Every User concerned about the security of their Automation Devices should report back to the corresponding vendor and manufacturer in order to improve the security of those devices. In particular, the OPC Foundation is working on securing the OPC protocol and moving away from the DCOM layer. The Microsoft Manufacturing User Group (MS MUG) [12] discusses at a high management level the needs on the Windows O/S from the perspective of Control Systems. Both forums are open for every User.

CONCLUSIONS

With the adaptation of modern IT standards to Control Systems and the subsequent growing interconnectivity between Controls Networks and business network, Control Systems became also exposed to the threats regarding computer security. However, many Control Systems are not prepared to cope with defending against cyber threats. Vulnerability tests using CERN's TOCSSiC have shown that especially Automation Systems are not secured at all and are highly vulnerable to different types of attacks. Different servers running on those devices can be crashed easily. Automation Devices can be stopped and remotely controlled by an intruder using information available on the Internet. Manufacturers have just become aware of this issue, such that proper solutions (e.g. encryption of the data exchange) can not be expected to come in the near future. Therefore, each User of Control Systems must ensure these and in particular the corresponding Controls Network are properly secured by a "Defence-in-Depth" strategy. A proper security policy must be set up and supported by the management. The primary question must be "Do we act BEFORE or AFTER the incident ?".

ACKNOWLEDGEMENTS

The author deeply appreciates the initial work done in this domain by J. Rochez (CERN IT/CO), R. Brun (CERN AB/CO) and J. Brahy (CERN AB/CO) and their support on PLCs. In addition, he would like to thank B. Figon (ESIEE, Amiens) and J. Arnold (EPFL, Lausanne) for their work on the TOCSSiC.

REFERENCES

[1] E. Byers, "Who Turned Out the Lights? Understanding the Changing Risks to Critical Control Systems from Cyber Attacks to Viruses ─ New Trends in Threats and Implications", ISA EXPO 2004 technical Conference, Houston, USA, October 2004.
[2] J. Schweiger, "Comparing Real-Time Ethernet ─ Are field busses going to disappear ?", 1st International Symposium on Industrial Ethernet, Berlin, Germany, June 2004.
[3] http://www.opcfoundation.org/
[4] Tenable Network Security, "Nessus Open Source Vulnerability Scanner Project"; http://www.nessus.org
[5] L. Constantin, "Netwox Network Toolbox"; http://www.laurentconstantin.com/en/netw/netwox/
[6] Fyodor et al., "nmap — Free Security Scanner for Network Exploration and Security Audits"; http://www.insecure.org/nmap/
[7] S. Lüders et al., "TOCSSiC ─ A Teststand On Control System Security at CERN", CERN EDMS 573062, June 2005.
[8] G. Combs et al., "Ethereal — The World's Most Popular Network Protocol Analyzer"; http://www.ethereal.org
[9] http://www.niscc.gov.uk/niscc/index-en.html
[10] http://www.bcit.ca/appliedresearch/security/
[11] U. Epting et al., "Computing and Network Infrastructure for Controls CNIC", these proceedings.
[12] http://public.arcweb.com/MSmug/default.aspx