ICS/SCADA Security
Analysis of a Beckhoff CX5020 PLC

Gregor Bonney, Hans Höfken, Benedikt Paffen and Marko Schuba
FH Aachen, University of Applied Sciences, Eupenerstr. 70, Aachen, Germany
{bonney, hoefken, paffen, schuba}@fh-aachen.de

Keywords: ICS, SCADA, Security, Vulnerability, Beckhoff, CX5020, PLC.

Abstract: A secure and reliable critical infrastructure is a concern of industry and governments. SCADA systems (Supervisory Control and Data Acquisition) are a subgroup of ICS (Industrial Control Systems) and known to be well interconnected with other networks. It is not uncommon to use public networks as transport route but a rising number of incidents of industrial control systems shows the danger of excessive crosslinking. Beckhoff Automation GmbH is a German automation manufacturer that did not have bad press so far. The Beckhoff CX5020 is a typical PLC (Programmable Logic Controller) that is used in today's SCADA systems. It is cross-linked through Ethernet and running a customized Windows CE 6.0, therefore the CX5020 is a good representative for modern PLCs which have emerged within the last years that use de facto standard operation systems and open standard communication protocols. This paper presents vulnerabilities of Beckhoff's CX5020 PLC and shows ways to achieve rights to control the PLC program and the operation system itself. These vulnerabilities do not need in-depth knowledge of penetration testing, they demonstrate that switching to standard platforms brings hidden features and encapsulating SCADA protocols into TCP/IP might not always be a good idea – underlining that securing ICS systems is still a challenging topic.

1 INTRODUCTION

Computers in automation technology are used to regulate industrial processes such as chemical production processes or assembly lines in the automobile industry. In the early years, computer control of automation systems was done in a local context only, i.e., with no connection to a corporate network or the Internet (European Network and Information Security Agency 2011b:1). In the past decade, however, the growing availability of the Internet, the globalization, and the growing number of decentralized companies led to ICSs (Industrial Control Systems) that had to be network- and Internet-enabled (European Network and Information Security Agency 2011c:14). From a business perspective this results in automation processes that are easier and thus cheaper to manage.

An essential part of ICS are SCADA systems (Supervisory Control and Data Acquisition) which are responsible for centrally collecting process relevant information and – based on the analysis of this data – send control instructions to the production systems (European Network and Information Security Agency 2011c:6). To this end, the SCADA systems need to be connected to various parts of the ICS, for example, to PLCs (Programmable Logic Controllers), which control the individual actuators or sensors in the machinery. Interconnection between central SCADA machines and PLCs is more and more based on standard networking technology. SCADA-specific protocol data units are, for instance, encapsulated in TCP/IP and transmitted via Ethernet on the link layer (industrial Ethernet) (Knapp 2011:66).

The discovery of the virus „Stuxnet" in 2010 made it obvious to the public, that modern ICS are vulnerable against cyber-attacks (Knapp 2011:38). As any modern computer system, SCADA systems and PLCs have vulnerabilities that can be exploited with off-the-shelf or targeted malware. Internet search engines like Shodan (SHODAN 2014), which collect information about machines connected to the Internet, and fast Internet scanners like Zmap (ZMap 2014), make the discovery of vulnerable machines even simpler (Knapp 2011:117). The effects of cyber-attacks on ICS could be devastating: production processes could be manipulated or disrupted. In the worst case, there could be personal or environmental damage or loss.

This paper describes the results of an initial security analysis of a Beckhoff CX5020, a commonly used PLC in SCADA/ICS systems. The goal of the investigation is to find out, if a modern PLC, which is based on a well-known platform like Windows CE, has exploitable vulnerabilities in the platform or the PLC part of the system. The description of our investigation will start in chapter 2 with a brief description of ICS, SCADA, the protocols used and the specifics of a Beckhoff CX5020. Chapter 3 and 4 explain our analysis approach and results which lead to a set of possible attacks described in chapter 5. Chapter 6 gives a set of recommendations to the manufacturer and to users of the Beckhoff CX5020, which protect against the described attacks.

2 ICS/SCADA SECURITY

2.1 SCADA Systems and Protocols

A typical SCADA system consists of different parts. The low-level control algorithm is running on a PLC or RTU (Remote Terminal Unit). These devices are connected to sensors and actuators. They retrieve sensor data, evaluate the local system state and control actuators based on the data evaluation result. Multiple SCADA systems operate as MES (Manufacturing Execution System) and several MESs are controlled by ERP (Enterprise Resource Planning). The layering of the different systems is depicted in the automation pyramid in Figure 1.

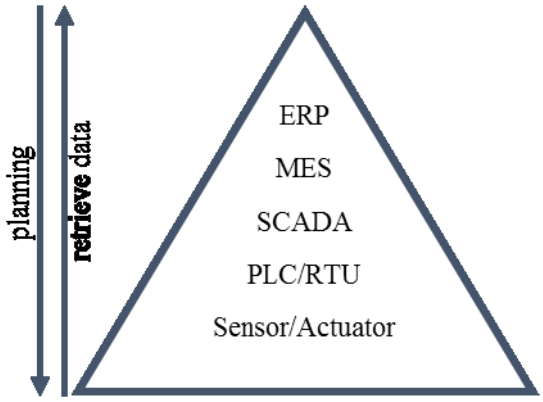

Figure 1: Automation pyramid.

An HMI (Human Machine Interface) is used to present the current system state and allows to manually edit parameters. An HMI's control directive is not limited to one PLC or RTU, it is more likely to control multiple devices via a single HMI. Therefore the PLC or RTU and HMI have to be interconnected. A local setup is called remote site. The MTU (Master Terminal Unit) is a central place where the system state of multiple remote sites is supervised and controlled from (Krutz 2006:7). To achieve supervisory control and data acquisition an EWS (Engineering Workstation) is running at the MTU. It is a normal computer with specific SCADA software installed that allows remote diagnostics, sending control instructions and reprogramming. A so-called historian saves retrieved telemetry data of remote sites into a central database for future evaluation (Trend Micro Incorporated:5).

SCADA makes use of networks protocols to transport PLC administration and programming commands. The protocols are also used for communication between PLCs. The connection to corporate networks and/or the Internet – for instance, for remote maintenance – is frequently realized through standard programs such as HTTP, Telnet, or FTP. Connectivity on the link layer usually takes place via Ethernet.

2.2 General SCADA Security Issues

Many SCADA systems nowadays are based on or encapsulate higher layer protocols in unencrypted and unauthenticated protocols like Telnet. Integrated HMIs, which simplify control, usually operate over HTTP and have no encryption for login credentials.

Many of the special programs and protocols used for programming of PLCs and controlling the infrastructure of ICSs are unsecure as well. At the time of their development security was not part of the requirements. Therefore, they turn out to be a security risk (European Network and Information Security Agency 2011a:27).

It is this kind of vulnerabilities, which allows viruses like "Stuxnet" to be successful. Stuxnet was not only able to exploit operating systems in the control centre, it was also able to continue the attack on downstream PLCs, which had no protection against the attack. Vulnerabilities in the protocols helped to obtain further rights and infected machines, using for instance hardcoded passwords of the PLCs or the credentials of the database server.

As a reaction to these new threats the automation industry has started to develop better and more secure components. Still, security by design, as it is applied in software engineering by the traditional software industry, is still a new area for ICS manufacturers and mistakes are made. And even if new and more secure

components are made available for retrofit or replacement of insecure parts of an ICS, many companies avoid modernization as any change to the systems means interruption of production, extensive testing, i.e., cost.

3 SECURITY ANALYSIS SETUP

In order to find out, if modern PLCs are "secure by design", an example for such a modern PLC was analysed. The Beckhoff CX5020 is an embedded PC running Windows CE 6.0 plus a Beckhoff proprietary software that makes it operate as a PLC. The built-in hardware uses an Intel Atom CPU with 1 GB of RAM and a flashcard serving as persistent memory. An integrated UPS provides emergency power for around two seconds and allows a secure shutdown of the device in case of power failure.

In order to retrieve and analyse the traffic coming and going to a remote site, a simplified test environment was set up. The test environment consists of an EWS and a CX5020 PLC. A third node, a PC, is used as port scanner and is later on connected to the mirror port of the interconnecting switch in order to capture the traffic.

Due to the use of Windows CE 6.0 on the CX5020 the analysis consisted of two phases. The first phase was a normal service and vulnerability discovery using scanning tools. After a full list of open services was received, additional information to each service was searched for inside the windows registry and the local file system. The second phase analysed the traffic between EWS and CX5020 while simulating SCADA use-cases like adding a new remote site to the system or controlling the PLC.

4 SECURITY ANALYSIS RESULTS

An nmap port scan of the CX5020 PLC discovered 16 open ports (cf. Table 1) which include well-known services like Telnet on port 23, a webserver listening on port 80, 5120 and 5357 plus unknown services on port 987, 48898 and 48899.

Some of these ports might be accessible from the Internet. Assuming that a remote site is protected via firewall but needs remote maintenance, it is likely that the respective SCADA and maintenance ports are open in the firewall access control lists. In the case of a CX5020 PLC, such common open ports would include port 48898 and 48899 as advised by the manufacturer Beckhoff on their customer service portal (Beckhoff Information System), and perhaps ports 23, 80 and 987 for Windows CE remote management.

Table 1: Port scanning result.

Port	Protocol	State	Service
23	TCP	Open	telnet
80	TCP	Open	http
139	TCP	Open	netbios-ssn?
443	TCP	Open	tcpwrapped
445	TCP	Open	netbios-ssn
987	TCP	Open	unknown
5120	TCP	Open	http
5357	TCP	Open	http
8080	TCP	Open	http-proxy
48898	TCP	Open	tcpwrapped
123	UDP	Open	ntp?
137	UDP	Open	netbios-ns
138	UDP	open/filtered	netbios-dgm
161	UDP	Open	snmp
1900	UDP	open/filtered	upnp
48899	UDP	open/filtered	unknown

Taking into account all open ports from Table 1, a vulnerability scan using OpenVAS was executed but did not reveal any vulnerability except for a public community name in the SNMP service that was classified medium.

Looking more closely at particular ports, the following was discovered.

4.1 Telnet

Telnet is enabled by default. When connecting to the port a greeting containing "Welcome to Windows CE 6.0 Telnet service on CX-ABCD" is presented while CX-ABCD is the hostname of the device. If the default passwords has not been changed it is possible to log on with username "webguest" and password "1". Because Windows CE 6.0 is a single user system, all logged in accounts get full administration privileges and are able to create new accounts by using a script called CxAddUser. The newly created accounts are able to use Telnet, FTP, SMB, and VPN.

4.2 Webserver

The webserver's index page presents a template file containing the hint "Welcome to BECKHOFF CE device". Beckhoff informs about one special URL for accessing a configuration interface: <ip>:5120/config (Beckhoff Information System). A registry inspection discovered that the webserver supports virtual directories and exports different hard disk paths, as depicted in Table 2.

The most interesting virtual directory is /remoteadmin which presents Microsoft's Windows CE remote management tool. This virtual directory is not documented in Beckhoff's manual and is not configured. Therefore, on first visit, it allows choosing a password with at least three characters length. Once set, these credentials give users full control on network, time, file, and print server settings.

Table 2: Virtual directories found in the Beckhoff CX5020's registry.

Virtual directory	Path on Hard Disk
/	\Hard Disk\www
/MsmqAdmin	\windows\msmqadminext.dll
/remoteadmin	\windows\ REMOTEADMIN.dll
/remoteadminimages	\windows\www\remoteadmin\ images
/upnp	\windows\upnp
/UpnpDevice	\Hard Disk\www
/upnpisapi	\windows\upnpsvc.dll
/UpnpWebsite	\Hard Disk\UPnP\Website

4.3 CeRDisp

CeRDisp is short for CE Remote Display and describes a remote desktop service for Windows CE devices. The service listens on TCP port 987. A client software named CeRHost for Windows desktop variants can be downloaded online. The connection requires a password that has to be set in the CX5020's control panel. The connection setup is transmitted in plaintext and can be attacked using ARP-Spoofing. After a successful authentication the user has full control over the PLC.

4.4 Vpn (Pptp)

A PPTP connection is the only way to encrypt traffic to the device. All other services use plain text transfer. If port 1723 is reachable, the default user "webguest" can connect with password "1". After creation of new users through Telnet, those new users can authenticate themselves and use the PPTP service, too. The default PPTP authentication mechanism is unsecure as it uses MS-CHAP v2 that can be easily cracked (Marlinspike 2013).

4.5 SCADA Service

Within a SCADA system the ADS (Automation Device Specification) protocol controls the CX5020 PLC systems. EWS operators use the Beckhoff TwinCAT System Manager software to search for PLCs. Such a discovery of PLCs is initiated by special UDP packets which are broadcasted or sent to a specific IP address on port 48899 UDP. ADS devices reply to these packets by sending 325 bytes of data encoding details of the operating system, hostname, ADS and PLC runtime version to the requesting host. Figure 2 shows the packet content of a respective reply. The first four bytes are the ADS packet header. Bytes 000C to 0011 represent the NetId, bytes 001C to 0025 the PLC's hostname.

```
0000  03 66 14 71  00 00 00 00   .f.q....
0008  01 00 00 80  05 14 3e 97   ......>.
0010  01 01 10 27  03 00 00 00   ...'....
0018  05 00 0a 00  43 58 2d 31   ....CX-1
0020  34 44 45 39  37 00 04 00   43E97...
0028  00 00 00 00  00 00 00 00   ........
....  00 00 00 00  00 00 00 00   ........
0138  00 00 00 00  00 00 00 00   ........
0140  04 00 02 0b  b9 08         ......
```

Figure 2: Information sent from the PLC to the EWS as reply to a search request.

Every ADS device has a unique ADS NetId. The TwinCAT System Manager uses this NetId and an optional password to establish an ADS route. If no device password has been set in the PLC's control panel any string will be accepted. Subsequently, only the host with the IP address sent within the route creation request is able to retrieve status information from the PLC.

Figure 3 shows a requests for the creation of an ADS route between source IP 192.168.1.50 with hostname WIN7VM-PC and the CX5020 PLC. The first 37 bytes are similar to Figure 2 but contain the EWS details. This packet includes the username "Administrator", a password "1234567" and the IP address the PLC will establish an ADS route to.

```
0000  03 66 14 71  00 00 00 00   .f.q....
0008  06 00 00 00  0a ff 02 0f   ........
0010  01 01 10 27  05 00 00 00   ...'....
0018  0c 00 0a 00  57 49 4e 37   ....WIN7
0020  56 4d 2d 50  43 00 07 00   VM-PC...
0028  06 00 0a ff  02 0f 01 01   ........
0030  0d 00 0e 00  41 64 6d 69   ....Admi
0038  6e 69 73 74  72 61 74 6f   nistrato
0040  72 00 02 00  08 00 31 32   r.....12
0048  33 34 35 36  37 00 05 00   34567...
0050  0d 00 31 39  32 2e 31 36   ..192.16
0058  38 2e 31 2e  35 30 00      8.1.50.
```

Figure 3: Packet send to the PLC from an EWS when trying to create the ADS route with password 1234567.

If a wrong password has been used, a non-zero error code is returned in the bytes at address 001C and 001D as shown in Figure 4.

```
0000  03 66 14 71 00 00 00 00 .f.q....
0008  06 00 00 80 05 14 3e 97 ......e.
0010  01 01 10 27 01 00 00 00 ...'....
0018  01 00 04 00 04 07 00 00 ........
```

Figure 4: CX5020's responded with error code 04 07 due to a wrong password.

Because of the simple and unencrypted packet structure the communication packets can be reverse engineered easily. On top, attackers who are able to create an ADS route could use some of the tools published on the manufacturer's internet platform to manipulate or interrupt the CX5020 PLC and the related SCADA system.

5 POSSIBLE ATTACKS

Two attacks are possible when a CX5020 PLC is reachable over a network connection. The first attack method uses the webserver's virtual directory /remoteadmin. After the attacker has set an initial password, the REMOTEADMIN.dll creates a new account ADMIN on the device. As all accounts are able to use Telnet, the attacker is now able to create a new account for VPN and therefore gains access into the SCADA network.

The fact that the PLC answers very fast and does not block a requester after too many wrong password attempts leads to the second possible attack method: a brute force or dictionary attack on UDP port 48899. Because an established connection allows for unlimited probing and evaluating of passwords, it is not necessary to create a new connection every time. It is even possible to use multiple connections in parallel, which improves the amount of passwords that can be tested per second. A benchmark test written in Python achieved up to ~8000 tested passwords per second using 8 parallel connections. The brute forced password can then be used with CeRHost to view and control the PLC's desktop.

Table 3 shows the performance of the developed Python script.

Table 3: Parallel brute force benchmark.

Passwords	Threads	Duration [s]	Passwords per second
200,000	1	183	1095
200,000	2	120	1665
200,000	3	74	2703
200,000	4	53	3752
200,000	8	25	7913
200,000	16	25	7971

6 RECOMMENDATION

The following advice is given to the manufacturer and users of the Beckhoff CX5020 to improve the system's security:

1. Remove the registry key for the /remoteadmin virtual directory and disable Telnet by default.
2. Implement a limitation for specific ADS packets per second to reduce the risk of password attacks. This can either be done on the device itself but could also be done by an intrusion detection and prevention system on the upstream path.
3. Deliver the CX5020 with strong default passwords that cannot be guessed. Users should check if their passwords are reasonably secure.
4. Use only secure protocols, e.g., a PPTP with a secure authentication mechanism.

7 CONCLUSIONS

ICS and SCADA systems have a central role in the automation of modern production facilities. The growing interconnection of ICS components among each other and to corporate or public networks like the Internet, leads to new security threats. Devices that are reachable via network can easily become the target of attackers. It is therefore crucial to take such new threats into account and to make sure that vulnerabilities in ICS systems are protected with suitable controls.

In this paper we have demonstrated that modern PLCs, like the Beckhoff CX5020, still lack the secure design and security testing that is commonplace for normal computer systems today. In particular a secure default configuration and protection against password attacks should be considered. Unsecure protocols like Telnet, HTTP, or PPTP with MS-CHAP v2 should be replaced with secure versions. For new components, security should be part of the design – and here the automation industry should quickly learn from the experience and competence of the computer world.

REFERENCES

Beckhoff Information System, *Scenario: ADS connection through a firewall*, viewed 5 November 2014, from http://infosys.beckhoff.com/english.php?content=./con

tent/1033/tcremoteaccess/html/tcremoteaccess_firewall.html&id=.

Beckhoff Information System, *TcWebAccess: Web based diagnostic and configuration interface*, viewed 5 November 2014, from http://infosys.beckhoff.de/english.php?content=./content/1033/sw_os/html/CX1000_TcWebAccess.htm&id=.

European Network and Information Security Agency, 2011a, *Protecting industrial control systems: Annex V*, Heraklion, from https://www.enisa.europa.eu/act/res/other-areas/ics-scada/annex-v.

European Network and Information Security Agency, 2011b, *Protecting industrial control systems*, Heraklion, from https://www.enisa.europa.eu/act/res/other-areas/ics-scada/protecting-industrial-control-systems.-recommendations-for-europe-and-member-states.

European Network and Information Security Agency, 2011c, *Protecting industrial control systems: Annex I*, Heraklion, from https://www.enisa.europa.eu/act/res/other-areas/ics-scada/annex-i.

Knapp, E., 2011, *Industrial network security: Securing critical infrastructure networks for Smart Grid, SCADA , and other industrial control systems*, Elsevier/Syngress, Amsterdam.

Krutz, R.L., 2006, *Securing SCADA systems*, Wiley Pub, Indianapolis, IN, from http://site.ebrary.com/lib/alltitles/docDetail.action?docID=10305459.

Marlinspike, M., 2013, *Divide and Conquer: Cracking MS-CHAPv2 with a 100% success rate*, viewed 5 November 2014, from https://www.cloudcracker.com/blog/2012/07/29/cracking-ms-chap-v2/.

SHODAN, 2014, *Computer Search Engine*, viewed 4 November 2014, from http://www.shodanhq.com/.

Trend Micro Incorporated, 'The SCADA That Didn't Cry Wolf: Who's Really Attacking Your ICS Equipment? (Part 2)', viewed 4 November 2014, from http://apac.trendmicro.com/cloud-content/apac/pdfs/security-intelligence/white-papers/wp-the-scada-that-didnt-cry-wolf.pdf.

ZMap, 2014, *The Internet Scanner*, viewed 4 November 2014, from https://zmap.io/.