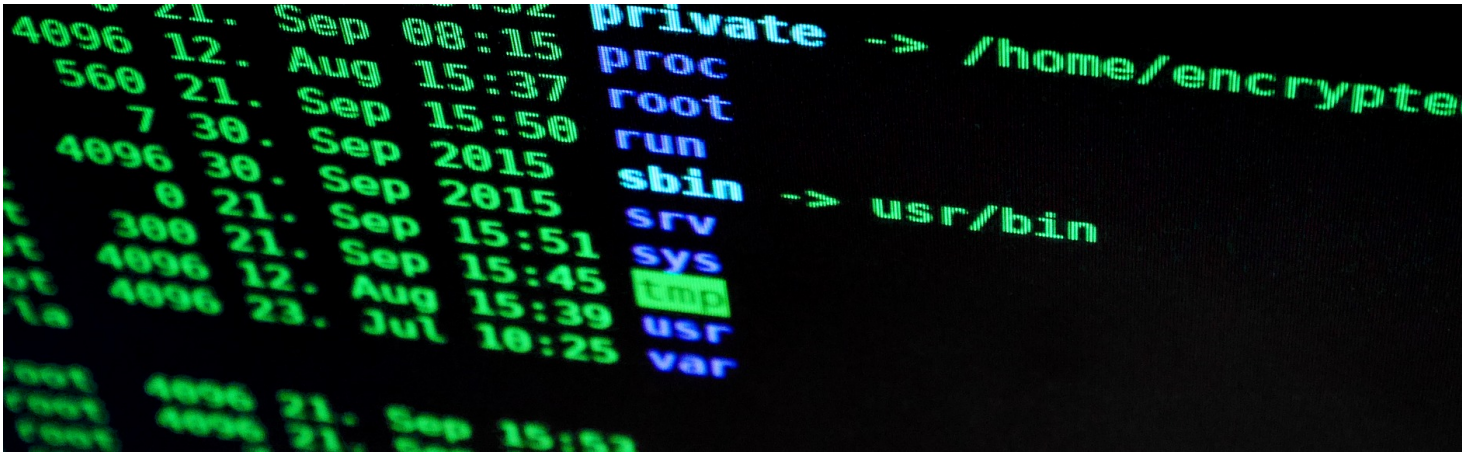
European Commission

JRC TECHNICAL REPORTS

Cyber Security Trends and their implications in ICS: Mid-year report 2016



Authors
Georgios Koutepas, Unisystems
Georgios Giannopoulos
Athina Mitsiara, I.R.I.S. Solutions & Experts

2016

EUR 28187 EN

Joint Research Centre

European Commission
Joint Research Centre
Institute for the Protection and Security of the Citizen

Contact information
Georgios Giannopoulos
Address: Joint Research Centre, Via Enrico Fermi 2749, TP 186, 21027 Ispra (VA), Italy
E-mail: georgios.giannopoulos@jrc.ec.europa.eu
Tel.: +033278 6211
Fax: +033278 5469

JRC Science Hub
https://ec.europa.eu/jrc

JRC 103512

PDF ISBN 978-92-79-63277-8 ISSN 1831-9424 doi:10.2788/933798

EUR 28187 EN

Luxembourg: Publications Office of the European Union, 2016

Abstract
The European energy sector pays great attention to the protection of its large scale energy infrastructure and facilities. Therefore, the European Commission (EC) Directorate-General for Energy has established a dedicated office in order to support information sharing in the domain of incident and threats with particular focus on the cyber domain.

The Incident and Threat Information Sharing - EU Centre (ITIS-EUC) aims to help in this direction by providing open source information on cyber vulnerabilities and incidents that take place at global level in order to support operators in the energy sector to obtain a high level of security.

In the present report we aim to summarize the first half of 2016 in terms of ICS vulnerabilities and threats that may have an impact on the energy sector. We provide a critical view on these vulnerabilities in order to demonstrate their importance for the function of critical systems in the energy sector and the functioning of the critical energy infrastructure in general as well as the trends for the next year and protection measures that can be taken by the operators.

Contents

Glossary

Adware Adware is software that once installed attempts to “flood” the victim with advertisements that appear without his consent (mainly in the browser). It also may be part of a wider malvertising campaign. 8

Attack campaign Attacks that have been continuous for a long period targeting specific industry sectors, use of the same Command and Control (C&C) infrastructures (therefore controlled by the same party), and in many cases utilizing the same code base for the malware used. 14

Attack vector Technical method to accomplish an attack. 19

Buffer Overflow In a Buffer Overflow situation the input to a program is malformed in such a way that the system memory will be overwritten with commands that will give access to the attacker. 3, 4, 8

CERT Computer Emergency Response Teams - CERTs (also Computer Security Incident Response Teams — CSIRTs): Dedicated technical teams with the purpose of helping in the event of a cyber attack with technical expertise and as an entrusted channel to communicate with other involved entities and the authorities. They may be public (government sponsored) or private (offered for hire or operating within an organization or even military). 11, 12

DoS A Denial of Service (DoS) attack aims to disrupt system operation by exploiting errors in the way it handles specialized situations. A DoS usually consists of single specially crafted packets that will exploit networking code errors at the victim, resulting in unexpected software operations (even a complete system halt). The term Denial of Service attack is general and could include cases that result in the physical destruction of the victim systems.. 10, 12, 13

Embedded operating system Some computing devices have dedicated purpose and minimal interaction with the user (e.g. home appliances). These devices also have an operating system (usually set to a minimal working version). This operating system and its software are embedded in the device. It should be noted however that it may be still vulnerable to attacks. 3, 8

Honeypot Honeypots are installations that mimic real information systems with the purpose to lure hackers and study their attack methods. 14

Malware A piece of software with malicious purpose. Malware may have been made to look (and behave) like a legitimate piece of software (that will however also achieve its purposes). It is then called a “Trojan” . 2, 5–8, 12–15, 18

Man-in-the-middle Attacks when the attacker has through various methods managed to divert some or all of a victim’s traffic through its systems. The attacker has then the choice of eavesdropping, modifying or blocking information to the destination. In order to continue this operation and remain undetected the attacker then re-routes the traffic to its legitimate destination. An obvious protection against this attack is cryptography. To achieve full protection however authentication of both communicating parties is also necessary. 12

Operations Technology Operations Technology or *OT* (in contrast to Information Technology or *IT*) refers to the collection of all the (automated) technical equipment that via the coordination of hardware and software accomplices the production goals of the organization at a technical level. In contrast, IT refers to the computing and communication equipment that supports the business side of the organization (which may include aspects of the OT).. 2, 9

Patch a piece of software that when installed in a vulnerable/erroneous system repairs the technical problems without having to reinstall or otherwise change the system. 9, 10, 18

Ransomware Malicious software that once the victim is infected it asks for a ransom to not perform destructive actions. These may include completely wiping the system, or encrypting it with an undisclosed key. In some cases ransomware may threaten legal action (faking the authorities) for alleged illegal actions of the user unless a "fine" is paid. 1, 9, 18

Remote Access Trojan A type of malware offering the attacker the opportunity to remotely access and control a system (such popular software are VNC, Remote Desktop Connection, etc.). 14

Sandbox A Sandbox is a protected environment that can be used to download and execute any potentially malicious content, analyzing its (possibly harmful) operation. 15

TLS Is a protocol used to secure a communication channel and authenticate the communicating parties. Over a TLS channel other types of communications may pass then pass without getting disclosed. Frequent uses of TLS (and SSL before that) are encryption of email channels between servers and connection with e-commerce/e-banking web servers (where server authentication is also important). 4

VPN A Virtual Private Network (VPN) is a separate communication channel set over existing networking infrastructure. Thanks to networking technologies traffic passing over the VPN is completely separated and (n most cases) encrypted. VPNs also offer authentication of the communicating parties. 4, 17, 18

CHAPTER 1

Cyber Security Trends and their implications in ICS
First Half of 2016 Review

1.1 Summary of IT Security developments affecting ICS – First half of 2016

The year 2016 has so far been quite active in the Industrial Control and Critical Infrastructure areas in relation to IT security. The shock of the December 2015 attacks against the Ukrainian electricity distributors has set the tone for the first half of 2016 as state authorities have taken serious steps to learn from these events and prevent similar incidents. In continuation of trends set in the last years we are also seeing a constant flow of new security vulnerabilities appearing in widely used ICS equipment by major manufacturers. In parallel to what happens in specialized industrial systems we have several security developments in the IT world that could ”spill over” to production environments. This has certainly happened in a number of cases where critical infrastructure was adversely affected by general IT security problems:

- The discovery of malware in a German Nuclear plant[1]
- The serious business impact of a Ransomware incident on a US-based water utility (please see below for details)

Other areas of concern in the IT sector have also been:

- The emergence of multiple serious attacks against the Android mobile operating system. (please see below for details)
- Several threats to networking infrastructure: networking equipment, protection (antivirus) platforms, GSM equipment.

This report comprises of the following parts:

a. The current state of threats against IT infrastructure

[1] For additional information on this event, please refer to ITIS-EUC Flash Newsletter of April 27, 2016

We present and attempt to analyze the main events affecting security of infrastructure in the Information Technology (IT) that also has implications in the Operations Technology (OT) world. These are the issues concerning newly discovered problems with established and trusted technologies and communication protocols. They serve to illustrate the current and emerging state of security. Such insights can serve as guidance for operators on their risk assessments and for their protection plans.

b. The main problems with OT equipment and the concerns they are raising

   In the previous months several new security issues have emerged with OT equipment. We attempt to pinpoint the most important of them.

c. The main IT security developments that could also concern industrial production environments

   These include new and continuing Malware threats and new attack techniques of the last six months. This is an indicative list of issues; an effort to highlight the threat environment and how this can affect energy operators.

d. Trends for the second half of 2016

   Based on the information gathered so far as well as the general security picture we try to determine the areas of concern for the near and mid-term future.

e. Protection directions

   In this as in previous reports we conclude with general protection guidelines that can help against current and projected threats.

Note: ITIS-EUC Newsletters referenced provide additional information, vulnerability indexing, links to open sources, etc.

CHAPTER 2

Main Security Events

2.1 Main Security Events

2.1.1 OpenSSH flaws

This has been one of the most serious disclosures of the year 2016, until now. The issue concerns OpenSSH[1], a software running on the majority of Unix installations, including important servers and Embedded operating systems[2], to implement the secure communications protocol SSH. SSH is one of the cornerstones of secure communications over public Internet, used both interactively (by administrators managing remote systems) and as part of automated process.

The two vulnerabilities are due to an undocumented feature in SSH clients, called ”roaming” that is supposed to allow a secure session to continue even after a disruption in communications. Specifically, they are:

(a) Credential stealing. After the client has authenticated on the real server an attacker intercepting their communication (even though he cannot decrypt it) can ask for the keys used for authentication which are left unencrypted at portions of the client memory. The attacker can then gain access to the server.

(b) Buffer Overflow. Under a number of conditions, the attacker can overwrite portions of the client memory that may lead to information stealing, operating system disruption or even remote command execution At the time of the issue announcement (Feb. 2016) it was estimated that about 70% of all installed SSH clients were vulnerable.

[1] For additional details on the OpenSSH flaw, please refer to ITIS-EUC Newsletter Issue 24, of February 2016

[2] ”Embedded operating systems” (or ”appliances”) are devices that offer specialized functionality based upon a computing system operating within. They feature an operating system (usually a ”trimmed down” version of any of the major OSes) upon which applications implementing system functions operate. Even though they do not ”look” like traditional computing systems, as such, they may still suffer from security vulnerabilities.

2.1.2 The DROWN TLS vulnerability

Following in the footsteps of last years' SSL/TLS vulnerabilities[3], the DROWN attack[4] presents yet another problem that has appeared to threaten this technology. TLS (Transport Layer Security), descendant of the SSL (Secure Socket Layer), is a widely used protocol that establishes a secure temporary channel[5] between client and server especially in Web application environments.

Due to its development history TLS/SSL in many cases still supports obsolete, less secure encryption protocols. Using the DROWN vulnerability, an attacker can deliberately lower the grade of encryption, between two parties, to that used in older SSLv2. He can then acquire and decrypt session's encryption key. With this knowledge he can then decrypt the whole communication.

DROWN affects almost all TLS based servers regardless of manufacturer. Furthermore, it is not limited to web communications but can also be used to attack Mail server, Mail client or Secure FTP communications[6].

2.1.3 Linux Glibc programming library vulnerabilities

This is a problem with one of the main Linux programming libraries, glibc, which was discovered in Feb. 2016. The programming library includes a DNS[7] function which is normally used to get the IP address of a host based on its name. An attacker controlled rogue DNS server can "supplement" a valid response with code that will overwrite the memory of the victim Linux system (a Buffer Overflow) leading to remote execution of commands. Glibc is extensively used on Linux systems including several situations where running programs need to perform DNS queries[8].

2.1.4 Quanta Mobile Data Router found vulnerable

The data transfer feature GSM (the mobile phone communication protocol) provides an important capability to Operators to connect to remote equipment even in areas without other telecommunication infrastructure. Weaknesses in GSM equipment therefore can seriously affect the administration of Operator systems installed at remote sites. The Quanta GSM mobile

[3] Characteristically:

- Heartbleed (information leakage), please refer to the ITIS-EUC document: Cyber Security Trends and their implications in ICS: 2014 Review and 2015 Trends, Challenges, and Protection Directions)
- FREAK (SSL/TLS vulnerability – Man in the Middle attack), please refer to ITIS-EUC Newsletter, Issue 8
- Logjam (TLS vulnerability – Man in the Middle attack), please refer to ITIS-EUC Newsletter, Issue 11

[4] For additional details on the DROWN issue, please refer to ITIS-EUC Newsletter Issue 25, of April 2016

[5] Contrary to the more permanent encrypted channel established in the case of Virtual Private Networks (VPNs)

[6] For additional details on the DROWN issue, please refer to ITIS-EUC Newsletter Issue 25, of April 2016

[7] DNS, the Domain Name Service, translates hostnames to IP addresses (that systems use over the Internet) and vise-versa. It is based on servers at various levels in a hierarchy.

[8] For additional details on the Linux Glibc vulnerability, please refer to ITIS-EUC Newsletter Issue 25, of April 2016

data router was found in April 2016 to contain numerous vulnerabilities that could not only disrupt normal communications but even lead their takeover by attackers. Specifically:

- Preconfigured ("hard-coded") SSH protocol keys could allow an eavesdropper listen to supposedly encrypted communications.
- There are backdoors offering various types of (unauthorized) connectivity to the Quanta devices themselves, namely Windows file sharing (Samba), Telnet, and SSH.
- The routers also offer WiFi connectivity with passwords that can easily be guessed
- It's possible to remotely execute code
- The devices are susceptible to Denial of Service attacks that would render them inoperable.
- Updates to the devices take place using expired certificates and hard-coded passwords
- The devices web interface offers backdoors to reveal significant internal information.

An effective protection approach is to implement encryption over any basic connection provided by the mobile network.

2.1.5 Threats to ICS installations by DNS abuses

In June 2016 at an ICS Security conference, a number of ways that the Domain Name Service (DNS) could be used to compromise industrial control installations were presented. Specifically:

- "DNS Squatting", the possibility to misspell DNS addresses can be used to spread Malware either by (a) visiting "the wrong" web sites (either directly at the "wrong" site or by automatically redirecting visitors to other web sites) or (b) by sending emails with misspelled domains to attacker registered domains. Such emails can reveal information about both the sender and the recipient.
- DNS can provide a "channel" for unauthorized communication, even from inside restricted ICS networks, for any installed Malware[9].

2.1.6 The continuing threat against the Android mobile OS

In 2016 so far we have seen an extensive range of attacks against the Android mobile platform. Even though the Android Operating Systems (OS) is mainly being used in mobile phones of various manufacturers, this attack trend is important for two reasons:

1. Operator equipment (especially used for servicing activities e.g. using tablets) may be based on the Android platform and thus be affected.

[9]For additional details on threats to ICS installations by DNS, please refer to ITIS-EUC Newsletter Issue 28, of June 2016

2. The widespread usage of mobile devices running Android makes it possible that such devices (belonging to Operator personnel) may be used to spy on operations or even spread Malware within closed network segments[10].

The most prominent cases of Android OS security problems have been the following:

- In March 2016 Security Researchers of the company Kaspersky Lab reported on a piece of Android Malware, which they characterized as ”the most advanced mobile Malware seen to date”. Called the ”Triada”, it is installed itself by other, advertising, Trojans that have managed to take hold in the device. Operating mainly in memory, therefore difficult to detect by antivirus applications[11], the Triada infects the OS template used to activate applications. It is therefore existent in every application that starts to run after the infection. This approach gives it considerable capabilities to hijack and spy normal device operations (e.g. access and control SMS messages).

  Further Information (simple to more technical)

  Triada Trojan Most Advanced Mobile Malware Yet: Kaspersky

  http://www.securityweek.com/triada-trojan-most-advanced-mobile-malware-yet-kaspersky

  Attack on Zygote: a new twist in the evolution of mobile threats

  https://securelist.com/analysis/publications/74032/attack-on-zygote-a-new-twist-in-the-evolution-of-mobile-threats/

- The ”Marcher” Malware, active since January 2016, operates in stealth mode and activates only when specific web sites (configured beforehand) are accessed by the user. It then can steal credentials or other information. Although it has been developed as a tool to steal banking credentials (its mode of operation allows it to hijack single-sign-on codes too) it’s being offered in underground marketplaces and could very well be utilized in attacks in other enterprises. According to reports in June 2016, its spread is continuously growing.

  Further Information

  Android.Trojan.Marcher

  https://info.phishlabs.com/blog/analyzing-android.trojan.marcher

  Marcher Android Malware Increases its Geographic Reach

  https://info.phishlabs.com/blog/marcher-android-malware-increases-its-geographic-reach

- A serious vulnerability in the Qualcomm mobile processor used in the majority of Android phones and tablets was discovered in May 2016. It allows the bypass of the Secure Execution Environment configured for applications and could potentially lead to remote control of the device. A major concern is that the vulnerability also affects older devices that cannot be patched or upgraded. Furthermore, in the Android phone ”ecosystem” many times the updates are pushed to the devices by mobile operators (wireless carriers) which introduces another factor of delay in the repair.

[10] An “Achilles heel” in closed network environments is the need of personnel to recharge mobile devices. A possible way for this to happen is to connect to computing system USB ports thus exposing them to any Malware in the mobile device.

[11] The Antivirus applications mainly look for known ”signatures” in files existing in a system, when these are executed or opened. Constantly being in memory bypasses this detection mechanism.

Further Information

Android Qualcomm Vulnerability Impacts 60 Percent of Devices

https://threatpost.com/android-qualcomm-vulnerability-impacts-60-percent-of-devices/118191/

- In May 2016 it was discovered that the Chinese chip integrator Allwinner was shipping Android devices with an easy to exploit backdoor. The exploit could also be activated remotely. The problem is a left-over of the internal debugging process of the manufacturer that found its way into production. The important thing in this case is that Allwinner uses Android in several different products including tablets and set-top boxes.

  Further Information

  Kernel Backdoor found in Gadgets Powered by Popular Chinese ARM Maker

  http://thehackernews.com/2016/05/android-kernal-exploit.html

- In March 2016, security researchers had announced that the exploitation of a combination of features in the OS could allow complete control of the victim device. In May 2016 the further advanced their attack making it potentially applicable to the majority (95,4%) of all Android devices. The vulnerability has been called ”Accessibility Clickjacking Exploit”. It is based on the case that a malicious application (without special privileges), e.g. a game, would be running as an overlay on the user's screen while on the background the Android device's Accessibility Services would be activated without the user's knowledge. Thinking he's clicking on the foreground application the user would actually click on the Accessibility Services to give full and privileged access to the attacker. Implications of this attack could lead to downloading and running malicious applications, sending the user's location, or wiping the device. Google (the Android OS manufacturer) has worked since then to limit potential access to the features that can lead to this exploit.

  Further Information

  Scope of Gaping Android Security Hole Grows

  https://threatpost.com/scope-of-gaping-android-security-hole-grows/118161/

- An Android Trojan, dubbed ”Hummer” had been active (and developing) since 2014. By June 30, 2016 it was reported that it had infected more than 1,2 million devices. The Trojan gives the attacker the opportunity to issue commands on the infected devices. Although this is a serious security exposure, the main action of the Malware seems to be the random presentation of advertisements and in some cases the installation and activation of unwanted (or malicious) applications.

  Further Information

  Millions of Android Phones Infected with ”Hummer” Trojan

  http://www.securityweek.com/millions-android-phones-infected-hummer-trojan

General Remediation Measures

The Android OS (as well as Apple's iOS and Microsoft?s Windows Mobile) even though operating in mobile devices should be considered in the context of Enterprise IT system protection. As such, mobile devices (phones, tablets, other) should be:

(a) at high level integrated in the IT protection governance (policies, measures, risk analysis) and

(b) at low level, be protected with strong security controls. As a source of threat the security controls should necessarily extend to devices privately held by the personnel. Specifically, some measures should be:

- All mobile devices with an Enterprise function (e.g. staff communications, handheld software applications etc.) should be indexed and part of an updated inventory that will readily supply information of their manufacturer, OS, software versions, etc. This should include devices that even if not mobile could be using any non-standard OS due to manufacturer's choice[12]
- Mobile devices of any manufacturer must be controlled centrally via an Enterprise Mobile Device Management (MDM). An MDM can restrict the functionality of such devices to the minimum necessary to execute their legitimate purposes. Among other things it can make sure the devices have updated OS, install antivirus, control and filter web sites visited, restrict files downloaded, centrally control software that can be installed, etc.
- Manufacturers to provide mobile devices should be judged by their track record in IT security[13] and be able to fulfil the need for quick dispatch of patches when new security threats arise.
- Users should be restricted from using their own devices for Enterprise operations
- Security awareness programs to inform users on the threats they face in their work as well as their personal life though careless use of mobile devices.
- Policies as well as practical technical controls should prevent users from connecting their own devices to Enterprise equipment.

2.1.7 Serious vulnerability in Symantec antivirus system

In the end of June 2016, Google Project Zero Security researcher team released information that indicated the antivirus manufacturer Symantec had a number of serious flaws in its engine. The main issue has been running "unpackers" (pieces of software required by the antivirus engines in order to "unpack" – decompress – and search into executable code) in the most central part of an Operating System, the kernel. As unpackers are a vulnerable piece of software any successful attack against them would lead to system memory overwriting (Buffer Overflow) and the subsequent control of the OS by an attacker. Unfortunately even though Symantec was notified patches and repair code would not be available before the mid of July 2016.

Further Information

Symantec security flaws are "as bad as it gets", claims Google's Project Zero

http://www.theinquirer.net/inquirer/news/2463219/symantec-security-flaws-are-as-bad-as-it-gets-claims-googles-project-zero

[12] For example, as a flexible Operating System, Android has found several uses in Embedded operating systems.
[13] Unfortunately, there have been cases of manufacturers who (intentionally or not) have provided mobile devices with preinstalled Malware/Adware/unneeded applications ("bloatware")

Symantec admits it won't Patch "catastrophic" security flaws until mid-July

http://www.theinquirer.net/inquirer/news/2464131/symantec-admits-it-wont-patch-catastrophic-security-flaws-until-mid-july

2.1.8 Ransomware and other IT events having an impact in enterprise operations

In a worrying trend, in 2016 so far we have seen a number of cases that IT security events had an impact on service utilities. Even though there have not been any direct effects on Industrial Control Equipment, in one case the IT systems of the company involved were rendered inoperable therefore severely effecting its capability to provide services to customers. The events underline that the IT systems, even when not directly connected to Industrial Control are an integral part of conducting business and any serious disruption will have serious business effects. It should also be pointed that the most serious of the cases highlighted here was a Ransomware attack[14]. Contrary to targeted attacks against infrastructure, ransomware does not require prior detailed knowledge of the architecture and the installed systems. Instead it renders any vulnerable systems inoperable.

The cases have been:

a. On April 25, the Board of Water and Light (BWL) in Lansing, Michigan was hit by a Ransomware attack. As it happens in such cases the affected systems were encrypted and thus rendered unusable. Although there had not been any direct effects on the control infrastructure (the *OT* – Operations Technology – part of the network), the company put all IT in "lockdown" as a precautionary measure to prevent further spread of the attack. It this respect, trying to prevent the attack escalation has the same effect as the attack itself. Another important point is that the attack was the result of a careless employee opening a malicious email. This is yet another example of how an event in the IT part of the Enterprise network can affect the OT segment. Separation between the two is a required security measure.

   Further Information

   Michigan Power and Water Utility Hit by glsRansomware Attack

   http://www.securityweek.com/michigan-power-and-water-utility-hit-ransomware-attack

   Ransomware Virus Shuts Down Electric and Water Utility

   http://thehackernews.com/2016/04/power-ransomware-attack.html

b. A Security Researcher in the end of May 2016 disclosed that a corporate database for the Pacific Gas and Electric (PG&E) utility had been openly exposed to the Internet, possibly providing access to sensitive information. The data contained provided a detailed picture of Enterprise systems and gave out important employee information.

   Further Information

   Database of California Electric Utility Exposed Online

   http://www.securityweek.com/database-california-electric-utility-exposed-online

[14] For an explanation of how a ransomware attack works, please refer to ITIS-EUC Newsletter Issue 6, of March 2015

2.2 Attacks against ICS equipment

2.2.1 Cisco Industrial Switch DoS

On February 15, 2016 Cisco Systems announced that its Industrial Ethernet switches were vulnerable to a Denial of Service (DoS) attack. The issue is due to the incorrect handling of some types of packets of the Cisco Discovery Protocol (CDP). Receiving the attack packets, the switch can reload (reboot) disrupting communications. The problem highlights the need to protect Industrial Equipment with ”traditional” IT measures (an Intrusion Prevention System – IPS – in this case should be able to inspect and control Layer 2 traffic that the attack utilizes) and keep the IT and OT networks separated[15].

2.2.2 Glibc IT vulnerability also affects Siemens ICS platforms

The same Glibc DNS vulnerability affecting Linux systems (referenced above) was disclosed by Siemens, in April 2016, to affect several of its Industrial Control devices. The vendor released Patch code but the seriousness of the case (which could potentially lead to device disabling – DoS – or even remote code execution) is such that operators of the equipment should also consider additional protective measures like filtering DNS queries and answers and operating packet analysis mechanisms and Intrusion Prevention Systems in the Operational network[16].

2.2.3 Vulnerabilities in the Ecava HMI

In May 2016, Security researchers announced that the Ecava HMI was vulnerable to numerous flaws, including:

- Unprotected network communications, vulnerable to eavesdropping.
- Remote code execution due to SQL injection[17]. Also unchecked inputs to the web application.
- Cross-site Scripting[18].
- Unprotected internal information in web pages[19].

[15] For additional details on the Cisco Industrial Switch DoS, please refer to ITIS-EUC Newsletter Issue 25, of April 2016

[16] For additional details on how the Glibc vulnerability affects ICS platforms, please refer to ITIS-EUC Newsletter Issue 26, of May 2016

[17] SQL injection is an attack method which, knowing that queries to a Web application will be handled by a separate system (an SQL database system) embeds database commands in submitted web-forms. If these will be passed unchecked to the database engine they can induce it to execute specific malicious actions on the host system.

[18] Cross-site Scripting or XSS is a web application problem in which the web client visiting a (third party) malicious web site can execute commands on the vulnerable site.

[19] For additional details on the Ecava HMI vulnerability, please refer to ITIS-EUC Newsletter Issue 26, of May 2016

2.2.4 Moxa serial server exhibits a number of serious vulnerabilities

Moxa MiiNePort is a server that offers a front-end to allow remote connections to ICS components that only offer serial interfaces. The server provides a web interface and command line access for remote management. On May 24, 2016, the Moxa devices were found by IT Security researchers to have a number of serious vulnerabilities:

- The device is not protected by any password
- Information kept in the device can be viewed on the device configuration file
- The web interface is vulnerable to Cross-Site Request Forgery (CSRF). In this web attack the server trusts the client and accepts HTTP requests sent by him. An appropriately crafted HTTP request can produce unwanted results on the server. The client is deceived to follow links creating the malicious HTTP request by following links contained in emails or other, specially crafted web sites.

The Moxa servers are widely used in several industries including the energy sector[20].

2.2.5 The Siemens SIPROTEC Protection Relays allow information leakage

In June 2016 ITI Security researchers disclosed that the Siemens SIPROTEC products are vulnerable to leakage of sensitive data. The problem is due to the integrated web server which, when accessed with appropriate request strings can reveal either information stored in the device or portions of the memory contents. The vulnerability could be used in attacks that once they have infiltrated the enterprise network aim to gather and export inspection information that will later allow an attack highly adapted to the environment[21].

2.2.6 Environmental Controls Systems Data Controller 8832 seriously vulnerable, cannot be repaired

This is a SCADA controller, mainly used in the Energy Industry, primarily in the United States. It is offering a web interface, as well as a management platform called StackVision to enable control of its functions. In May 2016, the US ICS-CERT issued an advisory about a number of serious problems in the included web server:

- Authentication bypass: an attacker could possibly gain control to the unit's configuration and modify it
- Privilege escalation: a simple user can, using a series of actions, gain additional rights in the management of the device, therefore controlling its operation.

[20] For additional details on the Moxa serial server vulnerabilities, please refer to ITIS-EUC Newsletter Issue 27, of June 2016

[21] For additional details on the Siemens SIPROTEC vulnerabilities, please refer to ITIS-EUC Newsletter Issue 27, of June 2016

Notably there is no prospect of a security update. The manufacturer had been informed about the problems as early as February 2015 with a full exploit available since May 2015[22].

2.2.7 The Irongate ICS malware

In June 2016, the Security Company FireEye published information on a new piece of Malware that is targeting ICS (SCADA) equipment. The Malware does not actually do any harm but rather may have been developed as a "proof of concept" on the Siemens Step 7 PLC Simulation Environment. The Irongate Malware infects PLC simulation software and monitors internal communication processes with the aim to apply a Man-in-the-middle between them.

Irongate is created in a way that can only affect the Siemens Step 7 PLC Simulation Environment. It is noteworthy that it seems to have been developed in 2012 and still managed to stay undetected inside Malware databases. The researchers have reported that it exists in more than one version[23].

2.2.8 SIMATIC S7-300 PLC DoS vulnerability

In June 2016, it was reported that the Siemens PLCs SIMATIC S7-300 contain a serious DoS vulnerability. The SIMATIC S7-300 uses the proprietary PROFIBUS protocol which operates on TCP port 102. A specially crafted packet on this protocol that will reach the device, can make it pass to an unresponsive state. To return to normal operation a complete restart is required[24].

2.2.9 Siemens SIMATIC WinCC component allows password leakage

An ICS-CERT advisory in June 2016, warned on the possibility of the Siemens SIMATIC WinCC Flexible, an ICS visualization product, not protecting credentials adequately during network communications. It seems that an eavesdropper on the network could potentially analyze captured traffic and from that to deduce system credentials[25].

2.2.10 Siemens SICAM PAS may expose passwords and other pieces of information

In June 2016, there were reports of vulnerabilities in the Siemens SICAM PAS (Power Automation System) ICS automation software. The problems allow an authenticated user to (a) gain

[22] For additional details on this issue, please refer to ITIS-EUC Newsletter Issue 27, of June 2016
[23] For additional details on the Irongate ICS Malware, please refer to ITIS-EUC Newsletter Issue 27, of June 2016
[24] For additional details on the SIMATIC S7-300 PLC DoS vulnerability, please refer to ITIS-EUC Newsletter Issue 28, of June-July 2016
[25] For additional details on the SIMATIC WinCC password leakage, please refer to ITIS-EUC Newsletter Issue 28, of June-July 2016

access to passwords (b) get access to information store in the system's database. The product is widely used to automate electrical substations[26].

2.2.11 Cisco IOS XR remote DoS vulnerability

This is a Denial of Service vulnerability: an attacker sending specially crafted packets could bring the affected devices to a non-operative condition that will require a system restart. The packets that will generate this problem are associated with the protocols of secure communication (Secure Shell – SSH, Secure Copy – SCP, and Secure FTP – SFTP). As these protocols are usually utilized for remote device management it is almost certain they will be available on the device (at least some of them) and will also be considered a normal part of the network traffic[27].

2.2.12 Juniper Web interface is open and offers administrator privileges

Juniper platforms running the company's operating system (JunOS) allow unauthenticated access, via the web management interface. An unauthenticated attacker that will manage to access the device will have the highest (administrator) privileges, enabling him to perform important actions. According to Juniper the problem is due to an "information leak" in the J-Web web server, meaning that requesting special URLs (even when unauthenticated) may reveal enough information to gain access to the interface[28].

2.2.13 Juniper SRX upgrade issue

On Juniper SRX devices, software upgrades to JunOS from version no. 12.1X46-D50 and lower, to version 12.1X46, when performed with a special combination of commands will result in a system status that allows connections with maximum ("root") privileges without password. The connections will be allowed on the text-only interface (Command Line Interface – CLI)[29].

2.2.14 PLC-Blaster: Automatically attacking Programmable Logic Controllers

After March 2016, work has been presented in various Security Conferences indicating the feasibility of automatically attacking Programmable Logic Controllers (PLC). A "worm", automatically propagating Malware, can after it gains a foothold on at least one PLC device, to infect others connected in the same network. It could then either disable them or offer remote control capabilities to an attacker. The researchers have demonstrated the feasibility of a PLC worm

[26] For additional details on the Siemens SICAM PAS vulnerabilities, please refer to ITIS-EUC Newsletter Issue 28, of June-July 2016

[27] For additional details on the Cisco IOS XR remote DoS, please refer to ITIS-EUC Newsletter Issue 29, of July 2016

[28] For additional details on the Juniper Web interface vulnerabilities, please refer to ITIS-EUC Newsletter Issue 29, of July 2016

[29] For additional details on the Juniper SRX upgrade issue, please refer to ITIS-EUC Newsletter Issue 29, of July 2016

and have found that their method could be applied to many widely used devices (they tested it on Siemens Simatic S7-1200 platforms)[30].

2.2.15 Report: Findings of operating a Power Grid Honeypot

In February 2016, the security company Malcrawler announced results of research involving attacks on (simulated) power grids. These findings were the results of operating a Honeypot[31] simulating power grid functions. Their main findings:

- Concerning open wireless access, it was found that all cases of connections were casual, from people seeking free Internet access.
- In the OT environment, it was too complicated for even the best hackers. This is mostly proprietary environments that will be difficult to analyze by attackers
- Malware in the IT section of the network was the most probable threat, the one that ended getting exploited most often[32].

2.3 New IT threats

2.3.1 The Adwind RAT

Adwind is a Remote Access Trojan (Remote Access Trojan)[33] that has been active in various reincarnations probably since 2013. The security company Heimdal reported in July 2016 of newer appearances of the Malware. Adwind is written in the multi-platform programming language Java and can therefore work in a variety of operating systems, including Microsoft Windows, OS X, Linux, even Android devices. According to the researchers, at the time of discovery Adwind was not detectable by any antivirus system, probably due to its continuous development and change to the low intensity of the Attack campaigns in which had been used[34].

2.3.2 Highly advanced espionage malware SFG, Furtim?s Parent

In the beginning of July 2016, the Security Company SentinelOne released details on a new, highly advanced piece of Malware they had analyzed. It demonstrated an extreme degree

[30] For additional details on PLC blaster, please refer to ITIS-EUC Newsletter Issue 26, of May 2016

[31] A honeypot is a collection of computer systems (virtual or real) configured in such a way to simulate a (vulnerable) IT setting. Attackers will get attracted by the opportunity to break in, revealing their methodologies and intentions in the process. Honeypots are both a research tool and a method widely employed by security companies to discover new Malware.

[32] For additional information on the findings of the Power Grid Honeypot, please refer to ITIS-EUC Newsletter Issue 24, of February 2016

[33] Also known as ”Remote Administration Tool”, a RAT is a malicious piece of software that can allow remote access and control of the victim system, not unlike the common Windows Remote Desktop application.

[34] For additional information on the Adwind RAT, please refer to ITIS-EUC Newsletter Issue 28, of June-July 2016

of sophistication against detection systems, usually deployed for IT protection. Among other characteristics:

- It deactivates filter drivers by removing the corresponding registry records. This is the mechanism antivirus platforms use to intercept and inspect any file the operating system is calling, before actually being executed.
- It employs a multitude of checks to ensure that (a) it is not detected by antivirus engines and (b) it is not being analyzed in a "Sandbox".

Analysis details also indicated a direction towards attacking important installations[35].

[35] For additional details on the SFG Malware, please refer to ITIS-EUC Newsletter Issue 29, of July 2016

CHAPTER 3

Prospective Security Trends and Protection Directions for operators

3.1 Prospective IT Security Trends for the second half of 2016

Following on the developments of the first half of 2016, we expect to see the following trends in the next 6-12 months:

- Continuous discovery of vulnerabilities in ICS equipment. Two particularly vulnerable areas associated with manufacturers are:
  - The update/upgrade channels manufacturers use to support existing equipment
  - Their integration of commercial (or open source) ”off-the-self” code in their systems without providing quick reaction and appropriate support when vulnerabilities in this code are disclosed.
- Furthermore, we expect to see a continuation of the trend to attack elements upon which organization communications are based (basic protocols and algorithms, routing or other communication equipment, VPN support systems, etc.)
- We expect that malicious actors will further develop (or may already be using) attack software that tries to avoid detection by limiting its fingerprint, staying mainly in memory, and anticipating the detection environment that will challenge it.
- Finally, it’s a worrying prospect that attackers may use additional types of equipment utilized in the enterprise, including mobile devices.

3.2 Protection Directions for operators

Directions in this section are general in nature, based upon the discussion and analysis that has preceded. For specialized technical measures addressing specific threats, you should refer to the ITIS-EUC Newsletters referenced.

From the security events analyzed above, concerning the IT or the OT worlds, or touching both areas a number of main protection directions emerge:

1. Pay attention to all cases that the Enterprise needs to communicate, especially to remote installations. Several of the protocols, as well as elements of the infrastructure (e.g. GSM modems, Industrial switches, VPN concentrators[1], etc.) upon which we rely to ensure secure and available communications have shown to be vulnerable to attacks. All such communications should be designed in such a way to ensure confidentiality (e.g. by using multiple encryption and protection schemes) and availability (e.g. by having multiple differentiated channels available). It follows that having ensure the two previous communication aspects Integrity will also be ensured.

2. Security developments are rapid and may at any moment affect established technologies (though time-proven until now) or equipment upon which we rely for critical operations. The barrier between IT and OT (when it exists) may delay the spill-over of an attack to the production environment but does not guarantee immunity. It is therefore critical (a) to follow all developments as soon as they appear and (b) be in a position to quickly judge which ones are relative to the organization's infrastructure to undertake remediation as well as protection measures.

3. The IT world offers a multitude of protection technologies. We have seen in the previous six months how these can fail in some cases (e.g. the case of the SFG Malware that goes to extreme measures to avoid detection – please see previously for additional information). Still, a multi-layered approach that will combine "signature-based" protection against known attacks along with "anomaly-based" detection of unusual behavioral patterns offers an effective solution in the majority of cases. Furthermore, since OT areas are not immune from attacks they should also be protected by the same equipment.

4. The example of the US water utility hit by Ransomware (please see previously for details) underlines the fact that even if IT is completely separate from OT (IT Security problems don't affect operations), maintaining an operational enterprise IT infrastructure is critical for the overall business continuity.

Some additional, more specific, measures include:

5. An updated inventory of IT hardware and especially software used in the organization, including information such as manufacturer, versions, uses, systems affected by its security status due to synergies, management processes, upgrade paths (taking into consideration Enterprise operation requirements). This can prove challenging in cases of specialized systems.

6. Operators should undertake a major Patching and upgrade efforts to protect their systems from new vulnerabilities. Issues that should be taken into consideration:

   - Embedded devices that are not readily patchable
   - Software that integrates functionality (even if not its main task) that can introduce additional vulnerabilities

7. Operators should deploy web traffic protection (including tools to check for the "legitimacy" of sites) to filter and restrict access to potentially harmful sites.

[1] The term "VPN concentrator" refers to IT networking equipment that receives Virtual Private Network (VPN) requests from remote locations and based on their access rights establishes a permanent secure channel.

8. To block covert communication channels, connection restrictions should be in place in protected areas (only connections between specific systems and on a need-to basis should be allowed).
9. Operators should through the use of appropriate equipment (e.g. Intrusion Prevention Systems) be in a position to protect by active traffic filtration (”virtual patching”) their systems when manufacturers do not respond quick enough to disclosed vulnerabilities.
10. Any type of equipment used in the enterprise environment (including mobile devices, external storage devices, even device charging mechanisms) can be part of an Attack vector and should therefore be protected appropriately.

European Commission
JRC 103512 EN – Joint Research Centre –**Institute for Protection and Security of the Citizen**

Title: **Cyber Security Trends and their implications in ICS: Mid-year report 2016**

Author(s): Georgios Koutepas, Georgios Giannopoulos, Athina Mitsiara

Luxembourg: Publications Office of the European Union

2016 – 28 pp. – 21.0 x 29.7 cm

LB-NA-28187-EN-N

JRC Mission

As the Commission's in-house science service, the Joint Research Centre's mission is to provide EU policies with independent, evidence-based scientific and technical support throughout the whole policy cycle.

Working in close cooperation with policy Directorates-General, the JRC addresses key societal challenges while stimulating innovation through developing new methods, tools and standards, and sharing its know-how with the Member States, the scientific community and international partners.

Serving society
Stimulating innovation
Supporting legislation

Publications Office

doi:10.2788/933798

ISBN 978-92-79-63277-8