Embedded Web Device Security

Michael Riegler
IT Solutions
RMTec
Baumgartenberg, Austria
michael.riegler@rmtec.at

Johannes Sametinger
Dept. of Information Systems – Software Engineering
Johannes Kepler University
Linz, Austria
johannes.sametinger@jku.at

***Abstract*—Due to the increasing networking of devices and services to the Internet of Things, security requirements are rising. Systems that were previously operated in isolation can be attacked over the Internet today. Industrial control systems often form the core of critical infrastructures. Their vulnerabilities and too lax security management can have fatal consequences. With the help of vulnerability databases and search engines, hackers can get instructions and targets to exploit. Routers, printers, cameras and other devices can be the gateway to the home or corporate network. Cyber criminals can enter sensitive areas through inadequately protected remote access. In a case study of a central water supply control system, we present typical security problems. We show that security vulnerabilities are wide-spread in current embedded web devices and demonstrate that appropriate countermeasures can reduce the attack surface significantly.**

Keywords-web; embedded devices; web security; industrial control systems.

I. Introduction

Embedded devices increasingly include connectivity as a standard feature, putting them at risk to malicious attack if not secured properly. Some device vendors are offering solutions to protect their embedded devices, including anti-malware technology, access control, data encryption, and real-time threat analysis, as well as maintenance, support, and update/patch services [8]. However, there is insufficient awareness of both device manufacturers and their users about the risks that stem from lacking protection. Take medical devices as an example. Today, even heart pacemakers communicate wirelessly. Parameter settings can be sent to the devices, and usage data including alerts are automatically sent to manufacturers and clinics. If not properly secured, these devices are a threat to patients' privacy as well as to their well-being and even life [12]. Users of devices like personal computers, smartphones as well as operators of web servers are typically aware to some extent about the security risks. Security risks of devices that we use more unobtrusively often go unnoticed. Such devices include printers, routers, and cameras [14]. Their use is widespread, they are connected to the Internet, they often provide web interfaces, and they are often unprotected. On the road to a secure Internet of Things (IoT) [3], we will have to do our homework and provide security as needed to all devices.

In this paper, we will describe security issues of what we call embedded web devices, i.e., embedded devices with web access. We will outline the importance of the security of such devices, demonstrate how neglected it is, and also present a case study of a water supply facility. The paper is structured as follows. Section II introduces embedded web devices. In Section III, we outline security aspects. Risks to industrial control systems are described in Section IV. Section V explains how vulnerable web devices can be found on the Internet. A case study is given in Section VI. Related work and a conclusion follow in Sections VII and VIII, respectively.

II. Embedded Web Devices

The Internet has started as a DARPA project, interconnecting computers through which everyone could quickly access data and programs from any site. Today's Internet provides access to a plethora of information from not just computers – back then only mainframes were available – but from devices like smartphones, and television sets. Additionally, access is not limited to other computers but is increasingly available to other devices like printers, routers or webcams. Web devices are any devices that are connected to the Internet via the Hypertext Transfer Protocol (HTTP) protocol, including web servers, personal computers and smartphones. Embedded web devices are with a different focus than just providing and retrieving information on the web. We have already mentioned printers, routers, and webcams. Additional examples include network devices, sensors in smart homes, smart meters in smart grids, smart TVs, etc.

A. *Embedded Web Servers*

Web servers are running on a combination of hardware and software. They deliver web content to be accessed through the Internet. Embedded web servers are components of systems that, like web servers, communicate via the HTTP protocol. Typically, they provide a thin client interface for traditional applications. Lightweight web servers work with small resources and are often used in embedded systems. Examples include Barracuda [41], Mongoose [26], Appweb [2], and RomPager [33]. Embedded web servers are used for special purpose and are not as extensive as major web servers like Apache [1] and Microsoft's IIS [25].

Embedded web servers are important for the IoT. Today computers and the Internet are almost completely dependent on humans for information. Radio-frequency Identification (RFID) and sensor technology enable computers to observe and identify the world without the limitations of data entered by humans [3]. IoT refers to uniquely identifiable objects, e.g., sensors having an Internet Protocol (IP) address, and their virtual representations in the Internet.

B. ICS – Industrial Control Systems

The term Industrial Control System (ICS) encompasses several types of control systems that are used in industrial production. Examples are Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and Programmable Logic Controllers (PLC). ICSs are instrumental in the production of goods and in the provision of essential services, e.g., to monitor and control processes like gas and electricity distribution or water treatment. The largest group of ICS is SCADA. For example, all nine Austrian Danube power plants are controlled centrally from Vienna. The stations are connected with optical fibers to the central control room and cannot easily be accessed over the Internet [42].

C. CPS – Cyber Physical Systems

Embedded systems contain computer systems with dedicated functions within larger mechanical or electrical systems, often having real-time computing constraints [13]. In Cyber Physical Systems (CPS) computational elements collaborate to control physical entities. CPSs have a tight integration of cyber objects and physical objects. They can be systems at various scales, e.g., large smart bridges with fluctuation detection and responding functions, autonomous cars, and tiny implanted medical devices [15].

III. Security

Security is about protecting information and information systems, including embedded devices, from unauthorized access and use. The core goals are to retain confidentiality, integrity and availability of information. Often used terms include IT security, network security, computer security, web security, mobile security, and software security. They describe different, but sometimes overlapping aspects of reaching the above mentioned core goals. For example, software security is "the idea of engineering software so that it continues to function correctly under malicious attack" [23], while network security involves the isolation and protection of assets via firewalls, demilitarized zones and intrusion detection systems.

A. Threats, Vulnerabilities, Risks

Threats refer to sources and means of particular types of attacks. Vulnerabilities are security bugs or flaws in a system that allow successful attacks. A security risk is the likelihood of being targeted by a threat. The most important potential threats to be addressed can be determined with a risk assessment. We can assess risks by enumerating the most critical and most likely threats, by evaluating their levels of risk as a function of the probability of a threat and the associated cost if the threat becomes true. Secure devices have to continue to function correctly even if under malicious attack. Vulnerabilities are mistakes in devices, typically in software, which can be directly used to gain access to the device. They pose a threat to the device itself, to the information it contains, to other devices it communicates with, and to the environment that it manipulates.

TABLE II. Security Goals in IT and ICS systems

Priority	IT system	ICS system
1	Confidentiality	Availability
2	Integrity	Integrity
3	Availability	Confidentiality

B. ICS Security

ICSs are often found in critical infrastructures, thus have a high need for security. A typical information network will prioritize its security objectives as CIA, i.e., first confidentiality and integrity, and then availability. Industrial control systems often have a high need for availability, reversing the security objectives for most control entities [8]. Table 1 shows these different security goals.

There are other crucial differences that have an influence on the security of these systems. Table 2 summarizes some of these differences. For example, ICSs are usually real-time systems, whereas in IT systems delays are acceptable most of the time. Also, an ICS has to run continuously and cannot simply be rebooted. More details are given by Stouffer et al. [36].

According to a security survey, 70% of SCADA system operators consider the risks to their systems to be high to severe, and 33% suspect they may have had incidents [21]. While IT security is not entirely different from ICS security, there are several differences; see [22]:

- ICS security failures often have physical consequences, thus having more severe and immediate impact.
- ICS security failures can easily and wrongly be interpreted as traditional maintenance failures, making them more difficult to diagnose and remedy.

Security management of an ICS is often much more difficult than of a regular IT system. They more often rely on

TABLE I. Differences between typical IT and ICS systems

Category	IT system	ICS system
Performance	Delay acceptable	Real-time
Availability	Reboot acceptable	24 x 7 x 365
Risk	Data confidentiality	Human safety
Interaction	Less critical	Critical
System	Standard OS	Proprietary OS
Resources	Sufficient	Limited
Lifetime	3-5 years	5-20 years
Support	Diversified	Single vendor
Location	Local, easy accessible	Remote, isolated
Virus protection	Standard	Complex

old systems that cannot be patched or upgraded any more. They often do not have a suitable testing environment. They also often require frequent remote access with commands that must not be blocked for safety or production issues [22].

IV. RISKS

Today, many systems are connected to the Internet, even though they were not originally intended for that purpose. Additionally, it has been shown that even systems without any connection to the outside world can be at risk [35]. This can be done by implanting tiny transceivers on hardware parts like USB plugs or small circuit boards in a device.

A. Software Bugs

Prominent software security bugs include buffer overflows, SQL injections and cross-site scripting. They can be exploited in any connected device, embedded or not. There are many examples, where these bugs have occurred and caused damage. While security bugs are problems at the implementation level, security flaws are located at the architecture or design level. A list of the most widespread and critical errors that can lead to serious vulnerabilities in software is presented in [39]. These errors are often easy to find, easy to exploit and often dangerous. In many cases, they allow attackers to steal and modify data, as well as to run arbitrary code on the attacked machine. The Open Web Application Security Project (OWASP) is a not-for-profit organization focused on improving the security of software. They regularly publish a list with the top 10 security bugs with the goal to raise security awareness [40].

B. Back Doors

Reverse engineering of firmware often reveals back doors to devices. Developers often have implemented hard coded user names and passwords for debugging and maintenance purposes. For example, two supposedly hidden user accounts are in the Sitecom WLM-3500 router. The manufacturer has released a new version of the firmware where these accounts were disabled, but thousands with the old version are still accessible via the Internet [30]. Other network devices like webcams or printers often suffer from similar problems. These devices are usually used for years without getting too much attention from their owners. But they can provide an ideal entry for malicious attackers. For example, thousands of webcams have been shown to be accessible via back doors at the Black Hat 2013 conference [14].

C. Configurations

Insecure default configurations make it easier for cyber criminals to enter systems. Default passwords are publicly known and are published on websites like [7][41].

Default running services like Universal Plug and Play (UPnP) are often unused and increase the risk of an attack. Google Hacking and Shodan simplify the search for such insecure systems; see Section 5. With the mobile exploitation framework Routerpwn [34] it is possible to get access to routers, switches and access points from over 30 manufacturers. The 150+ provided exploits could be executed over the browser locally and remote over the Internet. Predefined access keys especially for the wireless network can be discovered when the calculation methods are known.

D. Other Risks

Automatic update functions, as we know them from desktop operating systems, are not the general rule for ICSs. Firmware manufacturers usually take their time with the provision of updates. The fact that such updates are often provided for free apparently does not motivate to more frequent updates. Sometimes, updates are not even provided at all. But even if updates are available, private customers may not know about them or may simply not have any interest in installing them. Professional users may refrain from updates when they cannot be performed without shutting down the system. Updating a system can lead to crashes or may need reconfigurations of parts or even the entire system. System crashes can disrupt or paralyze business operations. In addition to technical risks, legal risks may also be involved.

Attacks can be a problem for managers. Insufficient security management can lead to personal responsibility. The company may use their staff or service providers to reach the security goals. However, the final responsibility remains with the company. Unsecured or poorly secured home networks have already led to court proceedings. In case of damage, device misconfiguration and insufficient secured smart home solutions can result in problems with the insurance.

E. Countermeasures

Measures for enhanced security are manifold and have to be taken at various levels. Measures at the technical level include software security, encrypted communication, authentication, authorization as well as firewalls and demilitarized zones. At the organizational level, example countermeasures include password management, patch and update management, backup, and security awareness. Requirements for establishing, implementing, maintaining and continuously improving an Information Security Management System (ISMS) are given in the International Organization for Standardization (ISO) 27000 standard. The ISO 27000 series of standards have been reserved for information security matters [38]. ISO 27000 certification demonstrates an organization's ability to provide information assurance services utilizing best practice processes and methodologies.

V. SEARCHING FOR VULNERABLE WEB DEVICES

Search engines are not only used for information search, they are also used to discover embedded web devices and data that were not meant for the public. Cyber criminals use this for victim search and attack preparation, because many of these devices provide sensitive information. The Google and Shodan search engines provide plenty of information that is useful for attackers.

A. Google Hacking

Johnny Long, a pioneer in the field of Google Hacking, has used Google to find security holes from websites and everything else on the web. Advanced search operators can be used to find passwords, internal price lists, confidential documents, as well as vulnerable systems. Hacker groups like *LulzSec* and *Anonymous* have used special search queries to break into foreign systems [5]. For example, the following search term can be used to find authentication data for Virtual Private Networks (VPN).

! Host=*.* intext:enc_UserPassword=* ext:pcf

The shown example works in a similar way with other search engines like Bing or Yahoo. These special searches are called Google Dorks and are collected in the Google Hacking Database; see [9]. The database has grown to include several thousand entries. The National Security Agency (NSA) has also been using special search operators for their Internet research. A previously confidential guide with over 640 pages has been published by the NSA [28].

B. Shodan Hacking

Shodan is a search engine that is specialized to find online devices like webcams, routers and printers, as well as industrial control systems from power plants, which are connected to the Internet. Even nuclear power plants can be found with Shodan [11]. The following search term provides industrial control system from Siemens in the United States.

"Simatic+S7" country:US

The Stuxnet worm had targeted these systems in Iran. Searching for webcams with Shodan is quite popular. For example, a search for “netcam” results in thousands of hits to TRENDnet webcams with a backdoor to access the video stream.

C. Exploits and Vulnerabilities

Besides the search for vulnerable web devices, it is also possible to search for their exploits and vulnerabilities. Many websites like the Exploit Database [10], Metasploit [24], Packet Storm [29], and others provide information, tools and sample code to exploit web devices. For example, the Exploit Database provides 20,000+ exploits for a variety of programs and systems. New entries are added almost daily. The global web application vulnerability search engine PunkSPIDER [32] scans websites for vulnerabilities and provides this highly sensitive information for the public. Script kiddies can use this information to attack computer systems and networks or to hack websites.

VI. Case Study: Water Supply Facility

Water supply facilities are used to take countermeasures to the variability and intensity of rainfall and to guarantee water supply for a specific geographic region like a town or city. To ensure water supply, water from wells or rainfall is pumped into big containers that make sure that water is available during dry seasons. Maintenance of a water supply facility includes checking of water levels, proper working of water pumps, checking for existing leaks. Recently, computerization has helped to automate these processes. The following case study deals with facilities that ensure water supply for several thousand people in a small community. We have developed a monitoring and control system that allows administrators to access all water supply facilities, to access remote cameras at these sites, and to turn on/off pumps. Additionally, various sensors have been installed at the remote sites. For example, if a door is opened or water is raising or falling above or below a predefined level, then an alarm will be raised by sending an email or text message to the administrators. Administrators may then check the status of facilities remotely by turning on video cameras, and make corrections by turning on/off pumps, etc.

We will depict the general architecture of the facility, and show threats due to computerization as well as countermeasures that were actually taken.

A. Architecture

Several water supply facilities are connected over the Internet to a control server. The control server provides a web interface that allows all systems to be monitored and controlled centrally. Figure 1 shows the general architecture of the system. Each water supply facility includes a control system that controls several pumps in the facility. Additionally, webcams are used to allow users to inspect the facility and also to read several gauges analogously. Features of the system include turning on/off pumps, defining on/off times for pumps, turning on/off lights, and choosing among various predefined operation modes.

B. Implementation Aspects

At each water supply location there is a PLC called Loxone mini server [20], called control system in Figure 1. Every mini server has an embedded web server with an interface to control connected pumps through HTTP requests, thus, allowing pumps to operate centrally from the control server. The mini servers monitor their area and send operational states to the control server. They also transmit statistical data for further evaluations. In addition to the mini servers, webcams, i.e., INSTAR IP cameras [16] have been installed at some locations. Because these cameras can be controlled through their web interface, they are also integrated in the

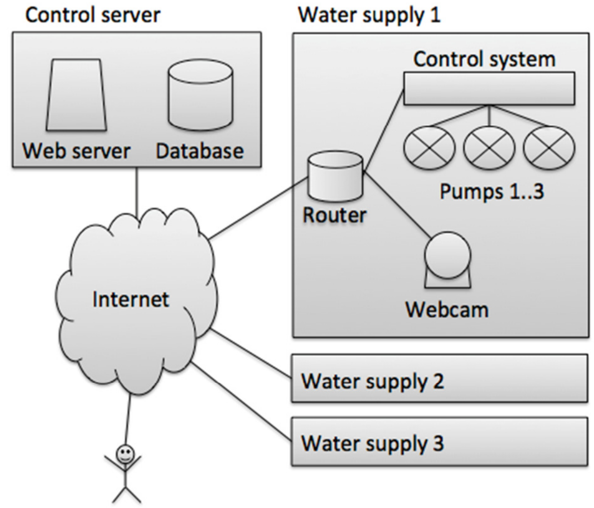

Figure 1. Architectural overview

central web interface of the control server. Thus, the mini server and the IP cameras can receive commands over the Internet. The routers at the water supply facilities use port forwarding. As the routers have no fixed IP addresses assigned, communication is based on domain names. Dynamic Domain Name Service (DDNS) is used to react to changed IP addresses.

On the server side there is a user interface for the central control and a web interface to receive data from the facilities. Both the user interface and the web interface have been programmed with PHP: Hypertext Preprocessor (PHP) [31] and use a MySQL database [27]. Data received from the facilities is checked for plausibility and then stored in the database. jQuery mobile [18] is used to create a user-friendly interface for various devices. Charts are generated with the JavaScript library d3.js [6].

C. Threats

Both the Loxone mini server and the cameras provide sensitive information in their service banner without authentication. Additionally, the firmware version of the mini server is revealed. The cameras provide even more sensitive information like device ID, firmware, etc., with the simple link http://ip-camera/get_status.cgi. Because the mentioned systems use unencrypted protocols like HTTP and File Transfer Protocol (FTP) for communication, the submitted credentials can easily be read through man-in-the-middle attacks. As systems are accessible via the Internet, they can also become victims of denial of service attacks. This can disrupt the water supply. Bugs in software and in firmware of the used components and backdoors can lead to dangerous situations. Outdated software and firmware versions increase the risk. If cyber criminals enter a system, they can manipulate values and settings. This could cause hidden error messages or simulated defects. Moreover, safety mechanisms could be overridden and endanger persons. If the IP cameras are deactivated it is no longer possible to monitor the physical access to the facility. Turning off the pumps can paralyze water supply. Repeatedly switching the pumps on and off within short periods of time can destroy them. When all pumps are at full power, the pressure in the lines can increase to a level so that they could burst.

D. Countermeasures

Because it is not possible with the current firmware of the devices to hide sensitive information and use secure protocols and services, the access through port forwarding on the router is only allowed for stored IP addresses as those from the control server. Thereby, access for Shodan, Google and others is denied. It is interesting to note that a Shodan search results in more 10,000+ Loxone systems. The used webcam can be found 700,000+ times.

The access to the web interface of the central control server is protected with digest authentication and blocks IP addresses after a certain number of incorrect login attempts. Furthermore, HTTP Secure (HTTPS) is used for an encrypted data communication between the control server and the clients. For further analyzes every user activity is logged.

An additional countermeasure is the secure data communication over the Internet with VPNs. VPN requires authentication and provides encryption, so that data is transmitted through a secure channel between a facility and the control server. Thus, insecure protocols like HTTP and FTP can be secured, and man-in-the-middle attacks can be prevented. The most important measure is to increase security awareness of users. Each technical measure is useless if users are careless. Passwords on post-it notes, insecure storage of access devices and evil apps can cause problems. Therefore, it is important to train users.

VII. Related Work

ISE researchers discovered critical security vulnerabilities in numerous routers for small offices and small home offices as well as in wireless access points. The found vulnerabilities allowed remote attackers to take full control of the device's configuration settings. Some even allowed a direct authentication bypass. Attackers were able to intercept and modify network traffic as it entered and left the network [17]. The authors reported that the rich service and feature sets implemented in these routers, e.g., Server Message Block (SMB), Network Basic Input/Output System (NetBIOS), HTTP(S), FTP, UPnP, Telnet, come at a significant cost to security. The incorporation of additional services typically exposes additional attack surfaces that malicious adversaries can use to gain a foothold in a victim's network.

Leverett examined results over two years through the Shodan search engine [19]. He located, identified and categorized more than 7500 such devices, i.e., Heating, Ventilation, and Air Conditioning (HVAC) systems, building management systems, meters, and other industrial control devices or SCADA servers. He concluded that combined with information from exploit databases, remote attacks on selected devices could be carried out or networks could be identified for further reconnaissance and exploitation.

A recent analysis of a widespread compromise of routers for small offices and home offices has been reported in [37]. Attackers were altering the device's Domain Name Service (DNS) configurations in order to redirect DNS requests of their victims to IP addresses and domains controlled by the attackers.

VIII. Conclusion

Embedded devices increasingly get connected to the Internet. If not properly secured, they are at risk to malicious attack. Malicious users find tempting targets across various markets, including consumer electronics, automobiles, medical equipment, and even military hardware. We have taken a closer look at devices that are accessible through the Internet today, but that are often not secured properly. We have also shown in a small case study that these devices, if unsecured, can pose a threat not just to the privacy of individuals and organizations, but also to the proper functioning of critical infrastructure. Appropriate countermeasures can considerably increase an attacker's effort needed to compromise a system with reasonable expenses on the defender's side.

REFERENCES

[1] Apache HTTP Server Project, http://httpd.apache.org. [retrieved: September, 2014]

[2] App-web, http://appwebserver.org/. [retrieved: September, 2014]

[3] K. Ashton, “That 'Internet of Things' Thing”, FRiD Journal, Jun 22, 2009. http://www.rfidjournal.com/articles/view?4986 [retrieved: September, 2014]

[4] Barracuda Web Server, https://realtimelogic.com/products/ barracuda-web-server/. [retrieved: September, 2014]

[5] F. Brown and R. Ragan, “Pulp Google Hacking: The Next Generation Search Engine Hacking Arsenal”, Black Hat 2011. https://media. blackhat.com/bh-us-11/Brown/BH_US_11 _BrownRagan_Pulp_Google.pdf [retrieved: September, 2014]

[6] D3.js - Data-Driven Documents, http://d3js.org. [retrieved: September, 2014]

[7] DefaultPassword, http://default-password.info. [retrieved: September, 2014]

[8] DHS, “Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-in-Depth”, Department of Homeland Security, Control Systems Security Program, National Cyber Security Division, October 2009. http://ics-cert.us-cert.gov/ sites/default/files/recommended_practices/ Defense_in_Depth_Oct09.pdf [retrieved: September, 2014]

[9] Exploit Database, “Google Hacking-Database”, http://exploit-db.com/ google-dorks. [retrieved: September, 2014]

[10] Exploit Database, http://www.exploit-db.com. [retrieved: September, 2014]

[11] D. Goldman, “Shodan: The scariest search engine on the Internet”, CNNMoney. April 2013. http://money.cnn.com/2013/04/08/ technology/security/shodan/index.html. [retrieved: September, 2014]

[12] D. Halperin, T. S. Heydt-Benjamin, K. Fu, T. Kohno, and W. H. Maisel, “Security and privacy for implantable medical devices”, IEEE Pervasive Computing, Special Issue on Implantable Electronics, January 2008.

[13] S. Heath, “Embedded systems design”, EDN series for design engineers, (2 ed.). Newnes, 2nd edition, ISBN 978-0-7506-5546-0, 2003.

[14] C. Heffner, “Exploiting Surveillance Cameras - Like a Hollywood Hacker”, Black Hat, July 2013. https://media.blackhat.com/us-13/US-13-Heffner-Exploiting-Network-Surveillance-Cameras-Like-A-Hollywood-Hacker-Slides.pdf [retrieved: September, 2014]

[15] F. Hu, Cyber-Physical Systems: Integrated Computing and Engineering Design, CRC Press, ISBN 978-1466577008, 2013.

[16] INSTAR IP cameras, http://instar.com. [retrieved: September, 2014]

[17] ISE – Independent Security Evaluators, “Exploiting SOHO Router Services”, Technical Report, July 2013. http://securityevaluators.com/ content/case-studies/routers/soho_techreport.pdf [retrieved: September, 2014]

[18] jQuery mobile, http://jquerymobile.com. [retrieved: September, 2014]

[19] E. P. Leverett, ”Quantitatively Assessing and Visualising Industrial System Attack Surfaces”, University of Cambridge, PhD Thesis, 2011. http://www.cl.cam.ac.uk/~fms27/papers/2011-Leverett-industrial.pdf [retrieved: September, 2014]

[20] Loxone Home Automation, http://www.loxone.com. [retrieved: September, 2014]

[21] M. E. Luallen, “SANS SCADA and Process Control Security Survey”, A SANS Whitepaper, February 2013. http://www.sans.org/ reading-room/analysts-program/sans-survey-scada-2013. [retrieved: September, 2014]

[22] T. Macaulay and B. L. Singer, “Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS”, Auerbach Publications, ISBN 978-1439801963, 2011.

[23] G. McGraw, “Software Security”, IEEE Security & Privacy, vol. 2, no. 2, pp. 80-83, March-April 2004.

[24] Metasploit, http://www.metasploit.com. [retrieved: September, 2014]

[25] Microsoft Internet Information Services, http://www.iis.net. [retrieved: September, 2014]

[26] Mongoose – easy to use web server, http://code.google.com/ p/mongoose. [retrieved: September, 2014]

[27] MySQL, http://www.mysql.com. [retrieved: September, 2014]

[28] NSA, “Untangling the Web-A Guide To Internet Research”, National Security Agency, 2007, released in 2013. http://www.nsa.gov/ public_info/files/Untangling_the_Web.pdf. [retrieved: September, 2014]

[29] Packet Storm, http://packetstormsecurity.com. [retrieved: September, 2014]

[30] R. Paleari, “Sitecom WLM-3500 back-door accounts”. Emaze Networks S.p.A., 2013, http://blog.emaze.net/2013/04/ sitecom-wlm-3500-backdoor-accounts.html. [retrieved: September, 2014]

[31] PHP: Hypertext Preprocessor, http://php.net. [retrieved: September, 2014]

[32] PunkSPIDER, http://punkspider.hyperiongray.com. [retrieved: September, 2014]

[33] RomPager Embedded Web Server, http://allegrosoft.com/ embedded-web-server. [retrieved: September, 2014]

[34] Routerpwn, http://routerpwn.com. [retrieved: September, 2014]

[35] D. E. Sanger and T. Shanker, “N.S.A. Devises Radio Path-way Into Computers”, The New York Times, Jan. 14, 2014. http://www.nytimes.com/2014/01/15/us/nsa-effort-pries-open-computers-not-connected-to-internet.html. [retrieved: September, 2014]

[36] K. Stouffer, J. Falco, and K. Scarfone, “Guide to Industrial Control Systems (ICS) Security”, NIST Special Publication 800-82, Revision 1, May 2013. http://csrc.nist.gov/publications/nistpubs/800-82/ SP800-82-final.pdf. [retrieved: September, 2014]

[37] Team Cymru, “SOHO Pharming: The Growing Exploitation of Small Office Routers Creating Serious Risk”, Whitepaper, February 2014. https://www.team-cymru.com/ReadingRoom/Whitepapers/2013/ TeamCymruSOHOPharming.pdf. [retrieved: September, 2014]

[38] The ISO 27000 Directory, http://www.27000.org. [retrieved: September, 2014]

[39] The MITRE Corporation, “2011 CWE/SANS Top 25 Most Dangerous Software Errors”, 2011. http://cwe.mitre.org/top25/. [retrieved: September, 2014]

[40] The Open Web Application Security Project, “OWASP Top Ten - 2013 – The Ten Most Critical Web Application Security Risks”, 2013. https://owasp.org/index.php/Top_10#OWASP_Top_10_for 20 13. [retrieved: September, 2014]

[41] Unknown Password, http://unknownpassword.com. [retrieved: September, 2014]

Verbund AG, “Freudenau Power Plant to Become the Danube's Central Nervous System”, Press Release, July 2011. http://verbund.com/ cc/en/news-media/news/2011/07/07/freudenau. [retrieved: September, 2014]