Assessment of Information Security Vulnerabilities in Common Seismological Equipment

Michael Samios*[1], Christos P. Evangelidis[1], and Emmanouil Serrelis[2]

Abstract

Modern seismic and Global Navigation Satellite Systems stations are nowadays equipped with Internet of Things devices that acquire, process, and transmit various geophysical parameters in near-real time.

This technological advance has introduced a new threat paradigm for common seismological devices. Such threats can be assessed with standard information security methods and practices.

This article aims to identify security weaknesses, describe weak security points and potential attacks on such environments, and anticipate the countermeasures needed.

Real tests and attacks have been applied to demonstrate the lack of data encryption and user authentication processes, the risks posed by unencrypted communication protocols, unsafe practices regarding settings and passwords, and poor design implementations.

All these factors may impact and possibly disrupt the daily operation of seismic observatories because they can lead to falsifying data, altering configurations, or producing malicious false alarms. These in turn may cause unnecessary public concern or distrust, financial losses, or even national security issues. For all these reasons, several countermeasures and solutions are also proposed and evaluated to address each of the identified vulnerabilities.

Cite this article as Samios, M., C. P. Evangelidis, and E. Serrelis (2021). Assessment of Information Security Vulnerabilities in Common Seismological Equipment, *Seismol. Res. Lett.* **92**, 933–940, doi: 10.1785/0220200151.

Supplemental Material

Introduction

Seismological devices are specialized high-tech and costly instruments that are used for highly accurate recordings of ground or structure vibrations. Their mode of operation, as typical Internet of Things (IoT) devices, poses a high risk to their safety and security, concerning the availability, integrity, and confidentiality of the devices themselves along with their produced and transmitted measurements. The potential impact of malicious third-party actions on these devices can be very serious, as recognized by several sources such as European Union Council (2008), Fisher and Lehnhoff (2018), and Dehling *et al.* (2019).

The alteration and unavailability of measurements may lead to missed or false actions by the competent actors, which could immediately endanger human lives or the security of buildings and structures. In this study, seismological instruments are recognized as IoT devices and their level of security is examined from the point of view of information security discipline. In this context, tests have been designed and implemented to detect any vulnerabilities in the secure operation and connectivity of seismological devices. More specifically, these tests include cyberattacks that threaten the three basic principles of information technology (IT) security such as the availability, confidentiality, and integrity of the data that these devices produce and communicate through the network.

IoT Ecosystem

During the past decade, there was a rapid evolution in microelectronics and computer communication technologies, which was extended beyond the purely computational systems to the realm of "Things" or data-producing objects (devices, instruments, etc.) that until now have been manufactured to operate individually and only after manual extraction of their generated data. Through this evolution, many locally networked devices have transformed into the modern IoT (Raman and Raj, 2017).

An electronic–mechanical device is considered as an IoT device if it can connect to a network or to another networked device and communicate by transferring data, controlling

1. Institute of Geodynamics, National Observatory of Athens, Athens, Greece;
2. Metropolitan College, Amaroussio, Greece

*Corresponding author: msamios@noa.gr; samios@netcover.gr

commands and monitor physical, mechanical, or biological properties (Russell and Van Duren, 2016). This way, IoT devices provide innovative and complex services in almost all sectors of human activity (transport, healthcare, security services, energy, government services, etc.). This has led to an exponentially growing demand for new IoT devices, as well as to a need of upgrading existing devices to fully networked IoT devices. An indicative prediction of the IoT market size has been made by Gartner Research, which states that the number of internet-connected IoT devices will grow to 20 billion in 2020 (Hung, 2017). Several researchers introduce related equipment and concepts, such as the "Internet of Geophysical Things devices" (Sepulveda and Pulliam, 2016) and "IoT remote lab for seismic monitoring" (Guerra *et al.*, 2017), which expand the general IoT trend to seismology as well.

IoT Ecosystem Security Issues

The IoT ecosystem operation is based on a heterogeneous mix of technologies required to interact, such as customized hardware, operating systems, firmware, and communication protocols. The trustworthy, reliable, and secure operation of this IoT ecosystem is a serious challenge for the IT community as noted by several sources, such as Zhang *et al.* (2014). In many application domains, the safe operation of an IoT device and the security of the produced and transferred data are more critical than the secure operation of established standalone computing devices (and their corresponding data), because the nature of operation of the IoT devices implies interaction with the physical world and directly affects human life and activities.

This has been demonstrated in many verified cyberattacks on IoT systems, which also had serious implications. As an example from 2016, the Mirai virus (Antonakakis *et al.*, 2017) was designed to take over IoT devices (cameras, routers, etc.) that were connected to the internet with the default manufacturer security codes. This virus allowed the capture of multiple IoT devices and the creation of remote-controlled bots, along with the execution of distributed denial-of-service (DDOS) attacks in many organizations and companies. A few months earlier, in 2015, a cyberattack against a car managed to take full control of the vehicle by gaining access to its systems through its parking assistance device (Miller and Valasek, 2015).

It is, therefore, becoming evident that the operation and use of IoT devices must be assured in both physical safety and electronic security terms. This assurance includes various aspects and related threats that need to be taken into account (Enisa, 2017):

- Physical security of the devices: Devices are typically installed in remote locations and are threatened by unauthorized physical access by malicious individuals who could intervene with the devices' proper operation.
- Security updates: New weaknesses (software or hardware related) are continuously become public, so to cover the detected security weaknesses, equipment vendors produce new software or firmware patches and releases, which, in many cases, cannot be applied to the IoT devices for practical reasons (e.g., remote installation, limited testing, and service disruption).
- Authentication to the devices: Devices are threatened by attacks to the automatic authentication procedures between IoT devices through machine-to-machine communication, which could allow access to the devices by malicious third parties.
- Data encryption processes: Data stored or communicated by these devices could be altered or disclosed due to inadequate encryption mechanisms, which are related to the usage, generation, and storing of the related encryption keys and digital certificates.
- Security of Application Programming Interfaces (APIs) that IoTs incorporate: Weaknesses are also revealed and exploited through the usage of the numerous APIs installed in IoT devices by the manufacturers, although these APIs aim to provide access and control methods of the devices data, typically without embedding strong security controls.
- Availability of IoT resources: The use of embedded advanced security systems may not be feasible due to limited system resources (e.g., central processing unit, random access memory, and network bandwidth), leaving the devices unprotected from several threats.
- IoT ecosystem complexity: The IoT ecosystem may not be consisted of a set of standard independent standalone devices, but it is usually a complex and broad set of interoperating devices, communications, interfaces, and people. This fact introduces complexity, which makes the devices management harder.
- Device programming: Rapid product deployment and marketing pressures along with low production costs usually lead to a reduction in efforts to develop security from a software development perspective, typically focusing on functionality.
- Cost of IoTs: The relatively low cost of IoT devices has an impact on the implementation of security measures. Manufacturers are prepared to reduce safety features to keep costs low.
- Expertise level: Extensive use of IoT devices is a relatively new domain and therefore there is a shortage of people with the appropriate skills and expertise in IoT devices security.

Security Assessment Methodology

This investigation has focused on performing security assessment in a way that could simulate potential real-world attacks on IoT devices at the basic information security properties: availability, confidentiality, and integrity (Cabric, 2015), although exploiting other complementary information security

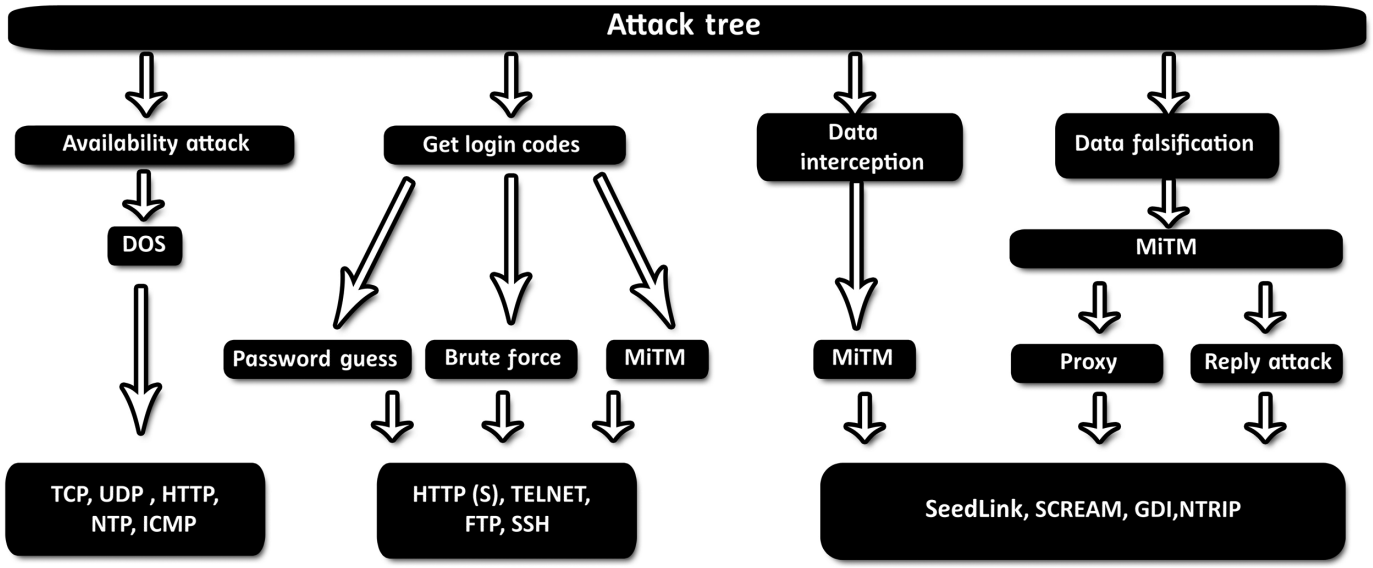

Figure 1. Theoretical security attack tree (as in attack methodology—Schneier, 1999) of a seismological Internet of Things (IoT) device, with possible attack vectors and techniques. DOS, denial of service; FTP, file transfer protocol; HTTP, hypertext transfer protocol; ICMP, internet control message protocol; MiTM, man in the middle; NTP, network time protocol; UDP, user datagram protocol.

requirements as well, such as reliability, nonrepudiation, and authenticity. To demonstrate the feasibility of such attacks and analyze the potential threats, the first three of the five steps of a typical ethical-hacking process have been followed, that is, reconnaissance, scanning and enumeration, and gaining access. Although closely related and equally interesting, the phases of maintaining access and covering tracks have been excluded from this particular study (MacLeod, 2018) and remained as a potential future area of interest.

The assessment laboratory included three different devices (seismograph, accelerograph, and Global Navigation Satellite Systems [GNSS] receiver) from different branded manufacturers. These devices were used as targets for the attacks with their default settings, except their Internet Protocol (IP) address. Based on the information obtained through their manufacturers' manuals and additional public information used for security audits, the following attack tree (Schneier, 1999) (Fig. 1) was created. The attack tree methodology, a method for identifying and assessing different threats and risk sources, has been used as a tool for the initial analysis of those risk areas. Still, the execution of all possible security tests depicted in the attack tree has not been an essential target of this article; thus, the following depiction of threats is considered nonexhaustive and only limited to the aforementioned devices (Fig. 2).

The attempt to obtain the user credentials (username and password) did not consider the default factory codes that may be used from the manufacturer's manuals. Hence, brute force techniques (i.e., the exhaustive testing of all possible values) were not executed, due to the lack of adequate computing power in the implemented laboratory. Instead, to obtain the user credentials, a man-in-the-middle attack (Benjamin and Hamilton, 2009) (see Fig. FS35 in the supplemental material available to this article) has been implemented using a malicious user computer (similated within the researchers environment) in the same network as the devices with Kali Linux and Wireshark software. Also performed an attempt to intercept seismic data through the SeedLink transmission protocol used by the seismograph and accelerograph devices. The Networked Transport of RTCM via Internet Protocol GNSS data transmission protocol interception test was not executed due to the absence of an antenna in the laboratory. For the attacks against the availability of the devices, the Low Orbit Ion Cannon (LOIC) software was used.

The security assessment of the selected devices was performed on a lab environment based on a local network (see Fig. FS35). More specifically, vulnerability scanning has been done in devices and software protocols via network access, without examining any security issues that arise from physical access. In addition, all tests have been performed using the existing settings on the devices (as is) without performing any additional hardening process that would reduce the potential attack surface. To simulate the network interconnections, an eight-port switch was used to connect IoT seismological Devices, a computer acting as server that collects data (normally operated by legitimate users) and a computer for the malicious user (hacker).

To accomplish all penetration tests, Windows 10 operating system was used in the malicious user computer, including the LOIC tool for denial-of-service (DOS) attacks and Nmap and Nessus tools to perform the vulnerability assessment. A virtual machine with Kali Linux has also been used to simulate the

	Availability attack	Password trapping		Data interception	
Technique	DOS	MiTM	Brute force	MiTM	
Seismograph	UDP	HTTP	HTTP	SeedLink	N/A
Accelerograph	UDP	HTTP, TELNET	HTTP, TELNET	SeedLink	N/A
GNSS	UDP	HTTP, TELNET, FTP	HTTP, TELNET, FTP	N/A	NTRIP

man-in-the-middle attack and Wireshark to monitor and analyze the data flow. Finally, the SeisGram2K seismogram viewer has been used in the user's computer, acquiring, and reading seismological data from accelerograph and seismograph devices in real time. Using the tools mentioned previously, the assessment focused on intercepting real-time data and devices credentials. (Detailed attack procedure and results are available in the supplemental material.)

Results

In general, the performed tests have shown that seismological devices are designed to focus on the accuracy and real-time data transmission of the generated measurements, although the potential security issues are not being equally addressed. Once a malicious user has access to the network in which a seismological device is connected, through the use of an infected or compromised computer, the user can relatively easily bypass safety measures and modify the operation of the device causing various types of problems depending on the purpose of the attack. In the following paragraphs, the results of the security audits performed during the attacks are described.

Attack against availability

The DOS attack launched against the devices was successful and caused their unavailability during the attack time period. Such attacks typically aim to exhaust all available resources of the devices communication capacity by sending an excessive number of packets, in this case to user datagram protocol (UDP) ports not used by any service. The devices are then just trying to cope with the flood of these packets reserving all their available capacity. When the attack has been concluded, the communication was restored immediately. For the GNSS device, the DOS attack with UDP caused additional malfunctions, as in this case, the communication was not automatically restored after the end of the attack and the device had to be hard restarted to resume its operation.

Attack against confidentiality

For the attacks against confidentiality, a man-in-the-middle configuration along with the network analysis software Wireshark was used to intercept the communicated data as transmitted by the standard nonencrypted protocols implemented at all the devices. Therefore, usernames, passwords, and seismic data had been also recorded in several occasions.

Figure 2. Initial plan of security assessment for the seismological IoT devices. All attacks in green boxes have been accomplished. N/A stands for "not applicable" to indicate cases in which protocol was not enabled by default or did not exist in the device. Brute force was not executed due to the lack of adequate computing power in the implemented laboratory. Global Navigation Satellite Systems (GNSS) Networked Transport of RTCM via Internet Protocol (NTRIP) data transmission protocol interception test was not executed due to the absence of an antenna in the laboratory. The color version of this figure is available only in the electronic edition.

The attempt to disclose passwords from the web interface was successful for the GNSS device. For the seismograph and accelerograph, the attempt managed to disclose only the username but not the password. This is due to the use of the digest encrypted authentication (RFC2716), which employs a complex encoding algorithm based on the Message Digest (MD5) hashing algorithm and the use of additional data. This method is mainly used when the communication protocol is unencrypted. It provides a satisfactory level of security for the authentication process, using encryption of codes but is vulnerable to man-in-the-middle attacks, downgrade attacks, and likely other weaknesses (Morgan, 2010).

In addition to the hypertext transfer protocol (HTTP), performed attempts included breaking the credentials for the nonencrypted telnet and file transfer protocol (FTP) protocols in all devices where these protocols were available. For the accelerograph, the attempt to break the password of the telnet protocol was successful. In this case, the absence of a mandatory username results to lower the security of access for this device configuration environment. Moreover, the performed tests showed that telnet password and webservices user passwords were the same. Thus, this password could be easily intercepted even if the HTTP uses the encrypted authentication digest (RFC2716).

For the GNSS device, the disclosure of username and password was possible for both telnet and FTP protocols. It should be noted that in this case telnet access was made without the need of a username, requiring only the password that is part of the device serial number, and this password was also used for the connection through the FTP and by manufacturer specific windows configuration software to connect to the device through a network connection (see Fig. FS31).

The repetition of the previous test on a second similar GNSS device was not possible due to the unavailability of an

	Dos attack	Password trapping			Data interception
	UDP flood	HTTP	Telnet	FTP	SeedLink
Seismograph	Success	Partial success	N/A	N/A	Success
Accelerograph	Success	Partial success	Success	N/A	Success
GNSS	Success	Success	Success	Success	N/A

Figure 3. Graphical representation of security assessment results. N/A stands for "not applicable" to indicate cases in which protocol was not enabled by default or did not exist in the device. Partial success means that we intercept only username or password (not both). The color version of this figure is available only in the electronic edition.

additional device. Such a check is considered necessary to confirm the aforementioned very important security vulnerability, which allows the password to be readily available only through a simple attempt to connect through telnet without the need to perform any aggressive malicious action against the device.

Finally, it was possible to intercept seismological data through the man-in-the-middle attack, which has been performed on the communication channel between the user's computer and the seismological devices. It should be noted that this vulnerability is feasible due to the use of the SeedLink protocol that lacks encryption and authentication and not to the specific implementation of the tested devices.

Attack against integrity

The alteration and modification of nonencrypted seismological data transmitted in real time were identified as a potential attack path for all unsecured protocols (e.g., SeedLink) by implementing the man-in-the-middle attack and using tools such as Paros proxy or transmission control protocol Replay suite.

Revealing the seismological device passwords by a malicious user has similar potential results because it is possible to modify the device's configuration, thus making the produced data incomplete to some extent or not reliable. An example of such an attack is the removal or modification of Global Positioning System time in the data, the change of naming in seismic station code and channels, the change of sampling frequency, and so forth.

Tests summary

The performed test results are shown in Figure 3. The DOS attack was successful and caused a loss of communication for all devices that were tested. Similarly, the attempt to intercept seismological data transmitted through the SeedLink protocol has been proven to be successful for both seismological devices.

Interception of usernames and passwords used in each web-service through which each device is configurable and controlled was successful for the GNSS receiver. However, it was partially successful for the seismograph and the accelerograph, in which only the username, but not the password, was obtained. Finally, it was possible to gain access to the GNSS device through the telnet and FTP protocols and to the accelerograph through the telnet protocol because the passwords on both devices were easily revealed and obtained.

Find exposed devices

The previously described and analyzed cyberattacks against three well-known manufacturing companies' devices are mostly used in seismic and GNSS networks. These attacks were carried out in a controlled local laboratory network. To locate the geographical spread of more exposed devices connected to the web that could be potentially fall victim to malicious attacks, three different IoT search tools were used with their parameters configured to specifically detect the particular devices that were tested against cyberattacks. It is noted that these parameters are not exposed for reasons of manufacturers' security. Figure 4 shows the search results for these specific exposed IoT devices from one of these search engines. (Results from all tree search engines are shown in Figs. FS32, FS33, and FS34.)

Consequently, it has become clear that many interconnected devices are immediately exposed to potential attackers and directly widely accessible. This access is feasible without any advanced penetration testing or in-depth technical actions.

Discussion

Having examined the results of this research, it was considered important to advance a more in-depth analysis that could highlight the potential impact of such attacks and define the way of handling the related weaknesses.

Potential impact of such attacks

The new generation of seismological instruments that operate as IoT devices allows near-real-time data acquisition. This provides significant advantages to the operational seismological agencies in terms of timely recording and determination of significant earthquakes, earthquake aftershock sequences, ground motion and shaking intensity, and structural response of critical infrastructures. Moreover, the information of the earthquake source, size, and location are inferred from ultrarapid processing of the early seismic waves collected as close as possible to the source. These can be broadcast to more distant sites

Accelerograph

Country breakdown

Country	Hosts	Frequency
United States	52	55.91%
Mexico	14	15.05%
Iceland	8	8.6%
Argentina	5	5.38%
Romania	5	5.38%
Republic of Korea	3	3.23%
Bulgaria	1	1.08%
Canada	1	1.08%
Costa Rica	1	1.08%
Italy	1	1.08%

GNSS

Country breakdown

Country	Hosts	Frequency
United States	51	30.0%
Russia	28	16.47%
Poland	23	13.53%
Denmark	14	8.24%
Italy	14	8.24%
Romania	12	7.06%
Bulgaria	10	5.88%
Canada	4	2.35%
Mexico	3	1.76%
Bolivia	2	1.18%

Seismograph

Country breakdown

Country	Hosts	Frequency
United Kingdom	17	38.64%
Turkey	7	15.91%
Pakistan	6	13.64%
Republic of Korea	3	6.82%
Cayman Islands	2	4.55%
Germany	2	4.55%
United States	2	4.55%
Czechia	1	2.27%
Greece	1	2.27%
Jersey	1	2.27%

Figure 4. IoT search engine result for our specific seismological IoT devices used to make the security assessment. The numbers represent exposed devices connected directly to the internet that could be potentially fall victim to malicious attacks. The color version of this figure is available only in the electronic edition.

before the arrival of strong shaking, providing a fast telemetry. Thus, in the seconds following the earthquake initiation, an earthquake early warning system (EEWS) can provide an automated alert message through machine-to-machine communication. These systems are operational or under testing in Japan (Hoshiba, 2011), Mexico (Espinosa-Aranda, 2009), United States (Kohler, 2017), and in countries with high seismicity levels (e.g., Taiwan, Italy, Romania, and Turkey) with various automated applications such as Short Message Service alerts, safety shut down and isolate systems of industrial lines and nuclear power plants, closing bridges and tunnels, preventing traffic.

Any EEWS false alarms will undermine the confidence in any of these systems. More specifically, if a system issues too many false alarms, then people will ignore future warnings. False alarms might be produced as a result of issuing early alerts without adequate data coverage. This is a known risk in the scientific community and under discussion (Minson, 2018).

Malicious attacks in seismological IoT devices that are part of operational seismic networks could simply halt the operation of a single seismic station or the entire network. In this simplest case, the near-real-time seismological monitoring of the affected area is getting very difficult, if not impossible. If this malicious attack affects the raw seismological data without disrupting the near-real-time data acquisition, it could even alter the calculated seismological parameters (e.g., origin, location, magnitude, and ground-motion parameters) without being noticed initially by the responsible seismological service.

In the worst-case scenario, malicious attacks in IoTs of EEWS could disrupt operation or even produce false alarms that will trigger all the subsequent automated procedures. These malicious false alarms have considerable consequences such as unnecessary public concern, significant industrial economical losses, and vulnerable national security.

Managing detected weaknesses

The handling of the vulnerabilities of IoT devices needs to be addressed by both manufacturers and operators. Both sides should be concerned not only with the production and processing of scientific data but also with the safety and reliability of these data.

Manufacturers should:

- remove unsafe protocols, or make them available only as a choice of the device;
- operator rather than have them activated by default;
- use safer authentication methods (e.g., use of Secure Sockets Layer or Transport Layer Security);
- improve continuously device security via regular firmware's updates; and
- impose change of default login password in the first use of the device.

IoT device administrators or IT security expert should:

- change factory default passwords;
- use of encrypted protocols like HTTPs, Secure File Transfer Protocol, FTPs, Secure Shell (SSH), telnet over SSH;
- disable unencrypted protocols like HTTP, FTP, and telnet;
- update firmware device with latest version. Check it regularly; and
- when unencrypted data traffic is used, IT security specialist must be involved to implement countermeasures based on existing network layout, needs, and security assessment. Network segmentation, firewalls, intrusion detection

system or intrusion prevention system, and virtual private networks are some of the solutions that can be followed.

Finally, networks devices like state-of-the-art firewalls and smart switches are the only way to mitigate a DOS attack. To protect against credentials interception and seismic data interception or falsification, encrypted communication protocols or channels must be used.

Conclusions

The results of performed tests and their analysis have shown that seismological and GNSS instruments that function as IoT devices have several weaknesses (technical vulnerabilities) in malicious attacks. These are like those mentioned in the relevant literature for all IoT devices, so it can be further deduced that many of the nontested IoT attacks are also applicable to the seismological and GNSS instruments.

In addition, the most notable security issues are the lack of data encryption, the user authentication processes, the use of unencrypted communication protocols, unsafe default settings of devices, and the common simple initial passwords, as well as the nonenforcement of mandatory change of factory user codes, and so forth.

In fact, it has been observed that there is lack of built-in security systems, such as access lists, firewalls, intrusion detection system or intrusion prevention system, encryption, and endpoint protection mechanisms. In addition, the specialized seismological data transfer protocol, SeedLink, is not designed to include secure functionality (e.g., encryption, authentication, etc.). It is therefore imperative for manufacturers to take all necessary actions to cover the previous issues. Moreover, seismological operators that manage such devices should invest in information security experts that are specialized in the protection and security enhancement (or hardening) of such seismological systems, civil protection services, and corresponding data.

Data and Resources

For this study, we used equipment from the Institute of Geodynamics, National Observatory of Athens and any information available for these devices from their manufacturer manual, technical specifications, and related product webpage. The supplemental material contains detailed procedure and screenshots of devices security assessment. The following sources were also used to accomplish the goal of this article: Wireshark network protocol analyzer (https://www.wireshark.org, last accessed July 2018), Nessus vulnerability scanner (https://www.tenable.com/products/nessus/nessus-professional, last accessed July 2018), Nmap security scanner (https://nmap.org/zenmap, last accessed July 2018), Common Vulnerabilities and Exposures (CVE) details vulnerabilities data source (https://www.cvedetails.com, last accessed February 2020), Kali—Penetration testing and ethical-hacking Linux distribution (https://www.kali.org, last accessed July 2018), Low Orbit Ion Cannon (LOIC) denial-of-service (DOS) utility (https://sourceforge.net/projects/loic/, last accessed July 2018), transmission control protocol (TCP) Replay suite (http://tcpreplay.synfin.net, last accessed July 2018), Paros web proxy (https://sourceforge.net/projects/paros, last accessed July 2018), Internet Engineering Task Force (IETF) RFC2716 (https://www.ietf.org/rfc/rfc2716.txt, last accessed July 2018), Anthony Lomax, SeisGram2K Seismogram Viewer (http://alomax.free.fr/seisgram/SeisGram2K.html, last accessed July 2018), SSH.COM—Telnet (https://www.ssh.com/ssh/telnet, last accessed July 2018), Microchip, "TCP/IP Stack" (https://www.microchip.com/SWLibraryWeb/product.aspx?product=TCPIPSTACK, last accessed July 2018), and miniSEED format (http://ds.iris.edu/ds/nodes/dmc/data/formats/miniseed/, last accessed July 2018).

Acknowledgments

The facilities and equipment of Institute of Geodynamics, National Observatory of Athens were used to accomplish this study. The authors thank K. Chousianitis for providing access to the Global Navigation Satellite Systems (GNSS) receiver and the two anonymous reviewers and the editor for their helpful comments to improve this article.

References

Antonakakis, M., T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, *et al.* (2017). Understanding the Mirai Botnet, *Proc. of the 26th USENIX Conf. on Security Symposium*, USENIX Association, Vancouver, Canada, 16–18 August 2017, 1093–1110.

Benjamin, A., and G. Hamilton (2009). Detecting man-in-the-middle attacks by precise timing, *2009 Third International Conf. on Emerging Security Information, Systems and Technologies*, Athens, Glyfada, 81–86, doi: 10.1109/SECURWARE.2009.20.

Cabric, M. (2015). *Corporate Security Management*, M. Cabric (Editor), Butterworth-Heinemann, 185–200.

Dehling, T., S. Lins, and A. Sunyaev (2019). Security of critical information infrastructures, in *Information Technology for Peace and Security*, C. Reuter (Editor), Springer Vieweg, Wiesbaden, Germany, doi: 10.1007/978-3-658-25652-4_15.

Enisa (2017). Baseline security Recommendations for IoT, Enisa, available at https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot (last accessed August 2018).

Espinosa-Aranda, J. M. (2009). Evolution of the Mexican seismic alert system (SASMEX), *Seismol. Res. Lett.* **80,** no. 5, 694–706, doi: 10.1785/gssrl.80.5.694.

European Union Council (2008). Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, available at https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF (last accessed July 2018).

Fisher, L., and S. Lehnhoff (2018). IT Security for functional resilience in energy systems: Effect-centric IT security, in *Handbook on Resilience of Socio-Technical Systems*, Edward Elgar Publishing, 316–340.

Guerra, H., A. M. Garcia, L. Gomes, and A. Cardoso (2017). An IoT remote lab for seismic monitoring in a programming course,

Proc. of the 2017 4th Experiment@International Conf., Faro, Potugal, 129–130.

Hoshiba, M. (2011). Outline of the 2011 off the Pacific coast of Tohoku earthquake (M_w 9.0)—Earthquake early warning and observed seismic intensity, *Earth Planets Space* **63,** 7, doi: 10.5047/eps.2011.05.031.

Hung, M. (2017). *Leading the IoT*, Gartner, Stamford, Connecticut, 2 pp.

Kohler, M. (2017). Earthquake early warning ShakeAlert system: West coast wide production prototype, *Seismol. Res. Lett.* **89,** 99–107, doi: 10.1785/0220170140.

MacLeod, J. (2018). Ethical hacking phases, available at https://www.infosec.lawyer/portfolio/ethical-hacking-phases/ (last accessed July 2018).

Miller, C., and C. Valasek (2015). *Remote Exploitation of an Unaltered Passenger Vehicle*, Black Hat, Las Vegas, Nevada.

Minson, S. (2018). The limits of earthquake early warning: Timeliness of ground motion estimates, *Sci. Adv.* **4,** no. 3, eaaq0504.

Morgan, T. D. (2010). *HTTP Digest Integrity*, Virtual Security Research, Boston, Massachusetts, 6 pp.

Raman, C., and P. Raj (2017). *The Internet of Things*, CRC Press, United Kingdom.

Russell, B., and D. Van Duren (2016). *Practical Internet of Things Security*, PACKT Publishing, Birmingham - Mumbai, 3–4.

Schneier, B. (1999). *Attack Trees*, SANS Network Security 99, New Orleans, Louisiana, 8 October 1999, 8–10.

Sepulveda, F., and J. Pulliam (2016). The internet of geophysical things: Raspberry Pi Enhanced REF TEK (RaPiER) system integration and evaluation, *Seismol. Res. Lett.* **87,** no. 2A, 345–357.

Zhang, Z.-K., M. Cheng Yi Cho, and C.-W. Wang (2014). IoT security: Ongoing challenges and research opportunities, *7th International Conf. on Service-Oriented Computing and Applications*, IEEE, Matsue, Japan, 17–19 November, doi: 10.1109/SOCA.2014.58.

Manuscript received 27 April 2020
Published online 10 February 2021