# Analysis of Human Awareness of Security and Privacy Threats in Smart Environments

Luca Caviglione[1], Jean-François Lalande[2,3], Wojciech Mazurczyk[4], and Steffen Wendzel[5(✉)]

[1] Institute of Intelligent Systems for Automation (ISSIA), National Research Council of Italy (CNR), 16149 Genova, Italy
luca.caviglione@ge.issia.cnr.it
[2] Inria, University Rennes 1, Supélec, CNRS, IRISA UMR 6074, 35065 Rennes, France
[3] INSA Centre Val de Loire, University Orléans, LIFO EA 4022, 18020 Bourges, France
jean-francois.lalande@insa-cvl.fr
[4] Institute of Telecommunications, Warsaw University of Technology, 00-665 Warsaw, Poland
wmazurczyk@tele.pw.edu.pl
[5] Fraunhofer Institute for Communication, Information Processing and Ergonomics (FKIE), 53113 Bonn, Germany
steffen.wendzel@fkie.fraunhofer.de

**Abstract.** Smart environments integrate Information and Communication Technologies (ICT) into devices, vehicles, buildings and cities to offer an increased quality of life, energy efficiency and economical sustainability. In this perspective, the individual has a core role and so has networking, which enables such entities to cooperate. However, the huge amount of sensitive data, social aspects and the mixed set of protocols offer many opportunities to inject hazards, exfiltrate information, mass profiling of citizens, or produce a new wave of attacks. This work reviews the major risks arising from the usage of ICT-techniques for smart environments, with emphasis on networking. Its main contribution is to explain the role of different stakeholders for causing a lack of security and to envision future threats by considering human aspects.

**Keywords:** Privacy · Security · Steganography · Smart buildings · Human aspects

## 1 Introduction

Smart buildings are an elementary component of smart environments, which aim at improving the comfort of individuals and their lifestyle. In essence, they integrate *Information and Communication Technologies* (ICT) into devices, vehicles and buildings to provide a higher quality of life, a reduced environmental footprint and economical benefits. Pushed to the limit, such basic blocks can be


T. Tryfonas and I. Askoxylakis (Eds.): HAS 2015, LNCS 9190, pp. 165–177, 2015.
DOI: 10.1007/978-3-319-20376-8_15

arranged to produce large-scale deployments known as smart cities. Smart environments are the result of a large interdisciplinary effort, ranging from civil engineering to cloud computing. However, in this work we focus on networking/devices, since they provide many important features such as: (*i*) the ability of collecting information from the surrounding environment, (*ii*) the possibility of sending remotely commands and feedback, also in a real-time fashion, (*iii*) the availability of an infrastructure to handle the resulting amount of data. Prime examples are, among the others: wireless loops used to gather information from sensors, *Radio Frequency Identification* (RFID) deployed to monitor the status of a physical area, and the *Internet of Things* (IoT) paradigm to access and control devices or assets like locks, light and household appliances [23].

Alas, smart technologies are tightly coupled with individuals, especially in terms of their lifestyles, bad habits and sensitive data. Therefore, all the information gathered, exchanged and stored within smart environments can lead to severe issues in terms of security and privacy. For instance, detailed personal information can be used for mass profiling or social engineering attacks. Moreover, misuse of devices, bad habits and poor understanding of handled technology can lead to severe security breaches. For example, smartphones are often used to control different parts of smart environments (e.g., buildings) and worms or infected applications could attack the discovered appliances of the user's environment.

In this perspective, this paper analyzes the most relevant security and privacy threats of users in smart environments. Given the example of smart building security, we highlight the practical background which leads to a lack of security functionality and awareness at the side of vendors, integrators and operators. The main contributions of this paper are the following: the systematic review of hazards rooted within the most relevant smart paradigms; an assessment of emerging threats arising by the mix of ICT technologies and human aspects; the discussion of possible countermeasures to mitigate identified security issues. We point out that this paper serves as an introductory work for the HAS session on *Human Aspects of Information Security, Privacy and Trust for Smart Buildings.*

The remainder of the paper is structured as follows: Sect. 2 describes the problem space generated by the smart paradigm. Section 3 deals with human aspects of insecurity of smart buildings, Sect. 4 concentrates on smartphones, and Sect. 5 reviews vehicles. Section 6 proposes a role-based perspective on threats related to smart environments and Sect. 7 gives our future vision of identified threats and possible countermeasures. Section 8 concludes the paper.

## 2 Description of the Problem Space

Smart environment is an umbrella term comprising different kinds of devices or specific deployments. As today, the most relevant areas of smart things are:

– **Smart Buildings:** they collate a mix of smart devices as to produce an integrated environment. For such a complex deployment, proper middleware in charge of offering a coherent access is usually adopted, as well as proper

computing facilities to store user data, process control directives and provide optimizations, especially in the field of energy management. Thus, this scenario can be used to exploit data hiding, for instance to covertly orchestrate a botnet.

- **Smart Devices:** they are quickly becoming widespread and one of the core blocks to pursue the vision of a more "human-centric" environment. Common examples of smart devices are gaming consoles, set-top-boxes, light bulbs and household appliances. These devices can be used to infer habits, even political views, for instance by evaluating the shows watched on the TV. Moreover, the availability of full-featured TCP/IP stacks can be exploited to produce new types of botnets in order to e.g. amplify spam campaigns. It must be emphasized that smart devices will not be investigated in details in this paper due to space limitations and their technical heterogeneity.
- **Smart Phones:** are the most popular tools used to interact with other devices, and can be used to remotely control buildings and vehicles. In addition, they are the preferred platform to connect to the Internet and to communicate using heterogeneous networks (e.g., cellular or WiFi). They store a huge source of sensitive details such as messages and contacts and can be paired with smart watches which increases their potential to collect personal data. As a result, they are one of the preferred targets for data exfiltration of users, while additionally empowering phishing, social phishing, cyber bullying and social engineering [4].
- **Smart Vehicles:** modern automotives offer features to geolocate vehicles, mainly through the *Global Positioning System* (GPS), and to plan routes. Such features are not only used by individuals, since they are at the basis of fleet management and intelligent/smart transportation services. Also, modern vehicles can remotely send telemetry data as to prevent fault and guarantee proper service levels, e.g., for goods delivery. This allows massive user profiling, which leads to understand habits to conduct physical attacks.

The resulting problem space is very composite and needs a thorough understanding of all the technical components used, both to evaluate the degree of (in)security and to engineer proper countermeasures and mitigation techniques. To this aim, functional entities needing an investigation are: (*i*) wireless networks (e.g., the IEEE 802.11) as well as the core protocols used to exchange data or grant human interaction (e.g., HTTP); (*ii*) elaborate a proper taxonomy/ranking to understand where the related weaknesses impact more (e.g., physical security vs. cybersecurity); (*iii*) understand how sensitive data can be used also jointly with those available on *Online Social Networks* (OSNs) as a method to produce a new wave of attacks; (*iv)* understand why standard detection methods can be defeated by the complexity and diversity of smart environments.

## 3 Smart Buildings

Smart buildings are automated buildings, i.e., those comprising *Building Automation Systems* (BAS) and inter-connected with the IoT. The importance of

BAS for today's societies increases steadily due to various reasons. For instance, being enriched with more features, buildings can perform an additional number of routine tasks such as energy saving and in the context of an aging society, smart buildings ensure that elders can stay longer in their homes before being forced to move to a nursing home.

Various vulnerabilities in the available standards of communication protocols used in BAS are known. Most of these communication protocols, e.g., EIB/KNX, LON or BACnet, were designed many years ago with very limited focus on IT security [11,12]. Improved standards for the most-widely used BAS protocols are already proposed or under development, however, the application of these enhanced protocols in practice and the integration into products is currently not present. Moreover, the integration of newer protocols into legacy BAS environments is hardly feasible and thus, novel solutions like *traffic normalization* must be applied which protect legacy systems [25]. From a human-oriented perspective, the major attacks which can be performed on buildings are:

- **Surveillance**: as shown in [20,26], it is technically feasible to perform surveillance of events in buildings, e.g., caused by inhabitants or employees. Therefore, passive and active attacks are known: the attacker either exploits side channels or directly requests sensor values from Internet-connected BAS. An attacker can, for instance, use surveillance to monitor the behavior of inhabitants or employees.
- **Remote Control**: while surveillance relies on sensor values and actuator states in a smart building, a remote control is feasible, too. Therefore, actuators are used to perform actions, triggered by the attacker. For instance, to break into a building, a thief can send commands to window actuators/door actuators and can attack the physical access control system. In worst case, remote control attacks influence the safety of inhabitants and people working in a building.
- **Physical Exploitation**: being a form of remote control, an attacker can at least indirectly get advantage of exploiting the BAS of other households. For illustration, we use the example of a house with two parties A and B, each possessing its own flat and own BAS. Imagine party A leaves his flat, which is underneath the flat of B, for winter holidays while party B is staying at home. Since the ceiling of A's flat is the ground floor of B's flat, B can attack the BAS of A to maximize the heating level in A's flat. As a result, the temperature of B's flat is also heated a little what saves heating costs for B while increasing the costs for A.
- **Availability**: the functioning of a building is essential for today's organizations. Hence, causing a *Denial of Service* (DoS) attack, e.g., by simple misconfiguration, can affect all areas of building automation, such as physical access control or fire alarm systems, and is thus not only harmful for enterprise processes but for the safety of people.
- **Smart Building Botnets**: when surveillance or remote control is not only performed for a single household or industrial building, but for a larger number of buildings, novel scenarios emerge. So-called *smart building botnets* can

perform mass surveillance and mass remote control [27]. For instance, a local oil distributor may rise his sales by slightly increasing the nightly heating levels of his customer's households. Such large-scale attacks potentially influence the privacy, safety, and living of inhabitants and employees in whole regions.

## 4 Smart Phones

For years, smartphones have been one of the most important tools to communicate and store personal data. Recently, the advent of frameworks for managing home appliances, monitoring the health of the owner and handling payments, led to an important paradigm shift. In essence, smartphones are the preferred dashboard to access smart homes, and interact with appliances or vehicles. In addition, the security is under the responsibility of the user, since he/she is in charge of managing the administration and installation of the applications, as well as of undertaking security decisions. Yet, there is not any guarantee about his/her level of technical knowledge, which makes the human an effective vector of attack. As a consequence, smartphones are prone to different attacks in terms of human aspects, specifically:

- **Data exfiltration**: capturing user's personal data is one of the primary goals of attackers [8]. After collecting the data, for instance via phishing, the malware uploads it to a remote server. Thus, personal or business information is not only stolen but also stored in a place inaccessible for the user.
- **Exploitation of acquired resources**: a classical secondary goal consists of exploiting the controlled smartphone [8]. For example, it can be used as: a client of a botnet network, to send premium-rate SMS, or to participate in computations for mining bitcoins. From the user perspective, it disturbs the normal behavior of the smartphone and can result in additional cost. As other smart entities can be controlled by an application on the user's smartphone, compromising the smartphone can also give a fresh starting point to attack other smart entities on the same network.
- **Surveillance**: a malware can try to access user's localization and report these data to the attacker. Using the collected positions, more complex attacks can succeed to infer the identity of the user [10].
- **Battery drain**: a severe fragility of smartphones is the intrinsic power limitation due to the usage of battery. Hence, its malicious depletion can be at the basis of a new kind of DoS attack, where the device is made unusable [17]. Possible mechanisms range from the injection of energy wasting code within a malware or a stimulation of the device via its air interfaces. In any case, this attack may isolate the victim, making communications with the rest of the world infeasible. This kind of hazard is also effective for the case of sensors or nodes of an IoT deployment and the victim could have his/her safety framework compromised.
- **Information hiding**: as a consequence of a full implementation of the TCP/IP protocol stack, and the diffusion of BAS over IP solutions, modern smartphones run several applications using a very mixed set of protocols.

The latter can be exploited for information hiding purposes. In essence, multimedia data and network traffic can be used as legitimately appearing carriers by information hiding techniques to make a third-party observer unaware of the resulting flow. This technique can be also used for mass-profiling [28] or for empowering malware exfiltrating data [18].

## 5 Smart Vehicles

The most useful scenario envisaged for smart vehicles concerns *Vehicular Ad-hoc Networks* (VANETs), which offer features such as, road safety, route planning, entertainment, tolling, traffic management and support for intelligent transportation. In such a deployment, humans should be not endangered by vehicles as a vehicle's misbehavior can lead to severe injuries and safety hazards[1,2]. In addition, the cooperative nature of VANETs puts the network in a central and critical role. Therefore, networking technologies used in vehicles must be protected against malicious activities, which are very effective [6,13]. Their main scopes are to propagate incorrect information about events on the road, to gain sensitive information, and to disrupt the network infrastructure to prevent users accessing the service [14]. Among the others, the most relevant attacks in terms of human aspects are:

- **Injecting bogus information**: an attacker deliberately injects false information into the network to produce arbitrary situations along a route [1]. As an example, a node sending false information to benefit from a reduction of traffic along a common path. This can be done via false information reporting traffic jams, road accidents, and blocked routes as to suggest alternative ways. The most popular methods to achieve such goals are: intentionally creating or modifying existing frames, repeating previously captured data (replay attack), and misleading vehicle's sensors (illusion attack).
- **Sybil attack**: it is based on spoofing the identity of nodes to flood the network with incorrect information [29]. Typically, the attacker produces multiple copies of false data to appear as legitimate. Then, such false data can be used to induce the same reactions previously explained.
- **Wormhole attacks**: it creates a tunnel between two attackers' vehicles as a way to inject false information and disrupt the vehicular network [1]. The wormhole attack can be especially dangerous since it makes routing tables incoherent, thus causing the unavailability of the service for humans.
- **Routing protocols attacks**: vehicular networks use a mixed amount of broadcast and multi-hop traffic, e.g., to deliver data to isolated nodes.

[1] Def Con 21 talk by C. Miller and C. Valasekentitled entitled "Adventures in Automotive Networks and Control Units" https://www.defcon.org/html/defcon-21/dc-21-speakers.html#Miller.

[2] Def Con 18 talk by M. Metzger entitled "Letting the Air Out of Tire Pressure Monitoring Systems" https://www.defcon.org/images/defcon-18/dc-18-presentations/Metzger/DEFCON-18-Metzger-Letting-Air-Out.pdf.

In this case, the injection of bogus routing information can cause the routing protocols to misbehave [16,24]. This may lead to the extension of packets' routes, the creation of routing loops, or the redirection of the traffic to an unreal node (blackhole attacks) or towards the attacker (greyhole attacks).
- **Man in the middle attacks**: there are no significant differences between Man in the middle attacks in VANETs and in typical wired networks. These attacks impact the authenticity of transmitted information which may threaten the privacy and identity of users.
- **DDoS attacks**: two main techniques are utilized to perform DoS attacks [29]. First, by disrupting the frequencies utilized for wireless communication, the attacker produces a jam in a given frequency range. This is quite easy to implement and its effectiveness mainly depends on the transmitting power of the jamming device. Second, by sending large amounts of network traffic by an authorized host, the attacker generates network messages that are valid but with high volumes/rates thus causing congestion, latency and intermittent connectivity. In both cases, the vehicle is unable to send/receive any information and the driver could potentially miss an important announcement, e.g. on the accident nearby or the worsening of weather conditions.
- **GPS spoofing**: it is based on sending a "louder" GPS signal to hide the legitimate one [29]. Current protection methods are mainly based on monitoring the power expected by a legitimate GPS satellite. This attack may lead to a car accident or to driving a vehicle in an abandoned area.

## 6 Human Awareness of Smart Environment's Threats: A Role-Based Perspective

When comparing human aspects of ICT-related topics with those in smart environments, a clear difference can be recognized. In ICT-related areas, a strong development of security features is achieved. Thus, vendors integrate security into their products and customers clearly demand for such features. In smart environments, especially the classic ones – such as factory automation – there is a clear lack of security, which we mainly illustrate in this section by reviewing the point of view of the different actors in the case of BAS. Most of these views were obtained owing to personal conversation with the different stakeholders.

*Vendors.* Vendors do not integrate security into their automation equipment as they lack know-how. They focus on engineering aspects and product quality is rather measured in longevity of components instead of in terms of security. When security features are integrated, these are in many cases implemented from scratch. For instance, a number of German BAS vendors promote their BAS network components explicitly with the "feature" that instead of buying a network stack from a country abroad, they have one competent engineer who implemented the stack himself. A one-person implementation of a network stack, such as BACnet, including its complex features is hardly feasible in a secure way by a single engineer.

*Customers.* On the other hand, the customers lack security awareness as well. Awareness-raising processes are currently taking place on a regional, national, and international scale. For instance, the 28th German *GLT Anwendertagung* – a leading event for professional customers – organized a security session on BAS in 2014. However, the effect of these awareness raising processes is small. For this reason, possessing still no (or very limited) awareness for security threats, customers do not demand security features from *vendors*, which, in turn, see the implementation of additional security features as costly.

*Operators.* Operators of smart buildings are usually janitors without any know-how on the IT security of their BAS. Even if the operators received additional education on BAS (e.g., certificates on building management), these courses lack any security features. The perspective of an operator is to ensure the functioning of a BAS, including its *safe* operation, for instance an intact fire alarm system, but security aspects are considered an additional overhead.

Additionally, *vendors* provide no tools to monitor or configure the security of BAS components and thus, even if *operators* would possess knowledge on IT security, they could not apply it in practice. In particular, as smart environments are in most cases networked environments, operators require *cyber situational awareness* [9], for example the awareness of any kind of suspicious activity taking place in cyberspace. In various cases, such as larger or inter-connected BAS, the number of events cannot be processed by human operators without any support. To this end, research came up with visualization approaches, which, for instance, present information in such a way that events with higher entropy are easier to spot. However, in practice, these tools are not available and if available are used for spotting misconfiguration problems or malfunctioning equipment instead of detecting cyber security-related attacks.

*Project Deployment.* Construction of a BAS suffers from non-optimized information exchange of the parties involved in the design, construction, and operation process of a building [21], which includes the planning, integration, and operation of a BAS. Moreover, know-how about the operation must be managed, including to consider its potential loss if operators leave the organization—a problem that is even more important for other critical smart areas such as operator centers for naval vessels or railways [3].

**Table 1.** Summary of human awareness from a role-based perspective for each "component" of smart environment.

| Smart "component" | Vendors | Customers | Operators | Deployment |
|---|---|---|---|---|
| Buildings | Low | Low | Low | Low |
| Vehicles | Medium | Low | Low | Low |
| Phones | High | Medium | High | Medium |
| Devices | Medium | Low | Low | Low |

This analysis is particularly pessimistic for BAS. Other smart components considered in this paper have made better security efforts. We summarize human awareness from a security perspective for each "component" of the smart environment in Table 1. Smartphones have received better attention than vehicles or devices. They benefit from two effects: customers ask for more security because of the increasing connectivity with OSNs; vendors can integrate adapted security technologies that have been matured for GNU/Linux operating systems, especially since Android has taken the lead in the market.

## 7 Future Vision on Threats and Countermeasures

Today, a number of the attacks presented in previous sections, e.g., smart building botnets, should rather be considered technically feasible than a real-world threat. However, given the linked risks for individuals and communities and the lack of awareness of the involved roles, the hurdles for attackers are considered not higher than for other ICT attacks. For this reason and since smart things of each type quickly gain more widespread, authors who discussed the particular attacks conclude the importance of a rapid countermeasure development as potential attacks are known before emerging on a larger scale in practice (e.g. [27]).

### 7.1 Future Threats

The potential of attacks can be considered larger if already known attacks from other areas of IT security are getting adapted to smart things. For instance, *watering hole attacks* [15] can be adapted to smart buildings/smart phones. Consider a community that is living in the same building. If an attacker wishes to access the BAS it is enough for her to infect only one inhabitant's smartphone which she uses to control the smart building and eventually other habitants will be infected. This scenario becomes even more significant as some hotels announced to enable smartphone-based hotel room access for guests.

In this perspective, smartphones will definitely be one of the preferred playgrounds to exploit threats. Especially, this is due to the complexity of their security policies, which discourages users to analyze and take adequate decisions. In addition, smartphones possess authentication tools that become of high interest for attackers.

One of the examples of how future mobile malware can covertly exfiltrate user's sensitive data is envisioned in [5]. The proposed steganographic method takes advantage of the built-in Siri service which has been offered for iPhone/iPad as a native service from iOS5 in 2011. Siri allows interacting with the iOS-based device using voice commands. To offload the device, the translation of voice inputs to text is performed remotely in a server farm operated by Apple. To this aim, the iPhone/iPad samples the voice, sends it to a remote facility, and waits for a response containing the recognized text, a similarity score and a time stamp. This characteristic feature can be exploited by an attacker

which could produce ad-hoc voice patterns to manipulate the throughput and encode a secret into its shape. In future, a similar approach can be applied to all services relying on a massive conversation between the user's device and similar services in the cloud like GoogleVoice for Android OS or Cortana for Windows Phone.

For other smart devices, the potential of attack is dramatically increasing. For example, the Rapid7 company published in 2013 a security report about several critical vulnerabilities of the UPnP library [19]. These vulnerabilities affect billions of devices, for example Smart TVs, and gives opportunities to build attacks and gain root shells on these devices.

Lastly, because smart devices typically reside inside smart buildings, a compromised device will help an attacker to attack smart buildings. The attacker can try to capture data, infer residents habits, such as food products ordered online (smart fridge) and TV shows watched (smart TV). This can significantly impact privacy and enable the production of a new wave of extremely precise (and effective) social engineering attacks.

### 7.2 Future Countermeasures

A number of futuristic protection approaches for smart things are imaginable. For smart vehicles, the used protocols should include validation algorithms as it is clear that there, many potential opportunities arise for an attacker to inject malicious information. As used protocols should react in a real-time fashion, the added security should be lightweight and distributed between participants in order to give robust results. These solutions, reviewed in [7], can be based on reliable cryptographic key distribution and has been already actively studied for example for ad-hoc networks. With such tools, the privacy of users should be guaranteed. Also, they can be based on the reputation systems already deployed for peer-to-peer architectures.

A mean for smart buildings could be to introduce multilevel security [26]. Such an approach could, for instance, prevent that devices in a storage room could read sensor values from the management floor of an organizational building.

For the attack vectors discussed for smartphones, the industry is currently working on *Trusted Execution Environments* (TEE) that would introduce a secured trusted space of execution while the regular operating system remains untrusted. This way, vendors would be able to split their applications and protect the critical parts into the smartphone's TEE [2]. Moreover, malware detection is one of the hot topics for researchers in mobile security. Nevertheless, current anti-malware products are easily defeated by transformation techniques of the malware's code [22]. Thus, these aspects remain to be addressed.

## 8 Conclusion

This paper discussed the human-related security and privacy aspects of smart environments. We highlighted the resulting consequences for humans when

various attacks on smart buildings, smart phones, and smart vehicles are performed, also by emphasizing the role of inter-connected things populating smart cities. Furthermore, by discussing the example of smart buildings, we conclude that awareness for smart things is a multifaceted problem. Vendors, customers, and operators as well as awareness for the deployment process of smart things must be considered. We pointed out that research efforts have already been started from smartphones but remain very limited for vehicles, devices and especially for buildings.

We also conclude that a variety of attacks will be possible in a near future. Therefore, we underline the importance of a rapid development of proper and effective countermeasures. Possible countermeasures have to be inspired by the efforts achieved in other fields like peer-to-peer, ad-hoc networks and regular computers. The customer's comprehensiveness of these future security measures is a central requirement in order to be effective. This is a prime research task both for the academia and the industry in order to improve the security of smart environments.

## References

1. Al-kahtani, M.: Survey on security attacks in vehicular ad hoc networks (VANETs). In: 2012 6th International Conference on Signal Processing and Communication Systems (ICSPCS), pp. 1–9, December 2012
2. Arfaoui, G., Gharout, S., Traoré, J.: Trusted execution environments: a look under the hood. In: The International Workshop on Trusted Platforms for Mobile and Cloud Computing, pp. 259–266. IEEE Computer Society, Oxford, April 2014
3. Bronkhorst, A., Post, W., te Brake, G.: From human factors to HSI and beyond: design of operations centers and control rooms. In: 9th Future Security - Security Research Conference, pp. 140–146. MEV Verlag, September 2014
4. Caviglione, L., Coccoli, M.: Privacy problems with web 2.0. Comput. Fraud Secur. **2011**(10), 16–19 (2011)
5. Caviglione, L., Mazurczyk, W.: Understanding information hiding in iOS. IEEE Comput. Mag. **48**(1), 62–65 (2015)
6. Checkoway, S., McCoy, D., Kantor, B., et al.: Comprehensive experimental analyses of automotive attack surfaces. In: Proceedings of the 20th USENIX Conference on Security, SEC 2011, pp. 6. USENIX Association, Berkeley (2011)
7. Engoulou, R.G., Bellache, M., Pierre, S., Quintero, A.: VANET security surveys. Comput. Commun. **44**, 1–13 (2014)
8. Felt, A.P., Finifter, M., Chin, E., Hanna, S., Wagner, D.: A survey of mobile malware in the wild. In: 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices, p. 3. ACM Press, New York, October 2011
9. Franke, U., Brynielsson, J.: Cyber situational awareness - a systematic review of the literature. Comput. Sec. **46**, 18–31 (2014)
10. Gambs, S., Killijian, M.O., Nunez del Prado Cortez, M.: De-anonymization attack on geolocated data. In: 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 789–797 (2013)

11. Granzer, W., Kastner, W., Neugschwandtner, G., Praus, F.: Security in networked building automation systems. In: 2006 IEEE International Workshop on Factory Communication Systems, pp. 283–292 (2006)
12. Granzer, W., Praus, F., Kastner, W.: Security in building automation systems. IEEE Trans. Indus. Electron. **57**(11), 3622–3630 (2010)
13. Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S.: Experimental security analysis of a modern automobile. In: 2010 IEEE Symposium on Security and Privacy (S&P), pp. 447–462, May 2010
14. Lipiński, B., Mazurczyk, W., Szczypiorski, K., Śmietanka, P.: Towards effective security framework for vehicular ad-hoc networks. In: Proceedings of 5th International Conference on Networking and Information Technology (ICNIT 2014) (2014)
15. Lowe, M.: Defending against cyber-criminals targeting business websites. Netw. Sec. **2014**(8), 11–13 (2014)
16. Chen, L., Hongbo Tang, J.W.: Analysis of VANET security based on routing protocol information. In: Proceedings 4th International Conference Intelligent Control and Information Processing (2013)
17. Martin, T., Hsiao, M., Ha, D.S., Krishnaswami, J.: Denial-of-service attacks on battery-powered mobile computers. In: Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications, PerCom 2004, pp. 309–318. IEEE (2004)
18. Mazurczyk, W., Caviglione, L.: Steganography in modern smartphones and mitigation techniques. IEEE Commun. Surv. Tutor. **PP**(99), 1 (2014)
19. Moore, H.: Security flaws in universal plug and play. Technical report, January, Rapid7 (2013). https://community.rapid7.com/docs/DOC-2150
20. Mundt, T., Kruger, F., Wollenberg, T.: Who refuses to wash hands? privacy issues in modern house installation networks. In: Proceedings 7th International Conference Broadband, Wireless Computing, Communication and Applications, pp. 271–277, November 2012
21. Nöldgen, M., Bach, A., Heinz, T.: Integration of resilience engineering in the transdisciplinary building design process. In: Proceedings 9th Future Security - Security Research Conference, pp. 125–132. MEV Verlag, September 2014
22. Rastogi, V., Chen, Y., Jiang, X.: Evaluating android anti-malware against transformation attacks. In: 8th ACM SIGSAC Symposium on Information, Computer and Communications Security, pp. 329–334. ACM Press, Hangzhou (2013)
23. Snoonian, D.: Smart buildings. IEEE Spectr. **40**(8), 18–23 (2003)
24. Biswas, S., Jelena Misic, V.M.: Performance analysis of black hole attack in vanet. In: Proceedings of 31st Interenational Conference Distributed Computing Systems (2011)
25. Szlósarczyk, S., Wendzel, S., Meier, M., Schubet, F., Kaur, J.: Towards suppressing attacks on and improving resilience of building automation systems - an approach exemplified using BACnet. In: Proceedings Sicherheit 2014, GI, pp. 407–418 (2014)
26. Wendzel, S., Kahler, B., Rist, T.: Covert channels and their prevention in building automation protocols - a prototype exemplified using BACnet. In: Proceedings 2nd Workshop on Security of Systems and Software Resiliency, pp. 731–736. IEEE (2012)
27. Wendzel, S., Zwanger, V., Meier, M., Szlósarczyk, S.: Envisioning smart building botnets. In: Proceedings Sicherheit 2014, LNI, GI, March 2014, vol. 228, pp. 319–329 (2014)

28. Wendzel, S., Mazurczyk, W., Caviglione, L., Meier, M.: Hidden and uncontrolled-on the emergence of network steganographic threats. In: Reimer, H., Pohlmann, N., Schneider, W. (eds.) ISSE 2014 Securing Electronic Business Processes, pp. 123–133. Springer, Wiesbaden (2014)
29. Zeadally, S., Hunt, R., Chen, Y.S., Irwin, A., Hassan, A.: Vehicular ad hoc networks (VANETS): status, results, and challenges. Telecommun. Syst. **50**(4), 217–241 (2012)