

# Who Controls Your Energy? On the (In)Security of Residential Battery Energy Storage Systems

Ingmar Baumgart, Matthias Börsig, Niklas Goerke, Timon Hackenjos, Jochen Rill and Marek Wehmer  
Competence Center for IT Security, FZI Research Center for Information Technology, Karlsruhe, Germany  
Email: {baumgart, boersig, goerke, hackenjos, rill, wehmer}@fzi.de

**Abstract**—The home Battery Energy Storage System (BESS) industry is on the rise [1]. Newer models are built as Internet-connected devices that offer new service models for customers and manufacturers alike. This approach, as can be observed from emerging Internet of Things (IoT) devices in the last decade, brings new challenges and issues with it. First of all, threats to user privacy and botnet attacks come to mind. More importantly, there are now substantial advances to put flexible BESS in more critical roles in the power grid and let them provide primary balancing power in order to compensate fluctuations [2].

However, while the *safety* properties of such systems are currently being explored by researchers [3], their *security* is mostly unexplored and unregulated. To explore the state of security of residential BESS, we systematically analyzed commercially available storage systems from ten different manufacturers, who have a combined market share of more than 60 percent in Germany [4]. We show that all of them have security issues and four of them contain severe security flaws. In order to exemplify the deficit in the industry to properly secure Internet connected devices, we present three attacks in detail.

## I. INTRODUCTION

The transition to renewable energies has led to a massive growth of photovoltaic system installations on residential houses. However, most of the generated energy is produced during times when it cannot be consumed immediately by the household and is instead sold and fed back into the power grid. Additional energy has to be purchased for a higher price in the morning and the evening when demand peaks, whereas the superfluous energy generated by the solar cells is sold cheaply when demand is low. Home Battery Energy Storage Systems (BESS) allow the surplus energy to be stored until it is needed, thus increasing the self-consumption rate significantly. In 2018, there were more than 120,000 BESS installed in Germany alone and by 2020 battery systems are expected to reach an annual installation volume of over 50,000 systems in Germany [1].

Modern BESS are connected to manufacturers' servers to facilitate additional services for customers as well as new business models for the manufacturers. This shift to always-online products has happened in many industries and is often subsumed under the term Internet of Things (IoT). While the interconnection of components is often considered a necessary step towards the smart grid [5], it also introduces new challenges for the security of these devices. In the past, IoT devices were often poorly engineered from a security standpoint and consequently have led to numerous flaws endangering user privacy and device integrity [6]. A direct result of this fact was

the rise of the Mirai botnet that infected up to 600,000 IoT devices and was responsible for several high-profile distributed Denial-of-Service (DDoS) attacks [7]. We hypothesize that BESS are attractive targets for those types of attack as well: they store and transmit fine-grained data about the power consumption and charging profiles of their households over the Internet, from which highly sensitive private information can be extracted [8]. They are further running without interruption and are connected to the Internet at all times, such as the devices targeted by Mirai.

As recent studies have shown, a large number of maliciously controlled high-wattage IoT devices can also be used to endanger the grid stability, leading to blackouts in the worst case [9]. Market developments show that, apart from being common IoT devices, the growing overall capacity of installed BESS allows them to be used for feeding-in energy in order to stabilize the power grid against fluctuations [2]. This could worsen the effect of attacks on the grid stability. Indeed, attacks to sabotage energy infrastructure are not purely theoretical: In 2015 an attack on Ukrainian transmission substations led to a temporary blackout reportedly affecting 225,000 people [10]. The sophisticated malware was designed specifically to target energy systems and their communication protocols to open breakers [11].

Previously, BESS were offline devices whose main functionality it was to save costs for homeowners. The current transition to always-online, critical components in the public power system raises the question if manufacturers have learned from past mistakes made by the IoT industry and can provide an adequate level of security to protect their products against manipulation. Notably, most BESS have an expected operational lifetime of over ten years, presenting a long-term potential for large-scale attacks if the manufacturers fail to properly protect and maintain their products for their whole life cycle. While security aspects of other trends in the energy sector (such as Smart Meter Gateways) have been discussed extensively, to the best of our knowledge, no systematic test of a larger number of BESS has been performed so far.

## II. OUR CONTRIBUTION

We systematically analyzed the state of security of ten different BESS with a focus on identifying security issues on each device and in the communication channels from and to the device. We show that:

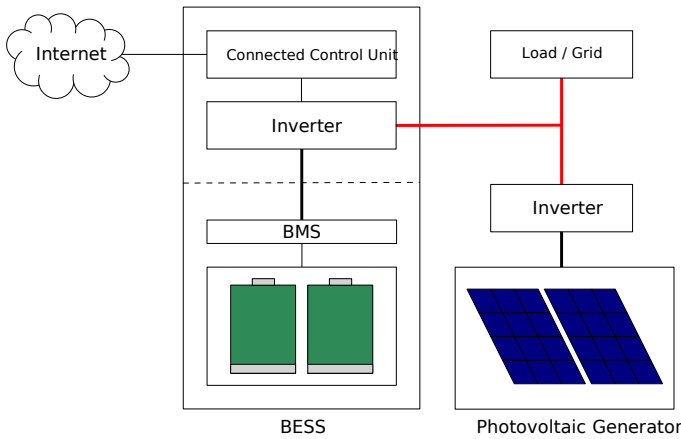


Fig. 1. Components of a typical BESS

- At least eight out of ten systems allow an attacker with access to the local network to manipulate the settings of the BESS<sup>1</sup>.
- None of the systems analyzed provide adequate protection of usage or personal data.
- At least three systems contain flaws, which allow attackers to compromise them remotely<sup>2</sup>. One contains a severe flaw, which enables a successful attacker to compromise identical systems from the same manufacturer too.

We have informed the manufacturers about the vulnerabilities. At the time of writing, the security flaws have not been fixed. Therefore, the names of all manufacturers are omitted.

### III. RELATED WORK

Security for IoT devices is currently discussed actively. Research on all kinds of IoT devices, e.g. vehicles, medical devices and smart home devices, repeatedly identifies severe security issues [12]–[14]. Bekara [5] analyzes security issues and challenges arising from connected IoT devices involved in the power grid infrastructure. However, there has been little academic work in the field of BESS. A security analysis of related devices has been performed but not academically published [15]. The stability of the power grid can be attacked as a whole, but specific weak links can be targeted by attackers to maximize the impact of targeted fluctuations [16]. Besides this threat to the stability of the power grid and the DDoS potential outlined in Section I, privacy threats are especially relevant for BESS: The authors of [8] show that a household’s electricity usage profile can reveal sensitive information about the owner, e.g. which channel the TV was displaying.

### IV. BATTERY ENERGY STORAGE SYSTEMS

Figure 1 shows the components of a typical BESS. The Battery Management System (BMS) handles charging and discharging the batteries and enforces safety parameters such

as the minimum and maximum cell voltage and current limits to protect the battery from physical damage. Most BESS allow feed-in operation to the power grid. The BESS’s inverter transforms the DC energy output, feeds it into the power grid and ensures adherence to local regulations for feed-in power and frequency. Most BESS contain a Connected Control Unit (CCU) to provide a configuration interface for both the homeowner and the installer. Usually, the installer uses a separate login to configure system parameters such as the regulatory domain and some BMS parameters. Homeowners are provided with energy statistics and some (often reduced) BMS settings. Typically, devices are connected to a cloud application of the manufacturer, allowing their users to view the status of their BESS and sometimes even change the configuration remotely.

### V. TEST SETUP AND METHODOLOGY

We had access to ten different off-the-shelf BESS from ten different manufacturers. All devices were purchased via normal sales channels and manufacturers were not involved or informed in advance about the tests. Most of the devices were installed in 2016, two models were added at the end of 2017 and early 2018. The systems were connected to a local area network under our control, Internet connection was enabled when needed.

#### A. Our methodology

Before starting the evaluation, we developed a test concept based on standard penetration testing methods similar to [17]. We defined different attacker types and threats relevant for our scenario. Furthermore, we chose to focus our tests on the CCU and its communication interfaces (see Figure 1). We did not test the impact of a compromise of the CCU on the physical safety of the BESS. As our research was performed independently of the manufacturers, we did not target their web portals. In contrast, the communication of the BESS with the portal was in scope of our tests.

We used active and passive information gathering techniques such as reading the manual, performing scans of the system, analyzing network traffic and examining the web interface of the BESS and the web portal of the manufacturer. To identify known vulnerabilities, we compared used software versions with public vulnerability databases.

Based on potential vulnerabilities and misconfigurations found, we used public and custom exploits to verify the vulnerabilities. Successful attacks yield additional information and increase the attack surface of the device, sometimes leading to further attacks.

The vulnerabilities found were scored using the industry standard Common Vulnerability Scoring System (CVSS) 3.0. In some cases, an attacker needs to combine multiple vulnerabilities into exploit chains that we also rated using CVSS.

<sup>1</sup>We could not verify the successful manipulation of settings for two BESS due to time constraints.

<sup>2</sup>We suspect one more system to be affected but could not verify the vulnerability for safety reasons.

## B. Attacker Capabilities

For our test, we considered two types of attackers.

1) *Network Attacker*: A network attacker has access to services available over the Internet. Typically, BESS are connected to a firewall-protected network. Thus, their locally provided network services are not accessible from the Internet by default and can thus not be accessed by this particular attacker. However, a network attacker can manipulate communication with servers outside the local network using a Man-in-the-Middle (MitM) attack (see Section V-C2).

2) *Adjacent Attacker*: An adjacent attacker has access to the local network and is thus more powerful than a network attacker. He can access the local web interface and other services only accessible from within the same network.

## C. Technical Terms

1) *Transport Layer Security*: Transport Layer Security (TLS) is a well-established protocol to provide an encrypted and authenticated connection between two devices. However, a TLS connection is only secure if it is setup properly. For example, by disabling certificate verification most of the security properties are lost.

2) *Man-in-the-Middle Attacks*: One common technique that is used to attack network connections (such as between a BESS and a remote server) is a MitM attack. During a MitM attack, an attacker intercepts and manipulates network packets between the two communicating parties and then forwards them to their intended destination. For example, this method can be used to decrypt and alter TLS encrypted traffic, if no proper authentication is done. To perform this attack, the attacker must have access to or become a networking node that the targeted packets pass through.

## VI. RESULTS

We found that none of the BESS tested offer full protection against targeted attacks. In all cases, potentially sensitive usage or personal data was not properly protected and could be accessed without authentication. Three manufacturers did not implement an authentication mechanism to restrict access from the local network, others failed at doing so correctly: four of the tested devices are shipped with a static default password that cannot be changed by the user. Eight of the ten devices do not properly encrypt and authenticate connections while sending sensitive data over the Internet and therefore are exposing personal information to remote attackers.

Of the eight devices that provide a firmware update functionality, at least two fail to implement the common procedure of signing the firmware cryptographically and therefore allow attackers to compromise the device with manipulated software. Both also omit the certificate check when downloading the firmware update from the manufacturer, allowing the device to be taken over by remote MitM attackers over the Internet. The manufacturer of a third device did not protect a part of the firmware that contains the files served by the web application. On a fourth device, we suspect that the firmware was not

signed, but could not verify the suspicion due to the risk of breaking the device prematurely.

Most devices are running a Linux operating system with proprietary software added by the manufacturer, often including a web interface for the end user and the installer. All devices connect to the server of their respective manufacturer; four of them allow remote administration using this connection. In three cases, we were able to gain full root user access on the underlying system and execute arbitrary code without prior knowledge or valid user passwords. On another device, we presumably could have replaced the code of the embedded bare-metal software, if the above assumption concerning the missing firmware signature is correct.

Table I contains an overview of the flaws found in the tested devices. The red cells, if not otherwise marked, indicate that we found flaws in the device and that we could perform the attack noted in the first column. The gray cells do not imply that the device contains no flaws, but only state that we were unable to successfully perform this attack in the testing period. A stronger assertion would be preferable, but is difficult to attain without source code audits or design documents from the manufacturer. Attackers willing to dedicate more resources may therefore still be able to break the security property.

In one case, we are confident all installed BESS of the same type can be compromised remotely over a misconfigured manufacturer remote administration access after extracting the credentials from one device. We suspect that at least two other BESS could be vulnerable to a similar attack, but did not verify if this is indeed the case because the manufacturer infrastructure was out of the test scope. Table II lists found all vulnerabilities with a CVSS score of 6.5 and higher. The score of the most severe vulnerability or exploit chain per BESS is also listed in Table I.

To illustrate how an attacker could abuse the vulnerabilities discovered, we describe three attacks in detail below.



### A. Attack 1

We describe an attack with a CVSS score of 9.4 (Critical) that a network attacker can perform on BESS No. 3 in Table I. Combining multiple vulnerabilities, the resulting exploit-chain allows him to gain remote administration access to all identical devices by the same manufacturer.

1) *System description*: The BESS uses a Linux operating system that runs a Virtual Network Computing (VNC) server (a protocol for remotely accessing graphical user interfaces) which requires the user to provide a password when connecting. After connecting, the user is shown a graphical interface with limited access to settings on the BESS. Using a different password (for the so-called expert mode), the user is able to manipulate more critical settings, such as operating limits depending on power grid voltage and frequency, and the power grid operating standard. The manufacturer provides a web portal from which authenticated users can use a browser-based VNC client to connect to their own BESS at home. Each BESS automatically connects to the manufacturer's web portal,

TABLE I  
SECURITY PROPERTIES OF THE TEST CANDIDATES

Device Number	1	2	3	4	5	6	7	8	9	10
Highest CVSS Score	7.9	6.8	9.4	5.4	8.8	5.4	6.3	7.0	5.4	7.1
<i>Basic Security Features</i>										
Default Passwords Changeable	–	X	–	–	– <sup>1</sup>	– <sup>1</sup>	– <sup>1</sup>	X	X	–
User Can Update Firmware	X	X	–	–	X	X	X	X	X	X
<i>Uncovered Flaws</i>										
Usage or Personal Data Exposed										
Transmitted Data Eavesdropped										
Compromised Remotely								2		
Firmware Updates Compromised			◦	◦				2		3

	The property was not broken during the tests
	The property was broken
◦	The property does not apply

- <sup>1</sup> No Password required  
<sup>2</sup> Unverified  
<sup>3</sup> Some parts of the firmware are unsigned

thus enabling the manufacturer to communicate with the BESS even through a firewall.

## 2) Vulnerabilities:

a) *Standard Password for VNC:* The password needed to connect to the VNC server is the same on all BESS. Using the password, the attacker can authenticate to any BESS he can connect to. This vulnerability has a CVSS score of 6.7 (Medium).

b) *Standard Password for Expert Mode:* The password for the expert mode is also the same on all BESS. Knowing the password, an attacker with access to the VNC server can elevate his access level to expert mode. This vulnerability has a CVSS score of 6.2 (Medium).

c) *Connecting to other BESS:* The manufacturer's web portal contains severe flaws enabling an attacker to set up a VNC connection to any BESS by this manufacturer without providing any authentication. The BESS are identified by a unique ID, which seems to increment continuously, making it easy to guess valid IDs. This vulnerability has a CVSS score of 0.0 (None). This is due to the fact that on its own, this vulnerability has no negative impact as the VNC password is required to access the graphical user interface (GUI).

3) *Performing the Attack:* An attacker with both passwords can connect to any device through the public manufacturer portal using a WebSocket and a standard VNC client. He can then gain access to the expert settings via the menu. In summary, this attack has a CVSS score of 9.4.

4) *Uncertainties:* In the course of our research, we have tested this attack only against the BESS provided to us. However, due to the genericness of the password of the VNC server and the fact that the password for the expert mode is included in the binary file of the GUI, we are confident that they are not specifically generated for each device, but are identical for all devices of this type.

5) *Impact:* Combining the three vulnerabilities as described above, an attacker is able to manipulate critical system settings on any BESS by this manufacturer. He can, for example,

perform (simultaneous) emergency shutdown operations or manipulate settings so that the BESS does not conform to legal requirements (such as power grid operating standards) or does not operate economically anymore.

## B. Attack 2

The second attack we present is a MitM attack with a CVSS score of 7.9 (Critical) that can be performed by a network attacker and affects device No. 1 in Table I. Using the vulnerability, allows to gain administrative access to the device.

1) *System description:* The BESS runs a Linux operating system and regularly connects to the manufacturer to report errors, upload data, and download updates.

2) *Vulnerabilities:* Even though the BESS uses TLS to download updates, a MitM attacker can eavesdrop on and manipulate the connection. The reason is that the BESS does not validate the certificate of the manufacturer's server correctly. The connection is used to transmit software updates, which are not protected by a cryptographic signature and are thus prone to manipulation.

3) *Performing the Attack:* An attacker can intercept the TLS connection between the BESS and the manufacturer and manipulate software updates during transmission. This allows him to install a backdoor by injecting code into software components that are installed on the BESS.

## C. Attack 3

We demonstrate a third attack, which affects device No. 5 and was rated with a CVSS score of 8.1 (High). This attack allows a remote MitM attacker or adjacent attacker to gain root privileges on the CCU of the BESS and unconditionally modify the software it runs.

1) *System description:* The CCU of the vulnerable BESS features an embedded Linux distribution and runs a web interface on port 80 for use by the customer. The web interface is available on the local network, but is also forwarded to

TABLE II  
VULNERABILITIES WITH A CVSS SCORE OF 6.5 AND HIGHER

Device	Summary	CVSS Score	Comment
1	Unauthenticated Firmware Updates over untrusted TLS-connection	7.9	
1	Insecure Remote Administration Access to manufacturer Server	7.3	
2	Unauthenticated Modification of System Settings	6.8	
3	(Chain): SSH Access via manufacturer remote access using default Root Password	9.4	
3	(Chain): VNC Access via manufacturer web portal using default Password	9.4	
3	Undocumented default Root Password	8.2	
3	Insecure Remote Administration Access to manufacturer Server	6.7	Unverified
3	Unchangeable default VNC Password for Remote Access to all Devices	6.7	Unverified
5	Arbitrary Code Execution in Local Web Interface	8.8	
5	Undocumented Default SSH Login	8.8	
5	(Chain) Remote Arbitrary Code Execution in Local Web Interface	8.1	
5	Unauthenticated Firmware Updates over untrusted TLS-connection	7.8	
5	Insecure Remote Administration Access to manufacturer Server	7.8	
5	Default Login for Log Storage FTP Server	6.9	Log retrieval unverified
8	Unauthenticated Firmware Updates over local Network	7.0	Unverified
10	Access to unprotected Installer Password for Remote Administration	7.1	Impact unverified

the manufacturer’s server, presumably to facilitate remote maintenance and support.

#### 2) Vulnerabilities:

a) *Insecure Backup and Restore:* The web interface contains a flaw in the backup functionality that allows an unauthenticated attacker to execute arbitrary code on the CCU. The backup file is an archive containing parts of the file system. Besides the expected configuration files, the backup file also contains script code that is executed as part of the web application which runs with root privileges. The downloaded backups can be modified and still be restored, thus overwriting parts of the system with attacker-defined data. This vulnerability is rated with a CVSS Score of 8.8 (High).

b) *Remote Access on Untrusted SSH-Servers:* The remote access is implemented by forwarding the local TCP port 80 to a remote server using the Secure Shell (SSH) protocol. The SSH protocol protects against MitM attacks by checking the host-key of the server against a local database. However, the SSH client of the BESS does not perform host-key verification. This configuration removes the burden of key management from the manufacturer, but facilitates MitM attacks and has a CVSS score of 7.8 (High).

3) *Performing the Attack:* The first vulnerability can easily be used by an adjacent attacker to inject code. The second vulnerability allows to execute this attack remotely over the Internet. By performing a MitM-attack on the SSH connection, an attacker can access the web interface through the forwarded port. This allows the attacker to open a backdoor to get full access to the system.

The overall attack chain is rated lower than the first vulnerability alone when using the CVSS methodology, because even though the attack can be performed remotely over the Internet it is considerably more difficult. Although this is not represented in the score, the threat from the chained attacks may be more relevant to most users.

#### D. Common Issues

The mistakes the manufacturers made are often similar and are usually considered solved problems in other areas. One example is the insecure implementation of firmware updates. Only half of the tested BESS provide a firmware update process that we did not break in the testing period. Two devices do not allow the user to update the firmware at all, which implies that vulnerabilities cannot be fixed. Three devices provide either automatic updates over the Internet or a way for users to manually perform the update, but fail to assert the authenticity of firmware images. Thus, attackers are able to manipulate the contained software and in two cases take over the device completely without prior knowledge or valid credentials.

Issues are widespread between manufacturers and most violate basic security best practices. Some of the default security features of standard tools were deliberately disabled: In two of the tested devices, certificate validation for outgoing TLS connections was omitted by setting the `curl -k` parameter. The devices transmit usage and monitoring data, and sometimes download (unsigned) firmware update images. Some devices also used the unencrypted and unauthenticated File Transfer Protocol (FTP) protocol to transmit logs and usage data.

Often manufacturers ignored a fundamental security paradigm and built custom solutions instead of using well-established algorithms and protocols. One manufacturer implemented a proprietary symmetric encryption scheme to send power consumption data over the Internet, which was easy to break. Others sent seemingly encrypted data over UDP or HTTP instead of using the time-tested TLS protocol.

From the above observations, we conclude that most manufacturers are missing the required software and security knowledge when making design decisions in the development process. We are confident that BESS would be more secure and

development effort could be reduced, if manufacturers used standard protocols and software.

## VII. CONCLUSION AND FUTURE WORK

To examine the state of security of BESS, we analyzed ten commercially available BESS by performing penetration tests. Since BESS are also being considered to fulfill more critical roles in the power grid, inadequate security measures could be especially dangerous.

We found numerous vulnerabilities in the software of all of the tested devices and rated their impact using CVSS. Issues range from moderate (like missing authentication) to highly critical (like the ability to compromise all connected devices remotely). In order to illustrate the types of vulnerabilities we found, we presented three flaws in detail.

Based on the types and distribution of issues between manufacturers, we conclude that the security of BESS is in a similar bad state as the security of other IoT devices. All systems we examined contained errors that stem from fundamental design flaws and violations of known best practices. This suggests that security does not play an important role in the development process and knowledge about security mechanisms and processes is lacking. In their current state, BESS should not be used for more important tasks in the power grid.

In future work, it should be investigated if standards, guidelines and certifications similar to what has been done with Smart Meter Gateways could contribute to prevent such mistakes from happening in the future.

## REFERENCES

- [1] A. Bräutigam, T. Rothacher, H. Staubitz, and R. Trost, *The Energy Storage Market in Germany*, Jan. 2019. [Online]. Available: [https://www.gtai.de/GTAI/Content/EN/Invest/\\_SharedDocs/Downloads/GTAI/Fact-sheets/Energy-environmental/fact-sheet-energy-storage-market-germany-en.pdf?v=12](https://www.gtai.de/GTAI/Content/EN/Invest/_SharedDocs/Downloads/GTAI/Fact-sheets/Energy-environmental/fact-sheet-energy-storage-market-germany-en.pdf?v=12) (visited on Apr. 1, 2019).
- [2] S. Enkhardt, *Sonnen to provide primary balancing power to German grid from networked home storage*, Dec. 2018. [Online]. Available: <https://renewableenergytimes.com/2018/12/05/sonnen-to-provide-primary-balancing-power-to-german-grid-from-networked-home-storage/> (visited on Apr. 2, 2019).
- [3] Battery Technical Center. (2019). Safetyfirst - solar power home storage on the test, [Online]. Available: [https://www.batterietechnikum.kit.edu/english/170\\_695.php](https://www.batterietechnikum.kit.edu/english/170_695.php) (visited on Jul. 17, 2019).
- [4] EuPD Research. (2018). sonnen und LG Chem als Führungsduo im deutschen Markt für Heimspeicher, [Online]. Available: <https://www.eupd-research.com/en/news/view-details/sonnen-und-lg-chem-als-fuehrungsduo-im-deutschen-markt-fuer-heimspeicher/> (visited on Jul. 24, 2019).
- [5] C. Bekara, “Security issues and challenges for the iot-based smart grid,” *Procedia Computer Science*, vol. 34, pp. 532–537, 2014.
- [6] M. O’Neill, “Insecurity by design: Today’s iot device security problem,” *Engineering*, vol. 2, no. 1, pp. 48–49, 2016.
- [7] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, *et al.*, “Understanding the mirai botnet,” in *26th USENIX Security Symposium (USENIX Security 17)*, 2017, pp. 1093–1110.
- [8] U. Greveler, B. Justus, and D. Loehr, “Multimedia content identification through smart meter power usage profiles,” *Computers, Privacy and Data Protection*, vol. 1(10), 2012.
- [9] S. Soltan, P. Mittal, and H. V. Poor, “Blacklot: Iot botnet of high wattage devices can disrupt the power grid,” in *27th USENIX Security Symposium (USENIX Security 18)*, 2018, pp. 15–32.
- [10] BBC News. (2017). Ukraine power cut ‘was cyber-attack’, [Online]. Available: <https://www.bbc.com/news/technology-38573074> (visited on Jul. 17, 2019).
- [11] Dragos Inc. (Jun. 2017). CRASHOVERRIDE - Analysis of the Threat to Electric Grid Operations, [Online]. Available: <https://dragos.com/wp-content/uploads/CrashOverride-01.pdf> (visited on Apr. 19, 2019).
- [12] C. Miller and C. Valasek. (2015). Remote exploitation of an unaltered passenger vehicle, [Online]. Available: [https://ericberthomier.fr/IMG/pdf/remote\\_car\\_hacking.pdf](https://ericberthomier.fr/IMG/pdf/remote_car_hacking.pdf) (visited on Apr. 29, 2019).
- [13] A. Raghunathan and N. K. Jha, “Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system,” in *IEEE 13th International Conference on e-Health Networking, Applications and Services*, 2011, pp. 150–156. DOI: 10.1109/HEALTH.2011.6026732.
- [14] O. Alrawi, C. Lever, M. Antonakakis, and F. Monrose, “Sok: Security evaluation of home-based iot deployments,” in *IEEE Symposium on Security & Privacy*, 2019, to appear.
- [15] W. Westerhof. (2017). Horus scenario - exploiting a weak spot in the power grid, [Online]. Available: <https://horusscenario.com/> (visited on Apr. 15, 2019).
- [16] B. C. Lesieutre, S. Roy, V. Donde, and A. Pinar, “Power system extreme event screening using graph partitioning,” in *2006 38th North American Power Symposium*, Sep. 2006, pp. 503–510. DOI: 10.1109/NAPS.2006.359618.
- [17] K. A. Scarfone, M. P. Souppaya, A. Cody, and A. D. Orebaugh, “Sp 800-115. technical guide to information security testing and assessment,” Gaithersburg, MD, United States, Tech. Rep., 2008.