Security Analysis of Devolo HomePlug Devices

Rouven Scholz
Institute of System Security, TU Braunschweig

Christian Wressnegger
Institute of System Security, TU Braunschweig

ABSTRACT

Vulnerabilities in smart devices often are particular severe from a privacy point of view. If these devices form central components of the underlying infrastructure, such as Wifi repeaters, even an entire network may be compromised. The devastating effects of such a compromise recently became evident in light of the Mirai botnet. In this paper, we conduct a thorough security analysis of so-called HomePlug devices, which are used to establish network communication over power lines. We identify multiple security issues and find that hundreds of vulnerable devices are openly connected to the Internet across Europe. 87 % run an outdated firmware, showing the deficiency of manual updates in comparison to automatic ones. However, even the default configurations of updated devices lack basic security mechanisms.

ACM Reference Format:
Rouven Scholz and Christian Wressnegger. 2019. Security Analysis of Devolo HomePlug Devices. In *12th European Workshop on Systems Security (EuroSec '19), March 25–28, 2019, Dresden, Germany.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3301417.3312499

1 INTRODUCTION

The growing dissemination of smart devices and their increasing entanglement in our everyday life emphasize the security requirements for protecting the privacy of users and their data [1, 7]. While convenient, every additional device potentially introduce new attack vectors—especially if connected to the Internet. Even worse, these devices and gadgets are often not designed with security in mind [25] and even if, vulnerabilities may still enable attacks with devastating effects [3, 23]. The weaknesses of a single device can then quickly compromise an entire network and the computers connected to it.

Unfortunately, the security of such devices and the convenient use of them often do not play well together, such that in many cases vendors opt for usability rather than restrictive access policies. This is particular troublesome when this not only concerns the devices themselves, but the network forming the backbone of these gadgets. Also for Wifi routers and so-called PowerLAN adapters, the automagical configuration and plug-and-play are top selling points. "PowerLAN" refers to network communication over power lines by modulating additional signals on top of the power frequency and is often used to retrofit homes for Internet connectivity and home automation, where additional wiring and house-wide Wifi coverage is not possible. Depending on the frequency used for modulation, the data throughput and range varies: For home networks, for instance, a range between 1–100 MHz is used [14] and sometimes referred to as broadband over power lines or "HomePlug" as the family name for the involved standards.

Spanning a local network over an physically not limited wiring might seem daring, but usually the risk is contained using frequency attenuation. Within the established network, such devices typically offer a web interface as a default way of remote administration. Sometimes, also an expert or development access and an additional layer for device-to-device communication is introduced. Usually, these interfaces are not exposed to the Internet and are authenticated to avoid unauthorized access and reconfiguration.

In this paper we investigate the security of a popular series of HomePlug devices from a large internationally operating vendor (Devolo [8]). We first dissect the firmware of the devices to collect information about the inner workings and systematically pinpoint weak spots. In the course of this, we have identified a number of critical vulnerabilities that may—in the worst case—be used to remotely take over the entire network and connected devices. All vulnerabilities have been responsibly reported to the vendor.

Moreover, we survey the dissemination of the devices, estimate the number of installations of individual firmware versions and measure how many devices are vulnerable to remote attacks. We find that in total 1,991 devices are openly connected to the Internet and expose the remote configuration interface that enables an attacker to fully take over control of a device. Three out of four of the found devices additionally allow external access to the web-based administration interface, where 95 % of them do so unauthenticated, not requiring any password. While these devices are comparably easy targets, the ratio furthermore suggests that also a large portion of HomePlug devices, which are not directly connected to the Internet, can still be exploited due to the lack of authentication by using specially crafted web pages or links in e-mails sent to a user on the target network in a phishing campaign.

In summary we make the following contributions:

- **In-depth security analysis.** We conduct a thorough analysis of the HomePlug (power line communication; PLC) devices of Devolo, a large internally operating network vendor, and uncover critical vulnerabilities that allow remote exploitation.
- **Analysis of the dissemination.** We actively look for vulnerable instances directly exposed to the Internet, which thus are reachable for remote attackers. In doing so, we are able to show that a large portion of the deployed devices indeed are attackable in practice.
- **Open-source tools.** We make all our tools for analyzing the devices' firmware publicly available to foster future research. We also provide proof-of-concept implementations of the attack that have also been responsible reported to the vendor.

EuroSec '19, March 25–28, 2019, Dresden, Germany

ACM ISBN 978-1-4503-6274-0/19/03…$15.00
https://doi.org/10.1145/3301417.3312499

Table 1: Selection of configuration variables of a Devolo dLAN 500 series device.

Variable	Functionality	Values	Writable via DHCI/Web
`HomePlug.SetFactoryDefaultPassword`	The default network password	`HomePlugAV`	
`System.Baptization.Hostname`	The device's host name	`string`	✓
`System.Baptization.RemoteSyslog`	Recipient of the system log	IPv4 address	✓
`System.Baptization.Telnetd`	Activate telnet daemon	`0,1`	✓
`System.DeviceType`	Type of device	`string`	✓
`System.FactoryDefaults`	Restore factory settings	`1`	✓
`System.Reboot`	Reboot device	`1`	✓
`System.SerialNumber`	Serial number of the device	`string`	
`Wireless.AP1.Active`	Enable Wifi	`on` / `off`	✓
`System.ProductName`	Name of the product	`string`	

The remainder of the paper is structured as follows: Section 2 provides an analysis of a popular series of HomePlug devices and describes several severe software vulnerabilities, before we inspect the dissemination of exploitable devices on the Internet in Section 3. In Section 4, we resume with a description of a remote attack to take over PowerLAN devices, even if they are not directly connected to the Internet. Subsequently, we look upon countermeasures in Section 5 and discuss related work in Section 6. Section 7 concludes the paper.

2 SECURITY ANALYSIS

We begin with a description and security analysis of the dLAN 500 HomePlug device series as distributed by Devolo. We use this particular device as an example for similar products of the same vendor, such as the successor series dLAN 550 and dLAN 1200.

The device is build upon the WiFi-enabled SoC board Atheros AR9331 and is powered by a MIPS 24KC CPU at 266 MHz [4]. The firmware consists of a rather old Linux Kernel version 2.6.31, for which, almost 10 years after its initial release, a number of vulnerabilities exist as of today. Also, while the system in principle ships with executable-space protection, the used CPU unfortunately does not support this. All this, however, is not part of our focus in this paper. We rather inspect the implementations on top of the operating system and the configuration of the provided services.

The dLAN 500 provides four different access points: 1) The PLC network interface for the underlying communication between devices on the power line, 2) an API for the automatic configuration of new device on the network, 3) the customer's web-based administration frontend, and 4) developer access using the Telnet protocol [22]. By default only the PLC network interface is authenticated. However, the default password is set to `HomePlugAV` and in practice it frequently is not changed. Also, after a factory reset the publicly documented default password is in place again, such that an attacker may use a reset as starting point of an attack. All other access points, even the Telnet service (if enabled), require *no* credentials. However, the customer may configure HTTP basic authentication for the web interface.

Devolo Host Configuration Interface (DHCI). In contrast to the other access points, this interface always remains unauthenticated to ensure the automatic configuration of devices on the same network. It operates on TCP port 22879 and communicates via HTTP `PUT` or `POST` requests similar to a REST API. Using this interface it is possible to set and retrieve configuration or status variables of the device. Response codes and result data are encoded as JSON objects. While only a few variables are required to realize the vendors "WiFi Move" service for automatically configuring devices, the DHC interface still allows to access and modify several hundred internal variables. A small selection is given in Table 1 to convey a feeling for the criticality of the exposed functionality. If an attacker gains access to this interface, she is able to retrieve the system's log, enable developer access via Telnet, perform a factory reset, or reboot the device. Under no circumstances the DHCI port should hence be accessible by unauthorized entities to prevent a security breach.

Firmware. Devolo uses a proprietary file format with the file extension `.dvl` for packaging the device's firmware. Each package starts with a 8 bytes magic value (`\x86dVL\x0D\x0A\x1A\x0A`) followed by a number of so-called chunks. Each chunk specifies its type as 4 byte long string, its size as 32 bit integer, the actual data and a CRC-32 checksum. The exact structure is presented in Figure 1.

This way, data from different sources are compactly bundled into a single file, such as: Kernel images (chunk type `KRNL`), entire file systems (`FLSY`), version information (`VRSN`), etc. The successor device series of the dLAN 500 also include a software signature to prevent unauthorized modifications. The model at hand, however, does not and thus an adversary can replace the firmware at will. Please note, that if the attacker already has access via Telnet even software signatures do not prevent the modification of the system.

```
typedef struct {
    uint32_t  size,
    char      type[4],
    uint8_t   data[size],
    uint32_t  checksum
} chunk_t;
```

Figure 1: Structure of a single chunk as used in the file format of Devolo firmware packages.

As part of our research we provide tools to unpack, modify, and re-package firmware images available at: `https://dev.sec.tu-bs.de/devolo`

2.1 Vulnerabilities

In the scope of our research, we have discovered vulnerabilities from different classes: 1) A cross-site scripting (XSS) attack in the web administration interface as well as a XSS filter bypass, 2) the possibility to evade the same origin policy using DNS rebinding, and 3) a denial-of-service. Table 2 summarizes our findings.

Table 2: Discovered vulnerabilities in the most popular device in our analysis, the Devolo dLAN 500 series.

Version	Vulnerability	Comment	Fixed
3.0.0	XSS	unescaped user input	✓*
3.2.0	XSS filter bypass	faulty URL decoding	
3.2.0	DoS	host name → "	
3.2.0	DNS rebinding	misconfiguration	

* Fixed in version 3.1.0

Cross-Site Scripting. Up to version 3.0.0 the web interface of the dLAN 500 series has contained a cross-site scripting vulnerability based on central parameters that are directly accessible via the web interface. In particular it has been possible to straightforwardly pass JavaScript code, embedded in `script` tags, to the parameters `_file`, `_style`, `_lang`, `_page`, and `_dir`. Moreover, the variable `_idx` has been embedded in JavaScript code, such that an attacker has been able to execute code by merely breaking out of a variable assignment: `";alert(. . . );//`. Fortunately, this vulnerability has been fixed in recent versions of the firmware.

Additionally, the program that handles values from the web interface and applies them to the device (`htmlmgr`), implements its own URL decoding function. Unfortunately, it not only decodes hexadecimal values (up to `%FF`), but all two-digit combinations of `[0-9a-zA-Z]` after a percentage sign. As an example, the values `%2S`, `%3C`, and `%ZC` consequently all refer to the less than sign '<'. In combination with the cross-site scripting vulnerability described earlier, this is a potent tool for a phishing attack. How such an attack can be implemented to take over the device is described in Section 4.

DNS Rebinding. For a successful phishing attack as suggested above it is essential to bypass the same origin policy [27]. This may be achieved using a cross-site scripting attack or in the absence of such, by DNS rebinding [16]. To mount the attack one needs to be in control of a domain, for which the adversary answers DNS requests with a low time-to-live (TTL). Using this domain the attacker also serves the initial exploit and rebinds the domain to the target IP in the local, externally not reachable, network for a second request. Thereby, it is possible to effectively bypass the same-origin policy as the browser concludes that both requests belong to the same origin (identical protocol, host, and port).

The HTTP server used by the HomePlug device implements effective counter measurements against DNS rebinding. However, per default the firmware is configured to not make use of this option.

Denial of Service. Up to the most recent version of the dLAN 500 series firmware (version 3.2.0 as of the time of writing) it is possible to cause a denial-of-service by providing faulty settings. If the host name is set to the quote character, the device's DHCP client does not assign an IP address, rendering the device unreachable. The host name is not modified during a factory reset, triggered by the reset button on the device, such that an end-user has no way of recovering the device. Further analysis has shown, that the device additionally assigns a random IP in the range `169.254.0.0/16`, such that one is able to reset the values using the DHC interface. To the best of our knowledge, this however is not documented.

3 DISSEMINATION

With the knowledge about the inner workings of the HomePlug device series of Devolo, we next investigate the dissemination of these devices in the wild. As PowerLAN adapters usually are not connected to the Internet, we are only able to estimate the absolute number and focus on those instances that are vulnerable.

We hence look for devices that expose the DHC interface on TCP port 22879. These are the most critical instances, as the management interface allows to take over the devices if they are not authenticated. To this end, we scan the Internet for open ports at 22879 using MASSCAN [11] and ZMap [9]. To avoid false positives we verify that the found hosts answer with DHCI-specific JSON responses. For such devices, we then additionally check whether also the web-based administration interface is reachable. Table 3 summarizes our findings. In total, 1,991 HomePlug devices expose crucial remote administration functionality to the general public using the Devolo's DHC interface. This already allows an attacker to directly take over the device by starting the Telnet service with an empty password (28 % of the networks do not filter TCP port 23) or flashing a new firmware. Interestingly, only for about three quarters of these, the web page for remote administration is reachable as well. This seems to indicate a certain awareness for the fact that sensitive information is being distributed via the web interface, by simultaneously not knowing about the DHCI functionality. Only 5 % of the reachable web interfaces are protected through HTTP's basic access authentication, though.

Table 3: Reachable HomePlug devices during our analysis.

DHCI	Web	Authenticated
1,991	1,427 (72 %)	72 (5 %)

Looking at the location of the gathered IP addresses, shown in Figure 2, reveals that affected devices are spread throughout Europe with particular prevalence in Belgium (686 devices), Germany (205), Sweden (166), and Switzerland (78). Given the fact that Devolo is a German vendor this distribution is not entirely surprising. However, the high number of occurrences in Belgium still is particular. By analyzing the landing page of the devices, we have discovered identical hardware with different vendor names. "VOO", for instance, is a Belgian cable company [20], that sells re-branded HomePlug devices from Devolo alongside contracts for Internet connectivity. This suggests that we are seeing large amounts of vulnerable default configurations packaged with an average contract.

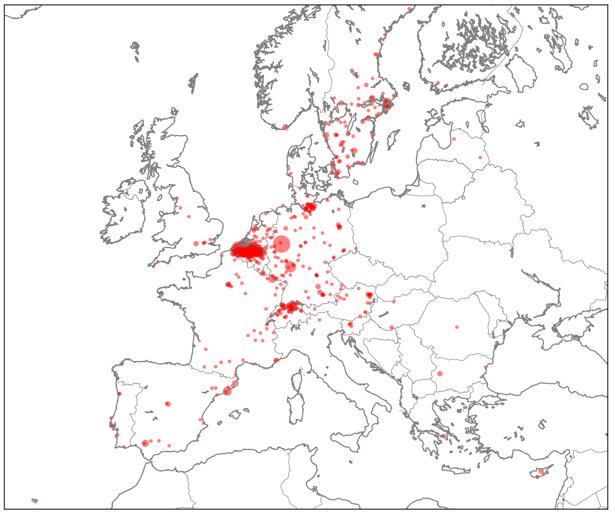

Figure 2: Vulnerable HomePlug devices across Europe.

We further evaluate the different hardware and firmware versions that are in circulation at the time. We have discovered devices from the two most recent series (dLAN 1200 and dLAN 550) as well as the older models (dLAN 500), which we have used for our initial analysis. As the landing pages have been gathered 24 h after the initial scan, not all devices have still been reachable: 44 % of the devices apparently operate on dynamic IP addresses and therefore could not be queried. The remaining 1,113 devices are listed in Table 4. Interestingly, 82–90 % of the devices run an outdated firmware. For the current device series, dLAN 550 and dLAN 1200, the most recent versions of the firmware are 1.2.0 and 2.2.0, respectively. Both have been released in August 2018, five months before our analysis. For the dLAN 500 series the release of version 3.2.0 dates back to December 2016. This clearly shows that a pull-based methodology for updating such devices (the customer needs to actively update the firmware) is not reliable for securing the system.

Table 4: Discovered hardware and firmware versions.

	Firmware		
Device	Version	Latest *	# Instances
500 Series	1.0.*		3 (1 %)
	1.1.*		1 (0 %)
	2.*.*		0 (0 %)
	3.0.*		131 (22 %)
	3.1.*		390 (67 %)
	3.2.0	✓	60 (10 %)
550	1.0.*		12 (11 %)
	1.1.*		88 (77 %)
	1.2.0	✓	14 (12 %)
1200 Series	1.0.*		42 (10 %)
	1.1.*		32 (8 %)
	1.2.*		45 (10 %)
	1.3.*		128 (31 %)
	2.0.*		90 (22 %)
	2.1.*		3 (1 %)
	2.2.0	✓	74 (18 %)
			1,113 (56 %)

* As of January 2019

Moreover, for the dLAN 500 series 22 % of the discovered devices operate on firmware version 3.0.0, for which we have discovered and reported a cross-site scripting attack. This vulnerability can be used for a fully remote attack even in absence of the DHC interface as we describe in the following section, but has been fixed in subsequent versions.

4 ATTACKING THE DEVICE

Finally, we present a fully remote attack against Devolo HomePlug devices, that does not rely on the DHC interface, but specially crafted phishing e-mails or web pages. We use the vulnerabilities described in Section 2.1, that have also been reported to the vendor. The attack requires three steps: 1) Landing the attack and localizing the target, 2) taking over the device, and 3) covering up one's tracks. If the DHC interface is accessible from the Internet, as it is the case for the 1,991 devices we have discovered earlier, we can directly proceed with the hostile takeover.

Landing the attack. As we assume that we have no direct access an adversary is required to craft a special web page that performs the attack once it is accessed by the victim on the target network. In practice this can be achieved using spear phishing [15, 28] or watering hole attacks [2]. This web page first scans the network for the target device, which is not accessible from the Internet but from the local network. Such rudimentary port scans can be done using JavaScript [12, 13]. At this point, the way forward depends on whether the web service is authenticated or not. If it is, the attacker additionally needs to rely on an existing session and Cross-Site Request Forgery [21, 26]. However, our study on the prevalence of HomePlug devices shows that 95 % of the web-based administration interfaces are *not* password protected.

Hostile Takeover. For a complete takeover of the device a new firmware may be uploaded and flashed to the memory. To this end, an existing firmware needs to be unpacked, modified and repackaged as described in Section 2. For uploading the firmware the web interface needs to be used. This however requires to bypass the same-origin policy, for instance, using DNS rebinding [16]. Alternatively, one might also make use of an XSS vulnerability as available up to version 3.0.0 of the dLAN 500 series.

Cover your tracks. In order to disguise the takeover an adversary may optionally retrieve the current configuration and settings from the device before flashing a new firmware in the previous step. All settings including passwords are echoed verbatim to the system's log of the device such that it suffices to retrieve this log file. Conveniently, this is possible by setting the device's `System.Baptization.RemoteSyslog` variable. The value specifies the IP that should receive the log on UDP port 514. This IP is *not* restricted to the local network. Figure 3 shows an except of an exemplary log output. After the reboot of the newly flashed firmware the variables can then be reset either using the DHC interface or directly via Telnet.

```
1  Registered external SvcMgr: "HtmlMgr", rv=OK, internal=0x40000002
         , external=0x40000001
2  SvcMgrProxy::command() is not implemented yet
3  SvcMgrHomePlug: checking for config changes
4  SvcMgrProxy::command() is not implemented yet
5  SysMgr: WARNING! USING OLD AND UNSAFE METHOD
6     Tree::setValue(
7         const std::string &key='SystemPassword',
8         const std::string &value='Lj9AS3ihzNdy'
9     )!
10 Size 0x8e3 (0x8e3)
11 'create': OK
12 Size 0x8e3 (0x8e3)
13 'update': OK
14 Config commit done.
```

Figure 3: Excerpt of a syslog as produced by the dLAN 500. Lines 5–9 show that even password are logged in clear.

5 COUNTERMEASURES

For preventing a remote takeover as described in the previous section and similar attacks on the device, a number of seemingly trivial actions can be performed: First and most importantly, the DHCI remote administration interface must not be accessible externally and under no circumstances without authentication. Especially the latter impairs usability to a certain extend, but is of utmost importance. Also whitelisting communication partners can be a reasonable option. The same holds true for remote receivers of the system's log. These should be strictly constrained to the local network and ideally disabled in production at all. Also, the availability of a Telnet client in a shipped product is questionable. In case of need, access should at least be restricted. Here, the Telnet services however does not require any credentials in the default configuration.

Basic configuration measures aside, providing new software in form of an entire firmware should at any prize be signed and the signatures verified before applying any changes. In subsequent models of the vendor (550 and 1200 series) this has fortunately been implemented. Finally, the discovered vulnerabilities that allow cross-site scripting, DNS rebinding or forcing the denial-of-service of course need to be fixed. While critical and with devastating effects in the present case, such vulnerabilities are part of the process. Hence, every software vendor is advised to establish a push-based update methodology rather than relying on the customer to pull new releases, in order to be able to quickly react to incidents.

6 RELATED WORK

In recent years the research community has addressed several aspects of the security of smart devices and the "Internet of Things". Many security analyses show the intimidating influence of technology in our everyday life and the impact of security breaches.

For example, Ronen et al. [23] demonstrate how a vulnerability in remote-controlled bulbs can be used to create an IoT worm that may blackout entire cities. Attacks however are seldom as physical as this one, but concern the security and privacy of sensitive data. Smart metering data, for instance, that directly reflect on the consumers behavior may be de-pseudonymized to certain extend using machine learning [17]. Moreover, Rouf et al. [24] show that Automatic Meter Reading (AMR) technology to gather such data often lacks basic security mechanisms and may be subject to spoofing and privacy breaches. Fernandes et al. [10], on the other hand, conduct a security analysis of the Samsung's SmartThings, that allow to interface with various devices in our home environment. Rather than individual apps and devices they inspect the underlying platform and find fundamental design flaws. Moreover, 55 % of the apps are over-privileged and run with full access to the device. While these examples address an entire different field of application as we do, they highlight situations where convenience is chosen over access control—very much like we have observed with Devolo's over-privileged DHC interface for automatically configuring new devices on the network.

Another strain of research has focused on analyzing and securing generic commodity IoT devices. Celik et al. [5] present a framework for statically analyzing platform-specific source code to identify sensitive data flows that might leak information. Kim et al. [18] employ formal methods to automatically analyze IoT protocols, show that especially DoS attacks are a wide-spread issue, and present a cryptographic counter measurement. Also, active vulnerability discovery has been successfully applied to IoT devices [6, 19] in the past.

7 CONCLUSION

Smart devices and IoT gadgets have repeatedly been reported to suffer from partly severe vulnerabilities. The omnipresence of these devices in our everyday life renders data breaches a particular serious privacy invasion. Especially troublesome are incidents, where not only a single device but the entire underlying network is compromised. We have analyzed the security of PowerLAN adapters, so-called HomePlug or PLC devices, and find a worrying state of (default) configurations, next to a number of vulnerabilities. Apparently, security and authentication have largely been neglected in favor of convenience and usability during the initial installation. We identify 1,991 devices that can be directly accessed and reconfigured via the Internet. Moreover, 87 % of these are not running the latest version of the firmware for the respective hardware. We have further discussed specific countermeasures for these particular devices and plead for push-based updates rather than burdening customers with the task of updating the hardware. With a more agile update methodology and consistent authentication smart devices can effectively secured.

DISCLOSURE

All software vulnerabilities described in this paper and found as part of our research have been responsible disclosed to the vendor of the Homeplug powerline products. In total, we have reported 4 vulnerabilities and have delayed publication for an extended disclosure period of six months.

AVAILABILITY

To foster future research and improve existing implementations, we make all tools for analyzing the devices' firmware as well as proof-of-concept implementations of the attacks publicly available at:

`https://dev.sec.tu-bs.de/devolo`

ACKNOWLEDGMENTS

The authors gratefully acknowledge funding from the German Federal Ministry of Education and Research (BMBF) under the project VAMOS (FKZ 16KIS0534) and FIDI (FKZ 16KIS0786K).

REFERENCES

[1] Omar Alrawi, Chaz Lever, Manos Antonakakis, and Fabian Monrose. 2019. SoK: Security Evaluation of Home-Based IoT Deployments. In *Proc. of the IEEE Symposium on Security and Privacy*. 208–226.

[2] Sumayah Alrwais, Kan Yuan, Eihal Alowaisheq, Xiaojing Liao, Alina Oprea, XiaoFeng Wang, and Zhou Li. 2016. Catching Predators at Watering Holes: Finding and Understanding Strategically Compromised Websites. In *Proc. of the Annual Computer Security Applications Conference (ACSAC)*. 153–166.

[3] Manos Antonakakis, Tim April, Michael Bailey, Matt Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J. Alex Halderman, Luca Invernizzi, Michalis Kallitsis, Deepak Kumar, Chaz Lever, Zane Ma, Joshua Mason, Damian Menscher, Chad Seaman, Nick Sullivan, Kurt Thomas, and Yi Zhou. 2017. Understanding the Mirai Botnet. In *Proc. of the USENIX Security Symposium*. 1093–1110.

[4] Atheros Communications Inc. 2010. *AR9331 Highly-Integrated and Cost Effective IEEE 802.11n 1x1 2.4 GHz SoC for AP and Router Platforms.* Technical Report. Atheros Communications Inc.

[5] Z. Berkay Celik, Leonardo Babun, Amit K. Sikder, Hidayet Aksu, Gang Tan, Patrick McDaniel, and A. Selcuk Uluaga. 2018. Sensitive Information Tracking in Commodity IoT. In *Proc. of the USENIX Security Symposium*. 1687–1704.

[6] Jiongyi Chen, Wenrui Diao, Qingchuan Zhao, Chaoshun Zuo, Zhiqiang Lin, XiaoFeng Wang, Wing Cheong Lau, Menghan Sun, Ronghai Yang, and Kehuan Zhang. 2018. IOTFUZZER: Discovering Memory Corruptions in IoT Through App-based Fuzzing. In *Proc. of the Network and Distributed System Security Symposium (NDSS)*.

[7] Tamara Denning, Tadayoshi Kohno, and Henry M. Levy. 2013. Computer Security and the Modern Home. *Commun. ACM* 56, 1 (2013), 94–103.

[8] devolo AG. 2002–2019. dLAN Powerline adapters. Internet and Wi-Fi in any room. https://www.devolo.com/. visited January 2019.

[9] Zakir Durumeric, Eric Wustrow, and J. Alex Halderman. 2013. ZMap: Fast Internet-Wide Scanning and its Security Applications. In *Proc. of the USENIX Security Symposium*. 605–619.

[10] Earlence Fernandes, Jaeyeon Jung, and Atul Prakash. 2016. Security Analysis of Emerging Smart Home Applications. In *Proc. of the IEEE Symposium on Security and Privacy*. 636–654.

[11] Robert David Graham. 2013–2018. MASSCAN: Mass IP port scanner. https://github.com/robertdavidgraham/masscan. visited January 2019.

[12] Jeremiah Grossman. 2007. Hacking Intranet Websites from the Outside (Take 2). In *Proc. of Black Hat USA*.

[13] Jeremiah Grossman and T.C. Niedzialkowski. 2006. Hacking Intranet Websites from the Outside. In *Proc. of Black Hat USA*.

[14] IEEE Working Group: BPLPHMAC Broadband Over Power Lines PHY/-MAC Working Group. 2010. *IEEE Standard for Broadband over Power Line Networks: Medium Access Control and Physical Layer Specifications.* Standard. IEEE.

[15] Grant Ho, Aashish Sharma, Mobin Javed, Vern Paxson, and David Wagner. 2017. Detecting Credential Spearphishing Attacks in Enterprise Settings. In *Proc. of the USENIX Security Symposium*. 469–485.

[16] Collin Jackson, Adam Barth, Andrew Bortz, Weidong Shao, and Dan Boneh. 2007. Protecting Browsers from DNS Rebinding Attacks. 421–431.

[17] Marek Jawurek, Martin Johns, and Konrad Rieck. 2011. Smart Metering De-Pseudonymization. In *Proc. of the Annual Computer Security Applications Conference (ACSAC)*. 227–236.

[18] Jun Young Kim, Ralph Holz, Wen Hu, and Sanjay Jha. 2017. Automated Analysis of Secure Internet of Things Protocols. In *Proc. of the Annual Computer Security Applications Conference (ACSAC)*. 238–249.

[19] Marius Muench, Jan Stijohann, Frank Kargl, Aurélien Francillon, and Davide Balzarotti. 2018. What You Corrupt Is Not What You Crash: Challenges in Fuzzing Embedded Devices. In *Proc. of the Network and Distributed System Security Symposium (NDSS)*.

[20] Nethys SA. 2006–2019. VOO. http://www.voo.be/en/. visited January 2019.

[21] Giancarlo Pellegrino, Martin Johns, Simon Koch, Michael Backes, and Christian Rossow. 2017. Deemon: Detecting CSRF with Dynamic Analysis and Property Graphs. In *Proc. of the ACM Conference on Computer and Communications Security (CCS)*. 1757–1771.

[22] J. Postel and J.K. Reynolds. 1983. Telnet Option Specifications. RFC 855 (INTERNET STANDARD). http://www.ietf.org/rfc/rfc855.txt

[23] Eyal Ronen, Colin O'Flynn, Adi Shamir, and Achi-Or Weingarten. 2017. IoT Goes Nuclear: Creating a Zigbee Chain Reaction. In *Proc. of the IEEE Symposium on Security and Privacy*. 195–212.

[24] Ishtiaq Rouf, Hossen Mustafa, Rob Miller, and Marco Gruteser. 2012. Neighborhood Watch: Security and Privacy Analysis of Automatic Meter Reading Systems. In *Proc. of the ACM Conference on Computer and Communications Security (CCS)*. 462–473.

[25] Bruce Schneier. 2017. *Security and the Internet of Things.* Technical Report. Schneier on Security.

[26] Thomas Schreiber. 2004. *Session Riding – A Widerspread Vulnerability in Today's Web Applications.* Technical Report. SecureNet GmbH.

[27] Jörg Schwenk, Marcus Niemietz, and Christian Mainka. 2017. Same-Origin Policy: Evaluation in Modern Browsers. In *Proc. of the USENIX Security Symposium*. 713–727.

[28] TrendLabs APT Research Team. 2012. *Spear-Phishing Email: Most Favored APT Attack Bait.* Technical Report. Trend Micro Inc.