An Investigation of Vulnerabilities in Smart Connected Cameras

Joseph Bugeja, Désirée Jönsson, and Andreas Jacobsson
Internet of Things and People Research Center and Department of Computer Science and Media Technology,
Malmö University, Malmö, Sweden,
joseph.bugeja@mah.se, DesireeJoensson@gmail.com, andreas.jacobsson@mah.se

***Abstract*—The Internet of Things is enabling innovative services promising added convenience and value in various domains such as the smart home. Increasingly, households, office environments and cities, are being fitted with smart camera systems aimed to enhance the security of citizens. At the same time, several systems being deployed suffer from weak security implementations. Recognizing this, and to understand the extent of this situation, in this study we perform a global vulnerability assessment using the Shodan search engine and the Common Vulnerabilities and Exposures database. This is done to detect smart connected cameras exposed on the Internet alongside their sensitive, potentially private, data being broadcasted. Furthermore, we discuss whether the discovered data can be used to compromise the safety and privacy of individuals, and identify some mitigations that can be adopted. The results indicate that a significant number of smart cameras are indeed prone to diverse security and privacy vulnerabilities.**

Keywords—IoT; IoT security; Shodan; smart connected cameras; smart connected homes; vulnerabilities

I. Introduction

A growing number of consumers install Internet-enabled devices and household appliances in their homes. This benefits the householders offering an improved ability to monitor, control, and automate relevant aspects of their homes and house chores. Remote surveillance technologies through the use of home devices, such as smart cameras, is an area that is gaining momentum to ensure home security. Many attribute this to the thriving of the Internet of Things (IoT), low cost of electronic devices such as image sensors, and advancement of image processing [1]. This progression spread the use of camera surveillance systems to privately owned properties.

The IoT is typically described as a combination of technologies that include sensors, actuators, and smart devices with the purpose of connecting different things for increased convenience and productivity. The number of IoT devices is growing rapidly, with recent surveys estimating the number of such devices to exceed 20 billion by 2020[1]. Fuelled by the growth of the IoT, according to a research report by IHS Markit [2], in 2017, 98 million network surveillance cameras and 29 million HD CCTV cameras are expected to be distributed globally. Despite this, many IoT-enabled devices suffer from various security vulnerabilities allowing malicious threat agents, e.g. hackers, to damage devices and possibly compromise the safety, privacy, and security of householders [3].

In 2012, a software security vulnerability present in TRENDnet's IP-connected cameras was exploited, and consequently, hackers posted links to the private live feeds of nearly 700 of the cameras. The feeds displayed "babies asleep in their cribs, young children playing, and adults going about their daily lives."[2]. On a larger scale, in 2014 over 73,000 video cameras were found to be streaming their surveillance footage live on the Internet [4]. The vulnerability exploited was the default ID/password combination of the video camera devices.

Given the impact that smart connected cameras have on the security and privacy of people, in this study we set out to explore the existing global vulnerability state of Internet-connected smart cameras around the world discovered using Shodan[3] search engine. Specifically, the aim of this work is to understand: i) what kind of data is publically accessible from Internet-connected smart cameras; ii) whether the discovered data can be used to cause privacy and security risks in a smart living space, e.g. a smart home; and iii) approximate the number of network-enabled cameras on a worldwide scale that can be retrieved and potentially accessed without requiring advanced technical skills such as embedded system programming knowledge. The fact that smart connected cameras are being purchased and installed by diverse users some of which are unaware of security vulnerabilities, and that there is a group of hackers that are non-security experts but rely on free tools and publicly available information to conduct cybersecurity and privacy attacks is a serious risk [5][6]. The main motivation for this research is thus to understand the gravity of the current situation, and at the same time to propose some mitigations that can be adopted.

In addressing these aims, an experiment consisting a proof-of-concept code was developed. This code leveraged Shodan IoT search engine for discovering data, in particular banner information from smart cameras. Additionally, the Common Vulnerabilities and Exposures (CVE)[4] system was consulted for identifying pertinent vulnerabilities. Although network camera security is not a new area of investigation and several publications exist that identify possible IoT vulnerabilities, little scientific work has been done that focuses particularly on

[1] https://www.gartner.com/newsroom/id/3165317 [accessed January 10, 2018].

[2] https://www.ftc.gov/news-events/press-releases/2013/09/marketer-internet-connected-home-security-video-cameras-settles [accessed January 10, 2018].

[3] https://www.shodan.io/ [accessed January 10, 2018].

[4] https://cve.mitre.org/ [accessed January 10, 2018].

978-1-5386-3227-7/18/$31.00 ©2018 IEEE

smart connected cameras and that assume a malicious threat agent with the least technical skills and capabilities. Furthermore, this work is different to what has been published as it does not limit itself to specific camera types and models.

The remainder of this paper is organized as follows. In Section II, we provide the technical background connected to IoT security threats and vulnerabilities and follow that with a review of related literature work in Section III. Next, in Section IV, we discuss the employed research design approach. The achieved results are summarized in Section V. Subsequently, we discuss some implications of our findings and provide some guidance to consumer and vendors for mitigating such vulnerabilities in Section VI. Finally, in Section VII, we draw conclusions and specify directions for future work.

II. Background

In this section, we provide background information about smart connected cameras, Shodan search engine, and vulnerability identification as a method for finding security flaws in an information system. Furthermore, we identify existing work related to this study.

A. *Smart connected cameras*

Video surveillance, e.g. through a smart camera, is one of the oldest and most widespread technologies of security [7]. Home and business owners rely on such a system to examine their property, people, and events. Police departments reach out to homeowners with surveillance cameras to get assistance in solving crimes more rapidly [1].

Smart cameras tend to be connected to the Internet, feature some degree of autonomy, and are oftentimes integrated or form part of another computerized system [7]. For instance, a smart camera may include motion sensors, that automatically trigger a home alarm system and report an intrusion to the local police or home guard department.

Modern network cameras can be of different forms, e.g. baby monitors, pet cameras, and remote security monitoring systems possibly functioning as a full-on home automation hub. Furthermore, unlike a traditional monitoring system, these systems tend to offer advanced features such as remote live streaming, commonly facilitated through the use of a smartphone application[5], two-way talk[6], and instant alert/notifications[7] example for events requiring immediate attention or action from the householders.

Despite their benefits, such systems can leak out private information, e.g. sensitive video and audio feeds, about an environment, possibly allowing hackers to snoop on unsuspecting homeowners in their living rooms or bedrooms, amongst other things. Recently, in 2017, researchers at Bitdefender identified two camera models that were prone to buffer overflow vulnerabilities [8]. Exploiting such weakness researchers could inject commands allowing them to monitor activity on the hacked camera, overwrite passwords, and move the camera for malicious purposes including espionage[8]. This vulnerability according to the researchers is present in over 100,000 Internet-connected security cameras.

B. *Shodan search engine*

Unlike a conventional search engine like Google, that crawls and indexes the Internet by retrieving and following hyperlinks, an IoT search engine works differently. Similar to a network scanner, it examines open ports of Internet nodes and indexes the header or banner information returned by connected devices [9]. Information that it may automatically index includes: device type, model, vendor, firmware version, and other information. Developed by the programmer John Matherly back in 2009, Shodan[9] is proclaimed to be “the world’s first search engine for Internet-connected devices.”.

Shodan allows users to search for different Internet-accessible device types, such as webcams, printers, and routers, both through an online web interface and also by integrating with its Application Programming Interface (API). Moreover, Shodan can also be used to gain additional insight such as the camera geographical-location and information about potential vulnerabilities of the discovered devices. A recent open-source alternative to Shodan designed in 2015 by Zakir Durumeric is Censys[10]. This offers similar features to Shodan including programmatic access to the gathered raw data.

In our work, we use Shodan for three primary reasons: i) it has been repeatedly used by different security researchers as a tool of choice for conducting IoT security assessments (e.g. [10], [11]); ii) it comes with extensive and actively maintained documentation; and iii) it offers intuitive APIs and Graphical User Interfaces. These factors allow Shodan to be used by different users, including a low-skilled malicious threat agent.

Furthermore, we mainly interface with its API rather than its online web portal. This is as this provides a more efficient way for accessing and analyzing a huge number of devices.

C. *Vulnerability identification*

A vulnerability is commonly defined as a weakness in the security system that when exploited may cause some form or harm or loss [12]. Vulnerability types between different connected cameras can range from weak passwords, poorly protected credentials, insecure configuration management, and more. As an example, a householder might assume that their web camera is only accessible by legitimate users given its host and port number. However, with the help of Shodan (or a similar IoT search engine) it can become available potentially to anyone with an Internet connection. This is possible as commonly web cameras have ports allowing for web services (HTTP) and the Real-time Streaming Protocol open [13]. Unfortunately, these ports can be left open without any password protection or with only the default password settings.

A common source for identifying publically disclosed security vulnerabilities is the CVE database. This database is main-

[5] https://canary.is/ [accessed January 10, 2018].

[6] https://nest.com/cameras/nest-cam-indoor/ [accessed January 10, 2018].

[7] https://getpiper.com/ [accessed January 10, 2018].

[8] http://www.zdnet.com/article/175000-iot-cameras-can-be-remotely-hacked-thanks-to-flaw-says-security-researcher/ [accessed January 10, 2018].

[9] shodan.io [accessed January 10, 2018].

[10] https://censys.io/[accessed January 10, 2018].

tained by MITRE[11], a non-profit organization that investigates challenges in, e.g. the cybersecurity sector. This data source provides targeted systems, applications, and gives idea about the vulnerability impact and likelihood [14]. Alternative databases that can be used for intelligence gathering include the Exploit Database[12], VulnDB[13], and Rapid7 Vulnerability and Exploit Database[14]. In our work, we rely on the CVE database as the main vulnerability database. CVE is considered the most comprehensive database of security vulnerabilities [15].

III. Related Work

Patton et al. [10] analyzed real system exposure at a global scale. Essentially, the authors checked for default passwords against Supervisory Control and Data Acquisition (SCADA) devices, printers, and the health network using Shodan. In particular, they found 47,159 online printers out of which 19,583 were accessible via telnet without requiring authentication. However, smart connected cameras were only partially included in their study and the authors did not elaborate on vulnerabilities pertaining to them.

Moody and Hunter [5] investigate how attackers relying solely on publicly available sources posted on the Internet can take advantage of weakly protected devices and exploit them. Similar to our work, the authors focus on a specific type of malicious threat agent, termed as a script kiddy. This intruder in general does not understand the underlying mechanisms of the attack they use. However, the authors focus on smart thermostat devices and assume physical access to a device. In our case, we are assuming instead remote access to smart cameras.

Papp et al. [15] conducted a systematic review of the existing threats and vulnerabilities in embedded system based on publicly available information. The authors derive an attack taxonomy to systematically identify and classify common attacks against embedded systems. Similar to our study, Papp et al. [15] relied on the CVE database for identifying information about security vulnerabilities. Despite this, their data collection stage relies on the manual inspection of documentation, in particular proceedings of computer security conferences. In our case, we collect data automatically from actual (live) systems.

Williams et al. [11] performed a large-scale vulnerability assessment of consumer IoT devices exposed on the Internet. The authors used Shodan and Nessus[15] for vulnerability scanning. In their study, they included devices such as webcams, smart TVs, and printers, and then categorized the security risks associated with each device category. Similar to our study, Williams et al. [11], used Shodan to discover IoT devices. However, they followed an active vulnerability assessment approach; whereas in our case we are interested in a passive vulnerability assessment approach [16]. Passive vulnerability assessment is considered less intrusive, and thus carrying a lower potential to corrupt or compromise a system when compared to active vulnerability scanning.

The method we follow is similar to that of Patton et al. [10], however we specifically target smart connected cameras, a device category that was not the main focus of the aforementioned study. Additionally, we assume a malicious threat agent that has arguably the least technical skillset, i.e. an attacker armed solely with ready-made tools and access to public information sources [6]. Similar to Papp et al. [15] we leverage the CVE database as our primary source for discovering security vulnerabilities but our study is different to theirs as our emphasis is not on building an attack taxonomy. Instead, we focus on discovering vulnerable smart connected cameras and discussing whether the data being transmitted can be used to compromise the privacy and security of individuals. The adopted research approach is elaborated on in Section IV.

IV. Research Design

Our research design consists of an experimental setup composed of three main components: data collection, data extraction, and vulnerability analysis. The vulnerability analysis stage feeds back to the data collection step with potentially new keywords. Figure 1 provides an illustration of the adopted research design approach.

In the data collection stage, a list of keywords (search terms) that can be used to locate target devices was created. This was primarily based on existing literature work and using the most popular ('Top Voted') filters ranked by Shodan users. Examples of keywords included "Network Camera", "IP Camera", "Webcam", and variants of these (e.g. including the specific manufacturer name to the search terms).

Second, in the data extraction stage, a proof of concept application, developed using Python programming language, was created to interface with Shodan API. Here, the official Python wrapper, named *Shodan[16]*, and its count (*Shodan.count()*) and search (*Shodan.search()*) methods were used to efficiently identify the total number of hosts, i.e. cameras, and to return possible general and banner information about each host, respectively. As input (query strings) to the program the same list of filters provided in the data collection step were used. For each retrieved result data were processed in memory and tagged for further processing if they disclosed elements, such as version information, that are commonly associated with the

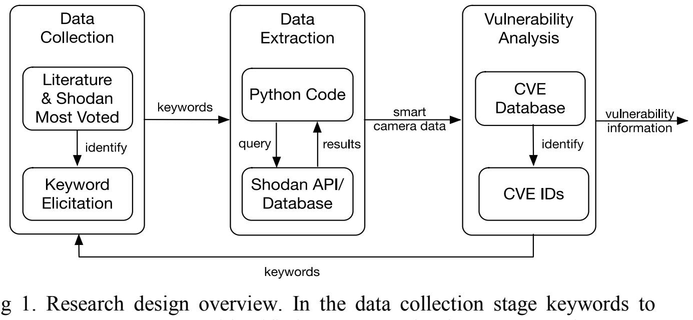

Fig 1. Research design overview. In the data collection stage keywords to detect smart cameras were identified. Consequently, these were used to query Shodan. Returned results were then analyzed for potential vulnerabilities by querying the CVE database. Obtained vulnerability information was then used to derive additional keywords to be used as input to the data collection stage.

[11] https://www.mitre.org/ [accessed January 10, 2018].
[12] https://www.exploit-db.com/ [accessed January 10, 2018].
[13] https://vulndb.cyberriskanalytics.com/ [accessed January 10, 2018].
[14] https://www.rapid7.com/db [accessed January 10, 2018].
[15] https://www.tenable.com/products/nessus-vulnerability-scanner [accessed January 10, 2018].
[16] https://shodan.readthedocs.io/en/latest/api.html [accessed January 10, 2018].

TABLE I –INFORMATION ABOUT CAMERAS OBTAINED AFTER EXECUTING THE FOUR MOST VOTED FILTERS RELATED TO CAMERAS ON SHODAN.

Keywords	Number of Hits	Operating System	Top Services
Server: SQ-WEBCAM	151	/	HTTP, NAS Web Interfaces
linux upnp avtech	78,586	Linux 3.x, Linux 2.6.x	HTTP, Kerberos, Qconn
netcam	8,655	Linux 2.4.x	HTTP, Qconn
webcamxp	1,174	Windows 7/8, Windows XP	HTTP, AndroMouse

information leakage threat [15].

Finally, after the data had been extracted, it was analyzed for security vulnerabilities. Here, pertinent data elements (e.g. the vendor name and firmware version) returned from the previous step, were scanned against the CVE database for identifying CVE IDs (a unique identifier for publicly disclosed cybersecurity vulnerabilities) and additional information about the vulnerability, if any. Obtained vulnerability information was logged and used to identify further keywords that were not initially captured.

V. Results

We discovered thousands of smart connected cameras broadcasting different information elements using Shodan. For instance, in November 2017, after running the Data Extraction stage with the keyword "uc-httpd" – this is a HTTP daemon (service) that is primarily used by security cameras[17] – a total of 542,270 devices, mostly surveillance cameras, were indicated to be active and with potential to be accessed (e.g. by compromising vulnerabilities in the reported service). This was noted by reading the returned authentication status "200 OK". The keyword is not commonly used in existing scientific literature but was noted only after executing the Vulnerability Analysis stage.

Different cameras exposed to various extents similar types of data. Overall, the retrieved data included: i) position of the smart camera, including exact location or deployment region; ii) product information such as the manufacturer name, firmware version, and software details; iii) open ports, e.g. file-transfer protocol port 21, and supported transport layer protocols, e.g. TCP; iv) default passwords that can be used to access a camera; v) pictures/video that can be used for live streaming; and vi) authentication status (HTTP) typically 200 "OK" or 401 "Unauthorized". To an extent, the different information elements in this list includes both sensitive (e.g. firmware versions) and private (e.g. pictures/video) data. In some instances, the banner information returned information about the default configuration, including privileged accounts, being used by the particular camera model. This information can in some cases be used to gain full-control over a camera. Table I summaries some of the data types retrieved from live cameras after running Shodan's most popular (voted) camera related queries.

TABLE II – EXAMPLES OF DISCOVERED VULNERABILITIES IN SMART CONNECTED CAMERAS. THE VULNERABILITIES ARE RANKED ACCORDING TO THEIR SEVERITY LEVEL AS IDENTIFIED IN THE NVD DATABASE.

CVE-ID	Target	Vulnerability	Severity	Risk
CVE-2015-2887	Video baby monitor	Hard-coded credentials	Critical	Complete compromise of security and privacy
CVE-2015-2886	Video baby monitor	Information disclosure	High	Obtain sensitive information
CVE-2007-5213	Home camera	Cross-site request forgery	High	Perform tasks with full privileges
CVE-2011-5261	Small business camera	Cross-site scripting	Medium	Unauthorized modification of data

Here, it is interesting to observe that most of the systems, as expected in the IoT realm, feature Linux operating system, and that in addition to the HTTP service include other supported protocols, e.g. Qconn.

By running some of the device identification keywords, e.g. "Network Camera", against the CVE database, and using some of the obtained banner information, e.g. the manufacturer name, we could easily identify a number of vulnerabilities. For instance, a relatively low amount of cameras were found to be prone to a cross-site scripting vulnerability – CVE-2011-5261[18]. Exploiting this vulnerability allows remote attackers to inject arbitrary code leading to altering the website integrity but also making it possible to stage further attacks against site visitors[19]. Other distinctive vulnerabilities that were noted included: CVE-2015-2887, CVE-2015-2886, and CVE-2007-5213, with risk levels, as per the National Vulnerability Database (NVD)[20], classified as critical, high, and high, respectively. These were identified after refining the keyword search with more terms, in particular with the string "iBaby" (a prominent manufacturer of Wi-Fi based video baby monitors) and "AXIS 2100" (a popular network camera). In Table II, actual examples of discovered vulnerabilities, characteristics of the target (affected) device, alongside vulnerability related information are presented. Here, it can be observed that the mentioned CVEs tend to target smart living spaces, in particular smart homes.

VI. Discussion

In the early days, hackers relied primarily on specialized security tools, such as Nmap[21], to find potential vulnerable targets. These tools, while still very popular, tend to require a steep learning curve and thus favoring technically skilled users. Nowadays, while similar tools are still being used, there are alternative solutions, such as Shodan, that attract also less technically skilled users. In this study, we have demonstrated that a malicious threat agent armed solely with a web browser and

[17] https://packetstormsecurity.com/files/142131/XiongMai-uc-http-1.0.0-Local-File-Inclusion-Directory-Traversal.html [accessed January 10, 2018].

[18] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-5261 [accessed January 10, 2018].

[19] https://vuldb.com/?id.63545 [accessed January 10, 2018].

[20] https://nvd.nist.gov/vuln/detail/CVE-2011-5261[accessed January 10, 2018].

[21] https://nmap.org/ [accessed January 10, 2018].

access to Shodan, can detect with relative ease the presence of smart connected cameras. While we assumed some elementary programming skills for developing the proof of concept code, discovering smart cameras and gaining information about a target, such as people and property, does not require such knowledge. Particularly, this is as the web interface offers a set of ready-made filters that can be accessed and tuned by a broad spectrum of users. Interestingly, the sophistication of this interface is increasing with Shodan lately adding a filter that captures image feeds from vulnerable cameras[22]. The more sophisticated such a tool gets the more likely it is to attract different categories of threat agents with different motivations.

Smart connected cameras can be attacked for various reasons. A malicious threat agent, e.g. a hacker, can compromise a smart connected camera for the thrill of it. This affects the personal privacy of individuals, especially if the camera is installed in a smart home. A different threat agent, e.g. a thieve, can obtain access to a surveillance camera live footage to detect when the residents are away and thus contributing to finding the right opportunity to steal home property. On the other hand, a nation-state actor may compromise manifold cameras, as part of cyber warfare, cyber terrorism or cyber espionage campaigns. This elevates the risk severity from being that of personal risk to an infrastructure or nation-wide risk. As an example, recently more than a million CCTV cameras and Digital Video Recorders were compromised and reconfigured by an attack to become part of a botnet [17]. This IoT botnet – Mirai (and more recently Reaper[23]) – then attacked other systems on the Internet. The consequences of this would vary a lot and can be extreme. This is especially if SCADA devices such as electrical grid, water plants, and nuclear plants, are involved. Vulnerabilities found within these types of devices can be exploited to inflict damage, control resources, or even held accountable from a political standpoint. Compromising these may lead to a severe, possibly global, impact.

We have noted more than half a million network cameras distributed around the world transmitting service banner information rich with information. This information can be used to gain intelligence about a target of interest (also called “reconnaissance”) and possibly used as a first step to mount a targeted attack. Observed locations in our dataset ranged from closed living spaces such as smart homes to open spaces such as cities. Additionally, in some cases there were also sensitive zones such as airplane hangars. This data was captured from different camera models, some developed by established vendors to startups, indoor to outdoor security cameras, and possibly included do-it-yourself (DIY) web cameras setup with Raspberry Pi or related technology. Interestingly, the number of detected network cameras was more than seven times the amount of cameras reported in 2014 [4] but less than 1% of the total amount of network cameras projected to be distributed globally in 2017 [2]. However, we did not calculate the amount of cameras with actual live streaming, and did not distinguish between cameras positioned in public and private areas. Possibly, the obtained value is indicative of increased adoption rates of IoT devices. However, at the same time, this reveals that weak security measures are still being adopted on a global scale.

In conducting our experiment, we observed that insufficient authentication/authorization, insecure web interfaces, and insecure software/firmware remain common vulnerabilities. As noted earlier, there were instances of cameras that utilized a built-in privileged account, e.g. administrator account (“admin”), and transmitted that openly. Even so, most of the cameras arguably employ weak or default passwords that are easily guessable. Although for ethical and legal reasons, we did not actively exploit any of the vulnerabilities discovered, we observe that there is code available on the Internet that can do so with relative ease. Thus, the risk of a low-skilled malicious threat agent discovering this code and running them against live smart connected cameras is a real one. The severity when such code is executed can be critical. For instance, the consequence of exploiting CVE-2015-2887 can lead to a total compromise of the security and privacy of a smart home environment. At the same time, depending on the nature of the camera, the effects of exploiting a critical vulnerability can range from wiping potential evidence to zooming-in on particular sensitive areas/zones. Removing evidence when criminal activity is involved can sabotage an investigation or steer attention away from a suspect. Adjusting the focus of a camera can help an intruder view confidential information (e.g. financial information in case of an indoor camera present in the accounting department), but it can also help identify individuals and activities being performed and thus hampering privacy.

Various security mitigations for the identified vulnerabilities have been extensively researched and proposed in both academic and industrial communities [4]. One common measure that can be adopted by consumers to remediate most of the observed vulnerabilities is that of changing the default passwords or by consistently updating system software. Despite this, we still observe that consumers are likely to be unaware of the ethical and security risks imposed by surveillance technologies and IoT in general. Deploying network-connected devices creates more entry points for hackers to exploit. This raises the importance for more intuitive guidance procedures to help consumers become aware especially of the privacy implications of smart connected cameras and IoT technologies in general. On the other hand, vendors, should adopt security best practices and bake-in security at the early stages of their development lifecycle [18]. Especially, vendors should conduct security and privacy risk assessment during development. This should consider the sensitivity of the data in question as well as the type and number of security risks [18].

As a final observation, we notice that some of the discovered connected cameras do not come with a security auto-update mechanism. Moreover, some devices like CCTV cameras have a long lifespan, and thus not easy to replace as is a traditional computer [19]. This means that they are likely to be rarely patched and can be arguably easily exploited. For instance, some cameras require users to manually locate a software update and then to apply it using the web interface. Unfortunately, people are nowadays used to auto-update features found on traditional computer systems but in the IoT realm in general there are no regular patches or over–the-air updates.

[22] https://www.techhive.com/article/3026217/security-cameras/security-camera-snooping-made-easy-thanks-to-the-shodan-search-engine.html [accessed January 10, 2018].

[23] https://www.theregister.co.uk/2017/10/27/reaper_iot_botnet_follow_up/ [accessed January 10, 2018].

This raises the need for more versatile security update mechanisms. At the same time, it is also interesting to observe that some of the identified vulnerabilities, e.g. CVE-2011-5261, that was originally released on 2013[24], a remediation to that still does not exist[25]. This makes us reflect whether this is indicative of the overall state of security of the current IoT deployments. Upgrading an IoT or embedded device tends to be more challenging than a traditional computer system, and, as we have shown; sometimes this is not even possible. If this is the case one safeguard that can be adopted by a consumer is simply not to expose the camera on the Internet and instead access it through a secure tunnel, e.g. a Virtual Private Network (VPN). For the long-term, regulation, legislation, and product liability, are considered the essential components for improving the current state of security of IoT [19].

VII. Conclusions and Future Work

Home and business owners are increasingly relying on smart connected cameras to check on their property, people, and events. As the world embraces more Internet-enabled smart devices, online services, and broader connectivity, the need for enhanced security will increase. Consumers and businesses expect security and privacy while at the same time benefitting from the remote features and automation support offered by IoT technologies.

In this paper, we have noted on a global scale numerous cases where cameras where found to be broadcasting granular data to the extent that it also included geographical-locations, installed software services, and sometimes username/password combinations. Alarmingly, we have observed that poor configuration and lack of even rudimentary security controls are indeed prevalent. Furthermore, we noted that an individual armed solely with free software tools, Shodan, can with relative ease compromise the personal privacy of individuals. At the same time, the compromise of a multitude of these cameras can elevate the risk factor to a national, possibly global level.

Given this, we argue that this represents a serious security and privacy threat, that needs more attention from the academic and industry communities. In particular, this is as smart connected cameras are increasingly being manufactured and adopted by different users with varying security knowledge. At the moment, the burden is mostly left to the individual, typically the home or business owner, but in some cases mitigations, as we mentioned, may demand specialized, sometimes uncommon, technical skills (e.g. networking and operating system knowledge to install VPN).

Looking towards the future, there are several avenues being explored to advance the research presented in this paper. First, we plan to extend this study to include other smart devices that are prominent in the smart connected home. Examples of these include smart speakers, smart TVs, and smart thermostats. Additionally, we plan to use an advanced vulnerability scanner, such as OpenVAS[26], to systematically classify the discovered vulnerabilities into different rankings, e.g. Critical, High, Medium, and Low. This is an important step towards performing a quantitative risk analysis. Finally, we plan to use the risk analysis to design holistic and effective security mechanisms that can safeguard the privacy of the householders.

Acknowledgment

This work has been carried out within the research profile “Internet of Things and People”, funded by the Knowledge Foundation and Malmö University in collaboration with 10 industrial partners.

References

[1] R. Abdallah, L. Xu, and W. Shi, “Lessons and Experiences of a DIY Smart Home,” *ACM SmartIoT '17 Proceedings of the Workshop on Smart Internet of Things*, 2017, vol. 4.

[2] IHS Markit, “Top Video Surveillance Trends for 2017”, 2016 [Online]. https://goo.gl/knxQVS.

[3] Z.-K. Zhang *et al.*, “IoT Security - Ongoing Challenges and Research Opportunities,” *IEEE 7th International Conference on Service-Oriented Computing and Applications*, 2014, no. 7, pp. 230–234.

[4] J. Bugeja, A. Jacobsson, and P. Davidsson, “On Privacy and Security Challenges in Smart Connected Homes,” *IEEE Intelligence and Security Informatics Conference*, 2016, pp. 172–175.

[5] M. Moody and A. Hunter, “Exploiting Known Vulnerabilities of a Smart Thermostat,” *IEEE Annual Conference on Privacy, Security and Trust*, 2016, pp. 50–53.

[6] J. Bugeja, A. Jacobsson, and P. Davidsson, “An Analysis of Malicious Threat Agents for the Smart Connected Home,” *IEEE Proceedings of the 1st IEEE PerCom International Workshop on Pervasive Smart Living Spaces*, 2017, pp. 557–562.

[7] K. Loukil *et al.*, “Design and test of smart IP-camera within reconfigurable platform,” *IEEE 2nd International Conference on Anti-Cyber Crimes*, 2017, pp. 25–29.

[8] Bitdefender, “Remote Exploitation of the NeoCoolcam IP Cameras and Gateway”, 2017 [Online]. https://goo.gl/qhmDJt.

[9] H. Lin and N. Bergmann, “IoT Privacy and Security Challenges for Smart Home Environments,” *Information*, 2016, vol. 7, no. 3, pp. 44–15.

[10] M. Patton *et al.*, “Uninvited Connections: A Study of Vulnerable Devices on the Internet of Things (IoT),” *IEEE Joint Intelligence and Security Informatics Conference*, 2014, pp. 232–235.

[11] R. Williams *et al.*, “Identifying Vulnerabilities of Consumer Internet of Things (IoT) Devices: A Scalable Approach,” *IEEE International Conference on Intelligence and Security Informatics*, 2017, pp. 179–181.

[12] O. H. Alhazmi, Y. K. Malaiya, and I. Ray, “Measuring, analyzing and predicting security vulnerabilities in software systems,” *Computers & Security*, 2007, vol. 26, no. 3, pp. 219–228.

[13] Q. Li, X. Feng, L. Zhao, and L. Sun, “A Framework for Searching Internet-Wide Devices,” *IEEE Network*, pp. 12–18, Aug. 2017.

[14] Carnegie Mellon University, “A Unique Approach to Threat Analysis Mapping: A Malware-Centric Methodology for Better Understanding the Adversary Landscape,” 2016 [Online]. https://goo.gl/cbkqtr.

[15] D. Papp, Z. Ma, and L. Buttyan, “Embedded Systems Security: Threats, Vulnerabilities, and Attack Taxonomy,” *IEEE Annual Conference on Embedded Systems Security Threats, Vulnerabilities, and Attack Taxonomy*, 2015, pp. 145–152.

[16] S. Samtani *et al.*, “Identifying SCADA Vulnerabilities using Passive and Active Vulnerability Assessment Techniques,” *IEEE Conference on Intelligence and Security Informatics*, 2016, pp. 25–30.

[17] K. Angrishi, “Turning Internet of Things (IoT) into Internet of Vulnerabilities (IoV): IoT Botnets,” *arXiv preprint arXiv: 1702.03681*, 2017, pp. 1–17.

[18] Federal Trade Commission, “Building Security in the Internet of Things”, 2015 [Online]. https://goo.gl/GBYrqp.

[19] S. Mansfield-Devine, “Weaponising the Internet of Things,” *Network Security*, 2017, vol. 10, pp. 13–19.

[24] https://nvd.nist.gov/vuln/detail/CVE-2011-5261 [accessed January 10, 2018].

[25] https://exchange.xforce.ibmcloud.com/vulnerabilities/71687 [accessed January 10, 2018].

[26] http://www.openvas.org/ [accessed January 10, 2018].