UNIVERSIDAD POLITÉCNICA DE MADRID

ESCUELA TÉCNICA SUPERIOR DE INGENIEROS INFORMÁTICOS

MÁSTER UNIVERSITARIO EN INGENIERÍA INFORMÁTICA

Cybercrime in the IoT Era

Autor: David Galán Berasaluce

Director: Maurice Dawson

Madrid, Julio 2019

RESUMEN

Durante los últimos años, el desarrollo al que se ha visto sometido la tecnología ha crecido exponencialmente. Cualquier tipo de dispositivo con acceso a Internet puede comunicarse con otros dispositivos. Estamos viviendo en un mundo hiperconectado que facilita el intercambio de servicios e información, pero también implica algunos riesgos. Organizaciones criminales tienen como objetivo atacar a estos equipos, los cuales muchos de ellos contienen capacidad de monitorización y videovigilancia, para atacar a otras empresas o simplemente con un propósito económico recogiendo, comprando y vendiendo información.

Es un área de estudio novedosa y por tanto hay mucho trabajo de investigación todavía por hacer. En el mercado existen una gran cantidad de fabricantes que intentan sacar los dispositivos lo antes posible, dejando de lado la aplicación de controles de seguridad. Además, la heterogeneidad de estos dispositivos junto con la limitación de recursos los hace más vulnerables ante cualquier ataque. En este trabajo se analiza el estado actual de la seguridad los dispositivos que forman parte del Internet of Things, relacionándolo con actividades criminales o no éticas como son el espionaje o cyberstalking.

Estos dispositivos son capaces de recoger y generar una gran cantidad de información. El desarrollo de una arquitectura secura para proteger confidencialidad e integridad es requerida en el proceso del flujo de datos. En este trabajo se ha realizado un análisis del proceso de comunicación llevado a cabo por un Sistema de Reporte de Crímenes Nacional de la Policía Nacional. Además, se propone una serie de controles de seguridad para proteger el flujo de datos siguiendo un framework de controles de seguridad.

Palabras clave: *Ciberseguridad, Internet of Things, Cyberstalking, Espionage, Sistema de Reportes, Contoles de Seguridad*

ABSTRACT

Technology has experienced a fast improvement during the last decade. Any type of device with network access capabilities can communicate with each other. A hyperconnected world is emerging easing the exchange of services and information, but also bringing some backwards. Criminal organization are targeting Internet of Thing devices, equipped with monitoring and surveillance capabilities, to perform attacks against other organizations or to collect, buy and sell information.

There is still a lot of research to do in this area. The develop of new devices with different manufacturers competing to put any device as soon as possible in the market is lacking required security controls. In addition to the heterogeneity and limited resources, it is making them more vulnerable.

Internet of Things are capable of collect and generate a high amount of data. Development of secure architecture that protect confidentiality and integrity is required through the data flow process. The communication process from a National Crime Reporting System for a Latin American country's National Police is assessed. Moreover. security controls to protect the data and the information system are proposed following the recommendations provided by a security framework.

Key words: *Cybersecurity, Internet of Thing, Cyberstalking, Espionage, Contract Killing, Reporting System, Security Controls*

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

We are experiencing an interconnected world in which people can control any kind of device with just the use of a mobile phone. Internet of Thing (IoT) era has done nothing but begin. However, the boost of privacy concerns has emerged during the last decade. Organizations such as WikiLeaks and especially the information provided by Edward Snowden has participated in this upsurge. Recent Facebook-Cambridge Analytica data scandal has also contributed. Privacy protection of users remain as a crucial challenge that must be addressed. However, the term data privacy has also diverged into a buzzword that companies, such as Google during the last Google I/O 2019 conference, are trying to exploit to get visibility of their new or updated products.

On the other hand, fast technology improvement is allowing companies and states to collect data about their adversaries. Some countries have already developed cyberdefense policies to protect themselves from the imminent security threats arisen and direct attacks against government critical infrastructure, such as supervisory control and data acquisition (SCADA) systems [1,2]. Cyber security in IoT should play a key role during the Industrial Revolution 4.0 we are living in, implying understanding security and privacy concerns, as well as the appropriate application of security controls, to mitigate risks and achieve security [58].

Current TV, cameras, printers, watchers, toys, and many devices are built-in with remote maintenance, management and administration capabilities. Devices are connected to the Internet and continuously sending and receiving any type of data. Data is the most important asset a company possesses, therefore safeguarding it must be priority. New technologies, endowed with varied and pervasive monitoring and surveillance capabilities, can collect an inconceivable amount of it. Security and privacy play a significant role in all markets globally due to the sensitivity of consumer’s privacy. Nevertheless, security is often not incorporated in the product development life cycle and consequently vulnerability often emanates from decisions made by the vendors. Moreover, the heterogeneity of technologies increases the complexity of the security processes.

Internet of Thing is at an early age of development. There exist few resources among the research of IoT devices due to its novelty and the considerable amount of different existing devices and companies that offer their own products. Neither standardization nor legislation of such as interconnected devices still exist. Therefore, the architecture in which new hyper connected devices are based on following the traditional Internet model, implying their own characteristics. In addition, IoT devices are equipped with different features. The heterogeneity and interconnection of technologies as well as the constrained capacity of computing resources bring critical security challenges and requirements to Internet of Thing (IoT) development.

The combination of Internet of Things technologies, cloud computing and artificial intelligence have led to more practical applications, but also an attractive target for cyber-attacks [7]. Multiple combination of existent technology is prone to new vulnerabilities and security threats. In addition, the extensive amount of data complicates their management and privacy protection. Criminal groups pursuits vulnerable devices to obtain this data and use it for their own interest.

New security and forensic challenges have to be addressed, such as authentication, authorization and access control, in addition to identification, collection, preservation and reporting of evidence [10]. Other challenges IoT request are interoperability, resource constraints, resilience to physical attacks and natural disasters, autonomic control, information volume, privacy protection and scalability. Risk assessment and analysis of security issues and vulnerabilities is crucial to determine appropriate countermeasures and mitigate possible cyberattacks. [3,16].

Use of standards policies and guidance ease the integration of technologies into everyday life. There are appropriate documentation and guidelines available through different organisms such National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO), Institute of Electronic and Electrical Engineers (IEEE), etc., that address risk management concepts and information recommendations, together with laws and organization policies, to harden devices architectures [65].

During the last decade there have been numerous researches that analyze and classify attacks vectors, impact attacks and defense mechanisms among IoT devices [3,7,56,57]. IoT devices are mainly targeted for their utilization as an espionage or ransomware tool, mining cryptocurrencies, as well as to their inclusion into botnets to perform Denial of Service (DoS) attacks.

2. PRIVACY AND ANONYMITY: THE USE OF THE DARK WEB

In the current hyper connected society, preserve anonymity and privacy is essential to battle against misuse and abuse of information. Software for anonymity and privacy protection such as Tor, a free and open-source software for anonymous communication, or The Amnesic Incognito Live System (Tails), a Debian-based Linux distribution [41], have been developed during the last decade.

Deep Web is a term used to describe public but no indexable content by usual search engines in the Internet. Other terms such as Dark web and Darknet are used interchangeably with deep web. However, these terms represent different concepts. The dark web content is hidden content that represents a minimal part of the Deep Web. Darknet encompass every independent network that compose the Dark web. Special Browsers, such as Tor, Invisible Internet Project (I2P) or Freenet are required to access these networks [54,55]. Access to the dark web requires specific software.

Darknet has the challenge between freedom of expression and what is ethically correct [53]. It is not just a place for illegal and criminal activities and services such as weapons and drugs trade, counterfeit money, credit card data, identity theft, malware or pedophilic content. It is also a platform that guarantee private and anonymous communication facilitating freedom of expression. This attribute is especially important in repressive countries where personal freedom is restricted.

However, the Darknet is directly associated to criminal activities. As appointed by Mirea et al [52], it is a tool and a system used by some individuals to penetrate illegal activities. Criminals may exploit the special attributes that the darknet offers to continue carrying illegal and unethical activities [50].

A research [57] gathered data for 6 months to analyze and classify the services offered on the dark web. They were able to collect 80,000 hidden services, the majority of them were criminally oriented. The most requested services were related to sexual abuse or pornographic services. Botnet command and control (C&C) servers were also frequently requested as a service. A command and control server is an infected computer that is remotely controlled. Command and control servers can be used to create a network and carry out Distributed denial-of-service (DDoS) attacks.

Activities behind the Darknet may be classified into three different categories [52]:

(1) Activism, journalism, and whistleblowing
(2) Criminal activities in virtual markets
(3) Cyber security threats including botnets, malware, and ransomware

IoT devices connected to the Internet are being targeted by criminals to gather, expose and sell data on the dark web market (cyberespionage) or to manage them to perform Distributed Denial of Service (DDoS) attacks.

Related to espionage, in the darknet exists sites offering contract killing services [67]. It is such a dark business that no one’s ever tried to investigate, therefore it cannot be deducted if such a service is real or just a scam or bait to attract individuals to steal cryptocurrencies.

3. CYBERCRIME

The term attacker usually englobes individuals that carry out network penetration tests to discover new vulnerabilities. Cyber criminals are unethical attackers, working independently or for large cybercrime organization, seeking for device vulnerabilities for personal gain or for malicious reasons. They usually buy, sell and trade toolkits, zero-day exploit code, botnet services and private information that they steal from enterprises and industry.

Cybercrime and cybersecurity tools are evolving concurrently with the technology improvement. According to the last IC3's Internet Crime Report [37] fraud, extortion and personal data breach were the type of crime that received more complaints in 2018. There has been a significant increase in Business Email Compromise/Email Account Compromise (BEC/EAC) scam attack complains. This kind of attack is carried out by social engineering or computer intrusion techniques. Cyber-attacks cause a huge amount of losses to business and nations, for example BEC/EAC have caused losses of around $1 billion, and confidence fraud $362 million. Cybercriminals demand virtual currency as the payment mechanism because it provides them anonymity.

Social ties have played an important role in the creation and operation of criminal network. However, Internet technologies are currently serving as a platform for criminals to develop their capabilities [40], reducing restrictions such as geographical closeness. Forums, where criminals can freely and widely available meet to exchange information, boost up the growth of a criminal network easing the seeking of suitable co-offenders and providing an endless amount of information. Cases studies carried out in Germany and Netherland shows this main role that technology provides for criminal seeking expertise [11, 12, 13, 14] No technical expertise is required to carry out cyberattacks, cybercriminal organizations can afford to hire skilled hackers with higher wages that the one they perceived working on the other side.

Cyberattacks have a considerable impact on society threat perception. Exposure to any form of cyberattack, which may not imply physically harm, significantly rise stress and cortisol levels on individuals [38]. Individuals who are exposed to attacks perceive threats and experience feelings of personal insecurity more frequently, impacting on political attitudes and contributing to the cycle of global cyberterror.

4. CYBERSTALKING AND ESPIONAGE

Cyberstalking involves the use of technology to threat or monitorize someone. This practice involves an invasion of a person's right to privacy. Cyberstalking is often committed by a person the target knows intimately or professionally. Software apps may contain hidden functionality that is gate to leak of sensitive data such as text messages, phone calls, contacts etc. Spyware apps implies a threat for a target who potentially become a victim of abuse or stalking. Cyberstalking is a critical privacy assault that can even sometimes involve murdering [64].

Spyware software is used as a tool aimed to nation-states, business and general-use audience as a security product to monitor the activities of citizens, employees, children or intimate partners. It offers the ability to remotely collect real-time GPS location data, bank account data, internet browsing data, phone conversations and agenda, text messages, and even collect microphone voice or camera data on the target device. Surveillance software has different social meaning depending on the vendor and is commodified for a general consumer audience [34]. This software is sold a security product but sometimes is illegally and invasively used violating surveillance laws.

Researchers from Cornell Tech, New York University, Technion, Cornell University and Hunter College conducted a study [32] about the spyware used in intimate partner surveillance. Abusers apply technology to intimidate, threaten, track, impersonate, harass or harm their victims [36]. In this research, they have found that antimalware failed to detect a significant portion of the spyware. What makes it harder to be detected as malware is the fact that some of the investigated app contains a dual purpose, like parent control or anti-theft, i.e.: this app has a legitimate use case, but their functionality enables the remote access to the device information. Abusers use intimate partner violence apps to cause emotional and physical harm. Security researcher Cian Heasley discovered a publicly accessible database in which MobiiSpy, an Android app used to track phone activity, left more than 95,000 images and 25,000 audio records. As a result, some security companies, such as Kaspersky, are starting to mitigate this threat by adding anti-spyware capabilities to their products [33].

4.1. Internet of Things Attacks

Internet of Things attacks are not too different from those carried out on traditional servers and desktop. However, their public exposure, restricted capabilities and lack of security controls make them an interesting target.

Botnet armies operating in the shadows by cybercriminals are a potential threat. According to NOKIA Threat Intelligence Report 2019 [17] 78 percent of the malware network activity detected in 2018 are due to IoT botnets. Cybercriminals spread malware through poorly secured IoT devices to form an army of zombie bots, known as a botnet, and perpetrate Distributed Denial of Service (DDoS) attacks.

A Denial-of-Service (DoS) attack results in interruption of service or business process causing a significant loss or impact. A DDoS attack is similar to a DoS attack but using multiple and coordinated sources.

However, botnets are evolving not only limited to one type of attack, they are featured with keystroke loggers, malware updaters or mechanisms to infect other devices. In addition, botnets are expanding their attack surface and becoming more devastating.

In September 2016, the most notorious IoT botnet, called Mirai, launched the largest DDoS attack on records. Since then, IoT botnet activity and newly released vulnerability exploits have substantially increased. New botnets are mainly based on the architecture and functionality of Mirai which source code was released in October 2018.

Mirai [28] is a worm family of malware that infected IoT devices and allow remote control from a centralized point, enclosing them into a botnet. Mirai basically targeted IP cameras, DVRs and routers. Mirai botnet was composed of hundreds of thousands of heterogeneous low-end IoT devices demonstrating the insufficiency of security best practices in the IoT area. The Mirai botnet represents a change in the development of botnets due to the simplicity through which devices are infected and its exponential growth. Nowadays, IoT botnets are evolving, granting botnets with new exploitable capabilities and newly released vulnerability exploits, like deploying cryptocurrency-mining bricking malware [29], that allow them to expand the attack vector [30]. Some recent IoT malware are show in table 1.

Name	Capabilities and features	Date
Hajime [18]	Based on other malwares: Rex, Mirai, NyaDrop More sophisticated	Oct 2016
IoT reaper [19]	Exploit IoT devices vulnerabilities. (9 exploits integrated) Integration of LUA execution environment	Sep 2017
Okiru/Satori [20] [21]	Exploit IoT devices vulnerabilities. Exploit Claymore cryptocurrency miners	Dec 2017
Okane and Omni [22]	Exploit IoT devices vulnerabilities. Target routers and surveillance devices Credential brute force attack.	May 2018
Mirai’s variant [23]	Exploit IoT devices vulnerabilities. (16 exploits integrated) Exploit vulnerabilities in Apache Struts open-source web application framework Target enterprise devices with outdated versions. Based on Gafgyt and Mirai	Sep 2018
Chalubo [31]	Implement anti-analysis techniques: use of ChaCha stream cipher Variety of both versions Copy of a few code snippets from Mirai Discovered by Sophos	Oct 2018

Yowai [24]	Exploit ThinkPHP vulnerability Use of dictionary attack to infect other devices	Jan 2019
Mirai's variant [25]	Include 27 exploits, 11 different in a Mirai varian Infect enterprise IoT devices Brute force attack Targets embedded devices like routers, network, storage devices, NVRs, Ip cameras	Jan 2019
Trojan.Linux.MIRAI. SMMR1 / ECHOBOT [26]	Backdoor and DDoS capabilities. Use of multiple available proofs of concept and metasploit modules.	Apr 2019
Backdoor.Linux.MIRAI.VWIPT [27]	13 exploits. All of them previously used. 11 at Omni. Used all of them in a single campaign. Flaws found in routers, surveillance products, and other devices.	May 2019

Table 1. Some botnets based on Mirai, one of the first larger botnets**.** Mirai botnet was launched in Aug 2016

Ransomware malware attacks are also emerging as a security challenge in the IoT. Hyperconnectivity and growth of IoT devices exposure, in addition to anonymous trading cryptocurrencies arising, enable attackers to infiltrate devices, encrypt the data and ask for ransom money. However, ransomware attacks in IoT are more difficult to launch due to device resource constraints in opposite to traditional devices. Yaqoob et Al. provides an amply study in the matter [15].

Sometimes the device does not need to contain any malware and be infected by using a trusted software update system. For example, researches from cybersecurity firm Kaspersky Lab discovered recently a sophisticated supply chain attack that installed a backdoor on thousands of ASUS computers because ASUS' server containing live software update tool was compromised. [51] Microsoft Window updating tool was also hijacked in 2012, but this time no server was compromised.

Baby monitors have also been targets of cyber-attacks. IP Cameras are integrated in baby monitors, so parents can monitor their babies even from their phones. This device can be compromised if they aren't properly secured. The greatest risk that this cameras offer is that an attacker could gather voice and image information [34]. An infected device supposes a threat in the network because an attacker could use it as a main system to infect other devices connected to the same network.

Security information expert Bruce Schneier supports regulation of devices by stating *If a company is specifically named, it is likely to improve the specific vulnerability described. But that is unlikely to translate into improved security practices in the future*. [49]

.

Speakers can be considered as a new attack surface. Wenrui Diao et Al. [45] introduces a launch bypassing attack from a zero-permission Android application (Google-Voice search) through the phone speaker. This approach can access private information, transmit sensitive data and gain remote control without any permission. Moreover, voice commands outputted from the speaker can be captured by the microphone as input. a malicious app can record phone conversations. Consequently, and as suggested by R. Schlegel et Al. [46] a malicious app can record phone conversations which may contain sensitive business information such as credit card and PIN number and extract them.

Intelligent assistant robots offer a myriad of applications that ease tasks management such as alarms and timers, intelligent outlets control, radio broadcast or light control. Researchers from the Air Force Institute of Technology in the USA express the importance of the security of such systems [39]. The transmission of such amount of data from the devices allows to monitor the users' activities creating an important source of information. Companies clean and analyze the data to understand the behavior of the user over their devices. Therefore, they can offer new products, create new features and improve the user experience.

Currently Alexa (Amazon), Siri (Apple) and Cortana (Microsoft) are the three main virtual assistant competitors in the market. These products are actively listening to the voices of the users around the device and collect, save and analyze it to improve their products. Apple's and Amazon's have been storing anonymized data for up to two years without user concern.

Users never know who is listening to them. Users don't monitor the network, so they don't notice what data is captured by IoT devices that they have in their home or working places. For example, Amazon's Echo device is listening passively until the pronunciation of the "key word". This means that its microphone is permanently activated, being as the perfect target for attackers that can use it as a spying backdoor [4]. Voice data (data interpreted by the device that may include sensitive topics or private conversations [59]) is uploaded for analysis and stored at the company storage system [60,61]. However, sometimes keeping recorded data may help to solve or at least as evidence in a crime case, as it was in 2017 when the data recorded by an Amazon Echo speaker was required as evidence in a murder case (against Amazon's willingness to preserve user privacy and opposition to inappropriate claims as a matter of course) [62].

According to a report by The American Consumer Institute Center for Citizen Research in 2018 [66], routers and household devices with Internet connectivity are vulnerable targets that compromise user privacy and personal data (criminals may carry out activities such as identity theft, fraud or espionage). IoT devices lack of enough security controls and are rarely updated leaving them unprotected against known security flaws.

Children are also vulnerable to espionage. In modern years, kids start from an early age to get their first technological device. Devices intended for children are equipped with new technologies gadgets, sometimes incorporating a technology such as Bluetooth to communicate with a mobile phone and/or built-in voice or video capabilities. For example, current smart watchers usually have integrated a microphone, a speaker and an app to manage them. They also employ GPS technology that save real-time information such as location history, phone numbers, parents details, etc., allowing parents to monitor them. In 2017, the Norwegian Consumer Council published a security analysis of children's GPS-connected smart watches [5]. In the analysis, researchers noticed that not only could parents monitor the children, but anyone else could also track them. Smartwatches can expose kids to a serious risk since attackers could locate or even communicate with them. Sometimes the system that gather the information is easily accessible, failing authentication mechanisms and allowing admin privilege escalation. For example, cheap Chinese GPS watches issue Insecure Direct Object Request (IDOR), PenTestPartners states [6] that the price of these devices is so low that there is little available revenue to cover the cost of security.

A recent analysis by Pen Test Partners [6] shows that security has not improved, instead data protection measures are still missing. For example, Enox Safe Kid One smartwatch, equipped with a GPS, microphone and speaker, does not comply with the Radio Equipment Directive and include a mobile application with unencrypted communication and unauthenticated access [63].

Avigilon Corporation (Canada), Axis Communications (Sweden), Bosch Security Systems (Germany), Dahua Technology (China), FLIR Systems (US), Hanwha Techwin (South Korea) and Honeywell Security Group (US) were the major players in the surveillance market in 2018 [44].

Devices developed by this companies can have been affected by some vulnerabilities that exploited grant an attacker with remote access. Some of the vulnerabilities of surveillance devices of the major players in the market are shown in the tables below.

Vendor	CVE	Affected Version	Affected device	Vulnerability Type
AXIS Communications	CVE-2015-8258	5.80.x and below	AXIS Communications products	Injection (CWE-74)
AXIS Communications	CVE-2015-8255	2.2	AXIS Communications products	Cross-Site Request Forgery (CWE-352)

Table 2. Vulnerabilities that have affected AXIS Communications surveillance products.

Vendor	CVE	Affected Version	Affected device	Vulnerability Type
Bosch Security Systems	CVE-2019-6958	9.0 and below	Bosch Video Management SYSTEM	Improper Access Control (CWE-284)
Bosch Security Systems	CVE-2019-6957	9.0 and below	Bosch Video Management SYSTEM	Buffer Errors (CWE-119)

Table 3. Vulnerabilities that have affected AXIS Bosch Security Systems surveillance products.

Vendor	CVE	Affected Version	Affected device	Vulnerability Type
Dahua Technology	CVE-2017-9317		Dahua IP devices	Permissions, Privileges, and Access Control (CWE-264)
Dahua	CVE-2017-9316		IPC-HDW4300S	Authentication

Technology			Some Dahua IP devices	Issues (CWE-287)
Dahua Technology	CVE-2017-9315		Dahua IP camera	Cryptographic Issues (CWE-310)
Dahua Technology	CVE-2017-9314	Software before DH_NVR5xxx_Eng_P_V2.616.0000.0.R.20171102	NVR50XX, NVR52XX, NVR54XX, NVR58XX	Authentication Issues (CWE-287)
Dahua Technology	CVE-2017-7927		DH-IPC-HDBW23A0RN-ZS, DH-IPC-HDBW13A0SN, DH-IPC-HDW1XXX, DH-IPC-HDW2XXX, DH-IPC-HDW4XXX, DH-IPC-HFW1XXX, DH-IPC-HFW2XXX, DH-IPC-HFW4XXX, DH-SD6CXX, DH-NVR1XXX, DH-HCVR4XXX, DH-HCVR5XXX, DHI-HCVR51A04HE-S3, DHI-HCVR51A08HE-S3, DHI-HCVR58A32S-S2	Use of Hard-coded Credentials (CWE-798)
Dahua Technology	CVE-2017-7925		DH-IPC-HDBW23A0RN-ZS, DH-IPC-HDBW13A0SN, DH-IPC-HDW1XXX, DH-IPC-HDW2XXX, DH-IPC-HDW4XXX, DH-IPC-HFW1XXX, DH-IPC-HFW2XXX, DH-IPC-HFW4XXX, DH-SD6CXX, DH-NVR1XXX, DH-HCVR4XXX, DH-HCVR5XXX, DHI-HCVR51A04HE-S3, DHI-HCVR51A08HE-S3, and DHI-HCVR58A32S-S2	Permissions, Privileges, and Access Controls (CWE-264)
Dahua Technology	CVE-2017-7253	3.200.0001.6	Dahua IP Camera	Permissions, Privileges, and Access Controls (CWE-264)
Dahua Technology	CVE-2017-6432	3.210.0001.10 build 2016-06-06	DHI-HCVR7216A-S3	Cryptographic Issues (CWE-310)
Dahua Technology	CVE-2017-6343	3.210.0001.10 2016-06-06 (1)	(1)DHI-HCVR7216A-S3 (2) Camera Firmware	Improper Access Control (CWE-284)

		2.400.0000.28.R 2016-03-29 (2) 1.16.1 2017-01-19 (3)	(3) SmartPSS Software	
Dahua Technology	CVE-2017-6342	3.210.0001.10 2016-06-06 (1) 2.400.0000.28.R 2016-03-29 (2) 1.16.1 2017-01-19 (3)	(1) DHI-HCVR7216A-S3 (2) Camera Firmware (3) SmartPSS Software	
Dahua Technology	CVE-2017-6341	3.210.0001.10 2016-06-06 (1) 2.400.0000.28.R 2016-03-29 (2) 1.16.1 2017-01-19 (3)	(1) DHI-HCVR7216A-S3 (2) Camera Firmware (3) SmartPSS Software	Improper Access Control (CWE-284)
Dahua Technology	CVE-2017-3223	prior to V2.400.0000.14.R .20170713	Dahua IP Camera	Buffer Errors (CWE-119)

Table 4. Vulnerabilities that have affected Dahua Technology surveillance products.

Vendor	**CVE**	**Affected Version**	**Affected device**	**Vulnerability Type**
FLIR Systems	CVE-2018-3813	4.1.53.166	FLIR Brickstream 2300 devices 2.0	Information Leak /Disclosure (CWE-200)

Table 5. Vulnerabilities that have affected FLIR Systems surveillance products**.**

Vendor	**CVE**	**Affected Version**	**Affected device**	**Vulnerability Type**
Hanwha Techwin	CVE-2018-6303		Hanwha Techwin Smartcams	Integer Overflow or Wraparound (CWE-190)
Hanwha Techwin	CVE-2018-6302		Hanwha Techwin Smartcams	Integer Overflow or Wraparound (CWE-190)
Hanwha Techwin	CVE-2018-6301		Hanwha Techwin Smartcams	Out-of-bounds Read (CWE-125)
Hanwha Techwin	CVE-2018-6300		Hanwha Techwin Smartcams	Buffer Errors (CWE-119)

Hanwha Techwin	CVE-2018-6299		Hanwha Techwin Smartcams	Uncontrolled Resource Consumption (‘Resource Exhaustion) (CWE-400)
Hanwha Techwin	CVE-2018-6298		Hanwha Techwin Smartcams	NULL Pointer Dereference (CWE-476)
Hanwha Techwin	CVE-2018-6297		Hanwha Techwin Smartcams	Security Features (CWE-254)
Hanwha Techwin	CVE-2018-6296		Hanwha Techwin Smartcams	Race Conditions (CWE-326)
Hanwha Techwin	CVE-2018-6295		Hanwha Techwin Smartcams	Out-of-bounds Read (CWE-125)
Hanwha Techwin	CVE-2018-6294		Hanwha Techwin Smartcams	Out-of-bounds Write (CWE-787)

Table 6. Vulnerabilities that have affected Hanwha Techwin surveillance products.

Not only attackers try to benefit from discovered software flaws on devices, but also can they use techniques to modify the physical aspect in which the system is built. One of this technique is called Intentional Electromagnetic Interface (IEMI) that has the potential to cause major accidents or economic disasters. Frank Sabath introduces some documental criminal usage of IEMI [47,48]. However, the use of this technique requires physical access, or at least remains close, to the system. IEMI sources and their components are available on the free market, and knowledge of using them can be grasped from open literature and the Internet.

4.2. Architecture flaw: Existence of microphones without user awareness

Users do not need to know the insights of the device but being aware of their components such as cameras and microphones that can compromise their privacy. In the market it exists surveillance items small enough to be hidden in any space without being notice. With the intention of collect information of their user’s behavior, some companies install them in their gadgets. Airline companies such as Singapore Airlines and American Airlines have been installing cameras in their in-flight entertainment systems [42]. These companies claim that the manufacturers sold the entertainment systems with embedded cameras for possible future feature. Although the companies claim they have never been used, it can be used for spy and monitor passengers. We can find another example on Google’s Nest system. They recently admitted that not revealing its system came with an in-built microphone was an error. Security alarm system Nest has always contained an embedded microphone for future use in conjunction with Google Assistant. The disposition of this microphone in the architecture of the device was undocumented. Therefore, some complaints have arisen when Google published a new software update that used the features of the microphone, making its existence public [43].

The problem rising in the last example is about users not being informed about features in the device that can be targeted by cybercriminals. An attacker who knows the existence of the microphone can exploit any vulnerability in the network or device to install a backdoor and activate the microphone for passive listening without user awareness.

4.3. Example of Voice-controlled device vulnerability

Voice-controlled or speech-controlled devices may be vulnerable to sounds that humans cannot perceive [4] or voice commands embedded into songs [8]. An attacker could hijack the device and attack it by hiding malicious voice commands. Voice commands embedded into songs, for example spread through Internet or radio, can control the target system through automatic speech recognition without being detected by a human when played. However, natural language understanding and speech recognition functionality is still weak and vulnerable to perturbations. Evolved voice assistants are developed to recognize sound and match it to real words.

Researchers from the University of Michigan in the US and Zhejiang University in China have discovered a new vector attack focus on the ability of hard disk to act as a microphone [9]. Hard disk drive can be turned into listening devices, using malicious firmware and signal processing calculations. The mechanical components behave as microphones with enough precision to extract and parse human speech. Give the right conditions and with digital filtering techniques, human speech can be detected from vibration on HDD. However, for now it is more a theoretical technique having some withdraw such as the requirement of a loud sound (85 dBA) to be recognized. In addition, security researcher Alfredo Ortega showed how a hard disk drive can be turned into a microphone by capturing vibration of voice from low-quality signals using pattern recognition.

5. CYBERCRIME IN LATIN AMERICA

Cybercrime issues have grown due to the fast usage increase of Internet and smartphones during the last decades. Violence rates in Latin America and Caribbean are the highest in the world according to a report published in 2010 [70]. This area is usually poorer and less educated than other regions. Nevertheless, there is neither a common crime pattern nor an established correlation between poverty, education and crime rates.

Caribbean has one of the highest regional homicides rates in the world. Cybercrimes in the Caribbean has expanded rapidly targeting their economies with the existence of many criminal networks in the region [71]. Caribbean islands represent a potential target for attacks in a wide range of external and internal threats due to their geographic position and proximity to other nations in the Americas. According to a report of violence and crime in the Caribbean [69], reporting rates in the islands are like the international average and higher than in Latin America, but still half of common crimes were unreported. In addition, most prevalent crimes like assault and threats are less reported, meanwhile assaults and personal theft were the most common crimes reported in the area.

To battle cybercrime many countries in Central and South America have approved high-tech legislation and created cyber defense systems. However, they lack comprehensive legislation, security policies and a unified regional strategy, as well as cybersecurity talent in the government service personnel and a governing organization, like the National Institute of Standards and Technology (NIST) in the U.S, that provides guidance and tools on different critical matters for enterprise systems [68]. Legislation on cybercrimes must be revised to enforce and adapt it to new tendencies. Novelty and inexperience in the field of cyber security in South and Central America, with scarce security strategies and criminal penalties, is weakening the prosecution of cybercriminals.

Although crime rates in Central and South America are higher compared to other areas, a large percentage of them are not reported. A lack of reporting might diminish public safety and the quality of life where citizens require assistance from law enforcement. The National Crime Reporting System would help these areas to protect citizens against future threats, reducing crime rate. It is worth mentioning that after applying any security mechanism, such as the one described, the violence rate may increment for a period until stabilization. Reached a stable point with the prosecution of criminals, violence rate drop should be the usual trend. In this project, security mechanisms for a crime reporting system for national law enforcement are proposed and analyzed, focusing on the data flow.

6. REPORTING SYSTEM DESIGN

Although governments know that citizens cooperation are a primary factor to reduce the crime rate through the area, the difficulties of a physical report process diminish the willingness of the citizens to cooperate. In addition, citizens may feel fear for possible revenge because of the lack of privacy in the actual physical reporting process, implying a loss of trust and reluctance to collaborate. An online reporting system aims to prevent and prosecute crime and provide help and protection to citizens. Therefore, it is crucial that the reporting system guarantee the confidentiality of the reporter against non-authorized personnel.

A reporting system provides citizens with a quick and easy way to report any accident or suspicious event. The objective of a reporting system is to deal with the input that it receives by sanitizing it, discording those that don't accomplish with the acceptance guidelines and analyzing the information to establish an action plan (Figure 1).

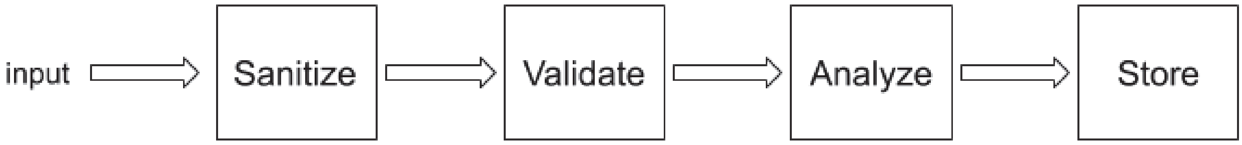

Figure 1. Data flow process

There are two groups of users: external users and internal users of the organization. The former are citizens who use a provided application to create and send a report. The latter are any possible user with a role from the organization, from officials to database system manager, reliability system engineer, etc.

Data flow need to be reliable and secure. Therefore, this project focuses on secure this process, both internal and external, of the system in accordance with organization or law requirements, policies or guidelines. Securing user application, i.e. application that serves as endpoint to carry out the report or extract stored information, is out of scope. In addition, it is assumed that assets are already identified.

6.1. Security element controls

Accomplishment of information security requirements are supported by the application of pertinent management, operational, and technical security controls from security and controls standards and guidelines. There are several cybersecurity frameworks existing in the Information and Technology industry to enhance cybersecurity strategies and improve security protocols within the enterprise. These frameworks are documented for theoretical knowledge and practical implementation procedures. The most frequent used cybersecurity frameworks are ISO 27000, NIST framework and Center for Internet Security (CIS) Security Controls.

The National Institute of Standard and Technology (NIST) defines security controls as *the management, operational and technical safeguards or countermeasures employed within an* *organizational information system to protect the confidentiality, integrity, and availability of the system and its information*. [72 page 12]

NIST has established a well-defined repository of security controls, specifically in the Special Publication 800-53. As specified by NIST *The purpose of NIST Special Publication 800-53A is to establish common assessment procedures to assess the effectiveness of security controls in federal systems*. NIST 800-53 has been used as a reference framework perspective for identifying security recommendations and controls to apply and improve the cybersecurity on the data flow and communication process within the national reporting system. Unlike other security frameworks such as ISO/IEC 27000 series, NIST documents are publicly available.

Requirements to ensure a secure communication and storage of information for the National Crime Reporting System and NIST 800-53 control family that address them are shown in Table 7. It is assumed that the organization has already defined policy and procedures.

Security Requirements	**Control Family (NIST 800-53)**
Policy and procedures	First control in every control family
Audit records	Audit and Accountability (AU)
Cryptographic protection	System and Communications Protection (SC)
Spam and scams protection	System and Information Integrity (SI) System and Communications Protection (SC)
Spoofing network	Access Control (AC) System and Communications Protection (SC)
Incident response	Incident Response (IR)
Contingency planning	Contingency Planning (CP)
Data reception	System and Information Integrity (SI)

Table 7. Security requirements and Control Family within NIST 800-53 that address them

The architecture design of the system shall protect confidentiality, integrity and availability of the information [SC-28 Protection of information at REST] from its source, going through storage, until delivered to appropriate official body. Moreover, the organization may contemplate duplication of data to maintain functionality regardless disruption or failure in the system by implementing an alternate storage site including security mechanism equivalent to that of the primary site [CP-6 Alternate storage site]. This control should be considered if information access from officials is made from different geographical locations.

In addition, the architecture design shall describe security mechanisms applied for both internal communication between the components of the system and external communication. This includes the use of cryptography techniques, specifically encrypting sensitive data to prevent unauthorized disclosure or modification [SC-8 Transmission confidentiality and integrity]. Communication process between reporter and the entry point of the system shall protect confidentiality and integrity of transmitted information during preparation for transmission and during reception, avoiding man-in-the-middle attacks. For example, enabling TLS protocol over an HTTP server. Anonymity of the reporter shall be considered once the input has been analyzed, thus legal actions may be performed in case of malicious content or intention.

The flow of information within the system and between interconnected systems shall be enforced and documented [AC-4 Information Flow Enforcement]. Information flow between systems represent different security domains, system may implement Write-Once Read-Many policy to information access, so once the report is stored in the database it only can be retrieved without modifying its content. Outside traffic that are not directed to the service must be blocked.

The information system shall separate logically or physically user functionality from information system management functionality (administer database, manage workstations, etc) by using virtualization techniques or different network addresses. Security mechanisms apply both internal communication with the system inside the organization and external communication from users with the service provided. Consequently, the system shall include identification and authentication process before establishing local, remote or network connection by using bidirectional authentication [IA-3 Device Identification and Authentication] (however, external user authentication may be no required according to organizational and legal requirements). Obtaining a public key certificate from an approved service provider [SC-17 Public Key Infrastructure certificate] may be required to establish a secure communication with the system.

A scheme design of the system architecture is presented in figure 2. It differentiates between three areas: an isolated zone that provide external service, such as the reporting service and authentication service, an isolated zone that stores and manages all received data, and a zone inside the organization to access the information. The implementation of such architecture may be or not in the same geographical area. If they are in different areas, a virtual private network may be established between the three areas for internal connection. In addition, it may exist another zone for storage replication.

The system shall operate isolated with established boundaries [SC-7 Boundary protection] and security mechanism at entry and exit points in order to protect and secure legal authority workstation environment against any threat or risk like Denial of Service (DoS) [SC-5 Denial of Service protection] or spam [SI-8 Spam Protection] attacks. A Denial of Service of attack is defined as *An attack that prevents or impairs the authorized use of information system resources or services* by NICCS™ Portal Cybersecurity Lexicon, National Initiative for Cybersecurity Careers and Studies. Some recommendations are implementing a Demilitarized zone or DMZ consisting of a subnetwork for public access to the reporting service physically or logically separated from the internal organizational network, considering the implementation of encrypted tunnels or virtualized system within routers, and configuring a packet filtering firewall.

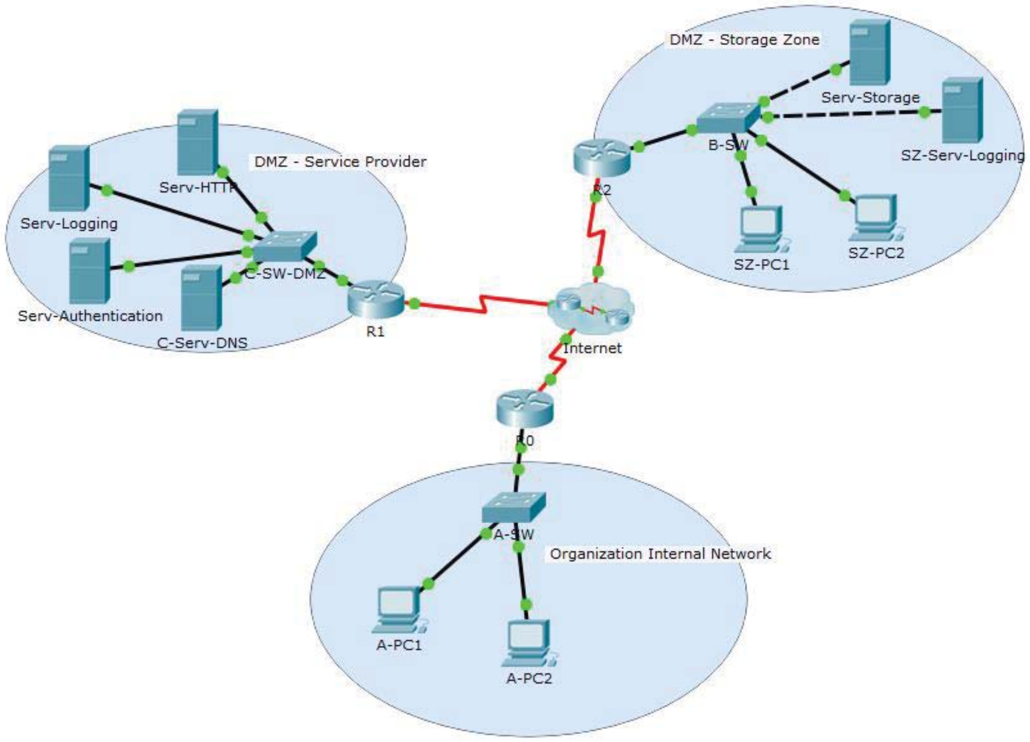

Figure 2.Architecture of the reporting system divided in three areas

Increase capacity and bandwidth combined with service redundancy may also prevent or limit the effect of a denial of service attack. This mechanism may solve some extraordinary circumstances or non-probabilistic event in which many reports may be detected as a DoS attack indicator.
The information system shall sanitize, classify and storage received reports (input of the system) so national authorities manage and analyze them. The information system checks the validity of the fields of the reports in accordance with specified organizational procedures [SI-10 Information input validation]. This includes check the validity of syntax and semantics, e.g., character set, length, numerical range and acceptable values or formats of defined fields, avoid content from being interpreted as commands and specify a whitelist, i.e. specify acceptable format for inputs discarding those that do no match (for example the format of the file evidence support).

The organization shall configure and manage malicious code protection mechanism at the reporting system entry and exit points to detect and erase malicious code [SI-3 Malicious Code Protection]. The system shall configure malware detection mechanism, such as firewalls or antivirus, to perform periodic scans of any file received as input at the entry service point, and update them in accordance with organization configuration management policy and procedures (if applicable).Besides, configuring an Intrusion Prevention System (IPS) or an Intrusion Detection System (IDS), an up-to-date antivirus that scans periodically any received file and a firewall in accordance with organizational security policy are highly recommended. In addition, the configuration of the system shall prevent the execution of any executable file or unauthorized code. Security mechanisms shall block any malicious code and send an alert to the administrator or personnel in charge. Actions in response to malicious detection shall be documented. The application of this control is directly associated to monitorization of the activities (Audit and Accountability) to detect anomalies in the system.

Any report may be used as a relevant and significant source by applicable federal laws, executive orders, directives, policies, regulations or standards [SI-12 Information Handling and Retention] as evidence to prosecute criminal activities, therefore auditing may be required [AU-3 Content of audit records]. Records shall contain information that establish what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, the identity of any individuals or subjects associated with the event, and evidence involved. The system shall generate timestamps that can be mapped to Coordinated Universal Time UTC or Greenwich Mean Time GMT [AU-8 Including date and time]. Moreover, in order to reduce the likelihood of potential loss or reduction of auditing capability, the organization shall consider the audit processing requirements when storing audit records [AU-4 Audit record storage].

6.2. Crime evidence storage

File storage represents a reference point in the system since images or videos are evidences that support and ease the crime prosecution. For this reason, this subsection analyzes existing methods to store data and details some security concerns to protect the system against bad intentioned uploads.

Factors such as space, performance, scalability, simplicity or manageability are fundamental to decide whether storing a file in a file system or in a database. Although there are solutions that provide good performance, and even some database management systems are equipped with some features, like SQL Server which provides file stream support [85] in which unstructured data (such as documents and images) is stored in the filesystem. Storing files in a database carries out some troubles because they are usually expensive and hard to scale. On the other hand, when scalability is not an issue, it may be a good idea to save the files in a database due to integrity between the image and metadata and auditing concerns.

Computers use plain text or binary formats to store data. There is no overall best storage format, it depends on the size and complexity of the data set.

- **Plain text formats**. All of the information in the file, even numeric information, is stored as text. A plain text file contains a header (metadata about the file) and content. A single character is represented by a byte or fixed number of bytes. There are different subtypes of plain text formats:
    - Delimited format: values separated by a special character (a delimiter)
    - Fixed-width format: allocate a fixed number of characters within every line
    - Comma-Separated Value (CSV): special case of plain text format

In addition, there are different plain text encoding. ASCII and UNICODE are the most common.

- ASCII encoding (American Standard Code for Information): letters, digits, special symbols and punctuation marks. It encodes 128 characters (7bits)
- Unicode [89]: attempt to allow computers to work with all of the characters in all of the languages of the world. Every letter in every alphabet maps a code point, for example U+0041 (numbers are hexadecimal) represents the letter A. UTF-16 allows two bytes per character text and UTF-8 one byte per character

- **Binary formats**. It provides faster and more flexible access to the data. It is a complex storage solution non-human readable. A binary format specifies how many bits or bytes constitute a basic unit of information within a file. The same block can be interpreted in different ways by different formats, for example each byte can be interpreted as a single character, as a two-byte integer, or as a four-byte real number. Therefore, it requires specific software to encode and decode the data.

The difference between binary formats and plain text formats is how the bytes of computer memory are used. For example, a PDF format could be interpreted as either 8-bit binary file or 7-bit ASCII text file

Microsoft Research team analyzed the performance of accessing large objects stored in a filesystem or in a database [86]. While objects smaller than 256K are best stored in a database and objects larger than 1M are best stored in the filesystem, they conclude that the storage option depends on the particular filesystem, database system and workload and that fragmentation and performance degradation are some considerations to take into account.

There are different options to consider when storing binary files in the database:

- Store in the database with a BLOB: Integrity and atomicity of transactions are preserved but increase storage requirements
- Store on the filesystem with a link in the database
- Store in the filesystem but rename to a hash of the contents and store the hash on the database

A Binary Large OBject (BLOB) is a collection of binary data stored as a single entity in a database management system. They are usually non-structured data such as images, audio or other multimedia objects Representing the data in binary format is more space-efficient and represents a direct mapping onto the internal representation of the data that the program is using**.** Some Relational Database Management Systems have individually covered it

6.2.1. Storing malware inside a database

From the point of view of a storage system, data is just perceived as a bunch of bytes. Both an executable file and a non-executable file should not cause any trouble to the system. However, the problem arises because different applications interpret and use the file’s properties (name, extension, size, etc.) in different ways. Embedded malware can target and exploit vulnerabilities in the operating system or any application that processes the data. If the software that reads a file have a bug, every file is a vector for malicious code execution. In other words, other applications such as antivirus scanner or a file preview generator handle files that can trigger the hidden code. We find some examples in Windows Metafile Vulnerability (or Metafile Image Code Execution) [87] and Microsoft Windows Media Player Buffer Overflow exploit [88]. In addition, malware can exploit bugs in the properties of the filesystem or execute a library file saved to the same directory where an application is vulnerable.

There are different ways and techniques of attacking a system with a file-upload service. These include, among others: file exploitation, file’s properties crafting, buffer overflows, exploitation of the software that executes the file or exploiting known file server vulnerabilities.

- Filename exploitation: Unicode shenanigans and filename overwritten belong to this type of attack. Unicode has a special character, U+202E, designed to display the text that follows in right-to-left order (RLO). Windows supports Unicode, including in filenames. This trick can be exploited to make a malicious file looks inoffensive. For example, exampleexe.doc could really be an executable named exampledoc[U+202E].exe [73,90]. On the other hand, if the system keeps the name of the uploaded file and it stores in the same location, files can be overwritten.
- File's properties crafting: a file contains metadata, i.e. information about the file. A document can be saved in another format that its property dictates. It could be considered a filename attack
- Buffer overflows: there are different techniques to cause a buffer overflow and execute arbitrary code on the server. If boundaries are not defined an application can copy user data into a memory buffer and overwrite adjacent memory; also, if the file is compressed it may contain a buffer-overflow malware for the decompressor. For example, if an image viewer allocated a buffer and computes the necessary buffer size just from a width * height * bytes_per_pyxel calculation, a malicious image could report dimensions sufficiently large to cause the above calculation to overflowing, causing the viewer to allocate a smaller buffer than expected and allowing for a buffer overflow attack when data is read into it. [80,81,82,83,84]
- Exploiting the software that opens the file: this technique hides code inside an image or video file. When this file is opened, the code hidden in the file is executed exploiting a bug in the software. For example Exploit.Win32.AdobeReader.K takes advantage of a vulnerability (CVE-2007-5020) [74] on the URI handling of PDF files; meanwhile Zero Day QuickTime mvhd is able to create controllable memory corruption by providing a malformed version and flags, and trigger an arbitrary write operation (CVE-2014-4979) [75]. Malware usually try to exploit video and music players [76,77,78,79]
- Exploiting known file server vulnerabilities: for example, some apache configurations would run script.php.jpg as php scripts. If a PHP code with a web shell within the file is named as ended in .jpg and uploaded in the same folder as the other .php files, the attacker could control the path to the file and then execute this script. Much of issues comes from old and historical configuration.

6.2.2. Defenses against file uploads

Some file upload defense guidance is listed below

- Use a whitelist of allowed file types
- Use server-side input validation and sanitation
- Set a maximum length for the file name and a maximum size for the file itself
- Convert the content of the file to a different format (then back to the original format if required)
- The directory to which files are uploaded (if it is stored in the filesystem) should be outside of the website root and in a non-execute directory
- All uploaded files should be scanned by antivirus software before they are opened
- The application should not use the file name supplied by the user. Instead, the uploaded file should be renamed according to a predetermined convention with safe characters ([a-z][A-Z][0-9])
- Check the mime type of file, not the value supplied by the user

7. LATIN AMERICAN RESPONSE SYSTEM

7.1. Architecture

The assessed system is split into three well differentiated main components: a reporting component, a client application and an administration and monitorization component.

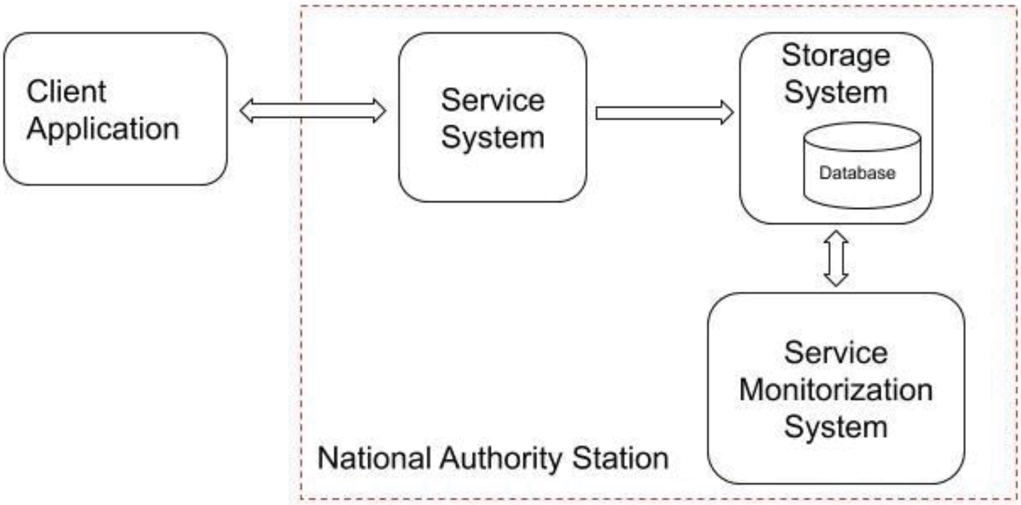

Figure 3. National Crime Reporting System design

The system allows citizens to report suspicious activities anonymously by providing a client interface (mobile application or web application) and an API to communicate with the backend in the reporting system. Between its features, it allows to upload crime evidence such as photos and videos (with a limited size or timing), to hold an anonymous chat with an official, as well as it features a panic button in case of genre violence with real time location and assistance.

The information received by the Service System is stored on a database within the Storage System. The Administration and Monitorization component classifies each type of report and delivers it to the correspondent police unit. Police officers analyze and manage the reports submitted by citizens through a desktop application.

7.2. Data Flow Assessment

The system uses a web server to provide the reporting service. It is not known if the system counts with a proxy (with or without a load balancer) as endpoint that delivers the request to an application hosted in a webserver.

The web server or proxy is configured with TLS/SSL to establish a secure communication channel and ensure confidentiality and integrity. TLS/SSL is a standard technology that uses encryption to keep a secure connection between two sides.

Although the specification of the system claims that anonymity is guaranteed, that statement is not completely accurate because for example images or videos contain metadata that can trace the user's movements. Moreover, information about the reporter may be required by law enforcement in case of bad use of the system as stated in the previous section.

The external boundaries of the service system are protected by an Intrusion Detection System and configured against DDoS or flooding attacks. The Client application (referenced as the application that realize the report) is never related to the storage system. It is not known whether the system where the web server operates has a firewall or the router to which it is connected to has it.

The system implements a database system for storage data, including media files. As explained in the previous section, this approach eases auditing and backup purposes. However, while storing files within the database is acceptable, video storage performs worse. It is unknown the security controls implemented in the database system and whether data within the database is encrypted.

It is not known if the Service System, the Storage System and the Service Monitorization System are placed in the same area or distributed geographically. However, according to the architectural design, internal communication is made through IPSec. IPSec is a framework based on standards developed by the Internet Engineering Task Force (IETF) for ensuring secure private communications over the Internet. On the other hand, it is using the weakest algorithm for encrypted data, i.e. it is using DES instead of 3DES or AES.

Switches and routers are replicated through the internal network ensuring availability to the Service Monitorization System when establish a connection to the Storage System. The most external routers (those further from the Service Monitorization System) also implement firewall and VPN solutions.

8. CONCLUSION

Internet of Thing fast development is enhancing communication and productivity, but also it brings many security flaws. System heterogeneity, together with lack of the application of security controls to IoT devices and the limited storage resources and computational capabilities make them vulnerable. In a novel area with still few research resources, such as the Internet of Things, standards and regulations are required to improve their cybersecurity.

Criminal organizations can afford to pay for Information and Technology expertise. They attempt to exploit devices vulnerabilities with network access to attack enterprises or gather as much data as possible for economic purposes. There is a hidden market in which different services and data are offered. But not only criminal organization benefit from the properties of the Internet of Thing devices. Ordinary devices such as smartwatches or mobiles phones are equipped with different features that allows them to collect a big amount of information. Consequently, cyberstalking and espionage are important security challenges to research and address. Monitorization and right to privacy are topics that will be concerning the following years.

This document aims to analyze the state of IoT security and relating it to criminal or unethical activities such as cyberstalking, espionage and contract killing. In addition, the communication and data flow of a national crime report system is analyzed and assessed following the guidelines and best practices by a security framework.

REFERENCES

[1] Dawson, M., Omar, M. and Abramson, J. 2015. *Understanding the Methods behind Cyber Terrorism*. Encyclopedia of Information Science and Technology, Third Edition, Hershey, pp. 1539-1549.

[2] Mansfield-Devine, S. 2016. *Securing the Internet of Things*. Computer Fraud and Security pp 15-20

[3] Radoglou-Grammatikis, P., Sarigiannidis P. G. and I. D. Moscholios. 2019. *Securing the Internet of Things: Challenges, threats and solutions*. Internet of Things, Volume 5, pp. 41-70, Elsevier

[4] Bispham, M.K., Agrafiotis, I. and Goldsmith, M. 2018. *Nonsense Attacks on Google Assistant*. arXiv preprint arXiv:1808.01947

[5] Forbrukerràdet. Norwegian Consumer Council. 2017. #WatchOut. *Analysis of smartwatches for children.* https://fil.forbrukerradet.no/wp-content/uploads/2017/10/watchout-rapport-october-2017.pdf

[6] Stykas, V. 2019. *GPS watch issues… again*. Pen Test Partners. Penetration testing and security services. https://www.pentestpartners.com/security-blog/gps-watch-issues-again/

[7] Heartfield, R., Loukas, G., Budimir, S., Bezemskij, A., Fontaine, J. R. J., Filippoupolitis,A. and Roesch, E. 2018. *A taxonomy of cyber-physical threats and impact in the smart home.* Computers and Security Volume 78 pp 398-428 Elsevier

[8] Yuan, X., Chen, Y., Zhao, Y., Long, Y., Liu, X., Chen, K., Zhang,S., Huang, H., Wang, X.,Andgunter, C. A. 2018. *CommanderSong: A Systematic approach for practical adversarial voice recognition.* arXiv preprint arXiv:1801.08535

[9] Andres Kwong, A., Xu, W. and Fu K. 2019 *Hard Drive of Hearing: Disks that Eavesdrop with a Synthesized Microphone*. In Proceedings of the 40th Annual IEEE Symposium on Security and Privacy

[10] Conti, M., Dehghantanha, A, Franke, K. and Watson, S. 2018. *Internet of Things security and forensics: Challenges and opportunities.* Future Generation Computer Systems Vol 78 part 2 pp 544-546 Elsevier

[11] Leukfeldt E. R. and Kleemans,. 2017. *Cybercriminal Networks, Social Ties and Online Forums: Social Ties versus digital ties within phishing and malware network*. British Journal of Criminology 57(3) pp 704-722

[12] Leukfeldt E. R., Kleemans, E.R. and Stol, W. 2017. *A topology of cybercriminal networks: from low-tech all-rounders to high-tech specialists*. Crime Law and Social Change 67(1) pp 21-37

[13] Leukfeldt E. R. 2013. *Cybercrime and social ties. Phishing in Amsterdam*. Trends in Organized Crime. 17(4) 231-249

[14] Bijlenga, N. and Kleemans E. R. 2017. *Criminals seeking ICT-expertise: an exploratory study of Dutch cases.* European Journal on Criminal Policy and Research Vol. 24, Issue 3, pp 253-268

[15] Yaqoob, I., Ahmed, E., Habib ur Rehman, M., Ahmed A. I. A, Al-garadi, M. A., Imran, M. and Guizani, M. 2017. *The Rise of ransomware and emerging security challenges in the Internet of Things*. Computer Networks Vol 129 part 2 pp 444-458 Elsevier

[16] Randaliev, P., De Roure, D. C., Nicolescu, R., Huth, M., Montalvo, R. M., Cannady, S. and Burnap, P. 2018. *Future developments in cyber risk assessment for the internet of things*. Computers in Industry Vol. 102 pp 14-22

[17] Nokia Threat Intelligence Report 2019. White paper

[18] Edwards, S. and Ioannis Profetis, I. 2016. *Hajime: Analysis of a decentralized Internet worm for IoT devices*. Rapidity Networks Security Research Group

[19] Netlab. 2017. *IoT_reaper: A Rappid Spreading New IoT Botnet.* https://blog.netlab.360.com/iot_reaper-a-rappid-spreading-new-iot-botnet-en/

[20] Check Point Research. 2017. *Huawei Home Routers in Botnet Recruitment*. https://research.checkpoint.com/good-zero-day-skiddie/

[21] Netlab. 2018. *Art of Steal: Satori Varian is Robbing ETH BitCoin by Replacing Wallet Address*. https://blog.netlab.360.com/art-of-steal-satori-variant-is-robbing-eth-bitcoin-by-replacing-wallet-address-en/

[22] Nigam, R. 2018. *Unit 42 Finds New Mirai and Gafgyt IoT/Linux Botnet Campaigns*. Unit 42 Palo Alto Networks. https://unit42.paloaltonetworks.com/unit42-finds-new-mirai-gafgyt-iotlinux-botnet-campaigns/

[23] Nigam, R. 2018. *Multi-exploit IoT/Linux Botnets Mirai and Gafgyt Target Apache Struts, SonicWall*. Unit 42 Palo Alto Networks. https://unit42.paloaltonetworks.com/unit42-multi-exploit-iotlinux-botnets-mirai-gafgyt-target-apache-struts-sonicwall/

[24] Remillano, A. 2019. *ThinkPHP Vulnerability Abused by Botnets Hakai and Yowai.* Trend Micro Inc. Security Intelligence Blog https://blog.trendmicro.com/trendlabs-security-intelligence/thinkphp-vulnerability-abused-by-botnets-hakai-and-yowai/

[25] Nigam, R. 2019. *New Mirai Variant Targets Enterprise Wireless Presentation & Display Systems*. Unit 42 Palo Alto Networks. https://unit42.paloaltonetworks.com/new-mirai-variant-targets-enterprise-wireless-presentation-display-systems/

[26] Remillano, A., Urbanec, J., Galera, B. and Vicente, M. 2019. *Mirai Variant Spotted Using Multiple Exploits, Targets Various Routers*. Trend Micro Inc. Security Intelligence Blog https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/mirai-variant-spotted-using-multiple-exploits-targets-various-routers

[27] Remillano, A. and Urbanec, J.,2019. *New Mirai Variant Uses Multiple Exploits to Target Routers and Other Devices*. Trend Micro Inc. Security Intelligence Blog https://blog.trendmicro.com/trendlabs-security-intelligence/new-mirai-variant-uses-multiple-exploits-to-target-routers-and-other-devices/

[28] Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J.A., Invernizzi, L., Kallitsis, M., Kumar, D., Lever, C., Ma, Z., Mason, J., Menscher, D., Seaman, C., Sullivan, N., Thomas, K., and Zhou, Y. 2017. *Understanding the Mirai Botnet.* 26th USENIX Security Symposium

[29] Vicente, M., Galera, B. and Remillano, A. 2019. *Bashlite IoT Malware Updated with Mining and Backdoor Commands, Targets WeMo Devices.* Trend Micro Inc. Security Intelligence Blog

https://blog.trendmicro.com/trendlabs-security-intelligence/bashlite-iot-malware-updated-with-mining-and-backdoor-commands-targets-wemo-devices/

[30] Olenick, D. 2019. *Mirai botnet upgraded to work with new IoT processors*. SC Media. https://www.scmagazine.com/home/security-news/malware/mirai-botnet-upgraded-to-work-with-new-iot-processors/

[31] Easton, T. 2018. Chalubo botnet wants to DDoS from your server or IoT device. Sophos Labs. https://news.sophos.com/en-us/2018/10/22/chalubo-botnet-wants-to-ddos-from-your-server-or-iot-device/

[32] Chatterjee, R., Doerfler, P., Orgad, H., Havron, S., Palmer, J., Freed, D., Levy, K., Dell, N., McCoy, D., Ristenpart, T. 2018. *The Spyware Used in intimate partner violence*. Conference 2018 IEEE Symposium on Security and Privacy (SP).

[33] Greenberg, A. 2019. *Hacker Eva Galperin has a plan to eradicate stalkerware.* https://www.wired.com/story/eva-galperin-stalkerware-kaspersky-antivirus/

[34] Albrecht, K. and Mcintyre, L. 2015. *Privacy Nightmare: When Baby Monitors Go Bad.* IEEE Technology and society magazine

[35] Harkin, D., Molnar, A. and Vowles, E. 2019. *The commodification of mobile phone surveillance: An analysis of the consumer spyware industry.* Crime, Media, Culture: An International Journal

[36] Freed, D., Palmer, J., Minchala, D., Levy, K., Ristenpart, T. and Dell, N. 2018. *A Stalker's Paradise: How intimate partner abusers exploit technology.* Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems

[37] FBi's Internet Crime Complaint Center (IC3). 2018. *Internet Crime Report*

[38] Canetti, D., Gross, M. L., Waismel-Manor, I. and Levanon, A. 2017. *How cyberattacks terrorize: cortisol and personal insecurity jump in the wake of cyberattacks.* Cyberpsychology, Behavior, and Social Networking 20(2)

[39] Talbot, C. M., Temple M. A., Carbino T. J. and Betances J. A. 2018. *Detecting rogue attacks on commercial wireless Insteon home automation systems*. Computer Security Volume 74 pp 296-307

[40] Bijlenga, N. and Kleemans E. R. 2018. *Criminals seeking ICT-expertise: an exploratory study of Dutchcases.* European Journal on Criminal Policy and Research Volume 24 Issue 3 pp 253268

[41] Dawson, M. and Cardenas-Haro, J.A. 2017. *Tails Linux Operating System: Remaining Anonymous with the Assistance of an Incognito System in Time of High Surveillance*. International Journal of Hyperconnectivity and the Internet of Things. Volume 1. Issue 1

[42] Dalton, J. 2019. *Airlines admit having cameras installed on back of passenger's seats.* The Independent. https://www.independent.co.uk/news/world/americas/cameras-american-airlines-united-singapore-privacy-seats-planes-a8793846.html

[43] CSO. 2019. Nest Secure had a secret microphone, can now be a Google Assistant. https://www.csoonline.com/article/3336227/nest-secure-had-a-secret-microphone-can-now-be-a-google-assistant.html

[44] Markets and Markets. *Video Surveillance Market Research Report* 2018 https://www.marketsandmarkets.com/Market-Reports/video-surveillance-market-645.html

[45] Diao, W., Liu, X., Zhou, Z. and Zhang. K. 2014. *Your Voice Assistant is Mine: how to abuse speakers to steal information and control your phone.* In ACM Workshop on Security and Privacy in Smartphones & Mobile Devices (SPSM)

[46] Schlegel, R., Zhang, K., Zhou, X. Intwala, M., Kapadia, A. and Wang X.. 2011 *Soundcomber: A stealthy and context-aware sound trojan for smartphones*. In Proceedings of the 18st Annual Network and Distributed System Security Symposium, NDSS

[47] Sabath, F. 2012. T*hreat of Electromagnetic Terrorism: Lessons learned from documented IEMI Attacks*. Conference Paper

[48] Savage, E. and Radasky, W. 2012. *Overview of the Threat of IEMI (Intentional Electromagnetic Interference).* Electromagnetic Compatibility (EMC) IEEE International Symposium, pp. 317-322

[49] Schneier, B. 2019. Security Flaws in Children's Smart Watches. https://www.schneier.com/blog/archives/2019/01/security_flaws_3.html

[50] Sebba, L. 1984 *Crime Seriousness and criminal intent*. Crime & Delinquency, vol 30, no.2, pp.227-244

[51] Kaspersky Lab. 2019. *Operation ShadowHammer: A high-profile supply chain attack* https://securelist.com/operation-shadowhammer-a-high-profile-supply-chain-attack/90380/

[52] Mirea, M., Wang, V. and Jung, J. 2019. *The not so dark side of the darknet: a qualitative study*. Security Journal Volume 32 Issue 2 pp 102-118

[53] Tzanetakis, M. 2018. *The darknet's anonymity dilemma*. Encore. The Annual Magazine on Internet and Society Research pp. 118-125

[54] Weimann, G. 2016. *Going Dark: Terrorism on the Dark Web.* Studies in Conflict & Terrorism. Vol. 39 Issue 3. Pages 195-206

[55] Prokofiev, A. O., Smirnova Yulia S. and Silnov, D. S. 2017. *The Internet of Things Cybersecurity Examination*. Siberian Symposium on Data Science and Engineering (SSDSE)

[56] Mohamad Noor, M. and Haslina Hassan, W. 2019. *Current research on Internet of Things (IoT) security: A survey*. Computer Networks Volume 148, Pages 283-294. Elsevier

[57] Owen, G., and N. Savage. 2015. *The Tor Dark Net*. Paper Series no: Global Commission on Internet Governance

[58] Dawson, M. 2018. *Cyber Security in Industry 4.0: The Pitfalls of Having Hyperconnected Systems*. Journal of Strategic Management Studies. Vol 10. No.1. 19-28

[59] Canales, K. 2018. *A couple says that Amazon's Alexa recorded a private conversation and randomly sent it to a friend*. Business Insider. https://www.businessinsider.es/amazon-alexa-records-private-conversation-2018-5?r=US&IR=T

[60] Profis, S. and Broida, R. 2019. *You can finally delete most of your Amazon Echo transcripts*. https://www.cnet.com/how-to/amazon-echo-saves-all-your-voice-data-heres-how-to-delete-them/

[61] Whitney, L. 2013. *Apple hangs onto your Siri data for two years.* https://www.cnet.com/news/apple-hangs-onto-your-siri-data-for-two-years/

[62] McLaughlin, E. C. 2017. Suspect OKs Amazon to hand over Echo recordings in murder case. CNN Business. https://edition.cnn.com/2017/03/07/tech/amazon-echo-alexa-bentonville-arkansas-murder-case/

[63] European Commission *The Rapid Alert System for Non-Food Products* (RAPEX) https://ec.europa.eu/consumers/consumers_safety/safety_products/rapex/alerts/?event=viewProduct&reference=A12/0157/19&lng=en

[64] Krebs on Security. 2018. Serial Swatter and Stalker Mir Islam Arrested for Allegedly Dumping Body in River. https://krebsonsecurity.com/2018/12/serial-swatter-and-stalker-mir-islam-arrested-for-allegedly-dumping-body-in-river/

[65] Dawson, M. 2016. *Cyber Security Architectural Needs in the era of Internet of Things and Hyperconnected Systems*. Conference: 10th Annual International Academy of Strategic Management Conference

[66] The American Consumer Institute Center for Citizen Research. Securing IoT Devices: How Safe is Your Wi-Fi Router?

[67] Chertoff, M. and Simon, T. 2015. *The Impact of the Dark Web on Internet Governance and Cyber Security. Global Commission on Internet Governance*. Paper Series No. 6.

[68] Mattern, B. 2014 *Cyber Security and Hacktivism in Latin America: Past and Future* http://www.coha.org/cyber-security-and-hacktivism-in-latin-america-past-and-future

[69] Sutton, H., Álvarez, L., van Dijk, J., Van Kesteren, J., Ruprah, I. J., Godinez Puig, L., Jaitman, L., Torre, I. and Pecha, Camilo. 2017. *Restoring paradise in the Caribbean: Combating violence with numbers*.

[70] Soares R. R. and Naritomi, J. 2010. *Understanding high crime rates in Latin America: The Role of Social and Policy Factors*. Understanding High Crime Rates in Latin America: The Role of Social and Policy Factors pp 19-55

[71] Kshetri N. 2013. *Cybercrime and Cybersecurity in Latin American and Caribbean Economies.* Cybercrime and Cybersecurity in the Global South. International Political Economy.

[72] National Institute of Standards and Technology. Security and Privacy Controls for Federal Information Systems and Organizations, NIST Special Publication 800-53, Revision 4, 2013; https://nvd.nist.gov/800-53/Rev4

[73] Krebs on Security. 2011 'Right-to-Left Override' Aids Email Attacks. https://krebsonsecurity.com/2011/09/right-to-left-override-aids-email-attacks/

[74] Common Vulnerabilities and Exposures CVE-2007-5020 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5020

[75] Common Vulnerabilities and Exposures CVE-2014-4979 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4979

[76] Check Point Advisories VideoLAN VLC Media Player PNG Code Execution - Improved Performance (CVE-2012-5470) https://www.checkpoint.com/defense/advisories/public/2013/cpai-17-mar16.html

[77] vln - arbitrary code execution in Real RTSP and MMS support http://vuxml.freebsd.org/freebsd/62f36dfd-ff56-11e1-8821-001b2134ef46.html

[78] Microsoft Security Bulletin MS10-082 - Important. Vulnerability in Windows Media Player Could Allow Remote Code Execution (2378111) https://docs.microsoft.com/en-us/security-updates/securitybulletins/2010/ms10-082

[79] Microsoft. MS07-047: Vulnerabilities in Windows Media Player Could Allow Remote Code Execution (936782) https://docs.microsoft.com/en-us/security-updates/securitybulletins/2007/ms07-047

[80] Microsoft Security Bulletin MS05-009 - Critical. Vulnerability in PNG Processing Could Allow Remote Code Execution (890261)
http://technet.microsoft.com/en-us/security/bulletin/ms05-009

[81] Microsoft Security Bulletin MS04-028 - Critical. Buffer Overrun in JPEG Processing (GDI+) Could Allow Code Execution
http://technet.microsoft.com/en-us/security/bulletin/ms04-028

[82] Adobe Security bulletin. Security update available for Adobe Photoshop CS5
http://www.adobe.com/support/security/bulletins/apsb11-22.html

[83] Mozilla Foundation Security Advisory 2012-92. Buffer overflow while rendering GIF images
https://www.mozilla.org/security/announce/2012/mfsa2012-92.html

[84] Common Vulnerabilities and Exposures. CVE-2010-1205
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1205

[85] Microsoft. SQL Server 2017. Filestream (SQL Server)
https://docs.microsoft.com/en-us/sql/relational-databases/blob/filestream-sql-server?view=sql-server-2017

[86] Sears, R., van Ingen, C. and Gray, J. 2006. *To BLOB or Not To BLOB: Large Object Storage in a Database or a Filesystem? T*echnical Report msr-tr-2006-45. Microsoft Research. Microsoft Corporation

[87] Microsoft Security Bulletin MS06-001 Critical - Vulnerability in Graphics Rendering Engine Could Allow Remote Code Execution (912919)
https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2006/ms06-001

[88] Exploit Database. Microsoft Windows Media Player 11.0.5721.5145 - ‘.avi’ Buffer Overflow
https://www.exploit-db.com/exploits/35553

[89] The Unicode Consortium https://www.unicode.org/

[90] Spoof Using Right to Left Override (RTLO) Technique
https://resources.infosecinstitute.com/spoof-using-right-to-left-override-rtlo-technique-2