signals

MDPI

Review

Exploitation Techniques of IoST Vulnerabilities in Air-Gapped Networks and Security Measures—A Systematic Review

Razi Hamada [1] and Ievgeniia Kuzminykh [1,2,*]

[1] Department of Informatics, King's College London, London WC2R 2ND, UK
[2] Department of Infocommunication Engineering, Kharkov National University of Radio Electronics, 61000 Kharkov, Ukraine
* Correspondence: ievgeniia.kuzminykhl@kcl.ac.uk

Abstract: IP cameras and digital video recorders, as part of the Internet of Surveillance Things (IoST) technology, can sometimes allow unauthenticated access to the video feed or management dashboard. These vulnerabilities may result from weak APIs, misconfigurations, or hidden firmware backdoors. What is particularly concerning is that these vulnerabilities can stay unnoticed for extended periods, spanning weeks, months, or even years, until a malicious attacker decides to exploit them. The response actions in case of identifying the vulnerability, such as updating software and firmware for millions of IoST devices, might be challenging and time-consuming. Implementing an air-gapped video surveillance network, which is isolated from the internet and external access, can reduce the cybersecurity threats associated with internet-connected IoST devices. However, such networks can also be susceptible to other threats and attacks, which need to be explored and analyzed. In this work, we perform a systematic literature review on the current state of research and use cases related to compromising and protecting cameras in logical and physical air-gapped networks. We provide a network diagram for each mode of exploitation, discuss the vulnerabilities that could result in a successful attack, demonstrate the potential impacts on organizations in the event of IoST compromise, and outline the security measures and mechanisms that can be deployed to mitigate these security risks.

Keywords: Internet of Surveillance Things; IoT security; IP camera; air-gapped networks; vulnerabilities; exploitation techniques; IoT attacks; security measures

Citation: Hamada, R.; Kuzminykh, I. Exploitation Techniques of IoST Vulnerabilities in Air-Gapped Networks and Security Measures—A Systematic Review. *Signals* **2023**, *4*, 687–707. https://doi.org/10.3390/signals4040038

Academic Editor: Santiago Marco

Received: 10 March 2023
Revised: 8 June 2023
Accepted: 19 June 2023
Published: 13 October 2023

1. Introduction

The Internet of Surveillance Things (IoST) combines the advantages of IoT technology with video surveillance systems. The most prevalent IoST devices, including IP cameras and digital or network video recorders (DVR/NDR), are widely deployed not only in public places to monitor activities and behaviors that may pose threats to assets and people, such as thefts and criminal actions, but also as part of critical infrastructure deployments to ensure the security and safety of operational processes. IP cameras stream video and images to the cloud or internal servers and can be found in strategic locations such as manufacturing facilities, hospitals, police departments, financial markets, and airports [1–4]. The IoT technology provides access to these IP cameras via the internet and delivers their respective video streams to the analytical systems that can use AI technology to analyses data on the fly at edge devices or within the core network.

Internet of Surveillance Things security has received massive attention due to the rise in IoT-related security problems. The experience of the Mirai botnet attack in 2016, which converted IoT devices including IP cameras into "zombies" and caused a massive DDoS attack that brought down the domain registration services provider Dyn [5], revealed the weaknesses of internet-connected devices, and motivated the companies and manufacturers to improve the security of their products. However, regardless of the level of awareness

of possible attack vectors, the set of similar attacks shows that the lesson was not learned, and IoST is still susceptible to risks and vulnerabilities that can be difficult to mitigate. In 2022, the DDoS botnet attack was launched against a Chinese telecommunication company from almost 170,000 compromised devices, including security cameras from over 180 countries [6]. The recent hacktivist attack against the video security company Verkada in 2020 led to the exposure of over 150,000 internet-connected cameras that were being used in prisons, hospital intensive care units, schools, and major companies like Tesla and Cloudflare [7]. A network of 25,000 cameras that was infiltrated and was being prepared for an assault was discovered by PC Word in 2016 [8]. The cameras and recorders were used to cause havoc in US companies and network infrastructures, leading to a significant loss of productivity when the internet was down for nearly twenty-four hours in most of the USA, according to a report published in the Wall Street Journal in September 2016. Other vulnerabilities that were found in IoST include software and firmware vulnerabilities in digital video recorders (DVR) such as command injection vulnerability and IoT botnet malware, both exploiting the Lilin security camera's DVR devices [9,10] and the Wyze Cam camera's set of vulnerabilities, allowing access to video feeds [11].

Despite implementing cutting-edge cybersecurity measures, malicious insiders continue to pose a significant threat to businesses due to their extensive access to organizational resources, both physical and digital, and their comprehensive understanding of vulnerable internal procedures [12]. Many of the aforementioned attacks have leveraged publicly available IoST devices, discoverable through tools like Shodan, to get access and exploit various vulnerabilities. It might seem that by disconnecting an IoST device from the internet, the risk of vulnerability exploitation is eliminated; however, air-gapped networks, while challenging to breach from the outside, are vulnerable to insider threats, and breaches are not impossible. Over the past decade, it has been demonstrated that advanced persistent threats (APTs) can breach highly secure air-gapped networks via different IP camera exploitation techniques [13]. For isolated air-gapped computer networks, typically used by security-sensitive institutions such as government bodies, research and development organizations, critical infrastructure like electricity and nuclear facilities, banking institutions, and the military, the challenge of securing IoST becomes even more critical.

While there are numerous published surveys covering research trends on security in the IoT domain, there are fewer surveys specifically addressing the security of IoST. Takhar D. in [14] identified some of the topics addressed by researchers in the IoST area, including ARP poisoning, MITM attacks and access authentication weaknesses. Another study by Vennam et al. [15] explored attacks on video surveillance systems discussed in the literature, and proposed security measures to mitigate such attacks, but did not pay attention to totally isolated networks. The authors in study [16] classified research into various categories, such as network infrastructure, communication, application, and user interaction, but the security aspect was out of the scope of that review. There is currently no comprehensive survey that thoroughly examines IP camera and IoST exploitation to penetrate air-gapped networks. Only a few researchers, such as Guri and Bykhovsky [13], have touched upon techniques like infrared LED, but as a small part of their primary research interests.

This paper systematically reviews the existing research studies and use cases related to IP camera vulnerabilities and exploitation techniques. It primarily focuses on methods used to target organizations through their IoST systems installed behind a logically air-gapped network, the technique used, and the impact, followed by mitigation measures proposed in the literature. The paper maps each technique to a real-world use case and presents it with an attack diagram for enhanced clarity.

The remainder of the review is organized as follows. Section 2 presents the literature research methodology, the data source research questions, and the screening process. The analysis of the top exploitation techniques currently used and potential security measures is presented in Section 3. A summary of the findings with a discussion is provided in Section 4.

2. Literature Review Methodology

In this section, we present our methodology for discovering relevant literature. In order to conduct a systematic literature review, our standard practices were those based on the works of Wohlin et al. [17] and Petersen et al. [18].

2.1. Research Questions

To compose the research questions and relevant search queries, as well as to shape the scope of the review, the following PICOC criteria [18] were used:

- Population—The industry group of IP camera manufacturers such as Axis, Borsch, Wisenet, i-Pro and many others, including the OEM (Original Equipment Manufacturer) and the corresponding firmware;
- Intervention—The exploitation techniques and the ways used by video surveillance systems to exchange data;
- Comparison—Comparing the techniques by their areas of application, functionality and impact;
- Outcomes—Compared techniques are grouped into categories based on the type of network topology, exploitation technique, impact, and security measure recommendations to make the IoST more secure;
- Context—The review is performed within both academia, whitepapers, and magazines publishments.

Based on the above, we defined the following research questions:

RQ1: What are the techniques for exploiting IoST vulnerabilities in air-gapped networks?

RQ2: What best practices prevent IoST exploitations in air-gapped networks?

RQ3: What security measures can keep up with new IoST exploitation techniques without breaking the air gap?

To answer the above research questions, such keywords and key phrases were constructed as IP Camera Vulnerability AND Assessment tool, IoT Vulnerability AND Security, Attacks on IP Cameras, and Air-Gapped Networks. See Table 1 for more details.

2.2. Selection Methodology of Reviewed Material

The methodology follows the following sequence of stages:

(a) Initial retrieval of the result from the search queries

(b) Perform manual inclusion and exclusion based on titles and abstracts relevant to index and search terms

(c) Abstract, then full-text read-through

(d) Backward snowball sampling followed by quality assessment

As proposed by Petersen et al. [6], several exclusions and inclusions criteria were applied (EC and IC, respectively) to retrieve the most suitable subset for this review:

- EC1: Paper is not accessible in full text;
- EC2: Paper is not presented in English;
- EC3: The paper has no title;
- EC4: The paper's publishing date is before 2015;
- EC5: The paper is focused on telecommunication protocols like Sigfox, Lora, and NB IoT;
- IC1: The paper has one of the search queries' key phrases in its title (see search queries);
- IC2: The paper is focused on vulnerability exploitation in air-gapped camera networks.

Any paper was excluded if it satisfied all the ECs and included if it met IC1 or IC2.

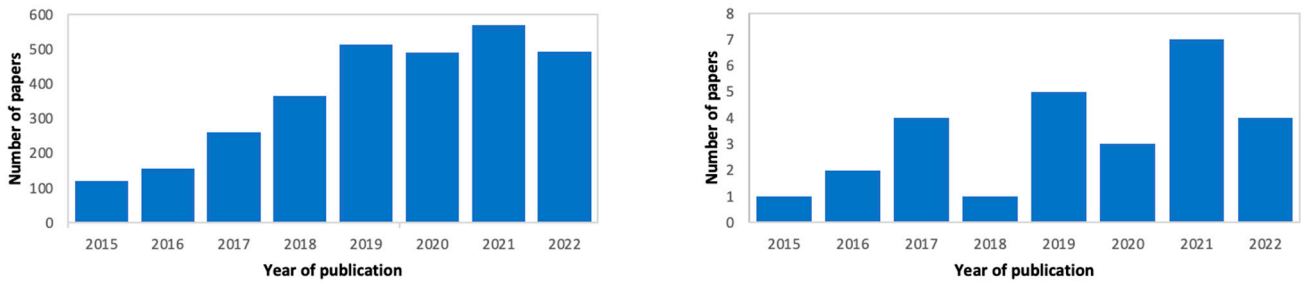
The possible limitation of our research methodology is that we searched only by the titles of the papers, acknowledging that some relevant papers could have been missed. We, however, believe that there is a sufficient number of papers collected using our approach to address the air-gapped camera networks.

Table 1. The paper selection and screening process.

No	Search Terms	Science Direct	IEEE	Scholar	KCL	Partners Digital Libraries	Total
1	IP Camera AND Vulnerability	151	18	917	56	6	1148
2	IP Camera Vulnerability AND Assessment Tool	14	0	0	2	1	17
3	Video Surveillance System AND IP Security	2	4	36	3	2	47
4	IoT Vulnerability AND Security	0	26	427	112	6	571
5	Attack AND IP Camera	1	5	1360	102	2	1470
6	CCTV Hacking	1	0	17	1	3	22
7	Cyber Kill Chain Attack	2	0	15	1	0	18
8	Air-Gapped Network AND IoT	0	1	2	0	0	3
9						Sub Total	3296
10						Do not match to IC and EC	−3176
11						Duplicates Excluded	−20
12						Excluded after Reading Title and Abstract	−45
13						Excluded after Reading Full Paper	−32
14						Backward Snowballing	5
15						Quality Assessment	−2
16						Total Selected Papers	26

2.3. Screening Process and Data Sources

Table 1 below shows the data sources, the screening process phases, and the number of papers discovered and excluded at each stage throughout the process. Figure 1a shows the papers returned during the initial search before and after applying IC and EC that were published each year. As can be seen from the timeliness of publications, the interest in the security of video systems connected to the internet gradually grew over the years in line with the development of IoT. Significant growth in 2017 was caused by the Mirai DDoS attack, which raised interest in the security of IoT and IoST as part of IoT exploited in the Mirai attack.



(**a**) (**b**)

Figure 1. Number of papers that are published each year related to our study (**a**) after removing duplicates and before IC and EC, and (**b**) selected for analysis.

The primary search was performed on ScienceDirect, IEEE, Google Scholar and KCL library in October 2022. The secondary research was performed using business partners'

digital libraries, with partner access granted, including Redinent and RAS Info Tech; the search was conducted in November 2022.

2.3.1. Satisfying IC and EC

After reviewing the selected papers in regard to matching the criteria EC1-5, IC1 and IC2, a vast number of the papers were excluded, as many of them were focused on telecommunication protocols and not focused on vulnerability exploitation in air-gapped camera networks.

2.3.2. Inclusion and Exclusion Based on Title and Abstract

Several papers were eliminated after applying the exclusion and inclusion criteria, the bulk of which were either specific to IIoT (Industrial IoT) or to the associated telecommunication protocols such as Sigfox, Lora, and NB IoT, which are not part of the IP camera area of interest for this review. This stage of exclusion of such papers can be seen in Table 1, indexing "Excluded".

2.3.3. Backward Snowball Sampling

According to Wohlin's [17] description, backward snowball sampling was employed to account for any important documents that might not have been found during the primary and secondary searches. Five pertinent papers were picked based on their titles, where they have been cited, and the writers.

2.3.4. Quality Assessment

According to [19] a critical appraisal is less about determining whether a paper is "good enough" and more about whether it satisfies specified criteria. The use of such criteria provides a systematic means of assessing an article's fit. We used a set of quality criteria adapted from City University of Hong Kong [20] that included: accuracy, authority, objectivity, currency and coverage. At this stage, two papers were excluded from the final set.

3. Critical Analysis of Selected Literature

After conducting the screening process mentioned in Section 2, this section identifies and explains the classification criteria and common themes for this review.

Costin, A. in [21] proposed seven criteria to classify vulnerabilities, exploitation techniques, attacks and security measures, namely: attack surface, attack type, attacker type, directly affected components, exploitation complexity, mitigation and mitigation complexity. In contrast, Papp et al. [22] employed a classification framework consisting of five categories, namely: precondition, attack method, vulnerability, target and effect. While the authors in [21] studied video surveillance systems (VSS), the authors in [22] focused on the cyber–physical systems in general, not specifically on IP cameras or video surveillance system components. Furthermore, both studies were published over five years ago, and may not encompass attacks and vulnerabilities that have emerged since 2016. A recent study of Vennam et al. [15] focuses only on attack and mitigation security mechanisms for VSS, omitting broader aspects, such as target and impact. Additionally, as highlighted in the introduction section, this study does not encompass air-gapped IP video networks.

This study tries to map the analysis to real-life scenarios, and thus classifies the findings according to the following five categories: network topology, vulnerability, exploitation technique, impact, and security measure. Use cases and attack diagrams have been added to enhance the explanation of the published attacks.

Before analyzing the most common and novel exploitation techniques, it is essential to differentiate between two network topologies: air-gapped and non-air-gapped. An "air gap" is a security measure that involves isolating a computer or network and preventing it from establishing an external connection. In the context of cybersecurity, an air-gapped computer is physically segregated and incapable of connecting wirelessly or physically

with other computers or network devices [23]. In a "non-air gapped" topology (Figure 2a), all IoST devices have public IP addresses, which means that anyone from the internet can send packets to these devices. In contrast, an air-gapped topology employs private IP addresses, ensuring that no one from the internet can send packets directly to the device. There can be both logical and physical air-gapped networks, as illustrated in Figure 2b,c, which differ in topology and in how the devices can be accessed; in the logical topology, the devices could be accessed using a VPN.

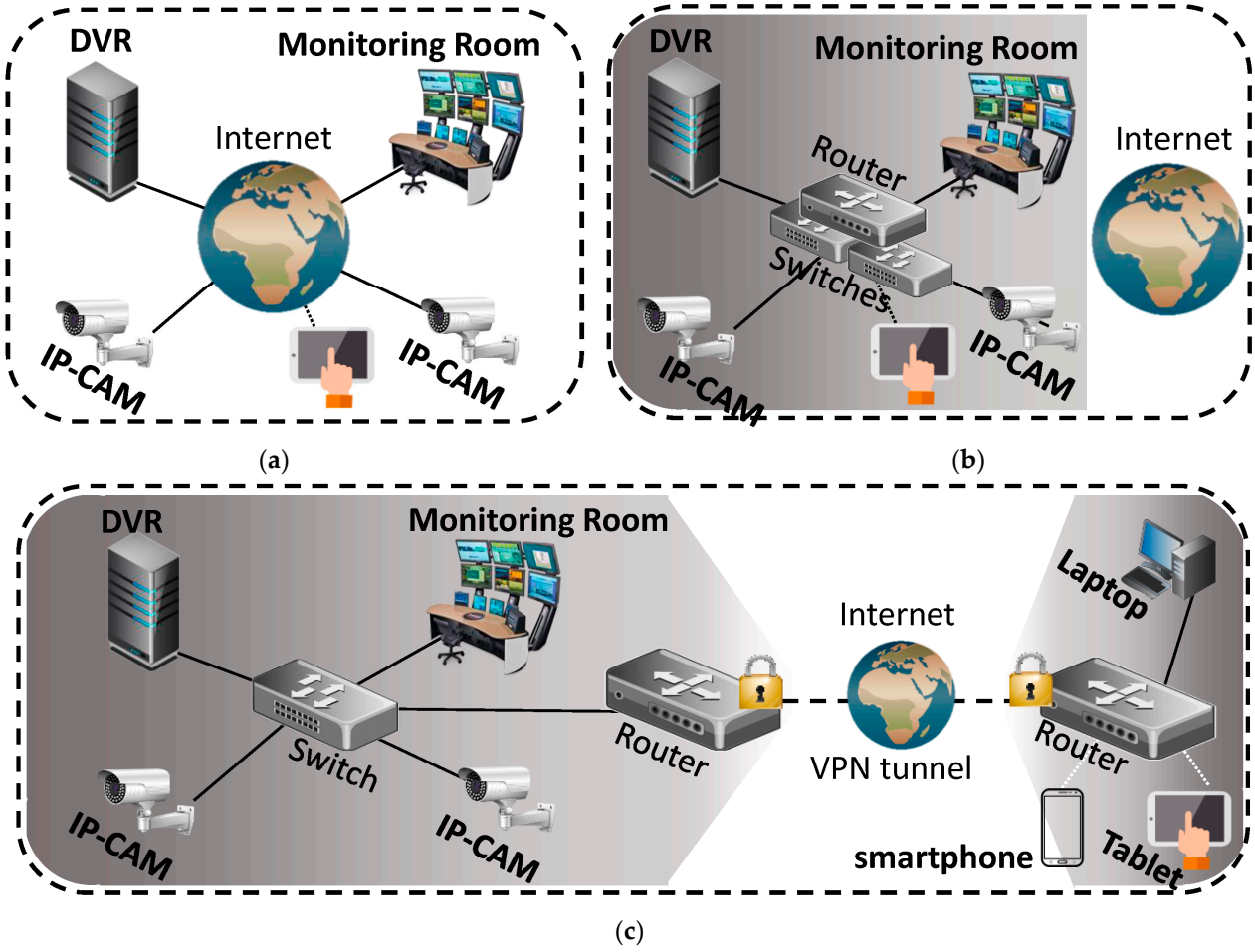


Figure 2. The topology of non-air gapped (**a**), physically air-gapped (**b**) and logically air-gapped (**c**) networks [24].

Costin, A. [21], Kalbo N. et al. [24], and Chiappetta A. et al. [25] have each examined physical air-gapped network topologies to some extent. Their analyses primarily focused on attacks related to covert channels and data exfiltration within these physically isolated networks.

Saleem D. and Carter C. in [26] explain that a logical air-gap can be configured at the network firewall using network segmentation with different Virtual LANs (VLANs). In this configuration, an air-gap represents an isolated network within a larger network, ensuring that cameras are not visible on the computer network or to external entities. This isolation is achieved by placing the cameras on a subnet physically distinct from the main network. In a logical air-gapped network, a remote connection to the DVR/NVR can still be utilized to log in and used as a bridge to observe the cameras. Neither an administrator nor a hacker can directly access the cameras without first logging into the NVR and knowing of the unique camera subnet mask for NVR. This is particularly significant because the majority of IoST exploitations occur through cameras rather than the NVR [8].

3.1. Human Error: Accidental Network Misconfiguration Vulnerability

Human errors can result in the incorrect configuration of network firewall rules, as shown in Figure 3, allowing the exploitation of specific ports/TCP/UDP communication into the air-gapped network from an untrusted or less trustworthy network. As observed by Nadir I. et al. [27], common misconfigurations often include firewall settings that allow malware to bypass security measures and exploit vulnerabilities that have existed for years in the devices, such as D-Link router vulnerabilities. Families of malware such as Hydra, Amnesia, NyaDrop and Mirai [28] can be used to get access to the router using built-in default passwords or D-Link authentication bypass exploitation. Another misconfiguration that can grant access to a network for an intruder is leaving default settings enabled on IP cameras and DVR/NVR, including not disabling unnecessary features, ports, services, pages, accounts, or privileges, using default accounts and their passwords, and revealing error handling messages to unathorised users.

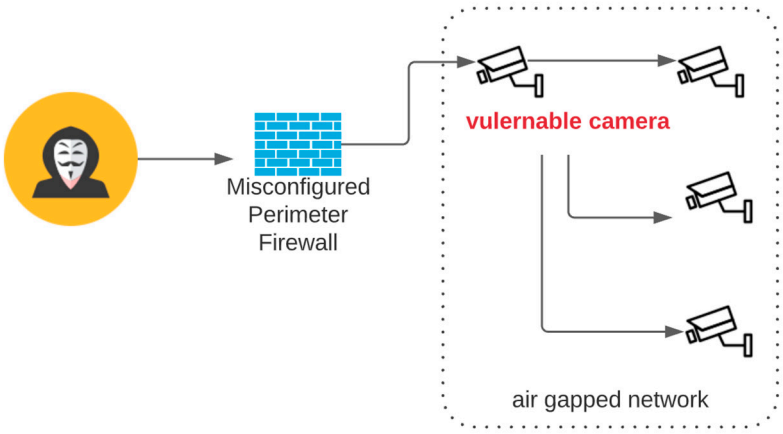


Figure 3. Exploitation diagram for network misconfiguration in a logically air-gapped network.

With the development of the network virtualization concept, a new type of attack has emerged. Kubernetes, a well-known container orchestrator, can play various roles in the IoST system, ranging from web servers to analytical centers. Older versions of Kubernetes have a flaw that allows the bypassing of authentication for both Kubelet and API access. To find a way to access the Kubernetes and configuration files, the attacker can use Shodan search for open ports Kubelet (10250) and its API server (6443), or can try to access the API server using path host:port/apis/apiextensions.k8s.io, which lists the API endpoints, as shown in Figure 4.

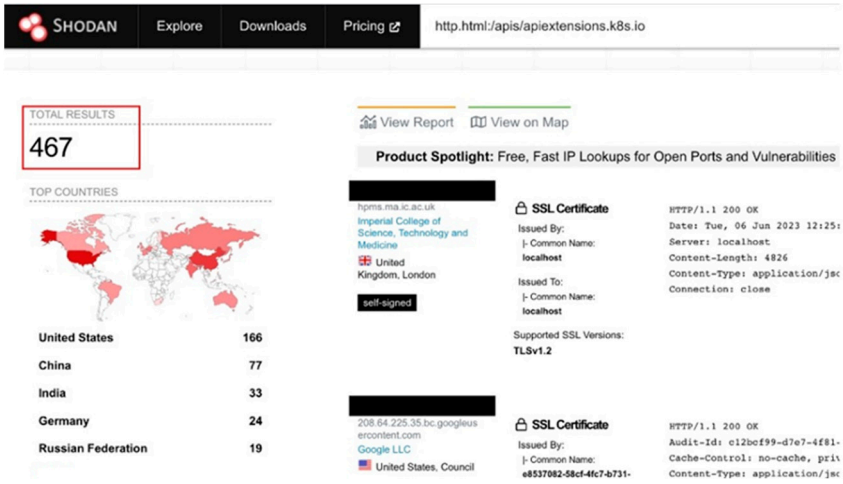


Figure 4. Results of search for open API server ports with possible unauthenticated access.

The impact-associated network configuration vulnerabilities could potentially grant an external attacker access to the more secure internal network entity, which is the main target of the attack.

Use case: The misconfiguration of the camera exposed the video stream that was supposed to be hidden from public view to internet users at a U.S. airport. According to the law, all cameras at U.S. airports must be part of an air-gapped network; however, in the case of Yellowstone Regional Airport, one of their cameras had guest access enabled and was discoverable by the general public through Google (Figure 5).

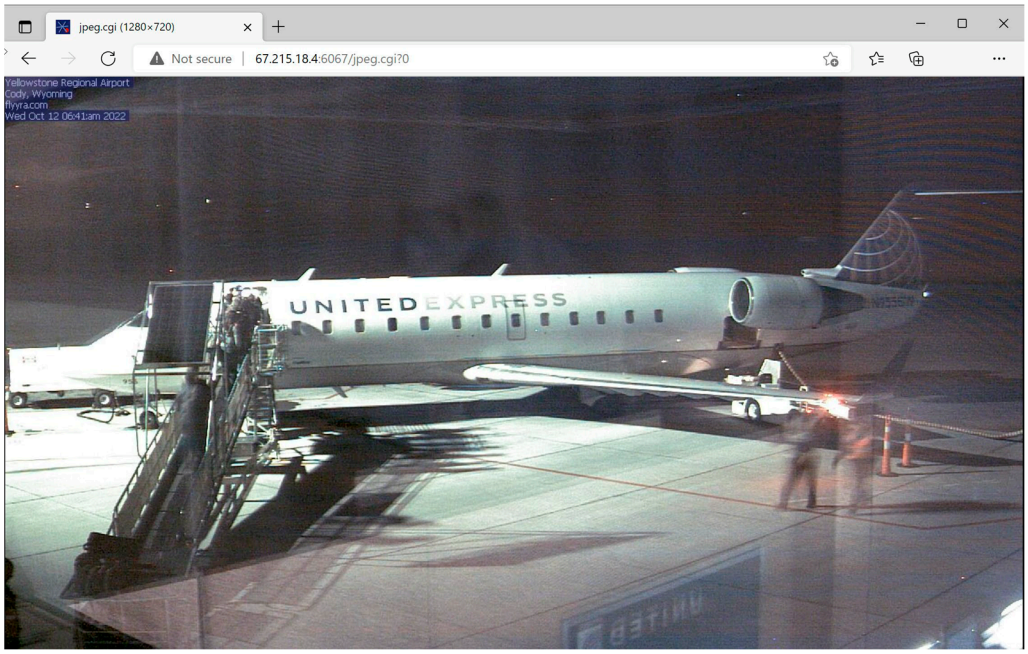


Figure 5. Use case of Yellowstone regional airport, human error in network misconfiguration.

Security measures: To mitigate misconfiguration vulnerabilities in air-gapped networks, network administrators should follow a set of best practices for securing these environments, as outlined in [26]. While many of the security measures detailed in [26] involve cryptographic techniques such as encryption protocols, message authentication digests, and certificates, some of the test cases presented in this report can be employed to identify network or device misconfigurations. Tests T1 and T2 from [26] can be particularly helpful in detecting suspicious activity related to man-in-the-middle and eavesdropping attacks. These tests examine TLS connections, TCP/UDP ports, and data intercepted during interception attempts. Nadir I. et al. [27], Manske A. [29] and Striegel M. et al. [30] also emphasized the importance of security measures, especially during initial system setup. The authors in [28] developed a dynamic sandbox for the analysis of IoT malware that exploits the misconfigured settings; the sandbox can capture network and system call traces, as well as configuration file changes. Additionally, Ref. [31] presents a telnet honeypot architecture designed to capture IoT malware, with a specific focus on Telnet access to IoT devices and network nodes. Manske A. [29] discovered several severe vulnerabilities during IP camera testing, including an open telnet port, default credentials, and logical errors in start scripts that prevented firmware updates without manual modification. One solution proposed was to enable the start script to use a relative path instead of an absolute one for executing programs. For virtualized environments, there are several measures outlined in [32] to protect nodes from unauthorized access. These measures include modifying the kubelet.conf configuration file to disallow anonymous authentication, using authorization modes like "Webhook", and refraining from exposing ports such as 10250 or any other port associated with Kubernetes to the internet.

3.2. Evil Twin Exploitation Technique

As our focus is air-gapped networks, one of the ways to attack an isolated network is through **vulnerable** employees or rogue staff, for instance, a malicious Wi-Fi dongle IoT device with the same SSID as a valid corporate Wi-Fi SSID is attached by the attacker. To penetrate the air-gapped network and gain access to the camera's video feeds, the attacker copies the entire network and sniffs the username, password, and other pertinent information, as shown on Figure 6. According to the guides that can be easily found on the internet and different IT forums, the steps for this attack include (1) sniffing the packets in and around the network using the airodump-ng command; (2) identifying the Wi-Fi network that you want to clone; (3) setting up the evil twin access point (AP) using the airbase-ng command with the same SSID name as the legitimate one; (4) setting up a DHCP server to allocate the IP address and network submask for rogue access point and for clients and resolve DNS requests; (5) cut down the connection to the legitimate AP using the command aireplay-ng --deauth 0, which will send an infinite number of disassociate packets to the legitimate AP. A user with significantly greater access rights to the video system equipment or firewall unintentionally connects to the evil Wi-Fi that the attacker has broadcasted. At this point, all traffic is going through the evil twin, which is capturing sensitive information. A more significant **impact** can occur if an external attacker gains access to the target organization's network through the further exploitation of a vulnerable camera. This could lead to a chain reaction of security breaches, including infecting additional computers within the network and gaining unauthorized access to sensitive and confidential data.

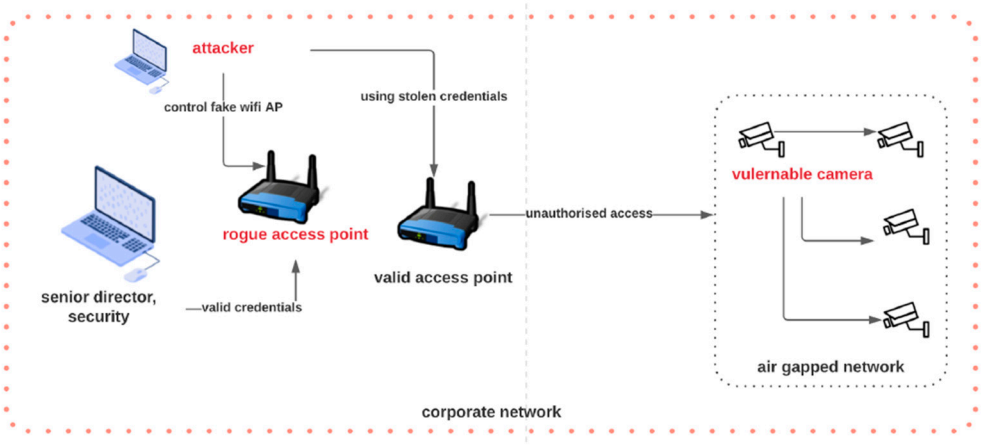


Figure 6. Exploitation diagram for the evil twin exploitation technique in a logically air-gapped network.

Use case: In 2020, an Interior IG IT team used an evil twin to deploy a fake access point with the same name as a true access point, and then recorded the credentials of all users attempting to log on. In this way, Wi-Fi networks of four departments were hacked [33].

Security measures: One of the innovative measures in the discovery of evil twin exploitation, as analyzed by Striegel M. et al. [30], involves using augmented reality to detect changes in network topology. However, this measure is often more for educational purposes than effective prevention. In practice, the primary defense against such attacks must come from the system administrator. Simpler mechanisms for mitigating this type of vulnerability, but which are still vulnerable to misconfiguration, include network segmentation and the use of authentication methods to restrict connections to rogue access points without proper digital certificates. Current methods for detecting evil twin attacks rely on various types of device information, such as MAC addresses or SSID names [34,35], signal strength indicators (RSSIs) [36,37] and network traffic analysis, including TCP/IP header inspection [38], monitoring changes in Simple Network Management Protocol (SNMP) MIBs like tcpActiveOpens, tcpPassiveOpens, and tcpAttemptFails, and the use of access

control lists [39]. Murugesan K. et al. [40] pointed out that evil twin access points can enable an attacker to conduct further attacks, such as man-in-the-middle, flooding the network with useless data, denial of service, and service disruption. The authors emphasize the use of 802.1X-based authentication, which applies an extensible authentication protocol and leverages digital certificates for authentication and Video Server validation. To strengthen authentication, the blockchain mechanism can be used instead of digital certificates [41–43]. Such a method was proposed in [43] for use in IoT networks deployed in 5G cellular networks, where sink and beacon nodes use the blockchain Proof of Authority (PoA) mechanism to ensure trust between nodes and the non-repudiation of both the service provider and the client, but it can also be applied to air-gapped VSS networks.

3.3. Supply Chain Exploitation Technique

The attacker can use third party suppliers to inject an attack into isolated networks. One of these techniques is known as supply chain exploitation. In this method, the attacker takes advantage of a **vulnerability** to compromise a patch update in the cloud instance of the camera software supplier, responsible for preparing or building the latest version of camera firmware. Similar attacks have been seen in the case of corporate firewall software, such as the SolarWinds incident. The attacker's goal is to replace legitimate patches with malware-infected ones. These infected patches are then installed directly from the cloud into local devices through middleware deployment services, which could include the corporate file server, as shown in Figure 7. Another type of supply chain exploitation technique is **Rouge Maintenance**. In this scenario, a compromised CCTV installer, supplier, or Annual Maintenance Contract (AMC) provider becomes involved. When a camera is sent to the service center for hardware repair and subsequently returned to the company premises after the repair, it may be reinstalled with malware, or firmware vulnerable to malware. This type of attack leverages trust in the maintenance and repair process to compromise the device.

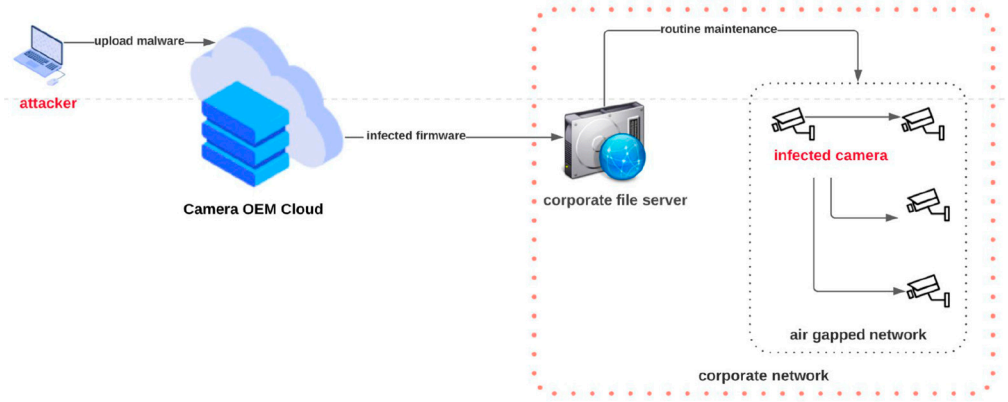


Figure 7. Exploitation diagram for supply chain exploitation technique in a logically air-gapped network.

Impact: With further exploitation of the vulnerable camera, an external attacker may potentially gain access to a more secure internal network of the intended target, infect other systems, and access confidential data. Biondi P. et al. [44] addressed the **potential risk of cloud-connected IP cameras** that gather a lot of data, which are subsequently sent to cloud storage servers. As a result, IP cameras analyze data to such an extent that it is crucial to evaluate security from the perspective of users' privacy. In IFSEC Global's Video Surveillance 2022 Report [45], the backdoors created by manufactures, including an improper patching process, were deemed to cause the most risk to VSS system customers, at 25%, while 73% of security end-users and consultants said they were worried about the vulnerability of their surveillance systems to cyberattacks.

Security measures: Liranzo and Hayajneh [46] highlighted the challenges surrounding the timely resolution of vulnerabilities in IoT devices. They point out that manufacturers typically have a window of 45 to 90 days to address a vulnerability after it is reported by researchers. Some manufacturers release a patch for their products before the vulnerability is publicly disclosed, but unfortunately, this proactive approach is not the norm. A significant challenge arises because, even if a patch is ready, it does not necessarily guarantee that the underlying issue has been fully resolved. Furthermore, disseminating information about a vulnerability and its patch can be challenging, because many **IP cameras rebrand the original product under generic names.** However, suppose the camera owners are fortunate enough to have a patch for their device. In that case, they will need to know the precise model of the device, visit the manufacturer's website, download the firmware, log into the IP camera, and upload the most recent firmware with the patch, which comes with a warning that it might render their device inoperable. Respondents said that cyber security was the shared responsibility of the whole supply chain, from manufacturers through to integrators and end-users. To effectively combat the "insider threat", due diligence is paramount for all parties involved. Manufacturers, integrators/installers, and end-users must establish trust and maintain open channels of communication [47].

Use cases: Many video surveillance cameras come from foreign countries and are manufactured by unknown companies. They might have embedded malware, backdoor access accidently included by the manufacture, or have a link to a malicious site and be set up to communicate with that site. This happened to Sony cameras purchased from Amazon and sold by a reputable seller that had an iframe in the management panel linking to a malicious host name that distributed malware [48]. Manufactures often have published factory default camera passwords that are not changed when the IP camera is installed, leaving video surveillance cameras wide open to hackers. Notable incidents include the attacks on video surveillance cameras managed by Verkada, which exposed 150,000 security cameras in Tesla factories, jails, and more [7]. Additionally, attacks on IoT devices, including industrial control systems and audio/video streaming devices, were used to create a massive botnet known as Russian RSOCKS [49]. Interestingly, both of these attacks employed a similar supply chain exploitation technique. In the former case, the attackers found admin credentials published on a third party public server, while in the latter case, default usernames and passwords were utilized to gain access to devices, effectively converting them into bots.

3.4. Cyber Kill Chain Exploitation Technique

According to Cooper M. [50], a kill chain is a military concept that describes an attack's key phases, which include Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control (C2) and Actions on objectives. Haseeb, Mansoori and Welch [51] modified the existing Cyber Kill Chain (CKC) model, and included IoT-specific attacks and steps taken by attackers in the exploitation of IoT devices. This model is called IoT Kill Chain (IoTKC); it includes nine phases compared to the seven phases in the CKC model: Discovering the IoT device, Entering the IoT device, Getting device information, Preparing the device, Downloading the package, Preparing the package, Installing the package, Removing traces, and Performing actions. However, this model has not been widely adopted by the research community.

In this type of exploitation technique, an attacker hacks a system connected to a network, which indirectly connects to the air-gapped network, as shown in Figure 8. This is a sophisticated type of attack that includes several underlaying attacks, including social engineering and injecting the malware; therefore, the **use case steps** could be the following:

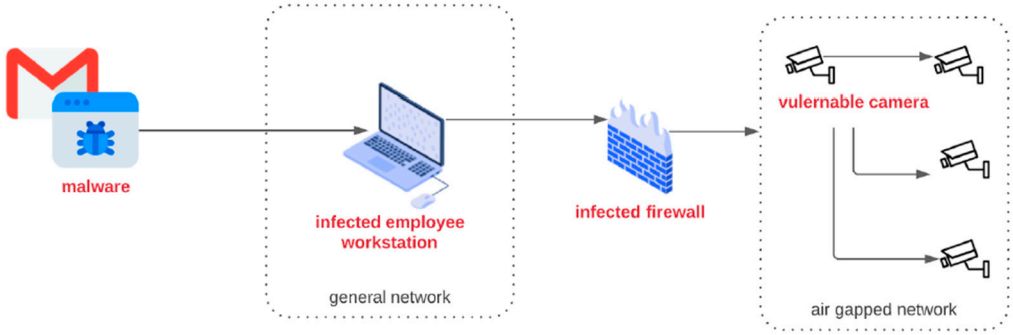


Figure 8. Exploitation diagram for Cyber Kill Chain exploitation technique in a logically air-gapped network.

1. An employee with a **vulnerable** workstation connected to the isolated network opens an email attachment containing malware;
2. The malware contains dual zero-days that exploit the nearby Cisco firewalls, open up certain ports in the firewall, and add rules to allow transparent connectivity between the infected workstation and the air-gapped VSS network;
3. It then uses the infected firewall as a bot to infiltrate the VSS network and exploits a particular vulnerability in the camera. It then uploads malware that transmits video feeds every few minutes to a remote IP that the attacker controls.

Impact: Same as Section 3.3.

Security measures: Mohsin and Anwar [52] agreed with [50] on the Mirai use case that to kill the kill chain, it needs to be split into seven phases, namely: **reconnaissance, weaponize, delivery, exploit, install, command and control and actions on objectives**. Each step is addressed separately with the relevant, appropriate defense measures. Figure 9 illustrates an example of controls applied to the industrial company with complex network infrastructure that includes servers, client's PCs, network devices and IoT components such as card readers, selling touch screens, HVAC and connected sensors, using the ontology-driven framework proposed in [52]. The framework identified the vulnerable assets and controls, and prioritized them according to the efficacy to cost (EtoC) ratio. The kill chain in the figure is divided into four phases: delivery, exploitation, installation, and action. Each phase features specific security measures aimed at mitigating potential attacks. The different colors represent various Advanced Persistent Threat (APT) attacks used for testing. Notably, many APT attacks employ social engineering tactics, using email or infected USB sticks for delivery. Consequently, we observe that filtering emails and blocking USB ports are two of the most prioritized security measures during the delivery phase.

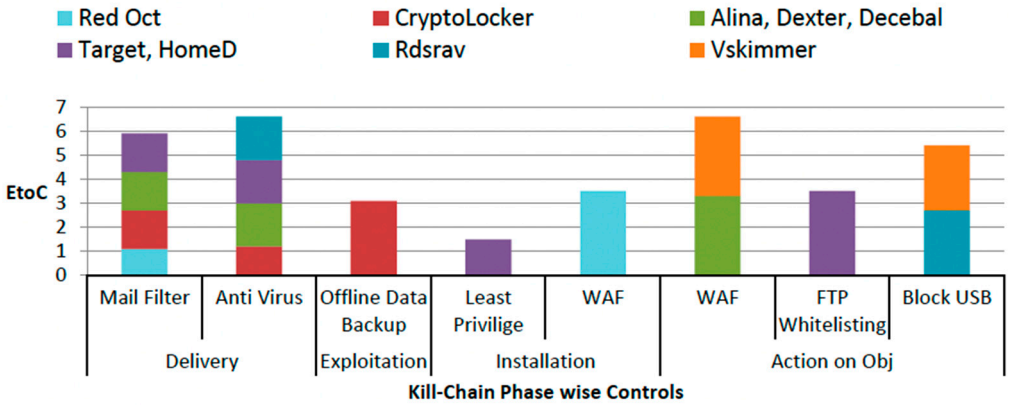


Figure 9. Framework for identifying the security measures in Cyber Kill Chain attacks.

To detect intruder actions, unauthorised access, unusual patterns in video camera feeds such as frozen images or camera shutdowns, DoS attacks and many others attacks from the

cyber kill chain, machine learning (ML) techniques can be used, which are considered the most advanced and promising methods in detection. The research studies on using ML for detecting attacks in IoT in general are summarized in [53].

3.5. In-Built Backdoor Exploitation Technique

This type of attack primarily occurs through the installation of backdoors [54], where an intentionally concealed administrative access user, known only to the Original Equipment Manufacturer (OEM), is referred to as a "backdoor user". Such a user is unknown to the organization being attacked, since neither the product manual nor the factory settings provide any reference to it. However, in their analysis of IoT firmware vulnerabilities, Nadir I. et al. [27] clarified that OEMs and ODMs (Original Design Manufacturers) frequently give little consideration to firmware or IoST device security. Even when they do address security concerns, some ODM code provided to an OEM may contain vulnerabilities or security flaws, leading to the introduction of a single bug across thousands of commercial devices. To streamline development and expedite time-to-market, some OEMs resort to utilizing outdated (and free) code bases and libraries. This practice frequently results in the deployment of specific vulnerable frameworks, leading to the creation of insecure firmware. Moreover, on the extreme side, Wang X. et al. [55] highlighted that distribution vendors simply acquire the device from an OEM, rebrand them, and then offer them for sale on the market.

Impact: With the further exploitation of the vulnerable camera, the outside attacker may find access to a more secure internal network of the intended target, infect other systems, and access confidential data, as shown in Figure 10.

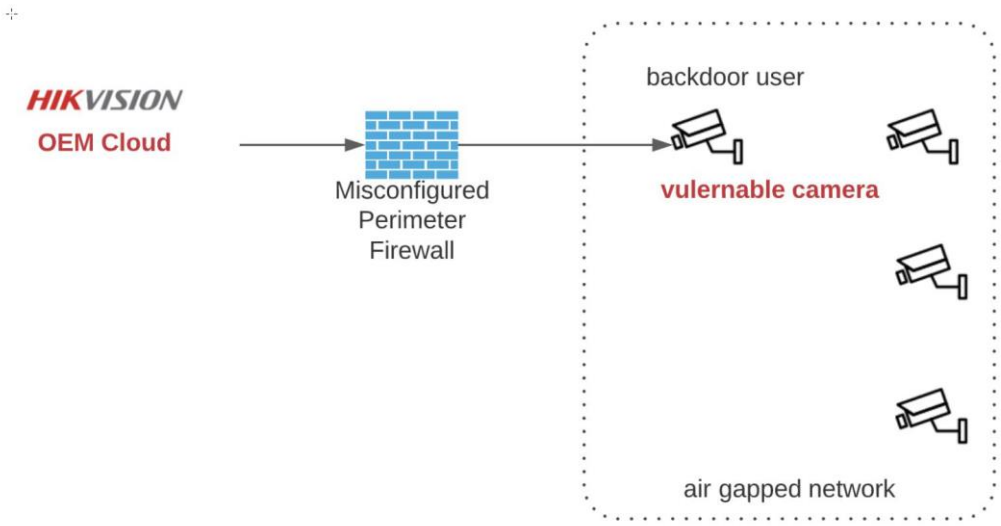


Figure 10. Diagram of the in-built exploitation technique in a logically air-gapped network.

Use case: The majority of Hikvision IP cameras remain vulnerable to the access control bypass due to a backdoor in firmware that allows the unauthenticated impersonation of any configured user account disclosed in 2017 [56], and to unauthenticated remote code execution, disclosed in 2021 [57]. One of the API handlers in this camera allows authentication with the logic of "if this exists, then skip all authentication", which developers had used for debugging and forgot to remove. This allows authorization by username only, with the password ignored. Another backdoor allows one to gain root access via SSH and bypass the camera admin web portal authentication.

Security measure: As a preventive measure, Big Brother Watch [58] in the UK, a civil liberties and privacy campaigning organization, recommends a ban on the sale and operation of Hikvision and Dahua surveillance equipment in the UK. They further urge the UK government to commission a nationwide independent examination of the scope, capabilities, moral implications, and effects of contemporary CCTV in the UK.

Shaukat et al. [59] discussed a more pragmatic reactive measure, emphasizing the importance of correctly identifying the OEM as a crucial factor in running the most relevant test cases when assessing vulnerabilities. In contrast, a traditional vulnerability assessment approach might label a Honeywell camera as a "Honeywell" camera and only run test cases relevant to Honeywell firmware. However, a modern-era tool would recognize a Honeywell camera and run Dahua test cases on it because many models of Honeywell cameras have Dahua firmware signatures underneath. This comprehensive approach provides a more accurate assessment of the security posture of the scanned IoST devices.

3.6. Infrared LED Exploitation Technique

Although infrared light is invisible to humans, various types of cameras can effectively capture it through optical means. Guri and Bykhovsky's [13] analysis revealed that an attacker could communicate over the air gap from tens to hundreds of meters using IR and surveillance cameras (Impact). The following study by Gong et al. [60] showed that IR can be used to conduct a so called Invisible Infrared Shadow Attack (IRSA) and reconstruct a picture of the environment where the camera is placed from deformed IR shadows. The IR lighting, typically used for legitimate purposes, can unwittingly serve as a vulnerability that attackers exploit to infiltrate and exfiltrate data to and from indoor air-gapped security cameras. In an exfiltration scenario, malware gains access to a surveillance camera connected to the local network, utilizing it to control the IR LEDs. These LEDs generate covert IR signals, as illustrated in Figure 11, which are subsequently modulated, encoded, and transmitted as binary data. An intruder with a line of sight to the security camera at a distance can intercept these IR signals and decode the binary data. Conversely, in an infiltration scenario, a remote attacker deploys IR LEDs to produce covert IR signals. These signals are then picked up by the surveillance camera and intercepted by malware operating within the network.

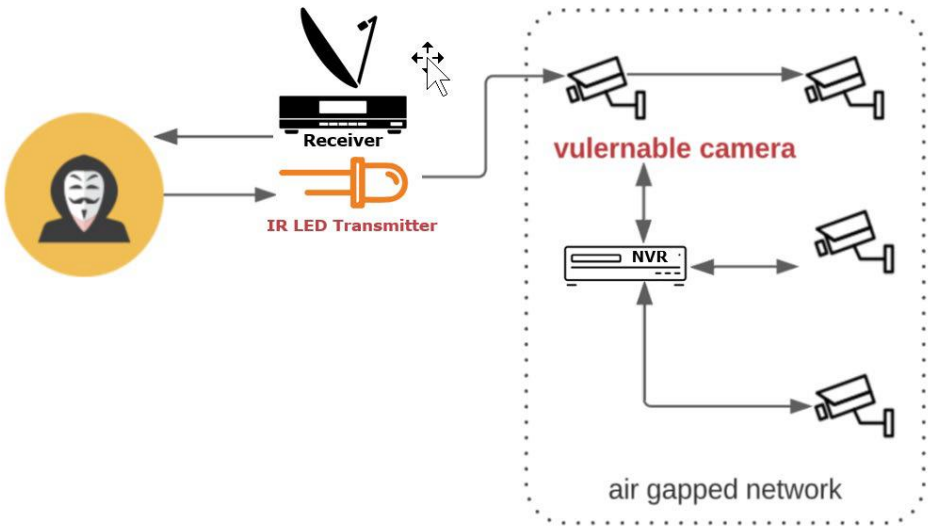


Figure 11. Diagram of the IR LED exploitation technique in a physically air-gapped network.

Security Measures: The organization may place surveillance cameras in restricted zones that are optically inaccessible to attackers (window shielding). In case of ISRA, a straightforward method to prevent this type of attack is ensuring that all windows are covered with thick curtains, so that no IR shadow can be projected towards the curtain surface.

Additional strategies to enhance security against ISRA and similar attacks include:

1. Disabling IR Control—Deactivating the IR control on surveillance cameras can mitigate the risk of attackers using IR signals for malicious purposes;

2. Signal Jamming with Unique Patterns—Introducing random and unique light patterns that are known only to the legitimate camera can disrupt unauthorized IR signal interception attempts, making it challenging for attackers to decode or misuse the signals.
3. Incorporating IR Filters—Installing IR filters on surveillance cameras can help filter out unwanted IR light and shadow, reducing the potential for exploitation.

By implementing these preventive measures, organizations can significantly enhance their security posture and reduce the vulnerability of surveillance systems to IR-based attacks.

4. Discussion

We present several exploitation techniques of IoST vulnerabilities, summarized in Table 2. The findings were analyzed in terms of five defined categories that were used for this review study: network topology, vulnerability, exploitation technique, impact, and security measure.

Table 2. A summary overview of exploitation techniques of IoST vulnerabilities in air-gapped networks.

#	Network Topology	Vulnerability	Exploitation Technique	Impact (Use Case)	Security Measure
1	Physical Air-Gap	Misconfiguration [61,62]	Social Engineering [24,52,63,64]	The leak of sensitive video feeds	Periodic change of passwords, physical access control [29], malware analysis sandbox [28], Telnet honeypots [31], protecting configuration files [32]
2		Serial Bus Ports [26,30]	Evil Twin [30,33]	Access to sensitive data	Network segmentation, authentication via digital certificates [41–43], authentication via blockchain [43], network changes monitoring using AR [30], AP setting [34–37] and network behavior [39]
3		IR-LED Sensor [13,60]	Infrared LED [13,60]	Data infiltration and exfiltration, objects identification, privacy leakage	Signal jamming [13], window tinting [60]
4	Logical Air-Gap	Open WAF Port [13,26,29,41,55]	Cyber Kill Chain [42,56]	Crippled 1Tbps of data	WAF-Hardening, NIDS, detecting of behavior changes using ML [53], risk assessment using ontology-based method [52]
5		OEM Firmware [13,27,48,50]	Inbuilt Backdoor [7,13,24,59,65]	Corporate espionage	Next-Gen Scanner, anomaly-based AV
6		Infected patch [13,24,29]	Supply Chain [13,24,66]	Access to video archive, footage	Anomaly-based AV, IDS/IPS, web application firewalls (WAF), ensuring trust relations [47]

As can be seen from the results, the most popular technique for compromising physically air-gapped networks is social engineering. The human factor remains the most attractive for hackers as the weakest link to expose an IP camera's security. In addition to forcing the people into changing the password, another way to help strengthen defenses for individuals is to establish procedures and protocols for accessing critical data points, including ensuring multi-level authentication or blockchain-based authentication between IoST components.

In the logical air-gapped IoST network, the most popular technique is implanting a backdoor through vulnerable software, untrusted libraries or insecure firmware. This

can be mitigated by applying dynamic and static source code analysis in conjunction with security scanning and risk assessment [67] before the product, such as an IP camera, goes onto the market.

In Table 3, we present a vulnerability assessment using the Common Vulnerability Scoring System (CVSS), used for measuring the severity of vulnerability [68]. The CVSS score is commonly used to provide a point of comparison between vulnerabilities, and to prioritize the remediation of vulnerabilities. We have used the base set of metrics proposed in CVSS, which is comprised of exploitability and impact.

Table 3. Severity and risk assessment of IoST vulnerabilities in air-gapped networks.

Vulnerability	Attack vector	Complex.	Privil. Req.	User Interact	Impact	Severity score	Likelihood	Risk
Misconfiguration, including configuration errors, weak or missing security controls	Remote	High	Low	None	Medium	High (7.0)	High	High
Insider human vulnerability that results in evil twin attack	Local	High	None	Required	Medium	Medium (6.5)	Low	Low
Access point misconfiguration that results in evil twin attack	Local	Low	None	None	Medium	High (8.0)	Low	Medium
Infrared LED communication	Local	High	None	None	Low	Low (3.1)	Low	Low
Vulnerabilities that result in Cyber Kill Chain	Remote	High	High	Required	High	Medium (6.7)	Medium	High
OEM firmware vulnerabilities	Remote	Low	Low	None	High	High (8.3)	Medium	High
Weak security controls of the supply chain	Remote	Low	Low	None	High	High (8.3)	High	High

The exploitability metric shows how much effort is required from the attacker to exploit the vulnerability and to launch the attack. We will consider models assessing the exploitability risk through such vulnerability attributes as *Attack Vector*, *Attack Complexity*, *Privileges Required* and *User Interaction*.

Attack Vectors vary on the level of access to the target system or network in order to exploit the vulnerability (i.e., inside or outside of company's network). A vulnerability in a local access vector requires a physical presence, i.e., access to the physical port of the equipment. A vulnerability in an outside access vector can be exploited remotely [69]. The vulnerabilities that can be exploited remotely over a network are generally considered more severe.

Attack Complexity is based on the skill and knowledge required by the attacker to perform the attack. Vulnerabilities that require lower skills result in higher exploitability risk.

The Privileges Required factor determines the level of privileges an attacker needs to successfully exploit the vulnerability. If the attacker requires elevated privileges or administrative access, the exploitability score will be lower. However, if the vulnerability can be exploited with low privileges or without any user interaction, the score will be higher.

The User Interaction factor assesses whether user interaction is required for the vulnerability to be exploited. If the vulnerability can be exploited without user interaction, such as through automated means or remote attacks, the exploitability score will be higher. On the other hand, if user interaction is necessary, the score will be lower.

The impact level depends on the amount of damage done due to a loss of confidentiality, integrity, and availability. A vulnerability that affects all CIA components translates to the highest exploitability risk.

For simplicity, we map CVSS scores obtained using the CVSS v.3 calculator, which is measured in a range of 0 to 10, where 0 indicates no severity and 10 indicates the highest severity.

Table 3 is also extended with two columns that are outside the scope of CVSS vulnerability assessment and identify the likelihood of the vulnerability being presented and the risk of having certain vulnerability exploited in the system, where Risk is a product of Likelihood and Impact, and Likelihood is a product of Threat and Vulnerabilities ((Risk = (Threat × Vulnerabilities) × Impact) [67].

Research questions regarding security measures and best practices for securing IoST devices and infrastructure were also answered during this study, and the key findings of the study can be found in Table 4.

Table 4. A summary of the key findings from the research questions RQ1–RQ3.

Research Questions	Key Findings
RQ1: What are the exploitation techniques for IoST vulnerabilities in air-gapped networks?	See Table 2
RQ2: What best practices prevent IoST exploitations in air-gapped networks?	(1) Changing the default camera password is the paramount rule in camera security. (2) Keep the cameras invisible by plugging them through the NVR's POE (Power over Ethernet) ports to use the physically isolated NVR's subnet from the network computer in the air gap. (3) If the air gap cannot be fully physically separated from the external network, in the case of corporations and large businesses, then a Virtual LAN is required to subnet the cameras. (4) Ensure that linked peripherals are kept to the bare minimum. External gear like printers, USB drives, and CD drives should not be connected to the system since hackers might use them as entry points. It is possible to restrict USB ports, which are frequently the most likely source of infection, using inexpensive devices like USB port locks. (5) Encrypt the air-gapped systems' data, given their sensitivity. This does not stop data breaches or assaults but can prevent attackers from using the information if exploitation is successful.
RQ3: What security measures can keep up with new IoST threats without breaking the air gap?	(1) Legacy anti-virus programs frequently require signature updates for newly identified threats. Some allegedly next-generation technologies heavily rely on their capacity to transmit telemetry to the cloud and process it remotely. Both will fail if the principal security posture does not require internet connectivity. Anon-device behavioral AI that is capable of autonomously detecting, guarding against, and resolving malware, ransomware, and device-based attacks from peripherals like USB drives is the solution to these issues, using the behavioral analysis of anomalies rather than signatures or file identities, detecting both well-known and new malware without the need for internet connectivity. (2) Install next-generation assessment tools that can identify underlying OEM beneath a white-labeled IP camera, thus addressing a significant gap in preventing attacks against IP cameras.

IoST devices in air-gapped networks are undoubtedly more secure because fewer attack vectors are available. However, this inherent isolation does not equate to absolute security or immunity from threats. It is a common misconception to assume that because these devices are not directly connected to external networks, they are inherently safe. To ensure the robustness of air-gapped infrastructure, organizations employing IoST devices must remain vigilant and proactive in addressing security concerns. This entails identifying and patching any potential security holes or vulnerabilities that may exist within these isolated networks.

With exploitation techniques evolving all the time, it is very important to know the correct security posture of each IoST device. This can be achieved by implementing the recommended best security practices and measures, as outlined in this review. Regular

audits, updates, and adherence to security protocols are key to maintaining the integrity and resilience of air-gapped systems in the face of evolving exploitation techniques.

5. Conclusions

In this work, we have performed a systematic literature review on exploitation techniques in air-gapped video surveillance systems. We found that there are many research studies on attacks and protection mechanisms in non-air gapped video surveillance systems, but significantly fewer studies on isolated air-gapped topologies. Further, the analysis of the selected papers shows that Internet of Surveillance Things exploitation techniques are mostly focused on exploiting the human factor and performing social engineering attacks, and on utilizing the firmware backdoors left by the manufactures. Less commonly utilized methods involve compromising intermediate network equipment within logical air-gapped networks and harnessing the infrared (IR) signals emitted by IP cameras. Additionally, we observed that there is no one-size-fits-all security control capable of mitigating all identified vulnerabilities and attacks. Each type of vulnerability necessitates a tailored approach and a specific set of security measures.

Based on our literature review, we have concluded that employing ontology-driven techniques, which automatically match countermeasures with potential security threats in IoST, is effective in enhancing the security of video surveillance systems. This approach is both time-efficient and offers fundamental solutions for securing IoT configurations through rule-based ontology reasoning.

Moving forward, we anticipate that manufacturers of IoST devices and companies providing video surveillance services will increasingly prioritize security, particularly for air-gapped networks. These networks are often deployed for critical services and infrastructures, making security and privacy paramount concerns.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Surveillance Camera Code of Practice. Biometrics and Surveillance Camera Commissioner, UK Government Guide. 22 November 2021. Available online: https://www.gov.uk/government/publications/update-to-surveillance-camera-code (accessed on 1 January 2023).
2. Lloret, J.; Garcia, M.; Bri, D.; Sendra, S. A Wireless Sensor Network Deployment for Rural and Forest Fire Detection and Verification. *Sensors* **2009**, *9*, 8722–8747. [CrossRef] [PubMed]
3. Lyu, Z.; Luo, J. A Surveillance Video Real-Time Object Detection System Based on Edge-Cloud Cooperation in Airport Apron. *Appl. Sci.* **2022**, *12*, 10128. [CrossRef]
4. Dašić, P.; Dašić, J.; Crvenkovic, B. Improving Patient Safety in Hospitals through Usage of Cloud Supported Video Surveillance. *Open Access Maced. J. Med. Sci.* **2017**, *5*, 101–106. [CrossRef] [PubMed]
5. Antonakakis, M.; April, T.; Bailey, M.; Bernhard, M.; Bursztein, E.; Cochran, J.; Durumeric, Z.; Halderman, J.A. Understanding the Mirai botnet. In Proceedings of the 26th USENIX Conference on Security Symposium (SEC'17), Vancouver, BC, Canada, 16–18 August 2017.
6. Stapel, G.; Klepfish, N. Record 25.3 Billion Request Multiplexing DDoS Attack Mitigated by Imperva. Imperva Blog. 2022. Available online: https://www.imperva.com/blog/record-25-3-billion-request-multiplexing-attack-mitigated-by-imperva/ (accessed on 1 January 2023).
7. Gartenberg, C. Security Startup Verkada Hack Exposes 150,000 Security Cameras in Tesla Factories, Jails, and More. Available online: https://www.theverge.com/2021/3/9/22322122/verkada-hack-150000-security-cameras-tesla-factory-cloudflare-jails-hospitals (accessed on 1 January 2023).
8. Best Practices for Preventing IoT Security Camera Hacks. Available online: https://www.getscw.com/support/preventing-iot-hacks (accessed on 1 January 2023).
9. Lakshmanan, R. New BotenaGo Malware Variant Targeting Lilin Security Camera DVR Devices. Available online: https://thehackernews.com/2022/04/new-botenago-malware-variant-targeting.html (accessed on 1 January 2023).

10. Merit LILIN Network Product Vulnerability Notification. Technical Support, Taipei. Available online: https://www.meritlilin.com/assets/uploads/support/file/M00163-EN.pdf (accessed on 1 January 2023).
11. Lakshmanan, R. Bugs in Wyze Cams Could Let Attackers Takeover Devices and Access Video Feeds. Available online: https://thehackernews.com/2022/03/bugs-in-wyze-cams-could-let-attackers.html (accessed on 1 January 2023).
12. Kuzminykh, I.; Ghita, B.; Such, J.M. The Challenges with Internet of Things Security for Business. In *Internet of Things, Smart Spaces, and Next Generation Networks and Systems. NEW2AN/ruSMART*; Koucheryavy, Y., Balandin, S., Andreev, S., Eds.; LNCS; Springer: Cham, Switzerland, 2021; Volume 13158, pp. 46–58. [CrossRef]
13. Guri, M.; Bykhovsky, D. aIR-Jumper: Covert air-gap exfiltration/infiltration via security cameras & infrared (IR). *Comput. Secur.* **2019**, *82*, 15–29. [CrossRef]
14. Thakar, D. Survey on IP Camera Hacking and Mitigation. *Multidiscip. Int. Res. J. Gujarat Technol. Univ.* **2020**, *2*, 28–33.
15. Vennam, P.; T. C., P.; B. M., T.; Kim, Y.-G.; B. N., P.K. Attacks and Preventive Measures on Video Surveillance Systems: A Review. *Appl. Sci.* **2021**, *11*, 5571. [CrossRef]
16. Chamasemani, F.F.; Affendey, L.S. Systematic Review and Classification on Video Surveillance Systems. *Int. J. Inf. Technol. Comput. Sci.* **2013**, *7*, 87–102. [CrossRef]
17. Wohlin, C. Guidelines for Snowballing in systematic literature studies and a replication in software engineering. In Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering (EASE), London, UK, 13–14 May 2014; pp. 1–10.
18. Petersen, K.; Vakkalanka, S.; Kuzniarz, L. Guidelines for conducting systematic mapping studies in software engineering: An update. *Inf. Softw. Technol.* **2015**, *64*, 1–18.
19. Petticrew, M.; Roberts, H. *Systematic Reviews in the Social Sciences: A Practical Guide*; Blackwell Publishing: Hoboken, NJ, USA, 2006. [CrossRef]
20. Literature Review—Finding the Resources, Research Guides. City University of Hong Kong. Available online: https://libguides.library.cityu.edu.hk/litreview/evaluating-sources (accessed on 1 January 2023).
21. Costin, A. Security of CCTV and Video Surveillance Systems: Threats, Vulnerabilities, Attacks, and Mitigations. In Proceedings of the 6th International Workshop on Trustworthy Embedded Devices (TrustED '16), Vienna, Austria, 28 October 2016; pp. 45–54. [CrossRef]
22. Papp, D.; Ma, Z.; Buttyan, L. Embedded systems security: Threats, vulnerabilities, and attack taxonomy. In Proceedings of the 2015 13th Annual Conference on Privacy, Security and Trust (PST), Izmir, Turkey, 21–23 July 2015; pp. 145–152. [CrossRef]
23. Gillis, A. What Is an Air Gap? Available online: https://www.techtarget.com/whatis/definition/air-gapping (accessed on 1 January 2023).
24. Kalbo, N.; Mirsky, Y.; Shabtai, A.; Elovici, Y. The Security of IP-Based Video Surveillance Systems. *Sensors* **2020**, *20*, 4806. [CrossRef]
25. Chiappetta, A.; Cuozzo, G. Critical infrastructure protection: Beyond the hybrid port and airport firmware security cybersecurity applications on transport. In Proceedings of the 2017 5th IEEE International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS), Naples, Italy, 26–28 June 2017; pp. 206–211. [CrossRef]
26. Saleem, D.; Carter, C. Certification procedures for data and communications security of distributed energy resources. In *Technical Report NREL/TP-5R00-73628*; National Renewable Energy Lab. (NREL): Golden, CO, USA, 2019.
27. Nadir, I.; Mahmood, H.; Asadullah, G. A taxonomy of IoT firmware security and principal firmware analysis techniques. *Int. J. Crit. Infrastruct. Prot.* **2022**, *38*, 100552. [CrossRef]
28. Costin, A.; Zaddach, J. IoT malware: Comprehensive survey, analysis framework and case studies. In Proceedings of the Black Hat Conference, Las Vegas, NV, USA, 9 August 2018.
29. Manske, A. *Conducting a Vulnerability Assessment of an IP Camera*; Degree Project in Computer Science and Engineering; KTH Royal Institute of Technology: Stockholm, Sweden, 2019.
30. Striegel, M.; Erasmus, J.; Jain, P. Evaluating Augmented Reality for Wireless Network Security Education. In Proceedings of the 2021 IEEE Frontiers in Education Conference (FIE), Lincoln, NE, USA, 13–16 October 2021; pp. 1–9. [CrossRef]
31. Pa Pa, Y.M.; Suzuki, S.; Yoshioka, K.; Matsumoto, T.; Rossow, C. IoTPOT: Analysing the rise of IoT compromises. In Proceedings of the 9th USENIX Conference on Offensive Technologies (WOOT), Washington, DC, USA, 10–11 August 2015.
32. Alcantara, A. Attacks via Misconfiguration on Kubernetes Orchestrators. Sidechannel Blog. 14 September 2022. Available online: https://sidechannel.blog/en/attacks-via-misconfiguration-on-kubernetes-orchestrators/ (accessed on 1 January 2023).
33. Interior IG Team Used Evil Twins And $200 Tech to Hack Department Wi-Fi Networks. Available online: https://www.nextgov.com/cybersecurity/2020/09/interior-ig-team-used-evil-twins-and-200-tech-hack-department-wi-fi-networks/168521 (accessed on 1 January 2023).
34. Sriram, V.S.; Sahoo, G.; Agrawal, K.K. Detecting and eliminating Rogue Access Points in IEEE-802.11 WLAN—A multi-agent sourcing Methodology. In Proceedings of the 2010 IEEE 2nd International Advance Computing Conference (IACC), Patiala, India, 19–20 February 2010; pp. 256–260. [CrossRef]
35. Agyemang, J.O.; Kponyo, J.J.; Klogo, G.S.; Boateng, J.O. Lightweight rogue access point detection algorithm for WiFi-enabled Internet of Things(IoT) devices. *Internet Things* **2020**, *11*, 100200. [CrossRef]
36. Tang, Z.; Zhao, Y.; Yang, L.; Qi, S.; Fang, D.; Chen, X.; Gong, X.; Wang, Z. Exploiting Wireless Received Signal Strength Indicators to Detect Evil-Twin Attacks in Smart Homes. *Mob. Inf. Syst.* **2017**, *2017*, 1248578. [CrossRef]

37. Kim, T.; Park, H.; Jung, H.; Lee, H. Online Detection of Fake Access Points Using Received Signal Strengths. In Proceedings of the IEEE 75th Vehicular Technology Conf. (VTC Spring), Yokohama, Japan, 6–9 May 2012; pp. 1–5. [CrossRef]
38. Hsu, F.-H.; Wu, M.-H.; Hwang, Y.-L.; Lee, C.-H.; Wang, C.-S.; Chang, T.-C. WPFD: Active User-Side Detection of Evil Twins. *Appl. Sci.* **2022**, *12*, 8088. [CrossRef]
39. Gayathri, R.; Usharani, S.; Mahdal, M.; Vezhavendhan, R.; Vincent, R.; Rajesh, M.; Elangovan, M. Detection and Mitigation of IoT-Based Attacks Using SNMP and Moving Target Defense Techniques. *Sensors* **2023**, *23*, 1708. [CrossRef]
40. Murugesan, K.; Thangadorai, K.K.; Muralidhara, V.N. PoEx: Proof of Existence for Evil Twin Attack Prevention in Wi-Fi Personal Networks. In Proceedings of the 8th International Conference on Future Internet of Things and Cloud (FiCloud), Rome, Italy, 23–25 August 2021; pp. 92–98. [CrossRef]
41. Khan, P.W.; Byun, Y.-C.; Park, N. A Data Verification System for CCTV Surveillance Cameras Using Blockchain Technology in Smart Cities. *Electronics* **2020**, *9*, 484. [CrossRef]
42. Asif, M.; Aziz, Z.; Bin Ahmad, M.; Khalid, A.; Waris, H.A.; Gilani, A. Blockchain-Based Authentication and Trust Management Mechanism for Smart Cities. *Sensors* **2022**, *22*, 2604. [CrossRef]
43. Abubaker, Z.; Javaid, N.; Almogren, A.; Akbar, M.; Zuair, M.; Ben-Othman, J. Blockchained service provisioning and malicious node detection via federated learning in scalable Internet of Sensor Things networks. *Comput. Netw.* **2022**, *204*, 108691. [CrossRef]
44. Biondi, P.; Bognanni, S.; Bella, G. Vulnerability Assessment and Penetration Testing on IP cameras. In Proceedings of the 8th International Conference on Internet of Things: Systems, Management and Security (IOTSMS), Gandia, Spain, 6–9 December 2021; pp. 1–8. [CrossRef]
45. Video Surveillance 2022 Report. IFSEC Global. Available online: https://www.ifsecglobal.com/downloads-resources/the-video-surveillance-report-2022/ (accessed on 1 January 2023).
46. Liranzo, J.; Hayajneh, T. Security and privacy issues affecting cloud-based IP camera. In Proceedings of the IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), New York, NY, USA, 19–21 October 2017; pp. 458–465. [CrossRef]
47. Trends, Opportunities and Challenges in Video Surveillance. IFSEC Global. Available online: https://www.ifsecglobal.com/wp-content/uploads/2021/06/IFSEC-Global-eBook-Video-Surveillance-2021-FINAL.pdf (accessed on 1 January 2023).
48. Osborne, C. Surveillance Cameras Sold on Amazon Infected with Malware. Available online: https://www.zdnet.com/article/amazon-surveillance-cameras-infected-with-malware/ (accessed on 1 January 2023).
49. Russian Botnet Disrupted in International Cyber Operation. Press Release from 16 June 2022, US Attorney's Office. Available online: https://www.justice.gov/usao-sdca/pr/russian-botnet-disrupted-international-cyber-operation (accessed on 1 January 2023).
50. Cooper, M. Using The Cybersecurity Kill Chain for Attack and Defence. *ITNow* **2022**, *64*, 38–41. [CrossRef]
51. Haseeb, J.; Mansoori, M.; Welch, I. Measurement Study of IoT-Based Attacks Using IoT Kill Chain. In Proceedings of the IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Guangzhou, China, 29 December 2020–1 January 2021; pp. 557–567. [CrossRef]
52. Mohsin, M.; Anwar, Z. Where to Kill the Cyber Kill-Chain: An Ontology-Driven Framework for IoT Security Analytics. In Proceedings of the International Conference on Frontiers of Information Technology (FIT), Islamabad, Pakistan, 19–21 December 2016; pp. 23–28. [CrossRef]
53. Abbas, G.; Mehmood, A.; Carsten, M.; Epiphaniou, G.; Lloret, J. Safety, Security and Privacy in Machine Learning Based Internet of Things. *J. Sens. Actuator Netw.* **2022**, *11*, 38. [CrossRef]
54. Ling, Z.; Liu, K.; Xu, Y.; Jin, Y.; Fu, X. An End-to-End View of IoT Security and Privacy. In Proceedings of the GLOBECOM 2017—2017 IEEE Global Communications Conference, Singapore, 4–8 December 2017; pp. 1–7. [CrossRef]
55. Wang, X.; Sun, Y.; Nanda, S.; Wang, X.F. Looking from the Mirror: Evaluating IoT Device Security through Mobile Companion Apps. In Proceedings of the 28th USENIX Security Symposium, Santa Clara, CA, USA, 14–16 August 2019; pp. 1151–1167.
56. IPVM Team. 2022. Hikvision Backdoor Exploit. IPVM. Available online: https://ipvm.com/reports/hik-exploit (accessed on 1 January 2023).
57. Unauthenticated Remote Code Execution (RCE) Vulnerability in Hikvision IP Camera/NVR Firmware (CVE-2021-36260). Vulnerability Disclosure Report. Available online: https://watchfulip.github.io/2021/09/18/Hikvision-IP-Camera-Unauthenticated-RCE.html (accessed on 1 January 2023).
58. Carlo, S.; Hurfurt, J. Who's Watching You? The Dominance of Chinese State-Owned CCTV in the UK. Available online: https://bigbrotherwatch.org.uk/wp-content/uploads/2022/02/Whos-Watching-You_The-dominance-of-Chinese-state-owned-CCTV-in-the-UK.pdf (accessed on 1 January 2023).
59. Shaukat, K.; Alam, T.M.; Hameed, I.A.; Khan, W.A.; Abbas, N.; Luo, S. A Review on Security Challenges in Internet of Things (IoT). In Proceedings of the 26th International Conference on Automation and Computing (ICAC), Portsmouth, UK, 2–4 September 2021; pp. 1–6. [CrossRef]
60. Gong, J.; Zhang, X.; Ren, J.; Zhang, Y. The Invisible Shadow: How Security Cameras Leak Private Activities. In Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (CCS '21), New York, NY, USA, 15–19 November 2021; ACM: New York, NY, USA, 2021; pp. 2780–2793. [CrossRef]

61. Singh, V.; Kharat, V. A Proposed System for Security in Campuses using IoT Platform: A Case Study of a Women's University. In Proceedings of the International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC), Mysore, India, 8–9 September 2017; pp. 305–310. [CrossRef]
62. Loy, K. Implementing Cybersecurity Best Practices in Five Steps. *SIA Insights* **2018**, *6*, 40–47. Available online: https://www.securityindustry.org/wp-content/uploads/2018/09/SIA-Technology-Insights-Fall-2018.pdf (accessed on 1 January 2023).
63. Rana, P. CCTV Cameras Hacking and Prevention Techniques. *Int. J. Sci. Res.* **2021**, *10*, 307–310. Available online: https://www.ijsr.net/get_abstract.php?paper_id=SR21507134453 (accessed on 1 January 2023).
64. Gunduz, M.Z.; Das, R. Cyber-security on smart grid: Threats and potential solutions. *Comput. Netw.* **2020**, *169*, 107094. [CrossRef]
65. Masood, A.; Masood, A. A Taxonomy of Insider Threat in isolated (air-gapped) Computer Networks. In Proceedings of the International Bhurban Conference on Applied Sciences and Technologies (IBCAST), Islamabad, Pakistan, 12–16 January 2021; pp. 678–685. [CrossRef]
66. Neshenko, N.; Bou-Harb, E.; Crichigno, J.; Kaddoum, G.; Ghani, N. Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2702–2733. [CrossRef]
67. Kuzminykh, I.; Ghita, B.; Sokolov, V.; Bakhshi, T. Information Security Risk Assessment. *Encyclopedia* **2021**, *1*, 602–617. [CrossRef]
68. FIRST. Common Vulnerability Scoring System Version 3.1: Specification Document. Available online: https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf (accessed on 1 January 2023).
69. Roumani, Y.; Nwankpa, J. Examining Exploitability Risk of Vulnerabilities: A Hazard Model. *Commun. Assoc. Inf. Syst.* **2020**, *46*. [CrossRef]