Security in Video Surveillance Systems

UP879148, UP813609, UP828826, UP864163, UP903492

Abstract - This paper will detail the security in modern commercial video surveillance systems; in particular to vulnerabilities onset from less than ideal generic firmware. With the increasing use of smart video surveillance systems in homes and small businesses, the robustness of said systems has as of late come under scrutiny. Many of the issues found to pertain to poor firmware. Therefore, the goal of this paper is to critically evaluate methods in which to protect modern video surveillance systems and propose new methods and/or practices that will further increase the security of both existing and new systems. Such methods include the implementation of network intrusion detection systems (NIDS), robust operating protocols and manufacturer firmware support. A method proposed in this paper is a method of our design and outlines a risk assessment framework enabling manufacturers to continually assess the security of their systems while also presenting potential solutions to vulnerabilities that pose the most risk to the overall system security.

Index Terms - B.4.3.h Wireless systems, C.2 Communication/Networking and Information Technology, C.2.0.f Network-level security and protection, C.2.5 Local-Area Networks

1.0 Introduction

A significant increase in internet usage and advancements in networking technology over the last decade has resulted in the increased affordability, accessibility and reliability of video security systems. Many homeowners and small businesses now rely on such systems to secure properties and monitor sensitive business areas.

Our research problem is to find common vulnerabilities in consumer-grade video security systems and propose solutions to mitigate them.

Systems of this nature will only become more vulnerable as internet technologies develop. For instance, 5G enabled networks are becoming ever more prevalent since their adoption privately as well as their adoption publicly through government initiatives. Qian Clara Li et al. suggests a global increase in mobile network traffic by a factor of 1000 over the next decade implying that the world would be more connected but all the while, increasing the likelihood of cyberattacks [1].

In this paper, we conduct a literature review on the types of common vulnerabilities and their corresponding exploits against these devices and evaluate possible countermeasures, and then we finally propose an enhanced solution by using a risk assessment that suits our problem best, providing results where applicable.

2.0 Related work or literature review

2.1 Background

A video surveillance system in and of itself is a tool used to improve the security of certain aspects of an institution, in particular to the physical security of assets, persons and dependent systems. However, preventing network-related cyber attacks in video surveillance systems is paramount because these systems inherently pertain to informational, cyber and physical security hazards and pose a significant risk if proper control measures are not implemented during a system's development life cycle.

2.2 Current Vulnerabilities

2.2.1 Man in the middle

Previously, threat actors have been able to manipulate the video streams of IP-cameras allowing them to inject edited footage or freeze a frame in addition to traditional methods of attack such as a denial of service (DoS) attacks [3].

2.2.2 Data exfiltration

Costin's [3] survey has shown that the aforementioned systems could be used to send and receive data through covert side-channels (for example, acoustic, thermal, optical, and electromagnetic). This vulnerability can be exploited in air-gapped systems to leak sensitive information such as passwords and documents and could be used to allow an advanced adversary to maintain a foothold in the network as a means to repeat an attack.

2.2.3 Insecure software

Many different vendors of IP CCTV cameras employ the use of simple generic firmware. The firmware lends itself to vulnerabilities (some made publicly known and listed as a CVE) given its simple architecture and apparent lack of development using modern network security practices.
If adequate due diligence in the form of encrypting source code and digital signing is not conducted throughout the deployment stage of the device firmware development, an attacker can reverse engineer the firmware to search for vulnerabilities in the code itself. An attacker could potentially upload a form of malware to the camera.[2] Of the two methods mentioned above, the practice of code encryption does not necessarily lie within the best interest of the manufacturer as obfuscating code decreases the likelihood of investigation by well-intended security researchers[10].
Attackers using arbitrary code execution (ACE) vulnerabilities found within the software can execute any command on the device running it. From this, it follows that the attacker can perform privilege escalation and perform other malicious tasks. ACE vulnerabilities have been found in IP cameras, DVRs, and routers. [4] According to cvedetails, ACE vulnerabilities are the most prevalent CVEs found [12].

2.2.4 Supply chain

During the manufacturing process, there's a risk that threat actors can insert a rootkit or hardware-based spyware into the firmware. This is called a supply-chain attack and it is very unlikely to occur but it could allow an advanced threat actor (such as an advanced persistent threat) to have complete control over the device as well as the local network. [4]

2.2.5 Protocol-based

WEP, WPA2 and WPA3 are security certification programs developed by the WiFi alliance. WPA2 is the most common certification currently in use, being used in 68.42% of polled networks [6], and was developed in 2004. While WPA2 is a set-up from the original WEP, being 16 years old it still has significant vulnerabilities. For example, WPA2 can be exploited by a method known as KRACK. [5] KRACK is where an intruder performs a replay attack exploiting the vulnerabilities of resending message 3 in the four-way handshake used by WPA2. This allows the attacker to manipulate the packets being sent. [6]

2.2.6 Botnet

With the bandwidth allowed to these sorts of devices, IP cameras can not only pose a vulnerability to the network they are active on and the business that owns them but also to the wider internet as well, an example of a situation like this that had come to pass would be the Mirai malware attack in 2016, a malware that specifically targeted IoT devices due to there weak security with a lot of them still relying on default passwords making them easy to infect [2]. This example attack managed to disrupt a significant portion of the internet at the time by attacking the DNS provider DYN with a DDOS attack using over 100,000 infected devices. This attack goes to highlight the massive impact that the array of security flaws in these devices can have.

2.3 Current solutions

2.3.1 Man in the middle

Denial of service attacks are mitigated or prevented by several solutions in current networks. A common and effective solution in use in most networks is a firewall. A firewall aims to channel the network traffic into distinct openings protected by the firewall. [7] This allows unauthorized packets to be denied access to the network. However, *Kalbo et al.* [4] also suggest that one of the best countermeasures could be the deployment of a network intrusion detection system (NIDS) which sniff packets in real-time and checks for certain types of packet signatures and uses heuristics to detect when an adversary has evaded the firewall. Network intrusion detection systems are not trivial to evade by the average threat actor.

2.3.2 Data Exfiltration

When it comes to Data Exfiltration methods, the best current practice is to implement all other current solutions effectively, this is due to the many options or avenues of attack that these methods pose from but by shoring up other defences in turn these methods are shored up against as well [3].

2.3.3 Insecure Software

Although a large number of IP cameras rely on generic software bringing with it aforementioned vulnerabilities [2], some vendors such as Hikvision and Samsung do allow and support firmware updates to address these vulnerabilities for existing systems.

Unfortunately, this level of support from manufacturers is the exception and not the rule. Hikvison and Samsung are good examples of how a well-implemented support framework for data-sensitive devices can negate firmware vulnerabilities.

2.3.4 Supply Chain

According to the research on PCB supply chain implants by Mehta et al, many companies outsource their manufacturing because it reduces costs however it can also introduce vulnerabilities in the supply chain. After all, untrusted third-parties can insert hardware trojans which are hidden as common components and can easily evade common testing methods such as in-circuit-testing, JTAG (Joint Test Action Group) and functional testing because these testing methods only work on testable modules in the PCB and are not originally designed to spot these types of attacks. The paper suggests that an automated visual inspection method is needed which can inspect the surface and subsurface layers of the PCB to find anomalies compared to a ‘golden sample’, i.e. a PCB that is made by trusted parties thus secure from hardware trojans. This paper only covers detection via testing however the authors also suggest that more research is needed to find suitable countermeasures and methods to prevent supply chain attacks from being effective [16].

2.3.5 Protocol Based

Released in 2018, WPA3 aims to build upon the problems in WPA2. WPA3 uses a 128-bit encryption key in-home networks making it more secure over the previous WPA2 which uses AES. [13] WPA3 also replaces pre-shared key (PSK) exchange with simultaneous authentication of equals, a more secure method of initial key exchange. Additionally, WPA3 also fixes some of the vulnerabilities present in WPA2 such as preventing the retransmission of Message 3 which prevents the KRACK exploit from being performed on a WPA3 router. [5] However, WPA3 is currently not widely used, being new, it is only being used on a very low amount of WiFi networks and consequently, in a lot of networks, the vulnerabilities that WPA3 aims to address are still exposed. Most wireless security systems which are mass-produced contain firmware which is only compatible with WPA2 or older meaning significant vulnerabilities are widespread still. The overall landscape of Wi-Fi enabled devices should see a gradual adoption of the WPA3 standard since on July 1st 2020 any device certified by the Wi-Fi alliance must support WPA3 [11].

3.0 Proposed Risk Assessment

In this section, we will present a risk assessment based on the previously identified vulnerabilities and solutions. We will quantify each vulnerability on how likely it is to be exploited and the potential risk to the network if it is exploited. We will be using a scale of 1 to 10, with 1 being low risk and 10 being the highest risk.

Please see the risk assessment table in the appendix.

4.0 Evaluation of Solution

Our methodology for evaluating our proposed solutions is to reference experiments from other sources and then evaluate them based on how well they solve the solution and how much we can learn from them. The reason behind this approach is due to the nature of some of these vulnerabilities we do not have the resources to set up a full experiment ourselves and collect data. For example, a supply chain attack.

4.1 Man in the middle

A study by Michael R. Lyu and Lorrien K. Y. Lau focuses on evaluating the effectiveness of Firewalls in networks. The study evaluates the performance and security of different types of firewalls. The study focuses on the fact that it is necessary to achieve a balance between security and performance when choosing a firewall.

Figure 1 from the study assesses firewalls with security policies of 1 to 7 with higher being more secure. Their study shows the effectiveness of firewalls in preventing MitM attacks and other vulnerabilities.

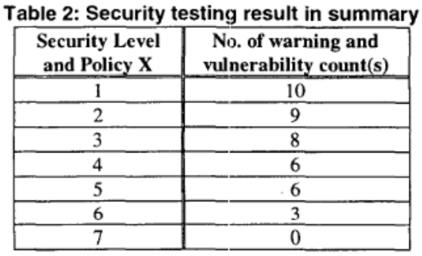


Table 2: Security testing result in summary

Security Level and Policy X	No. of warning and vulnerability count(s)
1	10
2	9
3	8
4	6
5	6
6	3
7	0

Figure 1 (Michael R. Lyu and Lorrien K. Y. Lau)

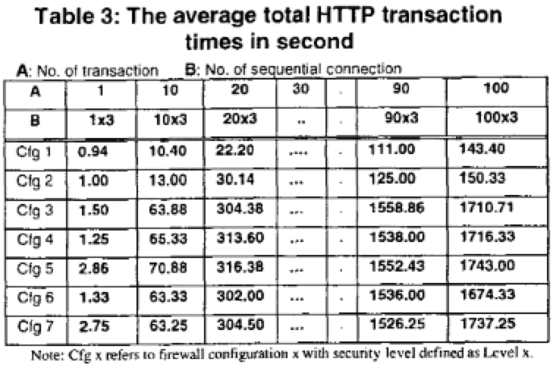


Table 3: The average total HTTP transaction times in second

A: No. of transaction B: No. of sequential connection

A	1	10	20	30	.	90	100
B	1x3	10x3	20x3	..	.	90x3	100x3
Cfg 1	0.94	10.40	22.20	....	.	111.00	143.40
Cfg 2	1.00	13.00	30.14	...	.	125.00	150.33
Cfg 3	1.50	63.88	304.38	...	.	1558.86	1710.71
Cfg 4	1.25	65.33	313.60	...	.	1538.00	1716.33
Cfg 5	2.86	70.88	316.38	...	.	1552.43	1743.00
Cfg 6	1.33	63.33	302.00	...	.	1536.00	1674.33
Cfg 7	2.75	63.25	304.50	...	.	1526.25	1737.25

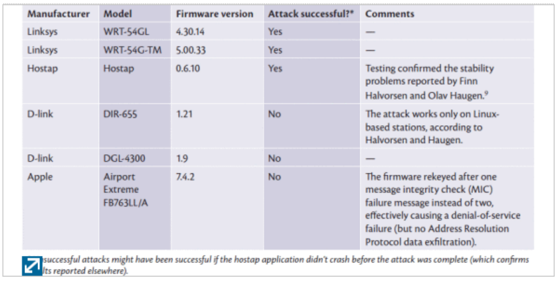
Note: Cfg x refers to firewall configuration x with security level defined as Level x.

Figure 2 (Michael R. Lyu and Lorrien K. Y. Lau)

It is also proven that generally, as the protection increases, performance decreases. See **Figure 2** which shows the direct transaction time increase with each security policy level. [18]

4.2 Insecure software

Furthermore, studies conducted by Frederick T. Sheldon et al showcased the impact of insecure software being used in wireless networks.



Manufacturer	Model	Firmware version	Attack successful?*	Comments
Linksys	WRT-54GL	4.30.14	Yes	—
Linksys	WRT-54G-TM	5.00.33	Yes	—
Hostap	Hostap	0.6.10	Yes	Testing confirmed the stability problems reported by Finn Halvorsen and Olav Haugen.[9]
D-link	DIR-655	1.21	No	The attack works only on Linux-based stations, according to Halvorsen and Haugen.
D-link	DGL-4300	1.9	No	—
Apple	Airport Extreme FB763LL/A	7.4.2	No	The firmware rekeyed after one message integrity check (MIC) failure message instead of two, effectively causing a denial-of-service failure (but no Address Resolution Protocol data exfiltration).

*successful attacks might have been successful if the hostap application didn't crash before the attack was complete (which confirms lts reported elsewhere).

Figure 3 (Frederick T. Sheldon et al)

The study investigates ways in which network security can be improved and how attacks can be mitigated. It is shown in **Figure 3**, which assesses different firmware versions against an attack, that firmware is crucial for network security. **Figure 3** shows that up to date firmware can be the difference between a successful attack or a failed one. The study concludes that having the most up to date firmware possible is the best approach to mitigate vulnerabilities. [19]

4.3 Supply chain

A study by Chad W Autry and L. Michelle Bobbit proposes a framework for supply chain security. In their study, they collected data from 31 supply chains to assess the security vulnerabilities of them and suggest improvements. In their proposed framework they suggest a series of technological improvements to increase the security of the supply chain. For example, based on data collected from supply managers, it suggests that electronically scanning shipments and using real-time technology to mitigate tampering. [17]

4.4 Protocol based

A study conducted by Cristian L. Leca in Romania conducted an assessment of over 100,000 networks assessing their security protocols.
The study showed that over 4 years, the city of Bucharest had an increase in more modern security certifications, up to 86% using WPA2 which is in line with the world standard. The results of the study showed that attacks on wireless networks decreased over the 4 years as a direct result of the adoption of more up to date protocols. [14]

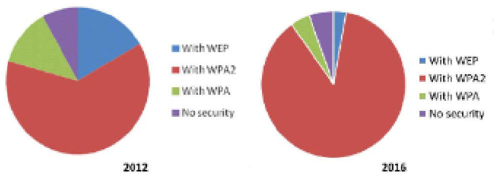


Figure 4 (Cristian L. Leca) Shows protocol usage in Bucharest from 2012 to 2016

5.0 Conclusion

In conclusion, with the world being ever more interconnected the importance of good security measures in video surveillance systems is as high as ever. With issues that can be present anywhere from default software and hardware to issues based on outdated protocols, it is highly recommended that users, as well as manufacturers, should enact the solutions outlined in our risk assessment to mitigate the corresponding risks. Though due to limitations in hardware availability and our ability to meet in person because of the COVID-19 pandemic we had to rely on previous data and results of other researchers which have been proven effective in their techniques for shoring up defences of the user in the fight against malicious attacks. However, with technology rapidly evolving new risks will always develop and users must keep themselves informed of new threats and ways to mitigate them to ensure network security in the future. Additionally, the vulnerabilities mentioned here is not a complete list of all potential threats, just the ones viewed as most significant.

Risk Assessment Table

Threat	Vulnerability	Asset and Consequence	Risk	Solution
MiTM	**High - 8/10** Loss of confidentiality and integrity during data transmission	Eavesdropping and tampering of confidential information	**High - 9/10** A third-party can view or change the original content before it's received by the intended recipient.	Secure firewall + Network Intrusion Detection System (NIDS)
Data exfiltration	**Moderate - 5/10** Devices can be used to exfiltrate confidential data from within a private network using covert side-channels.	Confidential data such as personal user data, organisation secrets (e.g national, organisation, etc)	**High - 8/10** An attacker could gain a foothold within the network from the outside even if it's not connected to the internet.	Apply All other solutions / remove air gap from system to secure.
Insecure software	**Moderate - 6/10** When the firmware on the device is inherently flawed it can be exploited.	The device running the software is vulnerable to exploitation.	**High - 7/10** It could allow an attacker to compromise the device and potentially other devices on the network.	Ensure the system has up to date software and preferably permits software updates. Otherwise, change systems.
Supply chain	**Low - 2/10** Advanced persistent threats can exploit vulnerable supply chains during the manufacturing of the device.	Remote control into the device which is connected to the network. Backdoor	**High - 7/10** Each device in the same batch could contain a hardware-trojan allowing advanced persistent threats (APT) full control over the device.	Automated visual inspection of the PCB; avoid outsourcing to untrusted parties
Protocol-based	**High - 9/10** Out of date protocol can leave a network open to attacks such as KRACK.	Packets can be read and/or manipulated by an intruder.	**High - 9/10** Can potentially down the network or intercept traffic and manipulate it.	Ensure hardware and software compatible with WPA3 and update to it.

References

[1] Qian Clara Li; Huaning Niu; Apostolos Tolis Papathanassiou; Geng Wu, 5G Network Capacity: Key Elements and Technologies https://ieeexplore.ieee.org/abstract/document/6730679, 31st January 2014

[2] Cusack, B., & Tian, Z. (2017). Evaluating IP Surveillance Camera Vulnerabilities. Retrieved 10 November 2020, from https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1202&context=ism

[3] Costin, A. (2016, October). Security of CCTV and video surveillance systems: Threats, vulnerabilities, attacks, and mitigations. In *Proceedings of the 6th international workshop on trustworthy embedded devices* (pp. 45-54).

[4] Kalbo, N., Mirsky, Y., Shabtai, A., & Elovici, Y. (2020). The Security of IP-Based Video Surveillance Systems. Sensors (14248220), 20(17), 4806. https://doi.org/10.3390/s20174806

[5] Christopher P. Pohlios & Thaier Hayajney, A Comprehensive Attack Flow Model and Security Analysis for Wi-Fi and WPA3, 24th September 2018, Section 2.3.2,
https://www.mdpi.com/2079-9292/7/11/284/htm

[6] Bobzilla, Arkasha, & Uhtu. (2020). *WiGLE*. https://wigle.net/stats

[7] W. A. Arbaugh, N. Shankar, Y. C. J. Wan and Kan Zhang, "Your 80211 wireless network has no clothes," in IEEE Wireless Communications, vol. 9, no. 6, pp. 44-51, Dec. 2002, DOI: 10.1109/MWC.2002.1160080.

[8] Sharif, M., Bhagavatula, S., Bauer, L., & Reiter, M. K. (2016, October). Accessorize to a Crime: Real and stealthy attacks on state-of-the-art face recognition. In *Proceedings of the 2016 ACM sigsac conference on computer and communications security* (pp. 1528-1540).

[9] D. J. Fehér and B. Sandor, "Effects of the WPA2 KRACK Attack in Real Environment," 2018 IEEE 16th International Symposium on Intelligent Systems and Informatics (SISY), Subotica, 2018, pp. 000239-000242, DOI: 10.1109/SISY.2018.8524769.

[10] Silver, 2017. Should firmware images for IoT be encrypted for security reasons?. [Blog] *Stack Overflow*, Available at <https://security.stackexchange.com/questions/168620/should-firmware-images-for-iot-be-encrypted-for-security-reasons>.

[11] CETECOM™. 2020. *Wi-Fi CERTIFIED WPA3™ Will Become Mandatory On July 1, 2020*. [online] Available at: <https://www.cetecom.com/en/news/wi-fi-certified-wpa3-will-become-mandatory-july-1-2020/> [Accessed 31 December 2020].

[12] Özkan, S. (n.d.). *Vulnerabilities by type*. cvedetails. https://www.cvedetails.com/vulnerabilities-by-types.php

[13] Kohlios CP, Hayajneh T. A Comprehensive Attack Flow Model and Security Analysis for Wi-Fi and WPA3. *Electronics*. 2018; 7(11):284.

[14] C. L. Leca, "Overview of Romania 802.11 wireless networks security," 2017 9th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Targoviste, 2017, pp. 1-4, DOI: 10.1109/ECAI.2017.8166386.

[15] Mirsky, Y., Doitshman, T., Elovici, Y., & Shabtai, A. (2018). Kitsune: an ensemble of autoencoders for online network intrusion detection. *arXiv preprint arXiv:1802.09089*.

[16] Mehta, D., Lu, H., Paradis, O. P., MS, M. A., Rahman, M. T., Iskander, Y., ... & Asadizanjani, N. (2020). The big hack explained: Detection and prevention of PCB supply chain implants. *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, *16*(4), 1-25.

[17] Autry, C. and Michelle Bobbitt, L., 2008. Supply chain security orientation: conceptual development and a proposed framework. *The International Journal of Logistics Management*, 19(1), pp.42-64.

[18] M. R. Lyu and L. K. Y. Lau, "Firewall security: policies, testing and performance evaluation," Proceedings 24th Annual International Computer Software and Applications Conference. COMPSAC2000, Taipei, Taiwan, 2000, pp. 116-121, DOI: 10.1109/CMPSAC.2000.884700.

[19] F. T. Sheldon, J. M. Weber, S. Yoo and W. D. Pan, "The Insecurity of Wireless Networks," in IEEE Security & Privacy, vol. 10, no. 4, pp. 54-61, July-Aug. 2012, DOI: 10.1109/MSP.2012.60.

Contribution Table:

UP879148	*
UP813609	*
UP828826	*
UP864163	*
UP903492	*