VULNERABILITY ANALYSIS OF IP CAMERAS USING ARP POISONING

Thomas Doughty[1], Nauman Israr[2] and Usman Adeel[3]

[1]BSc (Hons) Cyber Security and Networks, Teesside University,
Middlesbrough, UK
[2]Senior Lecturer in Networks and Communication, Teesside University,
Middlesbrough, UK
[3]Senior Lecturer in Computer Science, Teesside University, Middlesbrough, UK

ABSTRACT

Internet Protocol (IP) cameras and Internet of Things (IoT) devices are known for their vulnerabilities, and Man in the Middle attacks present a significant privacy and security concern. Because the attacks are easy to perform and highly effective, this allows attackers to steal information and disrupt access to services. We evaluate the security of six IP cameras by performing and outlining various attacks which can be used by criminals. A threat scenario is used to describe how a criminal may attack cameras before and during a burglary. Our findings show that IP cameras remain vulnerable to ARP Poisoning or Spoofing, and while some cameras use Digest Authentication to obfuscate passwords, some vendors and applications remain insecure. We suggest methods to prevent ARP Poisoning, and reiterate the need for good password policy.

KEYWORDS

Security, Camera, Internet of Things, Passwords, Sniffing, Authentication

1. INTRODUCTION

IP cameras have become ubiquitous in today's world due to their price and accessibility in comparison to CCTV. IP cameras can be found in most shops, organisations, and in many homes. But these cameras have a history of being insecure. Recent events such as the Mirai Distributed Denial of Service (DDoS) attacks in 2016 [1], have again highlighted this. The Mirai botnet allowed hackers to barrage websites with up to 1.1 Terabytes per second of traffic [2], and the hacked Internet of Things devices used in this army included IP cameras. According to Liranzo and Hayajneh [3], cameras can also allow strangers on the internet to view the inside of other people’s homes, as many IP cameras now utilise port forwarding and cloud storage to send, store and access camera footage. This privacy issue is often reported in the news [4].

In this paper we will examine the security of a sample of six Internet Protocol (IP) cameras. We perform Man in the Middle attacks (MitM), and leverage this position to perform Packet Sniffing, Denial of Service Attacks and gain unauthorised access to the camera feeds.

A MitM attack is the act of intercepting traffic from a source and forwarding it to its destination, acting as a gateway and allowing for messages to be manipulated without the knowledge of either party [5]. This is done by performing Address Resolution Protocol (ARP) Poisoning. According

Dhinaharan Nagamalai et al. (Eds) : SAI, NCO, SOFT, ICAITA, CDKP, CMC, SIGNAL - 2019
pp. 163-172, 2019. © CS & IT-CSCP 2019 DOI: 10.5121/csit.2019.90712

to Arote and Arya [6], devices map MAC addresses to IP addresses and store them in their ARP cache tables. The attacker sends ARP Reply packets to the victim and replaces the gateway address with its own, and then sends ARP Reply packets to the gateway and replaces the victim address with its own.

2. BACKGROUND

2.1. SECURITY AND TRUST FOR SURVEILLANCE CAMERAS

Boyarinov and Hunter [7] identified integrity, security and trust issues surrounding IP Cameras, and demonstrated these vulnerabilities by performing various attacks on the Reolink RLC-410WS IP camera, and their setup included an attacking host, the IP camera and a victim host. Due to this camera being ONVIF (Open Network Video Interface Forum) compliant they suggest that their findings may be relevant to a wide range of cameras which support this standard. There is a strong likelihood of this, given that the ONVIF Conformant Products page displays 11443 products from many prominent manufacturers such as Axis Corporation, Hikvision Digital Technology, Panasonic Corporation and Sony Corporation [8].

Boyarinov and Hunter performed a MitM attack using Ettercap. They were able to successfully perform ARP Poisoning to spoof the Victim Device’s IP address, allowing them to intercept packets sent by the IP camera. According to their findings they were able to obtain the cameras feed as a result of this, and this attack facilitated further exploits.

After their successful MitM attack, they further leverage their position by performing a Denial of Service attack, redirecting the camera feed and preventing the rightful recipient from obtaining the packets. While they indicate that the packets intercepted were encrypted, they were able to successfully sniff a username and password used by the Xeoma Surveillance App, as this information appeared in plain text. The most interesting attack performed was that of the Integrity Violation exploit which replaced the genuine camera feed with a fake one. By collecting a series of User Datagram Packets (UDP), they were able to create a camera loop, however the attack, whilst impressive, did have room for improvement. As they have stated, the camera packets had a limited time period, and when assembled the image included a time stamp and would flicker. If a person or object moved during this attack it would be detected by the camera, however it is not clear if this is done by the camera’s object/motion detection or if the feed would be broken by movement. Nonetheless, their Integrity Violation attack remains impressive, and could still have important implications. If the attack were performed on an old, inexpensive camera in a shop, burglars could take advantage of the brief time window before staff or authorities are alerted. They suggest that ARP Spoofing may be prevented by checking all MAC addresses on the network and suggest that other cameras may already do this. We did not observe this in our findings. One issue with this study was the small sample size used when testing for vulnerabilities. While the Reolink camera may conform to the ONVIF standard, this alone may not be enough to generalise the vulnerabilities to the wide range of vendors and products available to consumers. It should also be noted that Reolink is not officially listed as an ONVIF conformant manufacturer. A larger sample of IP cameras should be tested, which has been acknowledged by the authors.

2.2. AN IOT ANALYSIS FRAMEWORK: AN INVESTIGATION OF IOT SMART CAMERAS' VULNERABILITIES

Alharbi and Aspinall [9] proposed an analysis framework for IoT devices and used smart cameras as their main point of focus for their paper. They outlined a threat model which highlights five areas as potential attack vectors: the stream data in transit, the physical and network security of the device, the security of the hosted web interface, the security of mobile applications associated with the smart camera, and the privacy policy and agreements which users must agree to. From their threat model and analysis framework, we will be focusing on the capturing of the video stream and examining the physical and network security of the device.

Alharbi and Aspinall found that the Ring Doorbell Smart Camera was using Real-time Transport Protocol (RTP) to transmit the unencrypted video stream to users. They suggest that protocols not using encryption must be abandoned in favour of their encrypted successors, such as Secure RTP [10]. They also found that weak default passwords and password policies were also a security threat. The impact of the Mirai attack supports this, as well as the privacy concerns raised in the news which are caused by weak and unchanged default passwords. The five IP cameras used in this study as well as the strength of the analysis framework provides good results. However, the study makes no mention of the ONVIF standard which modern cameras attempt to comply with, and the study only uses one common camera vendor (Netatmo). The other cameras used in this study are less prominent when compared to manufacturers such as Hikvision. In addition to this a larger sample size of devices would enhance findings and widen the scope of the study, allowing vulnerabilities to be generalised to other IP cameras.

3. MAN IN THE MIDDLE ATTACKS

3.1. THREAT SCENARIO

The Threat Scenario involves a Threat Actor who plans to burgle a small business or home. The building is fitted with one to many IP cameras, and a user may be viewing the stream(s) periodically. We assume that the attacker has connected unlawfully to a Wireless Access Point (WAP) using the Aircrack-ng suite [11], or by finding that the access point is unsecured.

The Threat Actor is a criminal with limited knowledge of hacking tools, who wishes to break into the premises. Their intention is to steal as many valuables as possible without raising suspicion. The Threat Actor may access IP cameras to perform reconnaissance, steal information or break in at a later date. They also wish to disrupt the camera feed to avoid being identified during the burglary. While the main motivation in this scenario is money, a political motivation could also be applied.

The Target Assets include the IP Cameras (their feed, connectivity and accessibility), the layout of the building and valuables inside, the user's device used for streaming, and any personal information that could be used to identify the individuals who may work or reside in the building.

3.2. SETUP

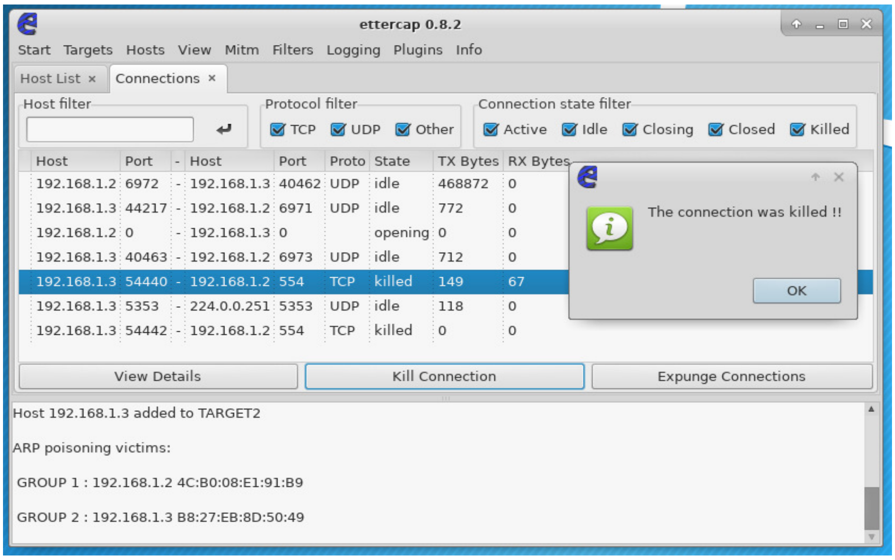
We used a Raspberry Pi with the 64bit ARM version of Kali Linux - this was the Attacking Device. The Target Device was a laptop using Ubuntu MATE. The cameras used were the Foscam FI9826W [12], the Hikvision DS-2CD2535FWD-I(W)(S) [13], the Merit-LILIN LR2522E4 [14] and IPR722ES4.3 [15], and the Sricam SP008 [16] and SP017 [17]. All cameras were connected via Ethernet. Ettercap was used to perform MitM attacks, as well as Bettercap, the command line-based successor to the software suite. Ettercap was used for its graphical interface and ease of use, while Bettercap was used for its ability to select multiple targets and disrupt their overall connectivity. In addition to this, Wireshark was also used to monitor network traffic, as well as closely inspect intercepted packets. By observing packets with Wireshark, we discerned what protocols were used by devices. The Target Device used Mozilla Firefox, VLC media player, Xeoma, and OpenCV to open stream URLs. Xeoma was chosen due to the security flaw found by Boyarinov and Hunter [7], but also for its ability to connect to ONVIF compliant cameras, as well as its Linux support. An Android Smartphone was also used with Onvifer to test ONVIF connections. We used this application to generate further traffic, attempt to sniff credentials, and to test connectivity.

3.3. Denial of Service

Denial of Service is a primary goal for the attacker, as this can delay the raising of the alarm, and deny the gathering of evidence after the incident has been detected.

Once the attacking device was positioned between the camera and the victim, we were able to easily kill the connection to any camera feed (see Figure 1), or even place an ARP ban on the victim altogether. The Target Device could use VLC media player, and ONVIF compliant software such as Xeoma to access the stream or use an OpenCV python script to access the RTSP feed. All cameras were affected by this attack, and all active streams could be instantly interrupted. When using OpenCV and Xeoma, an error message was displayed which could alert a user. However, when using VLC the stream simply stopped without any feedback. This did not indicate any breach in trust or malicious tampering and could easily be mistaken for a connection failure. The user could re-establish the connection, though if they are pre-occupied or they are unfamiliar with using the cameras, they may not be able to catch the threat actor in the act of stealing. If the connection is re-established the alarm will be raised, and the criminal may be recorded on camera.

The Threat Actor can prevent this altogether by using Bettercap to place an ARP ban on the IP cameras in the building; or a less subtle but equally effective method would be to place a ban on the victim machine. The user will realise they have no internet connectivity, but they may not attribute this to a malicious attack, but rather hardware issues or a bad internet service provider.



☑ TCP ☑ UDP ☑ Other

☑ Active ☑ Idle ☑ Closing ☑ Closed ☑ Killed

Host	Port	-	Host	Port	Proto	State	TX Bytes	RX Bytes
192.168.1.2	6972	-	192.168.1.3	40462	UDP	idle	468872	0
192.168.1.3	44217	-	192.168.1.2	6971	UDP	idle	772	0
192.168.1.2	0	-	192.168.1.3	0		opening	0	0
192.168.1.3	40463	-	192.168.1.2	6973	UDP	idle	712	0
192.168.1.3	54440	-	192.168.1.2	554	TCP	killed	149	67
192.168.1.3	5353	-	224.0.0.251	5353	UDP	idle	118	0
192.168.1.3	54442	-	192.168.1.2	554	TCP	killed	0	0

The connection was killed !!

```
Host 192.168.1.3 added to TARGET2

ARP poisoning victims:

 GROUP 1 : 192.168.1.2 4C:B0:08:E1:91:B9

 GROUP 2 : 192.168.1.3 B8:27:EB:8D:50:49
```

Figure 1. Interrupting the camera stream using Ettercap.

If a camera loses connectivity it may still record footage by storing the data on a MicroSD card. The Threat Actor would then be recorded and potentially identified at a later time. It is entirely possible that no MicroSD card has been inserted into a camera, as all cameras tested supported this type of storage, but did not supply the customer with it. The same person who leaves the default authentication details unchanged may also neglect to insert a MicroSD card.

3.4. UNAUTHORISED ACCESS

Before breaking in, the attacker may wish to perform reconnaissance using the security cameras in place. By hiding and connecting to a Wi-Fi access point they may sniff the network for authentication details, or brute force the cameras to gain access.

3.4.1 Packet Sniffing with Wireshark

We used Wireshark to attempt to collect usernames and passwords, as this would be a goal for the attacker. By examining the captured packets, it was found that the Hikvision, Merit-LILIN, and Foscam cameras were using Digest Authentication to authorise users. However, it was unclear from the captured packets what method of authorisation the Sricam camera was using. Cryptographical nonces were found in packets exchanged between the victim machine and the cameras. This indicated that Digest Authentication was being used, and MD5 digests were used to create nonces and hash authentication details. Digest Authentication is an authentication scheme used in HyperText Transfer Protocol (HTTP) [18]. When using this scheme, the cameras challenge the user by providing them with a cryptographical nonce. The user must then encrypt the username, password, nonce, method, and a Uniform Resource Locator (URL). If the hash of these values is correct, they can then gain access to the camera feed.

MD5 is not considered secure [19] [20], but Digest Authentication creates a large obstacle for the Threat Actor in question, as they may not be able to use a replay attack to gain access to the cameras. Using the previous hashed value will not work if the nonce used expires after every session. The Threat Actor will find that it is more effective to use a brute force attack.

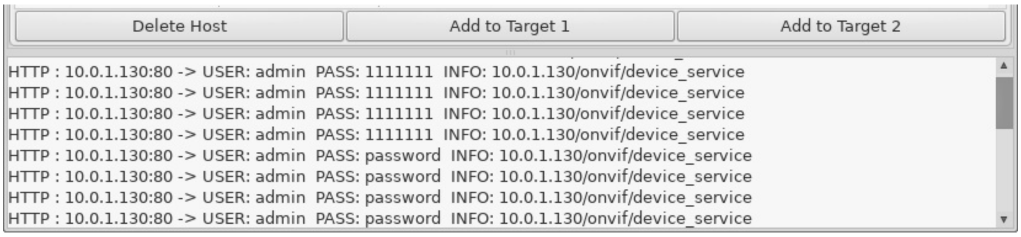
3.4.2 Brute Forcing with Hydra

Brute Force attacks involve an attacker using a list of words and values to login to a server, webpage or system. There are several tools that can be used, such as Jack the Ripper, Ncrack and THC Hydra [21]. While on the network, or even using Shodan.io to search for the cameras, the Threat Actor can use traditional brute forcing tools that are included with Kali Linux, or accessible for many Linux distributions. The captured packets revealed the usernames used to gain access to the cameras. The username for the Hikvision, Foscam and Merit-LILIN cameras was 'admin', providing us with 50% of the login details, which could then be used with brute forcing tools such as Hydra or Burp Suite. The Mirai password list is available on Github, allowing the Threat Actor to take advantage of any default usernames and passwords which have been left unchanged.

3.4.3 ONVIF Software

Using VLC, Xeoma and Onvifer it was found that the Sricam camera required no authentication at all when using the following URL: rtsp://x.x.x.x/onvif1. On the ONVIF applications the stream would automatically appear, and the threat actor could easily spy on anyone present in the building. Boyarinov and Hunter [7] found that this application revealed usernames and passwords when using Ettercap. As of version 18.11.21, this is still the case. When connecting to a camera that used Digest Authentication (such as the Hikvision camera), Xeoma would instead use Basic Authentication which is revealed automatically by Ettercap. These findings therefore support Boyarinov and Hunter.

In the process of proving this, it was discovered that the Xeoma application automatically tried to login to cameras with a Brute Force attack (see Figure 2). The application used a basic wordlist to attempt to gain access to cameras, presumably for the convenience of the users. This was discovered when Ettercap sniffed the login details of the Hikvision camera. Ettercap also showed Xeoma using 'password' and '1111111' as well as other combinations. It was due to this that the application gained access to the Foscam camera, as this device had a default username and password. Because of this process, any unchanged usernames and passwords would increase the chance of the Threat Actor gaining access via the Xeoma application. The application is no doubt highly accessible for home and business users, however it is also a seemingly harmless tool that can be used effectively by the Threat Actor. Once connected to the WiFi, the burglar can use Xeoma to check the layout of the building, as well as any signs of activity from people who live or work there.



```
HTTP : 10.0.1.130:80 -> USER: admin  PASS: 1111111  INFO: 10.0.1.130/onvif/device_service
HTTP : 10.0.1.130:80 -> USER: admin  PASS: 1111111  INFO: 10.0.1.130/onvif/device_service
HTTP : 10.0.1.130:80 -> USER: admin  PASS: 1111111  INFO: 10.0.1.130/onvif/device_service
HTTP : 10.0.1.130:80 -> USER: admin  PASS: 1111111  INFO: 10.0.1.130/onvif/device_service
HTTP : 10.0.1.130:80 -> USER: admin  PASS: password  INFO: 10.0.1.130/onvif/device_service
HTTP : 10.0.1.130:80 -> USER: admin  PASS: password  INFO: 10.0.1.130/onvif/device_service
HTTP : 10.0.1.130:80 -> USER: admin  PASS: password  INFO: 10.0.1.130/onvif/device_service
HTTP : 10.0.1.130:80 -> USER: admin  PASS: password  INFO: 10.0.1.130/onvif/device_service
```

Figure 2. Xeoma using a password list to connect to a camera.

3.4.4 Feed Interception

Using Wireshark to collect packets containing the camera feed it was desirable to replicate Alharbi and Aspinall's [9] capture of the unencrypted video stream. Unfortunately, we were unable to achieve this. However, the ONVIF software, Xeoma did allow us to wrongfully access the Sricam and Foscam cameras. The attacker would opt to use this due to its ease of use.

3.5. Results

Table 1 Shows that MitM attacks (ARP spoofing in this case) still remain highly successful. When the attacker sends poisoned ARP packets to the cameras and the Target Device, the devices do not examine the existing IP addresses and MAC addresses within their ARP cache tables. For example, the Hikvision camera is sending the stream to the viewer via a gateway with an IP address of '192.168.0.1' and a MAC address of 'AA:AA:AA:AA:AA:AA'. Suddenly the camera receives an ARP request stating that the gateway is now associated with 'BB:BB:BB:BB:BB:BB'. The camera does not flag this event as suspicious or check to see if '192.168.0.1' still belongs to the original MAC address. Instead it trusts the new device and allows it to handle the traffic.

Table 1 shows that all of the cameras used, including the victim device were unable to check MAC and IP addresses and therefore unable to detect or prevent ARP spoofing and Denial of Service.

Table 1. Results of ARP Poisoning.

Device	ARP Poisoning
Hikvision DS-2CD2535FWD-I(W)(S)	Successful
Merit-LILLIN LR2522E4	Successful
Merit-LILLIN IPR722ES4.3	Successful
Foscam FI9826W	Successful
Sricam SP008	Successful
Sricam SP017	Successful

3.5.1 Prevention and Detection

Acting as clients, the Target Device or a local server could have detected the attack by using an intrusion detection system (IDS) such as Snort. Snort features a pre-processor which decodes ARP packets and detects IP address inconsistencies on the network [22]. Businesses and home users can utilise this software as it is an open source IDS. This can be used to detect ARP Poisoning and raise the alarm in the event of an attack. By detecting and preventing MitM attacks, local Denial of Service attacks could also be prevented. Table 2 shows that once ARP Poisoning is successful Denial of Service is highly effective. Tripathi and Mehtre [23] suggest the Antidote Scheme be used, in which a host on the network checks to see if previously cached addresses are still alive before amending their ARP tables. This solution could be built into future devices (or supported devices could be patched) to bolster security against MitM attacks.

Table 2. Results of Denial of Service Attacks.

Device	**Denial of Service Attack**
Hikvision DS-2CD2535FWD-I(W)(S)	Connections interrupted and Blocked.
Merit-LILLIN LR2522E4	Connections interrupted and Blocked.
Merit-LILLIN IPR722ES4.3	Connections interrupted and Blocked.
Foscam FI9826W	Connections interrupted and Blocked.
Sricam SP008	Connections interrupted and Blocked.
Sricam SP017	Connections interrupted and Blocked.
Ubuntu MATE Laptop	Connections interrupted and Blocked.

The Sricam SP008 and SP017 presented the worst security concerns as they allowed anyone on the network to access their stream without authentication as shown in Table 3. By using RTSP the stream could be accessed by simply typing an IP address followed by '/onvif1'.

Table 3 showed that the Hikvision and Merit-LILLIN cameras utilised Digest Authentication, which does present a significant obstacle for the threat actor when they attempt to sniff authentication details. Passwords are no longer sent in plain text, and the time and difficulty of attempting to decrypt and brute force MD5 digests ensures that many attackers will give up and potentially move on or try other methods. However, RFC 7616 [24] indicates that SHA-256 and SHA-512 are available and should be used, due to MD5's insecurity.

Table 3. Results of Unauthorised Access Attempts.

Device	**Unauthorised Access**
Hikvision DS-2CD2535FWD-I(W)(S)	Failed – Digest Authentication used.
Merit-LILLIN LR2522E4	Failed – Digest Authentication used.
Merit-LILLIN IPR722ES4.3	Failed – Digest Authentication used.
Foscam FI9826W	Accessed with blank default password.
Sricam SP008	Allows access without authentication.
Sricam SP017	Allows access without authentication.

All cameras were ONVIF compliant and it is positive to see that four of these cameras still required authentication. The Sricam SP008 and SP017 could be accessed by anyone and whilst this accessibility may appear beneficial to users, it creates a vulnerability that can be used by criminals. The Foscam FI9826W had a blank default password which also resulted in unauthorised access before the password was set.

With the Mirai password list available online as well as the numerous Brute Force tools available to criminals, we must reiterate the need for users to change default login details once cameras are in place. A strong, secure password will increase the time and effort spent performing a brute force attack and if this becomes too great, an attacker may give up entirely. The Threat Actor is a criminal of limited knowledge and skills and as a result they may choose to move onto another building or break in with a higher risk of being caught. The National Cyber Security Centre [25] advocates passwords that comprise of 'three random words' as this is easier for people to remember and understand. Following this guidance could prevent future incidents and safeguard homes and businesses.

4. FUTURE WORK

Future investigations will be conducted in order to recreate the Integrity Violation attack performed by Boyarinov and Hunter [7]. Their attack focused on replaying UDP packets in order to achieve a camera loop, we will adapt this attack to cameras using TCP for authentication and transmission. A larger sample of cameras with more variety should also be tested in future, and more exploits and vulnerabilities should be performed, as this was a limitation of the paper.

5. CONCLUSIONS

We have demonstrated that vulnerabilities remain in newer IP cameras though improvements have been made. We have used Ettercap and Bettercap to interrupt or block all camera streams completely. This could have serious implications for home and commercial security. IP Cameras are widespread and accessible but if they rely upon network connectivity for access or storage, they will always be vulnerable to disruption from successful MitM attacks. Criminals are incredibly adaptable when it comes to utilising technology. This can be seen from crimes such as ATM fraud and keyless car theft. If they gain the skills to perform MitM attacks they can use this to avoid arrest or prosecution. In order to prevent ARP Poisoning and Spoofing, devices should check their existing ARP cache with devices on the network before trusting and accepting new entries. Should the attacker claim to have an IP address that is known to be in use the MitM attack may be unsuccessful. As always, default passwords should be replaced with stronger passwords that increase the difficulty of Brute Force attacks. These security measures will help prevent future DDoS attacks and ensure that our privacy is protected.

ACKNOWLEDGEMENTS

Thank you to Cloudview UK for allowing us to use their IP cameras and for providing guidance and feedback.

REFERENCES

[1] H. Sinanovic and S. Mrdovic, “Analysis of mirai malicious software,” in 2017 25th International Conference on Software, Telecommunications and Computer Networks (SoftCOM), Sep. 2017, pp. 1–5. DOI:10.23919/SOFTCOM.2017.8115504.

[2] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, “Ddos in the iot: Mirai and other botnets,”Computer, vol. 50, no. 7, pp. 80–84, 2017, ISSN: 0018-9162.DOI: 10.1109/MC.2017.201.

[3] J. Liranzo and T. Hayajneh, "Security and privacy issues affecting cloud-based IP camera," 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), New York, NY, 2017, pp. 458-465. DOI: 10.1109/UEMCON.2017.8249043

[4] M. Smith. (2014). Peeping into 73,000 unsecured security cameras thanks to default passwords, [Online]. Available: https://www.csoonline.com/article/2844283/microsoft-subnet/peeping-into-73-000-unsecured-security-cameras-thanks-to-default-passwords.html.

[5] F. Callegati, W. Cerroni, and M. Ramilli, “Man-in-the-middle attack to the https protocol,”IEEE Security Privacy, vol. 7, no. 1, pp. 78–81, Jan. 2009, ISSN: 1540-7993.DOI: 10.1109/MSP.2009.12.

[6] P. Arote and K. V. Arya, “Detection and prevention against arp poisoning attack using modified icmp and voting,” in2015 International Conference on Computational Intelligence and Networks, Jan. 2015,pp. 136–141.DOI: 10.1109/CINE.2015.34.

[7] K. Boyarinov and A. Hunter, “Security and trust for surveillance cameras,” in2017 IEEE Conference on Communications and Network Security (CNS), Oct. 2017, pp. 384–385.DOI: 10.1109/CNS.2017.8228676.

[8] ONVIF. (2018). Conformant products, [Online]. Available: https://www.onvif.org/conformant-products/.

[9] R. Alharbi and D. Aspinall, “An iot analysis framework: An investigation of iot smart cameras' vulnerabilities,” inLiving in the Internet of Things: Cybersecurity of the IoT - 2018, Mar. 2018, pp. 1–10.DOI:10.1049/cp.2018.0047.

[10] H. Schulzrinne, A. Rao, R. Lanphier, M. Westerlund, and M. Stiemer-ling,Real-Time Streaming Protocol Version 2.0, RFC 7826, Dec. 2016.DOI: 10.17487/RFC7826. [Online]. Available: https://rfc-editor.org/rfc/rfc7826.txt.

[11] Aircrack-ng. (2018). Aircrack-ng, [Online]. Available: https://www.aircrack-ng.org/.

[12] Foscam. (2018). Fi9826w, [Online]. Available: https://www.foscam.com/product/2.html.

[13] Hikvision. (). Ds-2cd2535fwd-i(w)(s), [Online]. Available: https://www.hikvision.com/en/Products/Network-Camera/EasyIP-3.0/3MP/DS-2CD2535FWD-I(W)(S).

[14] LILIN. (2018). Model: Lr2522e4 / lr2522e6, [Online]. Available: https://www.meritlilin.com/en/product/LR2522E4LR2522E6.

[15] Sricam, (2018). Model: Ipr722es4.3 / ipr722es6, [Online]. Available: https://www.meritlilin.com/en/product/IPR722ESIPR722ES6.

[16] Sricam. (2018). Sp008, [Online]. Available: http://www.sricam.com/product/id/9d5d656a907f46e48da1d45b9d0115ed.html.

[17] Sricam, (). Sp017, [Online]. Available: http://www.sricam.com/product/id/66e005d40593482ca14957fe87562952.html.

[18] J. Franks, P. M. Hallam-Baker, J. L. Hostetler, S. D. Lawrence, P. J.Leach, A. Luotonen, and L. C. Stewart. (Jun. 1999). Http authentica-tion: Basic and digest access authentication, [Online]. Available: http://www.rfc-editor.org/rfc/rfc2617.txt.

[19] P. Hawkes, M. Paddon, and G. G. Rose, Musings on the wang et al. md5 collision, Cryptology ePrint Archive, Report 2004/264, 2004.[Online]. Available: https://eprint.iacr.org/2004/264.

[20] D. Pauli. (2016). Security! experts! slam! yahoo! management! for!using! old! crypto! [Online]. Available: https://www.theregister.co.uk/2016/12/15/yahoospasswordhash/.

[21] P. Shankdhar. (2018). Popular tools for brute-force attacks (updatedfor 2018), [Online]. Available: https://resources.infosecinstitute.com/popular-tools-for-brute-force-attacks/.

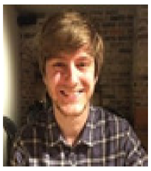
[22] T. S. Project. (2018). Snort1#1 users manual 2.9.12, [Online]. Avail-able: http://manual-snort-org.s3-website-us-east-1.amazonaws.com/.

[23] N. Tripathi and B. M. Mehtre, "Analysis of various arp poisoning mitigation techniques: A comparison," in2014 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), Jul. 2014, pp. 125–132.DOI: 10 . 1109 /ICCICCT.2014.6992942.

[24] R. Shekh-Yusef, D. Ahrens, and S. Bremer, "Http digest access authentication," RFC Editor, RFC 7616, Sep. 2015.

[25] E. W. (2018). Not perfect, but better: Improving security one step at a time, [Online]. Available: https://www.ncsc.gov.uk/blog- post/not-perfect-better-improving-security-one-step-time.

AUTHORS



Thomas Doughty is a graduate of Teesside University and received a BSc (Hon) in Cybersecurity and Networks. His research interests include Cyber Security and the Internet of Things.

Dr. Nauman Israr is currently a Senior Lecturer in Networks and Communication at Teesside University. His research interests are include Wireless Sensor Networks, Intelligent Computing and Cluster Communication.

Dr. Usman Adeel is currently a Senior Lecturer in Computer Science at Teesside University. He holds a PhD in Computing from Imperial College, London. His research interests are focused on Distributed Sensing Systems and their applications for Internet of Things, Cyber-physical Systems