Security of Connected Objects

O. Théophile Aballo, Roland Déguénonvo and Antoine Vianou

***Abstract*—** The expansion of connected objects continues to create privacy issues for people and becomes a target for attacks on information systems. Faced with this threat, the security measures to adopt are still at the heart of the debate. They consist in providing better control of risks within information systems by answering certain issues that take into account availability, integrity, confidentiality and traceability. Many are still indifferent about the consequences this has on information systems. In this work we proposed to show on the one hand, the impact of connected objects on information systems and on the other hand proposed the security policy set for these objects. Thus, intrusion tests on connected objects are implemented in order to identify the vulnerabilities and the consequences of these on information systems. The connected objects studied in our case present vulnerabilities that are exploitable. These flaws impact the security of information systems. We then became interested in the security policy implemented to improve the security of connected objects.

***Keywords*—** Connected objects, security policy, vulnerabilities.

I. Introduction

To ensure the security of connected objects, attempts to attack objects must be detected and a plan put in place to reduce the risk of illegal intrusion into these objects. Indeed, the detection of attacks attempts consists of identifying and exploiting the specific vulnerabilities associated with each connected object, performing intrusion tests on the objects and finally taking control of the connected objects. Indeed, the intrusion risk reduction plan consists in showing the impact of object vulnerabilities and their level of insecurity on the one hand and on the other hand writing recommendations to improve the security of connected objects. In this article we will first present the different threats of connected objects, then we will discuss the intrusion tests carried out and the equipment used to perform these intrusion tests and finally finish with the discussion of the results from the tests of 'intrusion.

II. Objects Connected To The Networks

The use of connected objects is becoming more and more essential. Connected objects are used for personal purposes or in a much larger context. We propose to make a case study on network cameras.

A. How Network Cameras Work

Network cameras capture data in the same way as a digital camera. A network camera has the ability to compress captured video and transmit it over the network. From an IP (Internet Protocol) x.y.z.w camera, you can see the viewing perimeter of the camera through a web browser directly on his computer or on a smartphone in the network. We also have the option to access it over the internet because it already has the software and memory to run as a standalone device. We have found that network cameras can be implemented in three types of networks:

- Wired Network: Connects the RJ45 port of network cameras to a LAN (Local Area Network) switch. Here the connectivity on a wired network offers security and maximum bandwidth

- Wireless Network: Connects network cameras that have a wireless option. However, there is a negotiation between the bandwidth and the security on the network.

- Cellular network: Many network cameras are equipped with integrated cellular chips. Cellular networks offer slow bandwidth speeds, but much higher levels of security than wireless networks.

Network cameras include many data transport protocols. TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) are protocols used for sending data.

B. Threats of network Cameras

Threats can be internal or external to the system:

- operational threats: they are linked to a state of the system at a given moment. They are the result of a software bug, an input filtering error,

- Physical threats: They are related to hardware failures, fires or frequent power cuts.

-the threats of human origin: They are directly associated with human errors, whether in the design of the system of network cameras.

C. Challenges of Computer Security

The basic idea of computer security is to provide a better control of risks within an information system that really weigh on users by answering certain issues that we present in four points:

-Availability: Guarantee access to resources, when needed, to authorize users to access resources.

-Integrity: Ensure that the data exchanged is accurate and complete.

-Privacy: Ensure that only authorized users can access network data and resources.

-Traceability: Logging and tracking actions and data processing to detect and, to the extent possible, prevent confidentiality, integrity or availability from being compromised.

O. Théophile Aballo, Roland Déguénonvo and Antoine Vianou, Polytechnic School of Abomey-Calavi, Abomey-Calavi University, BENIN.

III. Materials Used And Intrusion Tests

A. Materials Used

In this part we will detail the tools used and present the intrusion tests

A1. Network Cameras

The network cameras used are for POE IP cameras. We have found that these cameras are targets for DDOS attacks by hackers.

A2. Operating System

To conduct a penetration test, we have several tools. As part of our work, we opted for Kali Linux, a Debian-based GNU / Linux distribution. Kali-Linux is a specialized distribution in auditing and intrusion testing. It includes a set of necessary tools preinstalled for the realization of our work such as nmap, hydra, armitage, zenmap, metaspolit

A3. Programs

Some programs have achieved our goals. Among these programs, we can retain:

- Nmap: (Network Mapper) is an open source network exploration and security audit tool. Nmap is a port scanner. It is available for the most part on Linux operating systems in our case study. Nmap allows you to determine which hosts are active on a network, what services these hosts offer, what operating systems they use, what types of filtering devices are used, and other features.

- Hydra: This is brute force password tool. It supports a large number of attack protocols: ftp, ftps, https [s] -head | get, http [s] -get | postform, http-proxy, smtp [s], smtp-enum, ssh, teamspeak, telnet [s]. Hydra is very fast and flexible, and new modules are easy to add. We used Hydra in this study to gain unauthorized access to our camera's web interface.

Password dictionary

A password dictionary is a set of collected potential passwords. Potential passwords are common words in a given language (French, English, and Spanish). In our context, we used a dictionary of enough passwords collected by ourselves.

Fig. 1 Password dictionary

Indeed, we first wanted to use a fairly simple password dictionary before using a password dictionary complex enough to save time in case our target would be protected by the default passwords provided by the fora on the internet. There is enough password dictionary on the internet.

B. Intrusion tests

An intrusion test is a method of evaluating the security of a computer system or network by simulating malicious attackers or by malicious software. The intrusion test environment is defined as the space allowed to the attacker to perform the intrusion test. In our case study we worked in two different environments.

1st test environment

Our target camera is accessible at the 192.168.1.2 IP (Internet Protocol) address and that of the Pentester machine (an individual β that is responsible for monitoring the security of a system to prevent it from being hacked) accessible at 192.168.1.4. We first performed a port scan on our target to determine open ports using the nmap Next command:

nmap -open 192.168.1.2

open: to list only the open ports on our target.

Fig. 2 Services and related versions

2nd test environment

We also used nmap in this section: Nmap -sV -A 10.32.18.0/24

-sV: tests the open ports to determine the listening service and its version;

-A: Enable operating system and version detection.

Here is the result in FIG.4 and FIG.5 respectively within the camera bearing the 10.32.18.66 and the one bearing the 10.32.18.86 (these addresses were arbitrarily given to the cameras).

http-enum	//system.html: CMNC-200 IP Camera (401 Unauthorized)
http-slowloris-check	VULNERABLE: Slowloris DOS attack State: LIKELY VULNERABLE IDs: CVE:CVE-2007-6750 Slowloris tries to keep many connections to the target web server open and hold them open as long as possible. It accomplishes this by opening connections to the target web server and sending a partial request. By doing so, it starves the http server's resources causing Denial Of Service. Disclosure date: 2009-09-17 References: http://ha.ckers.org/slowloris/ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
http-stored-xss	Couldn't find any stored XSS vulnerabilities.
ssl-ccs-injection	VULNERABLE: SSL/TLS MITM vulnerability (CCS Injection)

Fig. 3 Slowloris attack by DOS

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
21	tcp	open	ftp	syn-ack	Axis M3024-L Network Camera ftpd	5.50.5.3	2015
80	tcp	open	http	syn-ack	Boa httpd		
	http-robots.txt	1 disallowed entry /					
	http-title	Index page					
554	tcp	open	rtsp	syn-ack	Axis M1054 or P3364 Network Camera rtspd		
	rtsp-methods	DESCRIBE, GET_PARAMETER, PAUSE, PLAY, SETUP, SET_PARAMETER, TEARDOWN					
57797	tcp	open	upnp	syn-ack	Portable SDK for UPnP devices	1.6.18	Linux 2.6.35; UPnP 1.0

Fig. 4 Result of nmap on the 10.32.18.66

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
21	tcp	open	ftp	syn-ack	Axis P5514-E PTZ Dome Network Camera ftpd	6.50.1.2	2017
80	tcp	open	http	syn-ack	Apache httpd	2.4.20	(Unix) OpenSSL/1.0.2j
	http-robots.txt	1 disallowed entry /					
	http-title	Index page					
554	tcp	open	rtsp	syn-ack	GStreamer rtspd		
	rtsp-methods	OPTIONS, DESCRIBE, GET_PARAMETER, PAUSE, PLAY, SETUP, SET_PARAMETER, TEARDOWN					
49152	tcp	open	upnp	syn-ack	Portable SDK for UPnP devices	1.6.19	Linux 4.4.27; UPnP 1.0

Fig. 5 Result of nmap on the 10.32.18.86

-Use of Hydra

Through the web interface of our camera, we tried to crack the password of the associated service using a password dictionary. For this action, hydra is executed with the command below :

Hydra -l admin -P password.txt -v -f 192.1681.2 http-get

- l: allows to specify the login;

- P: is used for the list of passwords;

-v: is used for the verbose mode, it shows connection attempts-f: exit after obtaining a valid user name and password once;

http-get is the method used.

FIG.6 shows the result of the command used

```
heaven@Sterm:~/test$ hydra -l admin -P password.txt -v -f 192.168.1.2 http-get
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret serv
ice organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2018-11-21 09:08:20
[WARNING] You must supply the web page as an additional option or via -m, default pa
th set to /
[DATA] max 6 tasks per 1 server, overall 6 tasks, 6 login tries (l:1/p:6), ~1 try pe
r task
[DATA] attacking http-get://192.168.1.2:80//
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[80][http-get] host: 192.168.1.2   login: admin   password: pass
[STATUS] attack finished for 192.168.1.2 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-11-21 09:08:21
heaven@Sterm:~/test$
```

Fig. 6 Cracked password using hydra

A valid login / password pair is therefore (admin, pass). Kali Linux has some password dictionaries located in / usr / share / word-lists.

-Use of [CVE-2013-4975] [19], [20] CVE-2013-4975 is an exploit written in python allowing access to the login credentials of the administrator and possibly all users from the identifiers of an unprivileged account. In order to take cognizance of all users having access to the camera, we executed this exploit on our target. The execution of this exploit generates us a file (.txt) passed largely in argument. When we make a strings on the file, we obtain the possible list of all users with an account with privilege or not. FIG.7 shows the result.

```
heaven@Sterm:~/MEMOIRE/POC$ ./CVE-2013-4975.py 192.168.1.2 admin 12345 credentials.txt
[*] Attacking 192.168.1.2
[*] Decrypting config
[*] Writing output file credentials.txt
Probably the admin user is  and the password is
If it doesn't make any sense, just do a strings of the output file
heaven@Sterm:~/MEMOIRE/POC$ strings credentials.txt
SMKH
CAMERA1
CST-8:00:00
Camera 01
davinci
UPNP DS-2CD4124F-I - 448068612
time.windows.com
www.hiddns.com
public
private
public
admin
12345
user
azerty
user1
azerty1
```

Fig. 7 Result of the execution of the cve-2013-4975

Scenario of a denial of service attack

We realized in this section a denial of service attack on our camera in local (1st Environment) .The attack is carried out with slowloris.pl , a script written in Perl. We first checked if the load balancing is used by our server as shown in Fig.8. Load balancing is usually done when a website receives a lot of incoming traffic. Load balancing activates the SYN-Cookies that help to get DDos attacks.

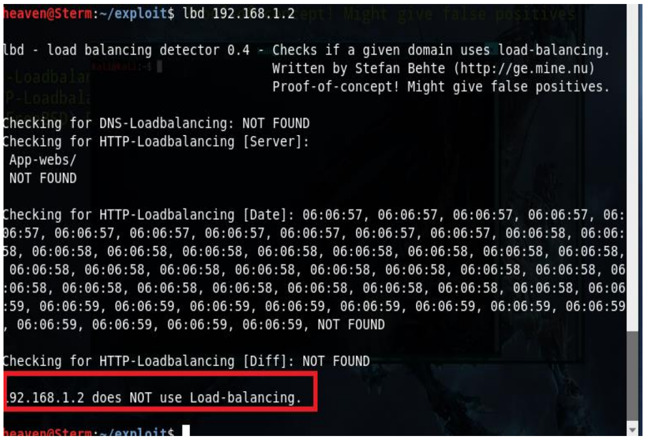

Fig. 8 checking lbd on the camera

We then launched our attack.

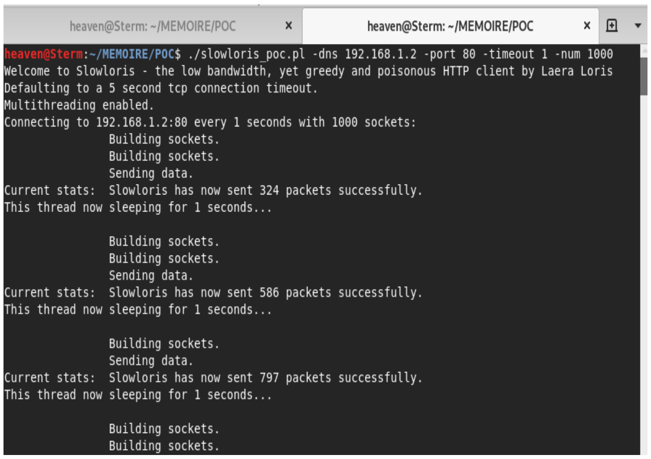

Fig. 9 Attack by denie of service on the camera

-dns: Specify the IP address of the target or the domain name;

-port: the open port on which the vulnerability is discovered;

-timeout: the limit of execution time of the order;

--num: the socket number.

After a few moments, we remade that the web interface of our camera no longer responds. The attack is effective

Fig. 10 Unreachable page following denial of service attack

IV. Discussions and Recommandations of Security Policy

In this part, it is a question of presenting and analyzing the results after the implementation of the intrusion test. It is also devoted to a discussion and recommendations in terms of security policy.

A. Results discussions

Our study is based on several general observations made on the security of connected objects, particularly on network cameras. The research and the intrusion tests allowed us to discover vulnerabilities on our IP camera, the cameras we have targeted and cameras connected to the Internet. We exploited the identified vulnerabilities. The IP camera requires a weak password which allowed us to use our little password dictionary for brute force. The brute forcing allowed us to obtain the identifiers of a user. This information helped us to obtain the IDs of all camera users and also to access the camera via the Telnet service. With this service, we have control of the remote camera. We have access to the root of the operating system as if we were on our computer. This leaves us the choice of any malicious operation. For example, run a script that performs Pings in a continuous loop on the server. The denial of service attack on the IP camera makes the web service inaccessible for a moment. During this moment, any dangerous operation likely to be visualized by the camera will not be seen. This poses a problem of availability. The camera scans revealed that only http services are open and accessible. In http, the data is not encrypted. This poses a risk because with Wireshark we can use a free and free software for packet analysis, to recover the packets on the network in Promiscuous mode, in order to analyze them and thus obtain the login credentials to the web interface of the cameras and possibly other connected objects. A malicious individual who obtains this information may, however, modify them thus forcing the administrator to possess a reset to recover the default credentials and to possess the configuration again. The results of our study are satisfactory since we were able to identify and exploit the vulnerabilities identified on the various cameras that were the subject of our study. We have also been able to demonstrate the impact of vulnerabilities in an information system.

B. Security Policy Recommendations

We outline the recommendations that are proposed to improve the security of network cameras. The synthesis of these recommendations is based on the Integration Level, the Installation Level, the Storage Level, the Data Security Level, the Maintenance Level and the Information Level.

V. Conclusion

The security of an individual's privacy and information systems in the face of the popularization of connected objects, in particular network cameras, is not an unknown subject. More and more, attacks are multiplying against network cameras. For this purpose, the fact is regrettable. Network cameras are vulnerable because of the negligence of design security and their administration.

References

[1] Kennedy David and al, “Hacking, sécurité et tests d’intusion avec Metasploit”, Pearson France, 2011

[2] Patrick Engebreston, “Les bases du hacking”, PEARSON 2013.

[3] Sabrina Feng,. Jean-Marc Cerles, Hervé Dalmas, Tru Dô-Khac, Boris Paulin, “Sécurité des Objets connectés”, 2014

[4] Konstantin Boyarinov. Burnaby, Aaron Hunter, “Security and Trust for Surveillance for Cameras”

[5] Waher Peter, “Learning Internet Of Things”, Packet Publishing, 2015.

[6] A.VEITCH D.."Wavelet Analysis of Long Range Dependent Traffic, Trans. Info Theory, Vol44,No.1, p.2-15, January 1998. https://doi.org/10.1109/18.650984
[7] A.E.AVRACHENKOV K, BARAKAT C.,"A Stochastic Model of TCP/IP with Stationary Random Losses", Proceedings of ACM SIGCCOMM, 2000.
[8] B.A.GUILLEMIN F., "Analysis of ADSL traffic on an IP backbone link", Proceedings of Globecom 2003, December 2003.
[9] B.R., ZHANG L., "Resource ReSerVation Protocol (RSVP) – Version 1 message processing rules", RFC, no 2209, September 1997. https://doi.org/10.17487/rfc2205
[10] RFC 6275 C. Perkins, Tellabs and D. Johnson, Mobility Support in IPv6, July 2011
[11] G.D,B. Pentland and R. Nelson, Effects of Fast Router Adverdisement on MIPv6 Handovers, July 2003, ISSC 2003.
[12] W.H,M. Frank, On Things to Happen During a TCP Handover, LCN'03, October 2003.
[13] SAT-PERFProject, Analysis of solutions for mobile and efficient transport layer in the context of terrestrial/satellite hybrid networks. March 12.
[14] E.A,T Bulogne, REl-Azouzi, T.Jimenez, and L.Wynter. A survey on networking games in telecommunications. Computers & Operations Research, 33(2), 2006. https://doi.org/10.1016/j.cor.2004.06.005
[15] M.ZBen-Hamouda.Conception, optimization robuste des réseaux de télécommunications.PHD thesis, Université Paul Sabatier, Toulouse, France, Rapport LAAS No 10462 25 Juin 2010.
[16] D.Rossi, C. Testa, S. Valenti, and L. Muscariello, « Ledbat : The new bittorrent congestion controp protocol, » in Computer Communications and Networks (ICCCN), 2010 Proceedings of 19th International Conference on , pp.1-6, Aug 2010. https://doi.org/10.1109/ICCCN.2010.5560080
[17] P.Ameigeiras, J.J. Ramos-Munoz, J. Navarro-Ortiz, and J.Lopez-Soler, « Analysis and Modeling of youtube traffic, « Transactions on Emerging Telecommunications Technologies, vol. 23, no.4, pp. 360-377, [Online].Available: http//dx.doi.org/10.1002/ett.254, 6,2012
[18] Y.Zhang and N. Ansari, "Fair quantized congestion notification in data center networks", IEEE transactions on Communications, vol. 61, no 11, pp. 4690-4699, November 2013 https://doi.org/10.1109/TCOMM.2013.102313.120809