Demonstration
Webcam Security

MegaGiga ASBL

Filip Pynckels

16 Januari 2025

Abstract

This document is distributed as part of a presentation for the members of the *MegaGiga Computerclub* regarding webcam security. It covers the basics of how webcams work, how to locate webcams on the internet, and how to hack a webcam that you own and that is connected to a network you own in order to assess and prevent security weaknesses.

License

Warning

This document is purely for educational purposes. The authors want to draw the reader's attention to the fact that the reader must comply with all legislation that applies to him. We do not encourage the reader to do anything illegal, quite the contrary.

1 Introduction to Webcams

A webcam is a small digital camera that is typically used to capture video or images and transmit them to a computer on a local network or over the internet. Webcams are commonly used for video calls, live streaming and video conferencing. They are also used to provide the public with images of a touristic landscape like a ski slope, a live view on a historic part of a city, etc.

Webcams can be built into laptops, smartphones, and tablets, but can also be external devices connected via USB to a computers.

Webcams can also be used for security purposes, allowing users to monitor an area remotely. In the latter case, they are mostly connected immediately to a network and accessible from a remote computer. These devices are part of the Internet of Things (IOT).

In this paper, we will focus on webcams that are part of the Internet of Things.

1.1 Webcams from the outside

The webcams we will consider in this paper have two external aspects. On the one side, there is the hardware aspect: the connection of the webcam to the exterior world. These days, such a connection is almost always an RJ45 network connection or a WiFi connection. Both can be considered the same for our purpose of security analysis, since we can grab the dataflow between the webcam and the exterior world with a plethora of different available software packages.

On the other side, webcams have a software aspect. More specific, webcams expose themselves to the exterior world by means of IP addresses, network ports and one or more protocols used to interact with the webcam.

The most common protocols webcams use to stream audio and/or video are the following:

RTSP (Real-time streaming protocol)
: Most IP cameras use this protocol to establish and control video and audio streams. RTSP does not provide configuration options. Most cameras support RTSP as a fallback protocol, even if they are using PSIA or ONVIF as a principal protocol.

PSIA (Physical security interoperability alliance)
: The PSIA protocol for web cams is designed to enable interoperability between various security devices, such as cameras, network video recorders, and other physical security systems. Specifically, PSIA focuses on creating standards for data communication and device integration within physical security systems, including the transmission of video and control signals for cameras.

ONVIF (Open network video interface)
: The ONVIF protocol is a widely adopted standard for IP-based security devices, including web cameras (network cameras). It provides a set of specifications that allow devices from different manufacturers to work together seamlessly in a security system. ONVIF's primary focus is on standardizing communication and interoperability between devices like network cameras, video recorders, and other physical security equipment.

In short, the mentioned protocols are used for:

	RTSP	PSIA	ONVIF
Camera discovery		✓	✓
Configuration		✓	✓
Live streaming	✓	✓ (using RTSP)	✓ (using RTSP)

From the network side, the default ports and communications protocols are:

	IP port	IP protocol
RTSP	554	TCP
PSIA	80	TCP, HTTP
	8080	TCP, HTTPS
ONVIF	8080	TCP, HTTPS (for discovery and configuration)
	8899	TCP (for video streaming)

Note that besides the above mentioned protocols for audio and video streaming, most camera's also use HTTP, HTTPS, SSH and other protocols to communicate with the users and with the administrators of the camera. In order to fully understand the functioning of a webcam, one must have a full view on all the protocols and what they are used for.

1.2 Webcams from the inside

The inside of a webcam is not useful within the frame of this paper. However, when one wishes to have a full understanding of a certain webcam, knowing what is inside the webcam is important. Besides that, it is a fact that well build, programmed and administered webcams require a more profound understanding of the red team hacker than only the exterior aspects.

More specific: one can only (or rather mostly) find serious flaws that can help to attack the integrity of a webcam by examining its interior. The interior being the used hardware and software that make the webcam function.

There are two classic methods to get a grasp on the interior of a webcam. The first method is finding information on the hardware and/or the software by means of publicly available sources (e.g. firmware updates to understand the software and a site like the *FCC databases* to understand the hardware). To analyze the firmware, tools like *binwalk* and *Ghidra* are very helpfull. There are a lot of tools, but these were the ones that came to mind.

The second method is to purchase one or more webcams of the exact make and model, and use one of them to disassemble the flash or eprom memory. There are lots of open source programs that will allow you to extract the contents of the disassembled memory chips. It goes without saying that you will also need a cheap (or in some cases not so cheap) hardware device to connect the memory chip to your computer.

It is obvious that the first method is easier and cheaper than the second method. And since the base principle of hacking is: "Start with the simplest solution first", one should always try the first method if feasible. An example is the *Axis M1034-W Network Camera firmware*.

As already mentioned, within the frame of this paper, we will not go into further details. However, *MegaGiga Computerclub* can provide in-depth courses if you are interested in further information on this topic.

2 How to find webcams on the Internet

2.1 Google dorking

The Google search engine offers a number of keywords that can be used to find web content that is made available by Internet of Things (IoT) webcams. Some examples are mentioned below. A more extensive list can be found at *hackers-arise.net*

Table 1: Google search phrases

allintitle;"Network Camera NetworkCamera"
intitle:"EvoCam" inurl:"webcam.html"
intitle:"Live View / - AXIS"
intitle:"LiveView / - AXIS" — inurl:"view/view.shtml"
inurl:"indexFrame.shtml" "Axis Video Server"
inurl:"axis-cgi/jpg"
inurl:"MultiCameraFrame?Mode=Motion"
inurl:"view.shtml"
inurl:"/view/views.html?id="

2.2 Shodan.io

The site shodan.io offers more detailed possibilities to find webcams. Some examples are:

Table 2: Shodan search phrases

product:"Axis M1034-W"
http.title:"Axis M1034-W"
Dahua country:IR
Dahua DH-SD59230U-HNI country:RU
RTSP/1.0 has_screenshot:true country:RU
port:554

By clicking on a retrieved IP address, one can see a more detailed dashboard of the specific device, including all open IP ports, an estimation of the software the device uses, vulnerabilities of the software in question, etc.

3 How to check the security of a webcam

Within the scope of this paper and the accompanying demonstration, we will not go into details on the disassembly and analysis of real camera hardware. However, we will give a basic explanation concerning the analysis of downloaded firmware.

However, first, we will, as already mentioned, use the simplest solutions first. These are looking for webcams that stream their audio and video to the Internet without further measures of security.

3.1 Public availability of private information

A simple but telling example is to enter the below search term in shodan.io:

```
RTSP/1.0 has_screenshot:true country:BE
```

Even without being a paying member, one can look at the first two pages of results, and webcams that disclose images from within the homes of people, showing them sleeping, showing them playing with their children, etc. In short, even this simple search term already shows frightening results concerning privacy and security issues.

3.2 Standard passwords

Always start with the simplest solution first! Maybe not surprisingly, the method of trying the standard passwords will be successful in a number of cases. People don't want to change passwords, or they don't know how to do it, or they create extra users but don't change the default administrator password, etc.

The below table can be found at *ipvm.com*:

Webcam	**UserId / Password**
ACTi	admin/123456 or Admin/123456
Amcrest	admin/admin
American Dynamics	admin/admin or admin/9999
Arecont Vision	none
AvertX	admin/1234
Avigilon	Previously admin/admin, changed to Administrator / <blank>in later firmware versions
Axis	Traditionally root/pass, new Axis cameras require password creation during first login (note that root/pass may be used for ONVIF access, but logging into the camera requires root password creation)
Basler	admin/admin
Bosch	None required, but firmwares above version 6.0 prompt users to create passwords on first login
Brickcom	admin/admin
Canon	root/camera
Cisco	No default password, requires creation during first login
Dahua	Requires password creation on first login. Previously this process was recommended but could be canceled; older models default to admin/admin
Digital Watchdog	admin/admin
DRS	admin/1234
DVTel	Admin/1234
DynaColor	Admin/1234
FLIR	admin/fliradmin
FLIR (Dahua OEM)	admin/admin
FLIR (Quasar/Ariel)	admin/admin
Foscam	admin/<blank>
GeoVision	admin/admin
Grandstream	admin/admin
Hanwha	admin/no default password, must be created during initial setup
Hikvision	Firmware 5.3.0 and up requires unique password creation; previously admin/12345
Honeywell	admin/1234
IndigoVision (Ultra)	none
IndigoVision (BX/GX)	Admin/1234
Intellio	admin/admin
Interlogix	admin/1234

Webcam	UserId / Password
IQinVision	root/system
IPX-DDK	root/admin or root/Admin
JVC	admin/jvc
Longse	admin/12345
Lorex	admin/admin
LTS	Requires unique password creation; previously admin / 12345
March Networks	admin/<blank>
Mobotix	admin/meinsm
Northern	Firmware 5.3.0 and up requires unique password creation; previously admin/12345
Oncam	admin/admin
Panasonic	Firmware 2.40 and up requires username / password creation; previously admin/12345
Pelco	New firmwares require unique password creation; previously admin/admin
Pixord	admin/admin
Q-See	admin/admin or admin/123456
Reolink	admin/<blank>
Samsung Electronics	root/root or admin/4321
Samsung Techwin (old)	admin/1111111
Samsung (new)	Previously admin/4321, but new firmwares require unique password creation
Sanyo	admin/admin
Scallop	admin/password
Sentry360 (mini)	admin/1234
Sentry360 (pro)	none
Sony	admin/admin
Speco	admin/1234
Stardot	admin/admin
Starvedia	admin/<blank>
Sunell	admin/admin
SV3C	admin/123456
Swann	admin/12345
Trendnet	admin/admin
Toshiba	root/ikwd
VideoIQ	supervisor/supervisor
Vivotek	root/<blank>
Ubiquiti	ubnt/ubnt
Uniview	admin/123456
W-Box (Hikvision OEM, old)	admin/wbox123
W-Box (Sunell OEM, new)	admin/admin
Wodsee	admin/<blank>

3.3 Brute forcing webcams

Sometimes, it sounds more difficult than it is to brute force a webcam. Especially if you can use the tools someone else has already developped.

Within the context of red team security assessments of webcams, there are tools like CameRadar and CameraShy that can help you obtain your goal. Some of the tools available on Internet are free, others aren't.

3.4 Downloading, analyzing and exploiting microcode

In order to keep the below part of this paper concise, we will work with an example. More specific, we will download the firmware for the *Axis M1034-W Network Camera*.

3.4.1 Downloading from the internet

The file can be found under the name *M1034-W_5_50_5_4.bin*

3.4.2 Downloading from the flash memory in the webcam

It goes beyond the scope of this paper to explain how to extract firmware from the flash memory of a webcam. However, there is a very good youtube channel (*Matt Brown*) that shows how this can be done and which hardware and software can be used to do it.

3.4.3 Analyzing the microcode

Starting from the downloaded file, we will use the Linux command line interface:

```
binwalk -Me M1034-W_5_50_5_4.bin
cd _M1034-W_5_50_5_4.bin.extracted
ls ./_2494C.extracted/_19000.extracted/cpio-root/
ls jffs2-root
find . -iname "passwd"
cat ./_2494C.extracted/_19000.extracted/cpio-root/etc/passwd
cp ./_2494C.extracted/_19000.extracted/cpio-root/etc/passwd ../pwd.txt
cd ..
john --format=crypt --show ./pwd.txt
```

Which leeds us to the same result that the table with user names and passwords above shows:

```
User: root
Pass: pass
```

An other method to find a weakness is by means of MetaSploit. Therefore, we need to find the Linux version in the firmwarecode:

```
find . -iname "kernel*"
find . -iname "busy*"

msfconsole
    search type:exploit platform:linux kernel
    search busybox
```

Of course, one can also use the Exploit database or other websites to find further weaknesses.

3.4.4 Exploiting the found weaknesses

Exploitation of the found weaknesses can go from getting information in the form of images, video or audio to changing the configuration of the webcam. All the before mentioned activities can be considered hacking and are beyond the scope of this paper. During the demonstration for the members of the *MegaGiga Computerclub* regarding webcam security, some legal examples will be provided to show the participants how intrusive a webcam that is not enough secured can be. An example: *License Plate Readers (Matt Brown)*

List of Links