Reverse Engineering A Mysterious UDP Stream in My Hotel

Tags: *reverse-engineering* *networking* *python*
Reading time: about 3 minutes

Hey everyone, I have been staying at a hotel for a while. It's one of those modern ones with smart TVs and other connected goodies. I got curious and opened Wireshark, as any tinkerer would do.

I was very surprised to see a huge amount of UDP traffic on port 2046. I looked it up but the results were far from useful. This wasn't a standard port, so I would have to figure it out manually.

At first, I suspected that the data might be a television stream for the TVs, but the packet length seemed too small, even for a single video frame.

> This article is also available in French.

Grabbing the data

The UDP packets weren't sent to my IP and I wasn't doing ARP spoofing, so these packets were sent to everyone. Upon closer inspection, I found out that these were **Multicast** packets. This basically means that the packets are sent once and received by multiple devices simultaneously. Another thing I noticed was the fact that all of those packets were the same length (634 bytes).

I decided to write a Python script to save and analyze this data. First of all, here's the code I used to receive Multicast packets. In the following code, *234.0.0.2* is the IP I got from Wireshark.

```
import socket
import struct

s = socket.socket(socket.AF_INET, socket.SOCK_DGRAM, socket.IPPROTO_UDP)
s.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR, 1)
s.bind(('', 2046))

mreq = struct.pack("4sl", socket.inet_aton("234.0.0.2"), socket.INADDR_ANY)
s.setsockopt(socket.IPPROTO_IP, socket.IP_ADD_MEMBERSHIP, mreq)

while True:
```

```
    data = s.recv(2048)
    print(data)
```

On top of this, I also used binascii to convert this to hex in order make reading the bytes easier. After watching thousands of these packets scroll through the console, I noticed that the first ~15 bytes were the same. These bytes probably indicate the protocol and the packet/command ID but I only received the same one so I couldn't investigate those.

Audio is so LAME

It also took me an embarrassingly long time to see the string `LAME3.91UUUUUUU` at the end of the packets. I suspected this was MPEG compressed audio data, but saving one packet as test.mp3 failed to played with mplayer and the *file* utility only identified this as `test.mp3: data`. There was obviously data in this packet and *file* should know when it sees MPEG Audio data, so I decided to write another Python script to save the packet data with offsets. This way it would save the file `test1` skipping 1 byte from the packet, `test2` skipping 2 bytes and so on. Here's the code I used and the result.

```
data = s.recv(2048)
for i in range(25):
    open("test{}".format(i), "wb+").write(data[i:])
```

After this, I ran `file test*` and voilà! Now we know we have to skip 8 bytes to get to the MPEG Audio data.

```
$ file test*
test0:    data
test1:    UNIF v-16624417 format NES ROM image
test10:   UNIF v-763093498 format NES ROM image
test11:   UNIF v-1093499874 format NES ROM image
test12:   data
test13:   TTComp archive, binary, 4K dictionary
test14:   data
test15:   data
test16:   UNIF v-1939734368 format NES ROM image
test17:   UNIF v-1198759424 format NES ROM image
test18:   UNIF v-256340894 format NES ROM image
test19:   UNIF v-839862132 format NES ROM image
test2:    UNIF v-67173804 format NES ROM image
test20:   data
test21:   data
test22:   data
test23:   DOS executable (COM, 0x8C-variant)
test24:   COM executable for DOS
test3:    UNIF v-1325662462 format NES ROM image
test4:    data
test5:    data
test6:    data
test7:    data
```

```
test8:    MPEG ADTS, layer III, v1, 192 kbps, 44.1 kHz, JntStereo
test9:    UNIF v-2078407168 format NES ROM image
```

```
while True:
    data = s.recv(2048)
    sys.stdout.buffer.write(data[8:])
```

Now all we need to do is continuously read packets, skip the first 8 bytes, write them to a file and it should play perfectly.

But what was this audio? Was this a sneakily placed bug that listened to me? Was it something related to the smart TVs in my room? Something related to the hotel systems? Only one way to find out.

```
$ python3 listen_2046.py > test.mp3
* wait a little to get a recording *
^C

$ mplayer test.mp3
MPlayer (C) 2000-2016 MPlayer Team
224 audio & 451 video codecs

Playing test.mp3.
libavformat version 57.25.100 (external)
Audio only file format detected.
=====
Starting playback...
A:   3.9 (03.8) of 13.0 (13.0)  0.7%
```

The Revelation/Disappointment

What the hell? I can't believe I spent time for this. It's just elevator music. It is played in the hotel corridors around the elevators. Oh well, at least I can listen to it from my room now.

Citation

If you find this work useful, please cite it as:

```
@article{yaltirakli201605hotelmusic,
  title   = "Reverse Engineering A Mysterious UDP Stream in My Hotel",
  author  = "Yaltirakli, Gokberk",
  journal = "gkbrk.com",
  year    = "2016",
  url     = "https://www.gkbrk.com/2016/05/hotel-music/"
}
```

▶ Not using BibTeX? Click here for more citation styles.

Comments

Comment

Name

Guest

Post Comment

Comment by **Guest**
2023-02-25 at 15:07
Spam probability: 0.0%

RESPONDING TO: or interjections of mysterious, echoed "voices from the past" at various intervals...Is there somebody there?...What are you doing?...This can't be real...the sound of a watermelon being smashed...reverbed laughter...a quiet child's voice... CREATE A TOOL TO SPOOF THE MULTICAST. BE SPOOKED COMPLAIN DEMAND A REFUND!

Comment by **noone**
2023-02-25 at 13:38
Spam probability: 0.0%

as it was UDP protocol, that would be interesting if you did the source spoofing for some fun

Comment by **Guest**
2023-02-25 at 06:55
Spam probability: 0.0%

now the immediate question i get is can you transmit your own packets and change what music plays?

Comment by **Hotel Guest**
2023-02-25 at 01:35
Spam probability: 0.0%

Nice one. Made me laugh!

Comment by **Vince**
2023-02-25 at 00:14
Spam probability: 0.0%

What a great article. Love the writing style and the digestible deep dive into reversing.

Comment by **JW**
2023-02-24 at 22:24
Spam probability: 0.0%

Sir, this is really inspirational.

Comment by **Yomom**
2023-02-24 at 20:04
Spam probability: 0.0%

Lol all for the elevator music. Was thinki g smart TV was snooping on everyone

Comment by **Guest**
2023-02-24 at 19:52
Spam probability: 0.0%

Legend.

Comment by **yo ss ef**
2023-02-24 at 17:14
Spam probability: 0.0%

I liked this article

Comment by **Guest**
2023-02-24 at 16:30
Spam probability: 0.0%

Well done and very entertaining. A good read and learn.

Comment by **Andrea**
2023-02-24 at 13:25
Spam probability: 0.0%

as most things in life what seems mysterious it's usually pretty disappointing. Love this article!

Comment by **Jesper Bylund**
2023-02-24 at 10:45
Spam probability: 0.0%

You sir, are an inspiration!

Comment by **Adrian**
2023-02-24 at 10:33
Spam probability: 0.0%

This is great!

Comment by **Phoneguy**
2023-02-24 at 10:14
Spam probability: 0.0%

Music on hold / elevator music is usually sent as multicast hence why you and the elevator speaker is getting it.

Comment by **kino**
2023-02-24 at 09:12
Spam probability: 0.0%

Would have been even funnier if one of the songs was Rick Astley's "Never Gonna Give You Up".

Comment by **Tldr'er**
2023-02-24 at 08:52
Spam probability: 0.0%

How long all this took?

Comment by **Person #3686426**
2023-02-24 at 07:33
Spam probability: 0.0%

I’m respectfully adding a vote for you posting that sweet elevator music file.

Comment by **YM**
2023-02-24 at 06:51
Spam probability: 0.0%

Like it

Comment by **Guest**
2023-02-24 at 06:41
Spam probability: 0.0%

I wonder if you could broadcast your own music on the same port?

Comment by **Why-offset**
2023-02-24 at 05:06
Spam probability: 0.0%

What made you think to save the data with offsets? Is that representative of the total time of the elevator musi c?

Comment by **big man**
2023-02-24 at 04:09
Spam probability: 0.0%

really interesting article

Comment by **Guest**
2023-02-24 at 01:35
Spam probability: 0.0%

Time to start streaming some black metal into the elevators.

Comment by **lurker**
2023-02-24 at 01:20
Spam probability: 0.0%

So glad there is evidence that I'm not the only one who would have gone down this rabbit hole!

Comment by **Tux**
2023-02-24 at 01:06
Spam probability: 0.0%

Gold! Thanks for the write up, and the ride.

Comment by **Resetnos**
2023-02-24 at 00:18
Spam probability: 0.0%

Appreciated this article wanted to say Thank you for sharing.

Comment by **Guest**
2023-02-24 at 00:15
Spam probability: 0.0%

Next step: Send out some mp3's with the same format to the same multicast address. Kick that hotel party up a notch.

Comment by **SDWAN nerd**
2023-02-23 at 23:57
Spam probability: 0.0%

Multicast is cool :)

Comment by **Guest**
2023-02-23 at 23:51
Spam probability: 0.0%

...or interjections of mysterious, echoed "voices from the past" at various intervals...Is there somebody ther e?...What are you doing?...This can't be real...the sound of a watermelon being smashed...reverbed laughter... a quiet child's voice...

Could be lots of fun

Comment by **Guest**
2023-02-23 at 23:42
Spam probability: 0.0%

love it!
nicely done

Comment by **ilya**
2023-02-23 at 23:18
Spam probability: 0.0%

elevator music or how ghosts communicate?

Comment by **kjkent**
2023-02-23 at 22:46
Spam probability: 0.0%

Looks like you missed out on a lot of free NES ROMs there!

Comment by **JR**
2023-02-23 at 21:22
Spam probability: 0.0%

Nice. Who would have thought?
I wouldn't have expected that you could reconstitute the mp3 by stripping N bytes and concatenating the rest.
Maybe someday I'll find a use for that. Thanks.

Comment by **reptoid clone of john wayne and elvis**
2023-02-23 at 20:25
Spam probability: 0.0%

now who woulda thought that they'd do it that way haha

now spoof it ;)

Comment by **Guest**
2023-02-23 at 20:13
Spam probability: 0.0%

Hilarious

Good job

Comment by **I am a guest**
2023-02-23 at 20:13
Spam probability: 0.0%

please now post the elevator's music you dumped

Comment by **I am a guest**
2023-02-23 at 20:12
Spam probability: 0.0%

I absolutly LOVE this kind of article! A mistery, a sharp mindad and a laptop.

Comment by **am I spam?**
2023-02-23 at 18:45
Spam probability: 0.0%

I want to buy this c0de for the elevator to enlarge arsenal of things. This is not sp4m. once in a lifetime oppor tunity.

Comment by **I am interested in the spam detector**
2021-07-25 at 09:29
Spam probability: 5.599%

Hi, Fantastic Blog Post! Thanks For Your Blog. Buy Burberry Here. Burberry Handbags.

Comment by **Jan**
2021-05-30 at 12:30
Spam probability: 0.0%

Interesting read, do you happen to have a capture (PCAP, plain blob etc) of the stream?

Comment by
2021-04-02 at 09:09
Spam probability: 0.0%

The suspense was killing me throughout. Funny ending, nice writeup.

Comment by **Anonymous Coward**
2021-04-01 at 23:45
Spam probability: 0.0%

So..... what would happen if you did ARP spoofing to silence the actual source, and multicasted something el se? I'm not going to suggest you multicast audio from an adult movie, but it is the 1st of April after all.....

Comment by **b1tninja**
2021-04-01 at 21:09
Spam probability: 0.0%

What you should have thought next was, hey holy shit, the elevator listens to udp rtsp stream? And I have the multicast group

Comment by
2021-04-01 at 19:51
Spam probability: 0.0%

Oh man, all that effort for elevator music. Beautiful. <3

Thanks for the chuckle.

Comment by **admin**
2021-04-01 at 17:30
Spam probability: 0.0%

Thanks for the report @Guest, I fixed the errors that were reported on this page. It should validate cleanly no w, unless anything got cached along the way.

Comment by **Zombielinux**
2021-04-01 at 16:57
Spam probability: 0.0%

Now I'm curious as to what hardware they're running to catch the stream.

Comment by
2021-04-01 at 16:13
Spam probability: 0.0%

For the future, why not use tail to not need to save the file offsets out?
`tail --bytes=+8 test.mp3 | file -`
You can use a sh FOR loop as well

Comment by **Guest**
2021-04-01 at 15:54
Spam probability: 0.0%

Just commenting en-passant to notify that no, it's not actually valid HTML. (but I CBA with an email for tha t)

Comment by **jimmy**
2021-04-01 at 15:33
Spam probability: 0.0%

I was kinda hoping to get a link to an mp3 file so I could listen as well.

Comment by **utahcon**
2021-04-01 at 15:20
Spam probability: 0.0%

great read, this was useful in understanding a bit of the RE mentality. Thanks! Enjoy your muzak!

Comment by **SmallProject**
2021-04-01 at 15:08
Spam probability: 0.0%

So... can you control the audio the hotel plays? Lots of fun potential if so

Comment by **Dude**
2021-04-01 at 15:07
Spam probability: 0.0%

But now you probably can broadcast your own music to elevator!

Comment by **Cam**
2019-06-10 at 23:52
Spam probability: 0.0%

Good read, thanks!

Comment by **iTacoTaco**
2019-06-05 at 23:38
Spam probability: 0.0%

On the bright side, now you can host a party in your room except it only plays elevator music.

Comment by **haha**
2018-11-02 at 23:50
Spam probability: 0.0%

was fun to read. but still idk why they streaming lame music to all folks in their network xD

10 Places On Earth You Are

18.2K views Feb 19, 20

yx

Follow me around

- 📡 RSS
- 💼 LinkedIn
- 💻 GitHub
- 📧 Email
- 🔁 Mastodon
- 🐦 Twitter

Support my work

Thanks for checking out my website.

If you want to support me and help me produce more free content, you can buy me a coffee.

☕ Buy me a coffee

Get notified of new posts

email address

Subscribe

(or use RSS)

Search

Search terms

More links

- Projects
- Videos
- List of tags

Recent comments

Guest on Reverse Engineering A Mysterious UDP Stream in My Hotel @ 2023-02-25

noone on Reverse Engineering A Mysterious UDP Stream in My Hotel @ 2023-02-25

Guest on Reverse Engineering A Mysterious UDP Stream in My Hotel @ 2023-02-25

Hotel Guest on Reverse Engineering A Mysterious UDP Stream in My Hotel @ 2023-02-25

Vince on Reverse Engineering A Mysterious UDP Stream in My Hotel @ 2023-02-25

JW on Reverse Engineering A Mysterious UDP Stream in My Hotel @ 2023-02-24

Yomom on Reverse Engineering A Mysterious UDP Stream in My Hotel @ 2023-02-24

Guest on Reverse Engineering A Mysterious UDP Stream in My Hotel @ 2023-02-24

yo ss ef on Reverse Engineering A Mysterious UDP Stream in My Hotel @ 2023-02-24

Guest on Reverse Engineering A Mysterious UDP Stream in My Hotel @ 2023-02-24

This page is valid HTML. Click to validate.

It's not actually valid? Send me an email.

Have you seen the log?