

# Defeating PlayStation 5 Network Encryption

Aapo Oksman - Juurin Oy

aapo (oksman)

founder @ Juurin Oy

- IoT cybersecurity consulting
  - IoT / devices
  - cryptography
  - network protocols

bug bounty hunter

vulnerability researcher



I wasn't always a hacker

# I wasn't always a hacker

- I love playing around with computers

# I wasn't always a hacker

- I love playing around with computers
- I love setting up a home network

# I wasn't always a hacker

- I love playing around with computers
- I love setting up a home network
- I love tinkering with devices

# I wasn't always a hacker

- I love playing around with computers
- I love setting up a home network
- I love tinkering with devices
- I love taking things apart

# I wasn't always a hacker

- I love playing around with computers
- I love setting up a home network
- I love tinkering with devices
- I love taking things apart
- I love fixing things



# I wasn't always a hacker

- I love playing around with computers
  - I love setting up a home network
  - I love tinkering with devices
  - I love taking things apart
  - I love fixing things
- 
- I was always a hacker?

# me & cyber security go way back



what makes IoT so special for me?

# what makes IoT so special for me?

- IoT = computers

# what makes IoT so special for me?

- IoT = computers
- IoT = networks

# what makes IoT so special for me?

- IoT = computers
- IoT = networks
- IoT = devices

# what makes IoT so special for me?

- IoT = computers
- IoT = networks
- IoT = devices
- IoT = cheap enough to take apart

# what makes IoT so special for me?

- IoT = computers
- IoT = networks
- IoT = devices
- IoT = cheap enough to take apart
- IoT = simple to enough to fix



# what makes IoT so special for me?

- IoT = computers
- IoT = networks
- IoT = devices
- IoT = cheap enough to take apart
- IoT = simple to enough to fix

IoT = very hackable

# what makes IoT so special for me?

- IoT = computers
- IoT = networks
- IoT = devices
- IoT = cheap enough to take apart
- IoT = simple to enough to fix

IoT = very hackable

IoT = Internet of Things = devices communicating over networks

# working with (network) protocols

- transferring data from one computer to another through a physical connection



# working with (network) protocols

- transferring data from one computer to another through a physical connection
- IoT = sending sensitive data over the network
  - attacker in the middle



# working with (network) protocols

- transferring data from one computer to another through a physical connection
- IoT = sending sensitive data over the network
  - attacker in the middle
  - encryption!



how to encrypt network data?

how to encrypt network data?

TLS



the S in HTTPS

# how to encrypt network data?

## TLS

- connect to a remote computer and exchange encryption keys



# how to encrypt network data?

## TLS

- connect to a remote computer and exchange encryption keys
- verify the identity of the other computer

# how to encrypt network data?

## TLS

- connect to a remote computer and exchange encryption keys
- verify the identity of the other computer
- send any data through the encrypted connection

# how to encrypt network data?

## TLS

- connect to a remote computer and exchange encryption keys
- verify the identity of the other computer
- send any data through the encrypted connection

TLS is a de-facto encryption standard and a proven technology

# how to encrypt network data?

## TLS

- connect to a remote computer and exchange encryption keys
- verify the identity of the other computer
- send any data through the encrypted connection

TLS is a de-facto encryption standard and a proven technology

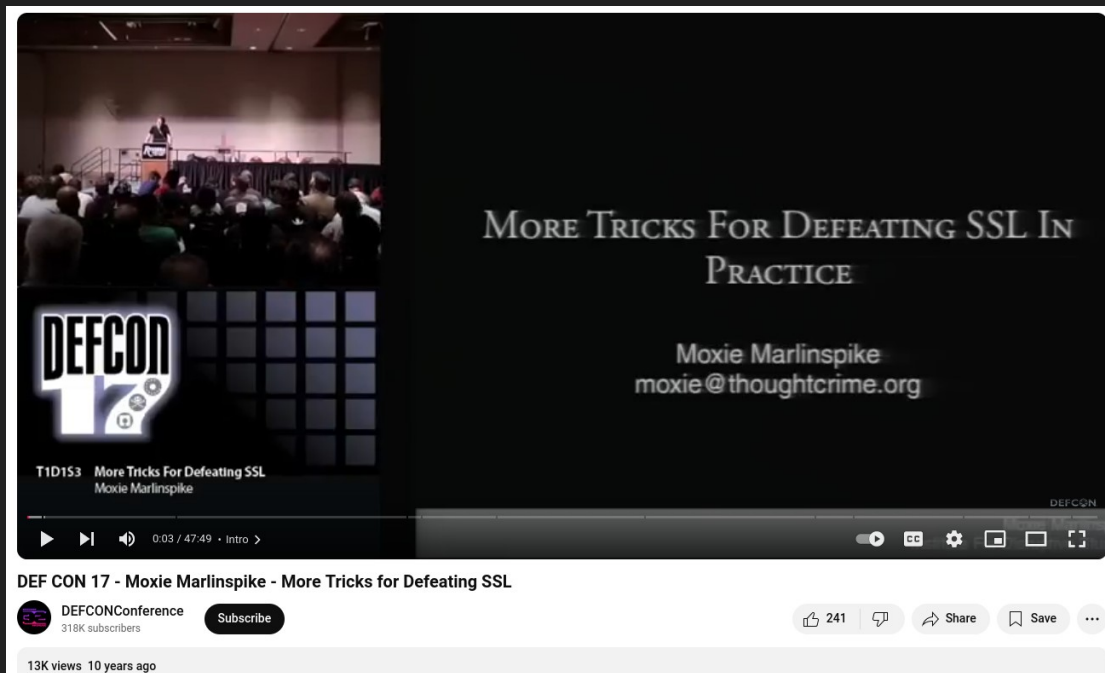
could I somehow hack it?

# how to attack TLS

- DEF CON

# how to attack TLS

- DEF CON
  - Moxie Marlinspike
- ^ released  
multiple TLS  
vulnerabilities  
ages ago

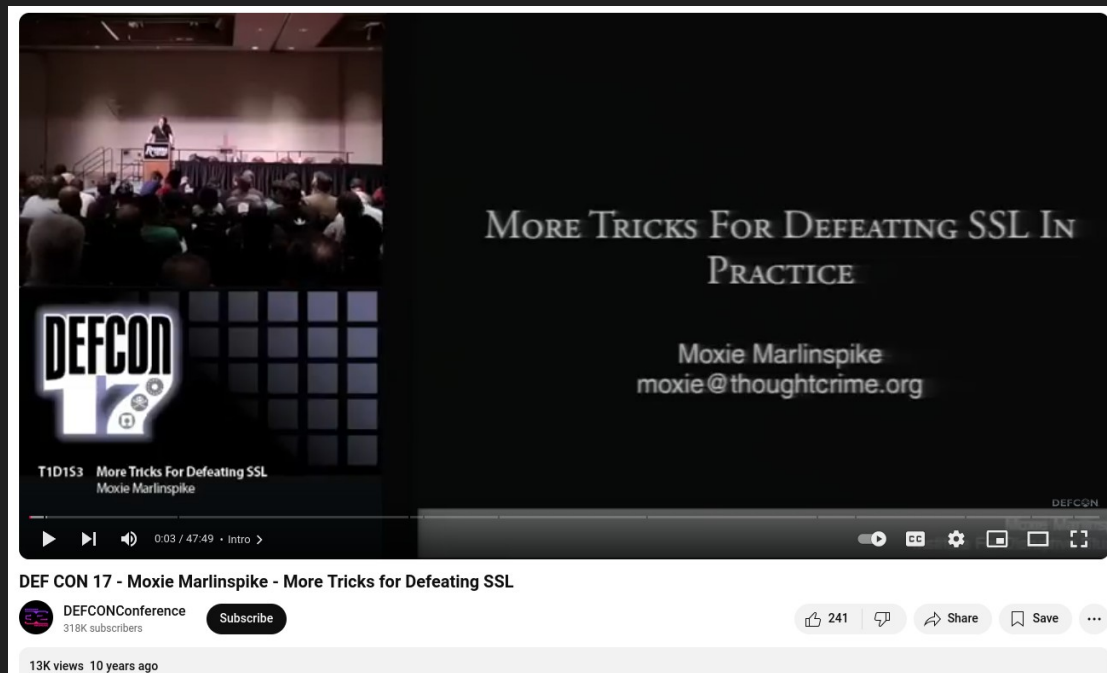


The image shows a YouTube video player interface. The video content is a presentation slide with a dark background. On the left side of the slide, there is a logo for 'DEF CON 17' with a gear icon. The main text on the slide reads 'MORE TRICKS FOR DEFEATING SSL IN PRACTICE' in a serif font. Below this, the speaker's name 'Moxie Marlinspike' and email 'moxie@thoughtcrime.org' are listed. The video player shows the video title 'DEF CON 17 - Moxie Marlinspike - More Tricks for Defeating SSL', the channel name 'DEFCONConference' with 318K subscribers, and a 'Subscribe' button. The video has 13K views and was uploaded 10 years ago. The video progress bar shows 0:03 / 47:49.

# how to attack TLS

- DEF CON
- Moxie Marlinspike
  - ^ released multiple TLS vulnerabilities ages ago

can these still work?



The image shows a YouTube video player interface. The video title is "DEF CON 17 - Moxie Marlinspike - More Tricks for Defeating SSL". The video content shows a stage presentation with a slide titled "MORE TRICKS FOR DEFEATING SSL IN PRACTICE" by Moxie Marlinspike, with the email address moxie@thoughtcrime.org. The video player shows a progress bar at 0:03 / 47:49. Below the video, the channel name "DEFCONConference" is visible with 318K subscribers and a "Subscribe" button. Engagement metrics include 13K views, 241 likes, and a share button. The video was uploaded 10 years ago.

# bug bounties

- I've spent a lot of time looking at IoT devices



# bug bounties

- I've spent a lot of time looking at IoT devices
  - I've spent a lot of time looking at TLS

# bug bounties

- I've spent a lot of time looking at IoT devices
  - I've spent a lot of time looking at TLS
- found so many issues using decades old techniques

# bug bounties

- I've spent a lot of time looking at IoT devices
  - I've spent a lot of time looking at TLS
- found so many issues using decades old techniques
  - why?

# bug bounties

- I've spent a lot of time looking at IoT devices
  - I've spent a lot of time looking at TLS
- found so many issues using decades old techniques
  - why?
    - no tools!

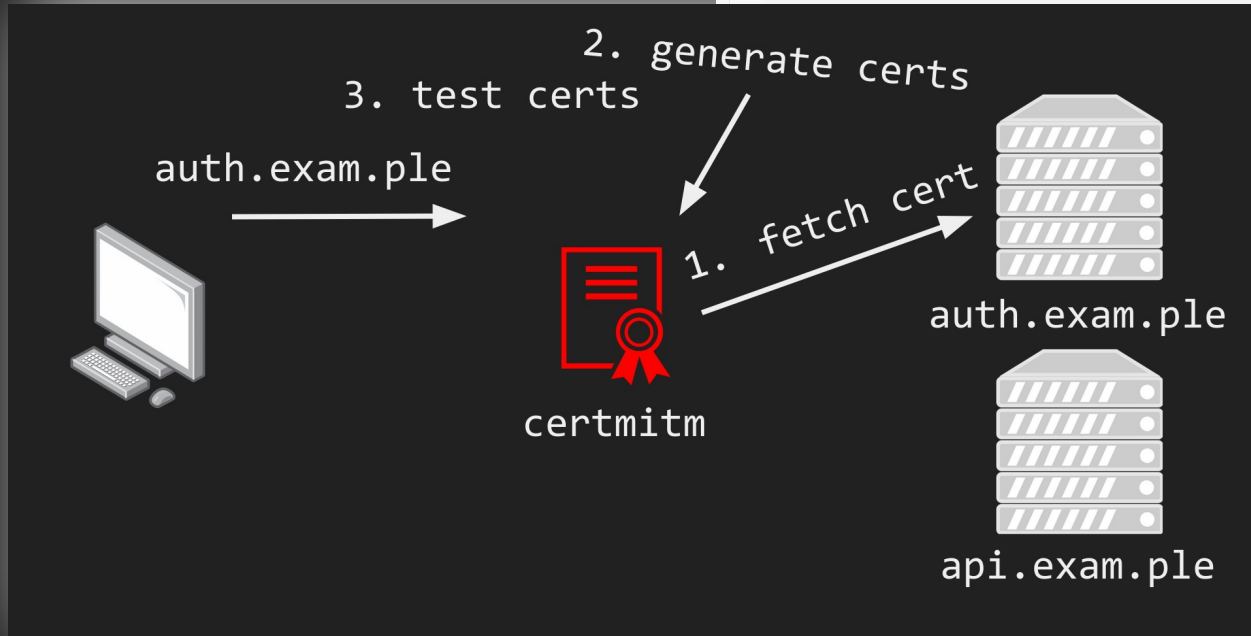
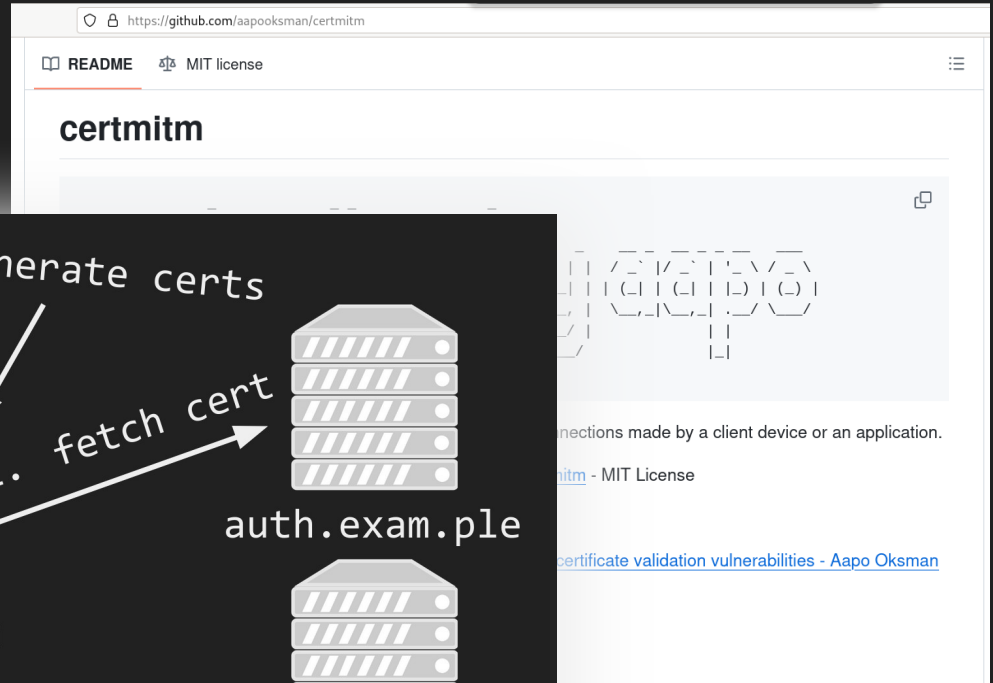
# bug bounties

- I've spent a lot of time looking at IoT devices
  - I've spent a lot of time looking at TLS
- found so many issues using decades old techniques
  - why?
    - no tools!
- started creating certmitm
  - based on TLS attacks previously shown at DEF CON

# bug bounties

- I've spent a lot of time looking at IoT devices
  - I've spent a lot of time looking at TLS
- found so many issues using decades old techniques
  - why?
    - no tools!
- started creating certmitm
  - based on TLS attacks previously shown at DEF CON
  - tested against bug bounty targets
  - gradually improved usability

# certmitm



# vulnerabilities with certmitm

- ~200 vulnerable applications found on Android, iOS, Windows, Mac, IoT etc.
- ~100 known 0-days currently
- over \$200,000 in bug bounties



# vulnerabilities with certmitm

- ~200 vulnerable applications found on Android, iOS, Windows, Mac, IoT etc.
- ~100 known 0-days currently
- over \$200,000 in bug bounties
- more vulnerabilities found every week

# vulnerabilities with certmitm

- ~200 vulnerable applications found on Android, iOS, Windows, Mac, IoT etc.
- ~100 known 0-days currently
- over \$200,000 in bug bounties
- more vulnerabilities found every week
- mostly implementation issues

# vulnerabilities with certmitm

- ~200 vulnerable applications found on Android, iOS, Windows, Mac, IoT etc.
- ~100 known 0-days currently
- over \$200,000 in bug bounties
- more vulnerabilities found every week
- mostly implementation issues
  - certificate validation is disabled by developer
  - TLS library APIs are used incorrectly

# vulnerabilities with certmitm

- ~200 vulnerable applications found on Android, iOS, Windows, Mac, IoT etc.
- ~100 known 0-days currently
- over \$200,000 in bug bounties
- more vulnerabilities found every week
- mostly implementation issues
  - certificate validation is disabled by developer
  - TLS library APIs are used incorrectly
- TLS libraries themselves seem to work well

# Video

- “for a brief time you could have your own certificate and you could sign anything with your certificate”
- “but this was a long time ago”
- “we want secure connections why would we not want secure connections”
- “browsers want secure connections and they are checking the certificates”
- “the problems are in the libraries or how you use them”
- “and the libraries currently have gotten some work so you can use the libraries securely nowadays”
- “currently the libraries work quite well”
- “there are some problems but not that much”

“currently the libraries work quite well”

## SSLSniff Documentation

Daniel Choi, Sumin Kim

### Usages for SSLSniff

1. Authority Mode: SSLSniff signs certificates dynamically using the passed in certificate
  - b. Using a Leaf Node Certificate as a Certificate Authority
    - i. We need a Browser that didn't implement basic constraints, probably a browser before 2002
    - ii. *“This mode is also useful for exploiting implementations that do not properly verify BasicConstraints, as any valid leaf node certificate could be used instead of a CA cert.”*

# Video

- “what is to stop me from doing this?”
- “creating another certificate for some other website and signing it with my leaf certificate”

“currently the libraries work quite well”

- that is mostly the case



“currently the libraries work quite well”

- that is mostly the case
- however, past problems tend to repeat

“currently the libraries work quite well”

- that is mostly the case
- however, past problems tend to repeat
  - thorough testing is cheap with automation

“currently the libraries work quite well”

- that is mostly the case
- however, past problems tend to repeat
  - thorough testing is cheap with automation
- certmitm includes checks against bad TLS libraries

certmitm is ready for DEF CON

certmitm is ready for DEF CON

- DEF CON = demos!

# certmitm is ready for DEF CON

- DEF CON = demos!
- found a vulnerability in a PS5 game with certmitm ages ago

# certmitm is ready for DEF CON

- DEF CON = demos!
- found a vulnerability in a PS5 game with certmitm ages ago
- I do not own a PS5

# certmitm is ready for DEF CON

- DEF CON = demos!
- found a vulnerability in a PS5 game with certmitm ages ago
- I do not own a PS5
- loaned a PS5 from a friend a week before DEF CON and started to record the demo



# certmitm is ready for DEF CON

- DEF CON = demos!
- found a vulnerability in a PS5 game with certmitm ages ago
- I do not own a PS5
- loaned a PS5 from a friend a week before DEF CON and started to record the demo

... and something strange happened

```
aapo@treasure:~/mitmlogs/*/*.bin (Fri Aug 4 16:00:55 2023) [8.582520]
Host: telemetry-console.api.playstation.com
User-Agent: libhttp/7.60 (PlayStation 5)
Connection: Keep-Alive
Content-Length: 1856
HTTP/1.1 200 OK
POST /api/telemetry/v1/publish/telemetry/telemetry/ HTTP/1.1
Cookie: _abck=CFB0D462EEB0A451E4C097101C93B21~-1-YAAQnIVJF2G9wbuJAAQAKP+iwAr96R6VJ4B1cvaILDldg/Ehy5CDA+ocxr7nffilrAxJAS3HNNLArZewC5fOFmpjyVfi6q1DzDnSwQWeaopbLJbQw/Bj9DJY96/YatvjCaWlbyppqI0h8bjemGUvKXCBk2XhEbaPoY5Lq1DqkxJEfjs6ifkUHmv7XNIw6qRywwhItxwhMuriuzkhWPNBidotBDmMoLav8RH843v69mbu+C9wsXKc2M6iKw9jJIGSDHV263ChLQzYAP5lkzXDYVcNoFj//BwakEyQjU8BbgS0ZHNBM1YntUnfiyGT3zaJv6a1NeUpEGx+vgJWQEd3o3QyN9uNd5I4mjczLEljYjyq61NwEr5kt1Yx3P2mtI0sr/jHfr8QBFumt7KunggjmhbtgDgZ10NZCGh1hk65kM588m~-1~-1; bm_sz=B25CBA3C866CED49A1AC8A7C9B0FA56-YAAQnIVJF1G0wbuJAAQ1r0iwBTEVv2PsoxMpez6QHC9Y71Vxh9ygnx47dhNxdJ1E1qkuB1lKka51yMryFgn8ZSKWXTPquUsmWgYAT+Mo8aF9mPiraCYJ8zyAKzcc+cxRO6QP1SUK/nuugd0U15fgzFJzL+ZHWF2e9rST090h/JNvWABImXfu0TykYUvAmQ7yXQB1+0xBky2h6Dw+9oE5U6LAgYib1CGmDK1Raxe9H0VjvnmqM3jzBMZ2oEEPOT4x9j9CJ1eSegMXfLKK66oEuQvNcQuyX4jT9199UKweYsnVM41rjgBfuterFmWfhckLlYP0IXCeID/KeRheaG4BRDUt37q04qrPfgZwKXyhdeBu0U1qWjW10BKv1Zr-4405059-3291204
Content-Encoding: gzip
x-np-environment: p1-np
eventName: loadtime
Content-Type: application/json; charset=utf-8
Host: telemetry-console.api.playstation.com
User-Agent: libhttp/7.60 (PlayStation 5)
Connection: Keep-Alive
Content-Length: 975
00] */mitmlogs/*/*.bin
```



```
aapo@treasure: ~ | certmitm
aapo@treasure: ~ | certmitm
aapo@treasure: ~ | certmitm
aapo@treasure: ~/Dropbox/BugBounty/certmitm/ps5

316V2tZvRzd1MS5eUvTnZTVzFEtVrHtPlWm1EaEtYmFtaERTU2pFQ5IsTswAnVudF9pZC18ImY40WIX0TQ5LWU30GGntNGFjMy040Q4LWNI2GE1NGY3YzLIMSIsImrJwN1fawQ101jJzTJmZTgyZC0yYzllLTr1NTgtOMN1Z1jNTImYzNH0DZ1NDU1LCJkZxZp2VfDh1wZS16
11B7N5IsImVud19pc3fMawQ101IyNTY1LCJleHA10jE20TExNTc1MDQsImdyW50k3R5eGU101Jzc29YfDg9rZwa1LCJpYXQ10jE20TExNTc1MDQsImLx2W00wXkIjpeYwxz25w1eKNZiJoIaHR0cH06L9ndXR0LmfY291bnQuc29ueS5jB20v1IiwanRp1JoIzJz0W15NMMtYzR
mN100ZTEZLThkYjctYTA2ZTKwMzFkMwEzIiwbgVgnYxfV291bnRyesT6IhZJiIwibG9jYxlltJoIzktRkklLCJydwUaw5N529uIjoIUFMI1Iwic3lzdGtX3NkA192ZJzaw9UjJoIMHgwHzYwMdwAwMwMDAwMBAxiIwic3lzdGtX3ZlcnNpb2410iZ1JlYmMCAwMA1LC1c2
Vyx2RldmlZV9pcCI6Ij0LjI1MCA4NDY0U0CisInzIic1I01JlIjQcNkX2pjmldV8C0ebIEkREDcFmQ5a1Z2Jh5hQk2GgR4RQU-j-12IR1cQQn9vAK810TUvXUSzuffnq81BLKkcT0xnXvQGF1Bk3VetXEHXCyc-0v8Fu-gR_tYrythIzprw30yG_UttV4sJpAJL00Hkwm8JVly
2yr28H61f57rj0D-t0VhyrMoa9jpujXHI_FajLuq10DPeozNlpMxZ-DHt1z1yNKaE8F8z_EECpetz51AmA71atpmrkf-f56wju-n9v0TAGYInV5vY258UabymZ3F4JqJGNfVvfyNyuMozrXUMDNM1A2LJUawwp_P-PQ-WpGb-B1h06MQskZbRmhuokU0iDEI7ep5yKk3EKCE1s5
5094ndY8suIR3_k8Be14nG5Ej1cnLagvH1hb0u0grXwen4oy5JR9ErFlxIztIqPj0ujgy5yb0ct56Z122ud0CwZ1ZvJKF4d0u8ehIYePgZtEzj56jvsx10D3mGh0Qm55T777jF86jv\Xn-PSN-PROTOCOL-VERSION: 2.\1\X-PSN-KEEP-ALIVE-STATUS-TYPE: 1z
V0Vr0
CRITICAL - 19.0.0.144; smetrics.aem.playstation.com:443 for test @eal cert as CA: tlstest_2023-07-02 = b'GET /b/s/snepdrglobal/1/gctxhr-4.15.0/s02204678904047AQB=1&ndh=1&pF=1&ce=UTF-8&pageName=ps53AmfX3Awelcom
&ch=ps53AmfX3Awelcom&server=undefined&events=evnt1%2Cevnt103&vid=ac8ce1e7ca38305740eccc0707c2415e9cc52dc99d8cc68eb24b1fd28cebd7e&ts=2023-08-04T123A583A32.377Z&r=ag=&t=4%2F7k2F202328153A583A42205%20-1
80&v1=0x3Ddpagename&c1=ac8ce1e7ca38305740eccc0707c2415e9cc52dc99d8cc68eb24b1fd28cebd7e&h1=0x3Ddpagename&v2=zz-und&c2=0x3Dv2&v3=guest&c3=0x3Dv3&v4=invalid&c4=0x3Dv4&c7=0x3Dv7&c14=1f41b8f6-a64d-477d-9135-57a634f46a
44&c45=0x3Dv90&v47=ac8ce1e7ca38305740eccc0707c2415e9cc52dc99d8cc68eb24b1fd28cebd7e&ac47=0x3Dv47&c55=0x3Dv55&v58=invalid&v60=invalid&v66=welcome&c66=0x3Dv66&c68=0x3Dv68&c69=2023-08-04T123A583A32.377Z&c71=0x3Dv7
1&v72=ps53Amf&c72=0x3Dv72&v74=wf&3A7.0.0x2B27593&c74=0x3Dv74&v75=ac8ce1e7ca38305740eccc0707c2415e9cc52dc99d8cc68eb24b1fd28cebd7e&c75=0x3Dv75&v79=en-gb&v81=7.0.2x2B285063A0.0.0&v82=7.60.00.07-00.00.00.0.1X3A13
0930X3Anormal&v91=client&3Anavigation&v95=1000&v132=welcome&v151=not%20logged&v20in&v156=7.0.0x2B936&v173=647&v174=20&AQE=1 HTTP/1.1\XnCookie: _abck=CFB0D462EEB0A451E4C097101C93B21~-1-YAAQnIVJF1S1wbuJAAQAL61wA
p5TzplKHdsFQeNfRQGFzri-naaRTUEX91Z4FTpu5J+nKUBBU/+q2NB8mYl/acIBtCuts2mkMnk/g0E4xpW+vc+GCR/iryPsV4kkR1YRpG7zxFLCAAG81B+NQ+omdMk7KZghNPuncJ/IpNAY/d839svrQcnpvvhfkx+/VKzpo5f8yzt3W10ukU0itVgk9V02xar5h7q9QEPXP3pM
POM2j0LX4YGEjQ5j0GvLlthMZ3qvd+np/nFktJ0J80Ux0UeGqB1W7AHHG0LS5ly+hdMqnos5EU0bmmTwd9Uz79yZjXkatsc52ufctGEGEjZVicsAJnl4RdrGabi1d9p96FywH775QIQ0bc1X36jFMGI-EZUTNK/Uhs0H5Q92+VAGrYQsgI4gEXRPU--1~-1~-1; bm_sz=B25
CBA3C866CED49A1AC8A7C9B0FA56-YAAQnIVJF1G0wbuJAAQ1r0iwBTEVv2PsoxMpez6QHC9Y71Vxh9ygnx47dhNxdJ1E1qkuB1lKka51yMryFgn8ZSKWXTPquUsmWgYAT+Mo8aF9mPiraCYJ8zyAKzcc+cxRO6QP1SUK/nuugd0U15fgzFJzL+ZHWF2e9rST090h/JNvWABIm
Xfu0TykYUvAmQ7yXQB1+0xBky2h6Dw+9oE5U6LAgYib1CGmDK1Raxe9H0VjvnmqM3jzBMZ2oEEPOT4x9j9CJ1eSegMXfLKK66oEuQvNcQuyX4jT9199UKweYsnVM41rjgBfuterFmWfhckLlYP0IXCeID/KeRheaG4BRDUt37q04qrPfgZwKXyhdeBu0U1qWjW10BKv1Zr-440
5059-3291204\XnHost: smetrics.aem.playstation.com\XnUser-Agent: libhttp/7.60 (PlayStation 5)\XnConnection: Keep-Alive\Xn'
```

# Ooops!

- certmitm could decrypt most TLS connections made by PS4 and PS5 consoles

# Ooops!

- certmitm could decrypt most TLS connections made by PS4 and PS5 consoles
  - passwords, account tokens, game data, PS operating system data

# Ooops!

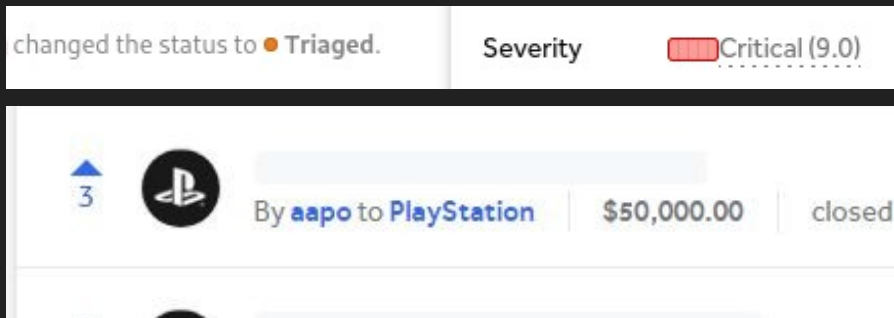
- certmitm could decrypt most TLS connections made by PS4 and PS5 consoles
  - passwords, account tokens, game data, PS operating system data
  - account takeovers, cheats, remote jailbreaks etc.

# Ooops!

- certmitm could decrypt most TLS connections made by PS4 and PS5 consoles
  - passwords, account tokens, game data, PS operating system data
  - account takeovers, cheats, remote jailbreaks etc.
  - some connections only trust internal Sony CAs -> secure :(

# Ooops!

- certmitm could decrypt most TLS connections made by PS4 and PS5 consoles
  - passwords, account tokens, game data, PS operating system data
  - account takeovers, cheats, remote jailbreaks etc.
  - some connections only trust internal Sony CAs -> secure :(
- critical vulnerability



# but what exactly happened?

- turns out that the libhttp library of PS4 and PS5 does not check for CA=true basicConstraint when making TLS connections



## but what exactly happened?

- turns out that the libhttp library of PS4 and PS5 does not check for CA=true basicConstraint when making TLS connections
- basically every PS5 TLS connection can be decrypted

# but what exactly happened?

- turns out that the libhttp library of PS4 and PS5 does not check for CA=true basicConstraint when making TLS connections
- basically every PS5 TLS connection can be decrypted
  - some connections only trust Sony CA's and are secure
  - most connections accept Let's Encrypt as CA

# but what exactly happened?

- turns out that the libhttp library of PS4 and PS5 does not check for CA=true basicConstraint when making TLS connections
- basically every PS5 TLS connection can be decrypted
  - some connections only trust Sony CA's and are secure
  - most connections accept Let's Encrypt as CA
    - however, they also allow you to issue certificates even without CA=true
    - Let's Encrypt -> certmitm.com -> playstation.net

# but what exactly happened?

- turns out that the libhttp library of PS4 and PS5 does not check for CA=true basicConstraint when making TLS connections
- basically every PS5 TLS connection can be decrypted
  - some connections only trust Sony CA's and are secure
  - most connections accept Let's Encrypt as CA
    - however, they also allow you to issue certificates even without CA=true
    - Let's Encrypt -> certmitm.com -> playstation.net
- certmitm "real\_cert\_CA" testcase
  - the only time I've observed this vulnerability in the wild

# quick fix & forced update by Sony

- reported to PlayStation HackerOne program on August 4th 2023

# quick fix & forced update by Sony

- reported to PlayStation HackerOne program on August 4th 2023
- triaged by the program on August 7th

# quick fix & forced update by Sony

- reported to PlayStation HackerOne program on August 4th 2023
- triaged by the program on August 7th
- August 11th:
  - “We would like to let you know that the vulnerability you reported has been patched via system software version 10.71 (PS4) and 23.01-07.61.00 (PS5) which were publicly released.”

# quick fix & forced update by Sony

- reported to PlayStation HackerOne program on August 4th 2023
- triaged by the program on August 7th
- August 11th:
  - "We would like to let you know that the vulnerability you reported has been patched via system software version 10.71 (PS4) and 23.01-07.61.00 (PS5) which were publicly released."
  - also: the PS5 refuses to operate if it is not updated to at least 7.61



# quick fix & forced update by Sony

- reported to PlayStation HackerOne program on August 4th 2023
- triaged by the program on August 7th
- August 11th:
  - "We would like to let you know that the vulnerability you reported has been patched via system software version 10.71 (PS4) and 23.01-07.61.00 (PS5) which were publicly released."
  - also: the PS5 refuses to operate if it is not updated to at least 7.61
- August 11th: certmitm is released at DEF CON 31

# Video

- “telling them that you’re going to DEF CON to talk about the tool really motivates developers to create fixes”

aapo@treasure: ~/Dropbox/BugBounty/certmitm

aapo@treasure: ~/Dropbox/BugBounty/certmitm

```

INFO - 10.0.0.144: 23.201.43.160:443:ps5.np.playstation.net for test replaced_key = [SSL: TLSV1_ALERT_UN
KNOWN_CA] tlsv1 alert unknown ca (_ssl.c:992)
INFO - 10.0.0.144: 23.201.43.160:443:ps5.np.playstation.net for test real_cert_tlstest_2023-07-02 = [SSL
: SSLV3_ALERT_BAD_CERTIFICATE] sslv3 alert bad certificate (_ssl.c:992)
INFO - 10.0.0.144: 23.61.218.182:443:fuk01.ps5.update.playstation.net for test replaced_key = [SSL: TLSV
1_ALERT_UNKNOWN_CA] tlsv1 alert unknown ca (_ssl.c:992)
INFO - 10.0.0.144: 23.61.218.182:443:fuk01.ps5.update.playstation.net for test self_signed = [SSL: TLSV1
_ALERT_UNKNOWN_CA] tlsv1 alert unknown ca (_ssl.c:992)
INFO - 10.0.0.144: 23.201.43.160:443:ps5.np.playstation.net for test real_cert_CA_tlstest_2023-07-02 = [
SSL: TLSV1_ALERT_UNKNOWN_CA] tlsv1 alert unknown ca (_ssl.c:992)
INFO - 10.0.0.144: 23.61.215.244:443:envelope2.np.dl.playstation.net for test real_cert_tlstest_2023-07-
02 = [SSL: SSLV3_ALERT_HANDSHAKE_FAILURE] sslv3 alert handshake failure (_ssl.c:992)
INFO - 10.0.0.144: 23.61.218.182:443:fuk01.ps5.update.playstation.net for test real_cert_tlstest_2023-07-
02 = [SSL: SSLV3_ALERT_BAD_CERTIFICATE] sslv3 alert bad certificate (_ssl.c:992)
INFO - 10.0.0.144: 23.61.215.244:443:envelope2.np.dl.playstation.net for test real_cert_CA_tlstest_2023-
07-02 = [SSL: SSLV3_ALERT_HANDSHAKE_FAILURE] sslv3 alert handshake failure (_ssl.c:992)
INFO - 10.0.0.144: 23.61.218.182:443:fuk01.ps5.update.playstation.net for test real_cert_CA_tlstest_2023
-07-02 = [SSL: TLSV1_ALERT_UNKNOWN_CA] tlsv1 alert unknown ca (_ssl.c:992)
INFO - 10.0.0.144: 92.123.135.81:443:sgst.prod.dl.playstation.net for test self_signed = [SSL: TLSV1_ALE
RT_UNKNOWN_CA] tlsv1 alert unknown ca (_ssl.c:992)
INFO - 10.0.0.144: 92.123.135.81:443:sgst.prod.dl.playstation.net for test replaced_key = [SSL: TLSV1_AL
ERT_UNKNOWN_CA] tlsv1 alert unknown ca (_ssl.c:992)
INFO - 10.0.0.144: 92.123.135.81:443:sgst.prod.dl.playstation.net for test real_cert_tlstest_2023-07-02
 = [SSL: SSLV3_ALERT_BAD_CERTIFICATE] sslv3 alert bad certificate (_ssl.c:992)
INFO - 10.0.0.144: 92.123.135.81:443:sgst.prod.dl.playstation.net for test real_cert_CA_tlstest_2023-07-
02 = [SSL: TLSV1_ALERT_UNKNOWN_CA] tlsv1 alert unknown ca (_ssl.c:992)
INFO - 10.0.0.144: 95.101.145.161:443:urlconfig.api.playstation.com for test self_signed = TLS/SSL connec
tion has been closed (EOF) (_ssl.c:992)
INFO - 10.0.0.144: 95.101.144.10:443:qgve.dl.playstation.net for test self_signed = [SSL: TLSV1_ALERT_UN
KNOWN_CA] tlsv1 alert unknown ca (_ssl.c:992)
INFO - 10.0.0.144: 95.101.144.10:443:qgve.dl.playstation.net for test replaced_key = [SSL: TLSV1_ALERT_U
NKNOWN_CA] tlsv1 alert unknown ca (_ssl.c:992)
INFO - 10.0.0.144: 95.101.144.10:443:qgve.dl.playstation.net for test real_cert_tlstest_2023-07-02 = [SS
L: SSLV3_ALERT_BAD_CERTIFICATE] sslv3 alert bad certificate (_ssl.c:992)
INFO - 10.0.0.144: 95.101.144.10:443:qgve.dl.playstation.net for test real_cert_CA_tlstest_2023-07-02 =
 [SSL: TLSV1_ALERT_UNKNOWN_CA] tlsv1 alert unknown ca (_ssl.c:992)
INFO - 10.0.0.144: 95.101.145.217:443:telemetry-console.api.playstation.com for test self_signed = [SSL:
TLSV1_ALERT_UNKNOWN_CA] tlsv1 alert unknown ca (_ssl.c:992)
INFO - 10.0.0.144: 95.101.145.217:443:telemetry-console.api.playstation.com for test replaced_key = [SSL
: TLSV1_ALERT_UNKNOWN_CA] tlsv1 alert unknown ca (_ssl.c:992)
INFO - 10.0.0.144: 95.101.145.217:443:telemetry-console.api.playstation.com for test real_cert_tlstest_2
023-07-02 = [SSL: SSLV3_ALERT_BAD_CERTIFICATE] sslv3 alert bad certificate (_ssl.c:992)
INFO - 10.0.0.144: 95.101.145.217:443:telemetry-console.api.playstation.com for test real_cert_CA_tlstes
t_2023-07-02 = [SSL: TLSV1_ALERT_UNKNOWN_CA] tlsv1 alert unknown ca (_ssl.c:992)

```

Games

Media

System software  
The system software update is  
complete.

Logged in to your PS5.



ASTRO'S PLAYROOM

# ASTRO'S PLAYROOM

Discover the future of play with intergalactic platforming  
hero - ASTRO!

Play Game



Friends Who Play

# aftermath



Wololo.net

<https://wololo.net> > 2024/01/13 > pl... · [Käännä tämä sivu](#) ⋮

## PlayStation just awarded a never-seen-before \$50K bounty ...

13.1.2024 — A hack report was just closed a few hours ago on **PlayStation's** HackerOne account, with a **bounty of \$50,000** awarded to security researcher **Aapo** ...

# aftermath



Wololo.net

<https://wololo.net> › 2024/01/13 › pl... · [Käännä tämä sivu](#) ⋮



Wccftech

<https://wccftech.com> › playstation-... · [Käännä tämä sivu](#) ⋮

## A PlayStation Console Critical Vulnerability Was Recently ...

19.1.2024 — **Aapo Oksman** reported yesterday on X/Twitter that Sony recently closed a HackerOne bug bounty ticket they submitted to their program last year.

# aftermath



Wololo.net

<https://wololo.net> > 2024/01/13 > pl... · [Käännä tämä sivu](#) ⋮



Reddit

<https://www.reddit.com> > comments > 50k\_on\_hackero... ⋮

## 50K On HackerOne Playstation?!?!?!? : r/ps5homebrew

13.1.2024 — There was. But in talking about new hypervisor being disclosed at a higher firmware to sony. Maybe I'm just optimistic.

[14 vastausta](#) · Paras vastaus: [Spoiler Alert Dont Update](#)

# aftermath



PSXHAX

<https://www.psxhax.com> > tags > 5... · [Käännä tämä sivu](#) ⋮

## \$50k h1 playstation bounty

Recently cybersecurity researcher **Aapo** was awarded a \$50,000.00 Bug **Bounty** for his **PlayStation** Hacktivity Report as part of Sony's HackerOne Program, ...



bugbounty.com.au

<https://bugbounty.com.au> > viewtopic · [Käännä tämä sivu](#) ⋮

## A PlayStation Console Critical Vulnerability Was ... - Bug Bounty

**Aapo** Oksman reported yesterday on X/Twitter that Sony recently closed a HackerOne bug **bounty** ... \$50,000, a value that is reserved only for the most critical ...

# aftermath



X

[https://twitter.com > status](https://twitter.com/status) · Käännä tämä sivu

## After Time X on X: "PlayStation 5 Console Jailbreak ETA ...

website reports an whopping **\$50,000 Bug Bounty** payment recently from Sony's **PlayStation** division to the Security Researcher known as "**Aapo**". Since it can ...



YouTube

[https://www.youtube.com > watch](https://www.youtube.com/watch) · Käännä tämä sivu

## #PlayStation Homebrew News (PS4 11.50 Beta, PS5- ...

19.1.2024 — ... **Aapo Oksman** on X: "Recently **Playstation** closed a **HackerOne** bug **bounty** ticket I submitted to the their bug **bounty** program last year. This ...



# aftermath



X

<https://twitter.com/status> · [Käännä tämä sivu](#) ⋮



大人のためのゲーム講座

<https://gamegaz.com> > ... · [Käännä tämä sivu](#) ⋮

## aapo氏が5万ドル報奨金を得たPS5の脆弱性 [hardwear.io](https://hardwear.io)で ...

19.1.2024 — HackeroneのPlayStation部門で、aapo氏が過去最高額の5万ドルの報奨金を得た脆弱性をセキュリティカンファレンスで発表する意向を表明しました。

## #PlayStation Homebrew News (PS4 11.50 Beta, PS5- ...

19.1.2024 — ... Aapo Oksman on X: "Recently Playstation closed a HackerOne bug bounty ticket I submitted to the their bug bounty program last year. This ...

# aftermath

As pointed out by [Al-Azif on Twitter](#), this is most likely related to the TLS mitm talk by Aapo at Defcon 31, back in August last year. The video below showcases how certmitm, his MitM automated test tool, operates (PS5 section at roughly 31 minutes in the video).

The MitM framework developed for this research, and used by Aapo in his presentation, can be found on his github at the link below.

# aftermath

As pointed out by [Al-Azif on Twitter](#), this is most likely related to the TLS mitm talk by Aapo at Defcon 31, back in August last year. The video below showcases how certmitm, his MitM automated test tool, operates (PS5 section at roughly 31 minutes in the video).

The MitM framework developed for this research, and used by Aapo in his presentation, can be found on his github at the link below.

“why no jailbreak?”

# aftermath

So yeah, \$50k sounds like a lot, but you have to either be lucky or output a God's level of work.

# aftermath

So yeah, \$50k sounds like a lot, but you have to either be lucky or output a God's level of work.

my methodology:

- analyze the attack surface
- watch a lot of DEF CON videos
  - employ known attacks
  - exploit common weaknesses
- profit

# lessons learned

- test for everything
  - past problems tend to repeat

# lessons learned

- test for everything
  - past problems tend to repeat
- test against everything
  - being a huge platform like PlayStation does not make you immune to stupid mistakes

# lessons learned

- test for everything
  - past problems tend to repeat
- test against everything
  - being a huge platform like PlayStation does not make you immune to mistakes
- automate what has not yet been automated
  - certmitm exploits 10-20 year old vulnerabilities



# thank you

find certmitm @

<https://github.com/AapoOksman/certmitm>

find me @

- cybersecurity conferences!
- [aapo.oksman@juurin.fi](mailto:aapo.oksman@juurin.fi)
- [linkedin.com/in/AapoOksman](https://www.linkedin.com/in/AapoOksman)
- aapo @ bug bounty