EECS 388: Embedded Systems

11. Security

Heechul Yun

Agenda

- Embedded systems security

Internet of Things (IoT)

- IoT ~= **Internet** connected embedded systems
- “Internet is evil and wants to kill you”

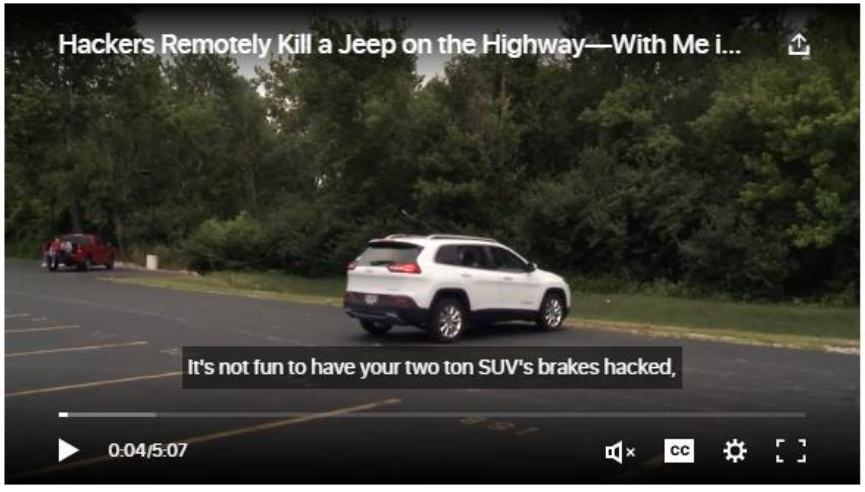
Remote Attack on Jeep (2015)

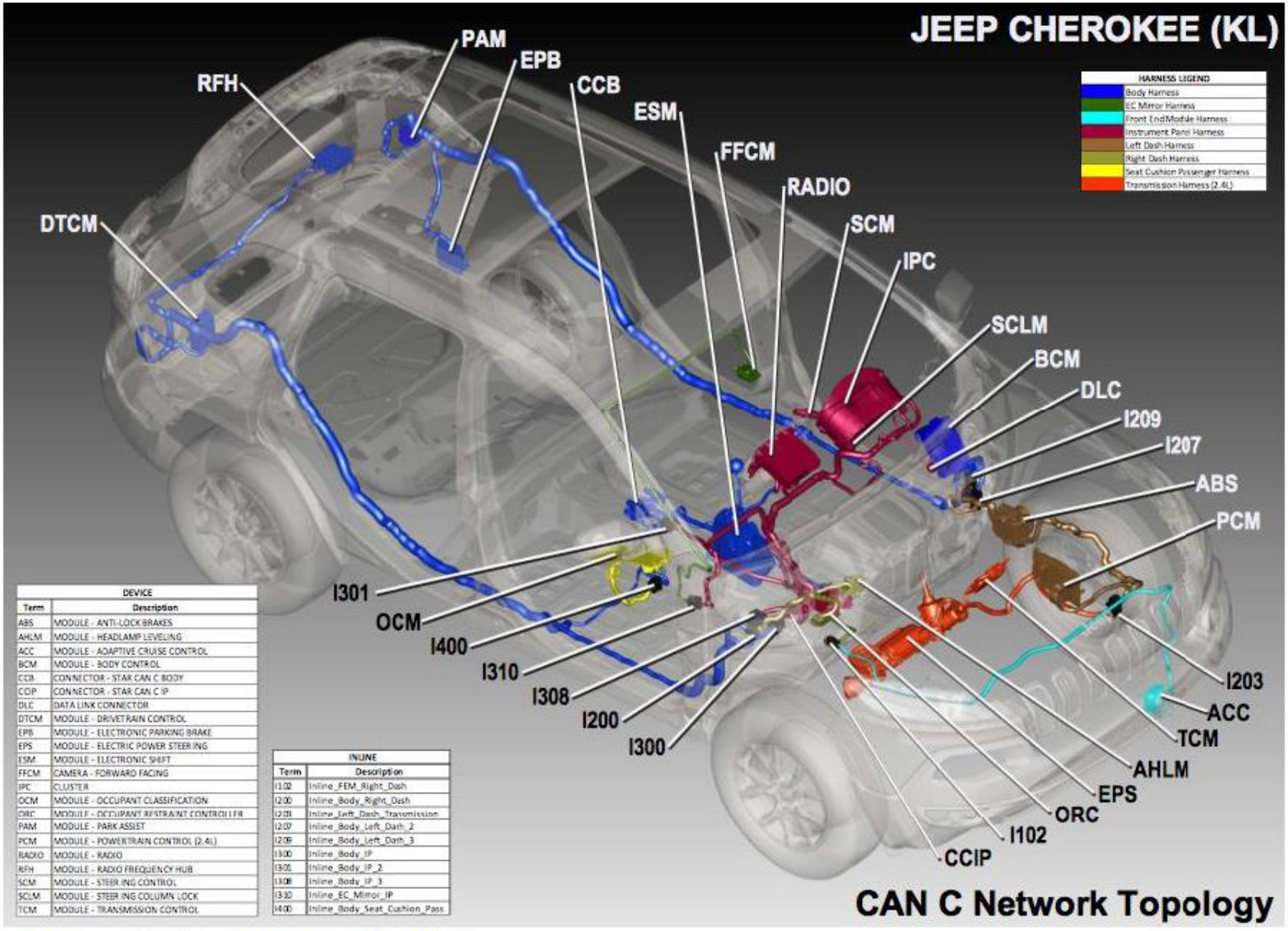
- Able to remotely (via cellular network) control steering, brake, and other critical functions via the car's infotainment system

ANDY GREENBERG SECURITY 07.21.15 06:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/





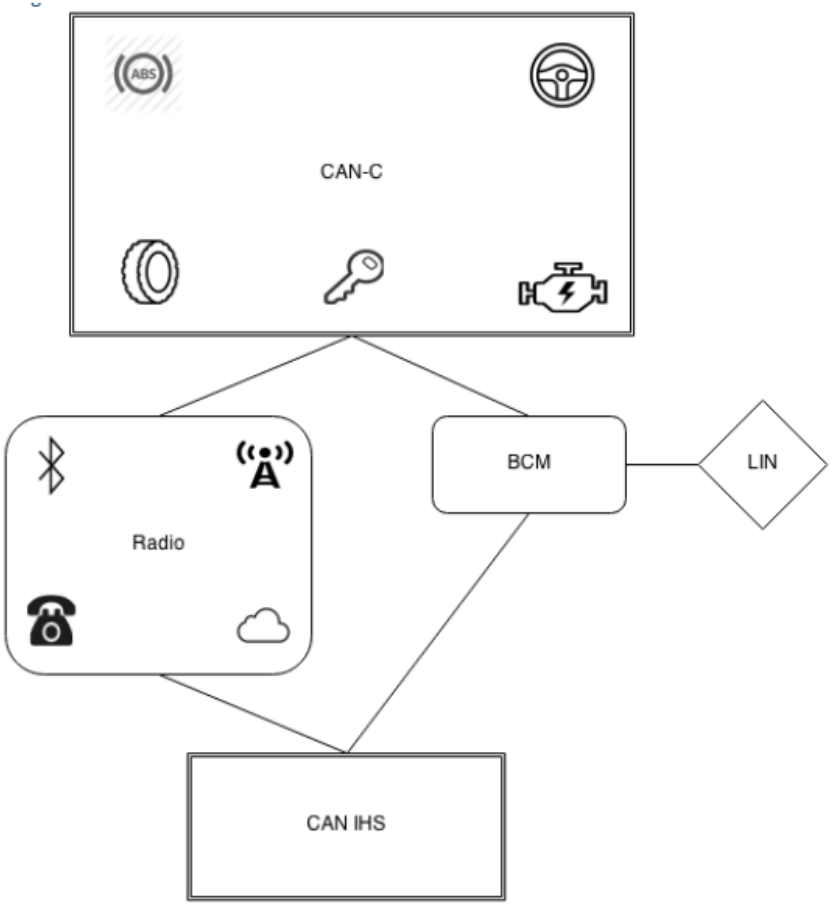
CAN-C Network – 2014 Jeep Cherokee

C. Miller and C. Valasek, “A Survey of Remote Automotive Attack Surfaces”

Remote Attack Surfaces

"…As cars move into the future, they are being more connected with features normally found in desktop computers like apps and even web browsers.

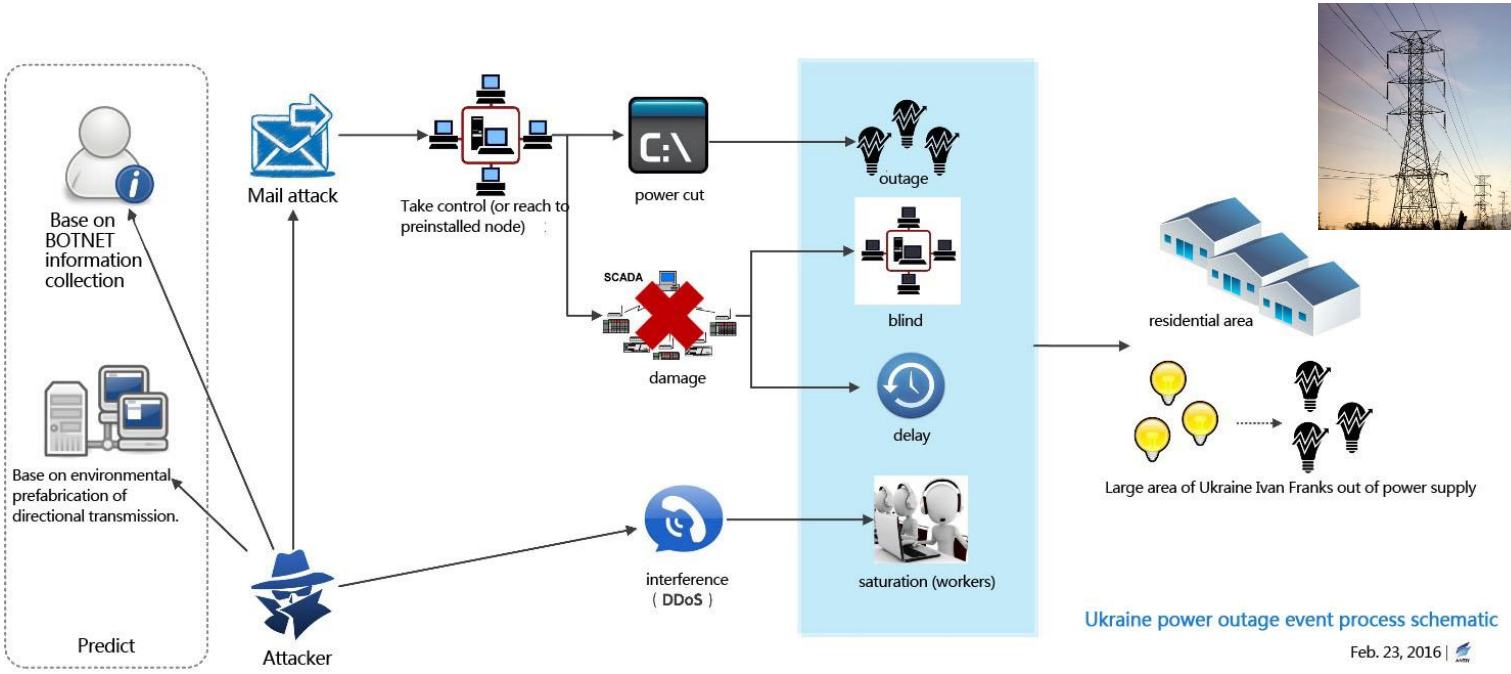
The 2014 Jeep Cherokee even has a Wi-Fi hotspot with open ports (when not using encryption)…"



C. Miller and C. Valasek, "A Survey of Remote Automotive Attack Surfaces"

Ukraine Power Grid Attack (2016)

- Attack on SCADA control network of a power grid in Ukraine, causing blackout on 80K users.

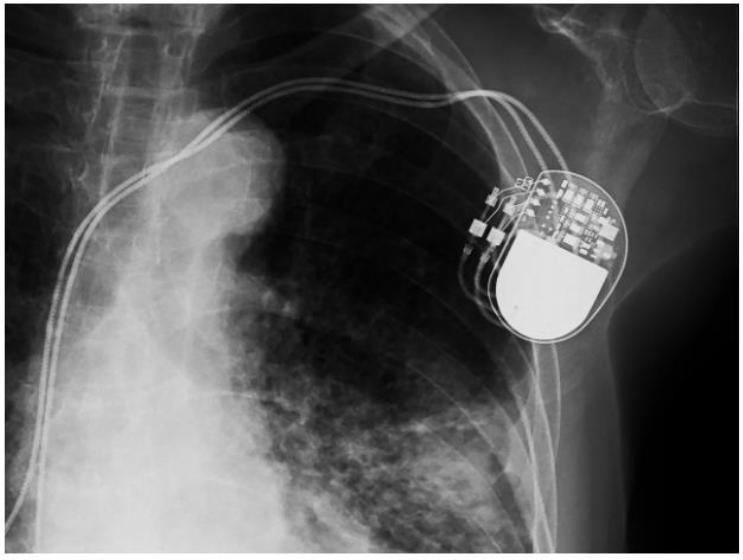


https://www.antiy.net/p/comprehensive-analysis-report-on-ukraine-power-system-attacks/

Pacemaker Hack (2017,2018)

A New Pacemaker Hack Puts Malware Directly on the Device

Researchers at the Black Hat security conference will demonstrate a new pacemaker-hacking technique that can add or withhold shocks at will.



CHOO CHIN/GETTY IMAGES

https://www.wired.com/story/pacemaker-hack-malware-black-hat/

Hacking risk leads to recall of 500,000 pacemakers due to patient death fears

FDA overseeing crucial firmware update in US to patch security holes and prevent hijacking of pacemakers implanted in half a million people

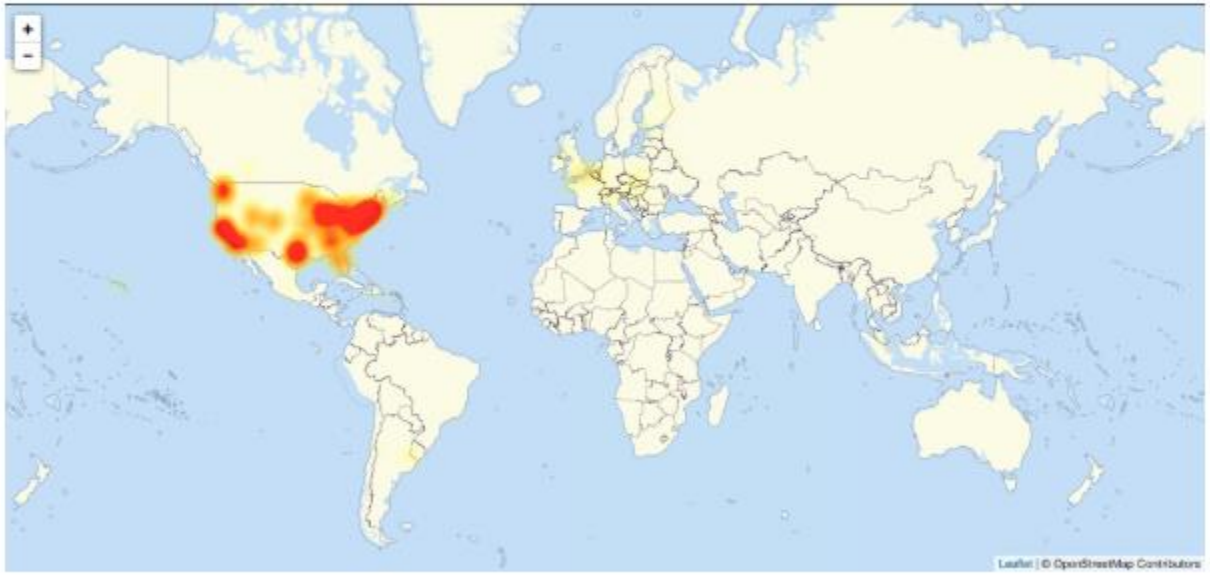
▲ Abbott / St Jude Medical's Accent MRI pacemaker, one of the affected devices that had to be recalled. Photograph: Abbott / St Jude Medical

https://www.theguardian.com/technology/2017/aug/31/hacking-risk-recall-pacemakers-patient-death-fears-fda-firmware-update

Mirai Bot DDoS Attack (2016)

The New York Times

Hackers Used New Weapons to Disrupt Major Websites Across U.S.



A map of the areas experiencing problems, as of Friday afternoon, according to downdetector.com.

New Weapons Used in Attack On the Internet

By NICOLE PERLROTH

SAN FRANCISCO — Major websites were inaccessible to people across wide swaths of the United States on Friday after a company that manages crucial parts of the internet's infrastructure said it was under attack.

Users reported sporadic problems reaching several websites, including Twitter, Netflix, Spotify, Airbnb, Reddit, Etsy, SoundCloud and The New York Times.

The company, Dyn, whose servers monitor and reroute internet traffic, said it began experiencing what security experts called a distributed denial-of-service attack just after 7 a.m. Reports that many sites were inaccessible started on the East Coast, but spread westward in three waves as the day wore on and into the evening.

https://www.nytimes.com/2016/10/22/business/internet-problems-attack.html

The Mirai IoT Botnet

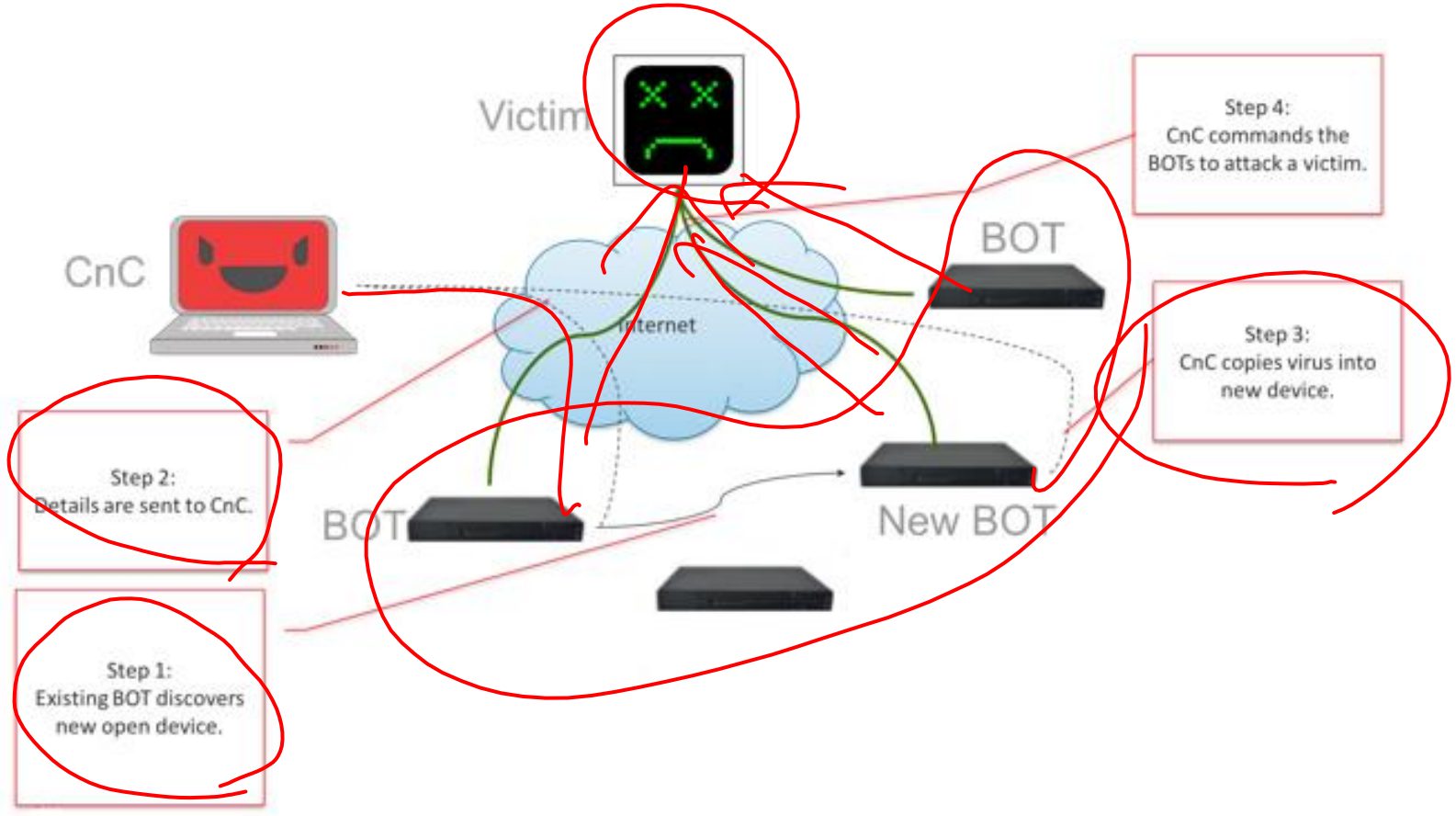


Figure 1 Mirai System

https://www.corero.com/resources/ddos-attack-types/mirai-botnet-ddos-attack

IoT WiFi Attacks (2019)

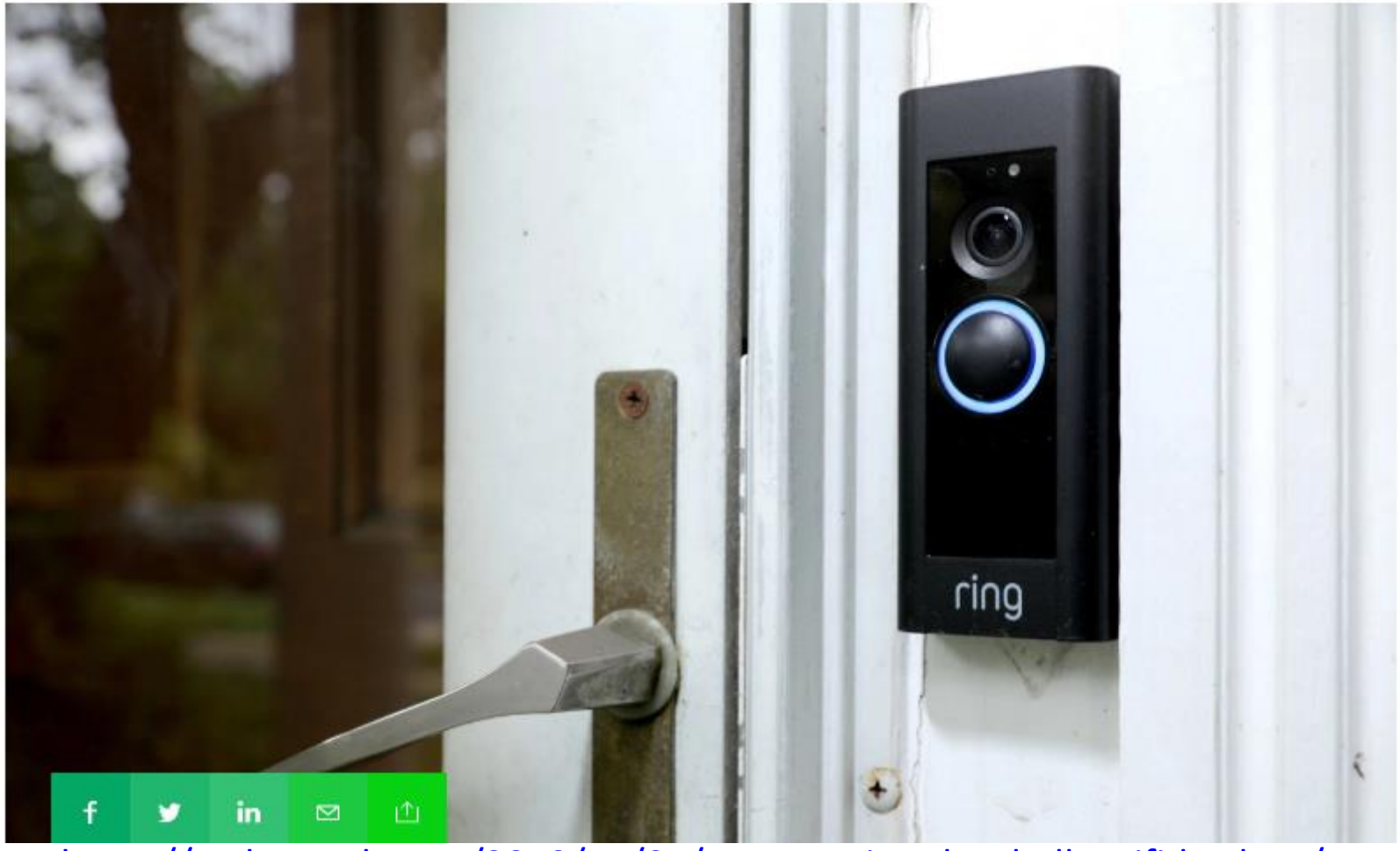
"… These EAP hacks are more troubling, and not just because session hijacking is more dangerous than a crash-DOS scenario. The ESP32 codebase has already been patched against them, but the older ESP8266 SDK has not yet. So as of now, if you're running an ESP8266 on EAP, you're vulnerable. We have no idea how many ESP8266 devices are out there in EAP networks, but we'd really like to see Espressif patch up this hole anyway. "

https://hackaday.com/2019/09/05/esp8266-and-esp32-wifi-hacked/

Amazon Ring doorbells exposed home Wi-Fi passwords to hackers

Zack Whittaker @zackwhittaker / 8:43 am CST • November 7, 2019

Comment



https://techcrunch.com/2019/11/07/amazon-ring-doorbells-wifi-hackers/

Agenda

- Security attributes
- Threat model
- Software security
- Information flow
- Encryption
- Digital signature and hashing
- SSL/TLS

Security

- What are the attributes of security?

Security Attributes

- Confidentiality
  - Can secret data be leaked?
- Integrity
  - Can the system be modified?
- Availability
  - Can the system function when needed?
- Authenticity
  - Am I interacting with the right person/thing?

System Security

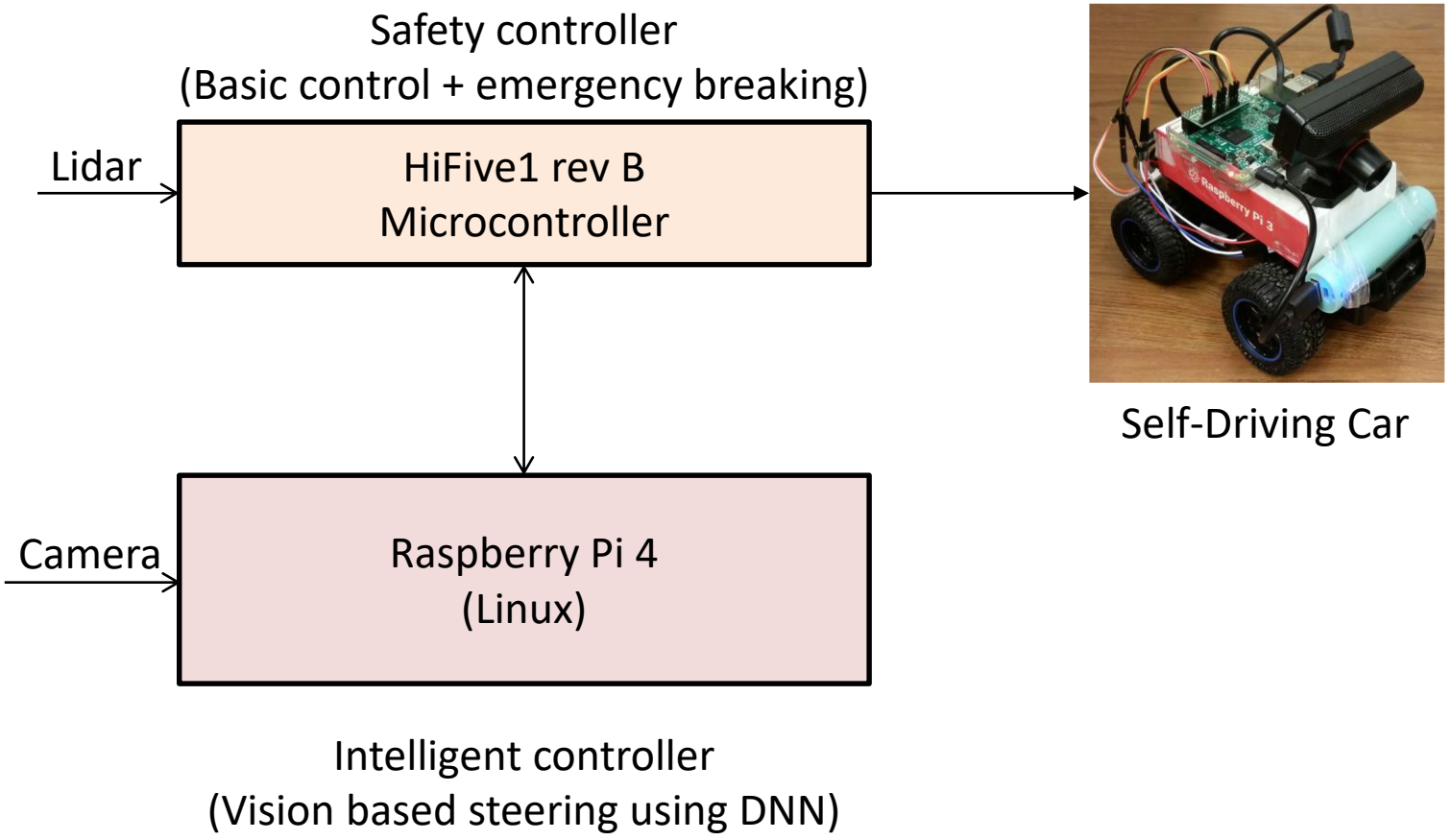
- A system is secure if it is used and accessed as intended under all circumstances
  - Unachievable

- A system security can be determined only in the context of a clear **threat model**

Threat Model

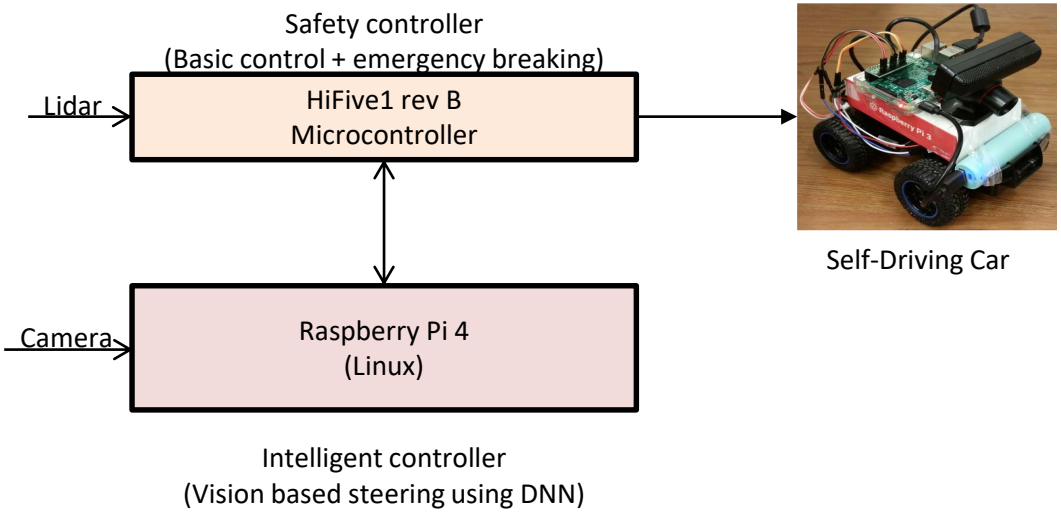
- Attacker's capabilities
  - What we assume the attacker can do
- Examples
  - Has a physical access to the system
  - Has a remote (network) access to the system
  - Can reprogram the software
  - Can eavesdrop the communication
  - …

Is Your Project Secure?



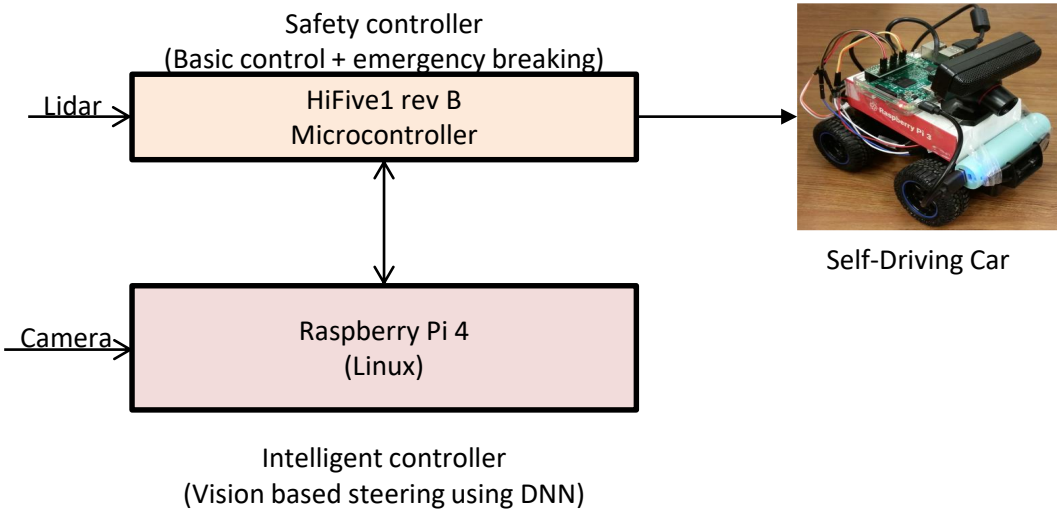
Can't be answered until you define the **threat model**.

Threat Model
(What Attacker Can Do)



- Have remote access to the same WiFi network?
- Have remote login capability to the Pi 4?
- Have physical access to the hardware?

Example Defenses



- Have remote access to the same WiFi network?
  - Encrypt all communications over WiFi (e.g., ssh)
- Have remote login capability to the Pi 4?
  - Don't give the sudo permission, patch bugs in OS, software
- Have physical access to the hardware?
  - Secure boot, remote attestation, encrypt serial communication, …

Memory Safety Vulnerabilities

- Stack overflow
- Heap overflow
- Use after free
- Double free
- Null pointer
- Uninitialized use
- …

Memory Safety Vulnerabilities

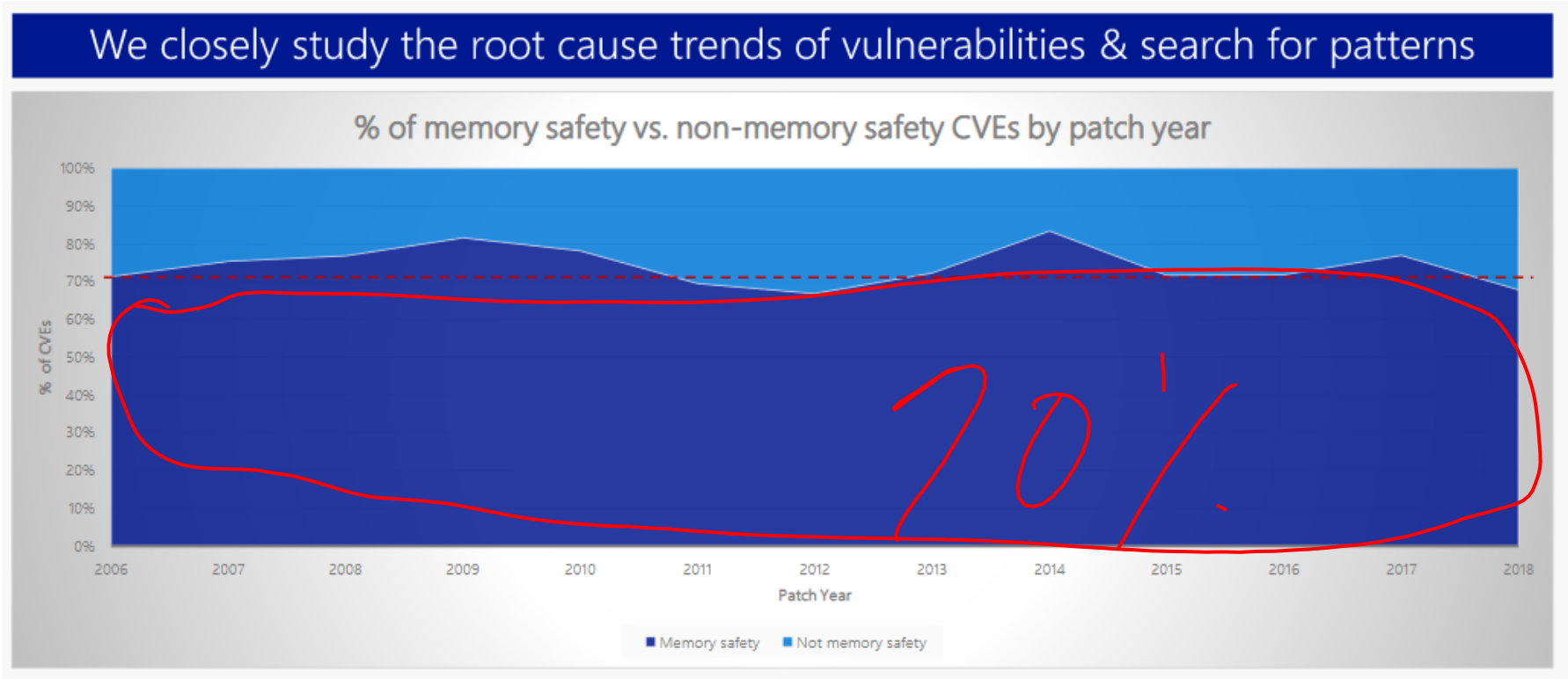


Image source: Matt Miller, Microsoft

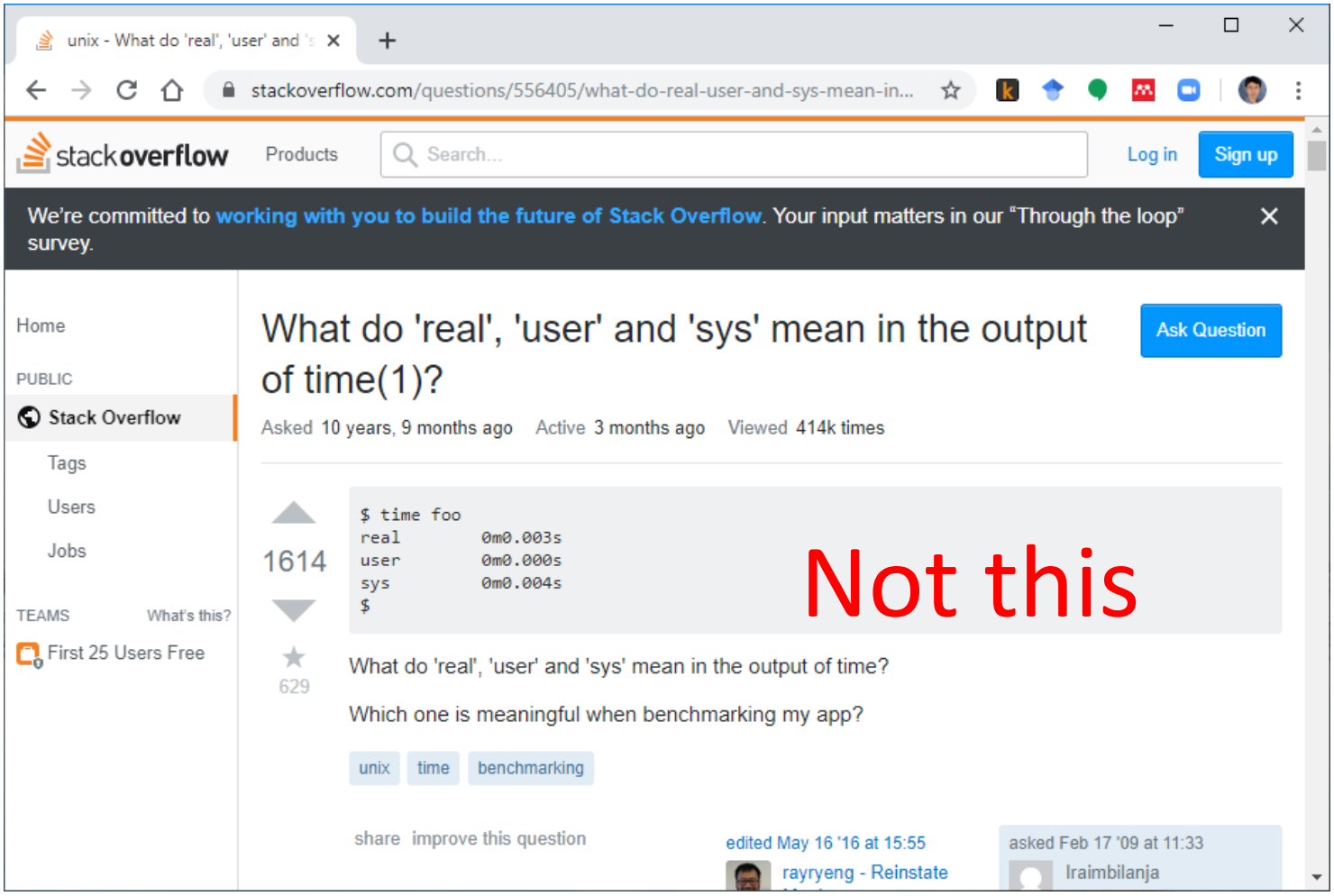
- Account for 70% percent of all Microsoft patches over the past 12 years

https://www.youtube.com/watch?v=PjbGojjnBZQ

Stack/Buffer Overflow

- Overflow either the stack or memory buffers
- Failure to check bounds on inputs, arguments

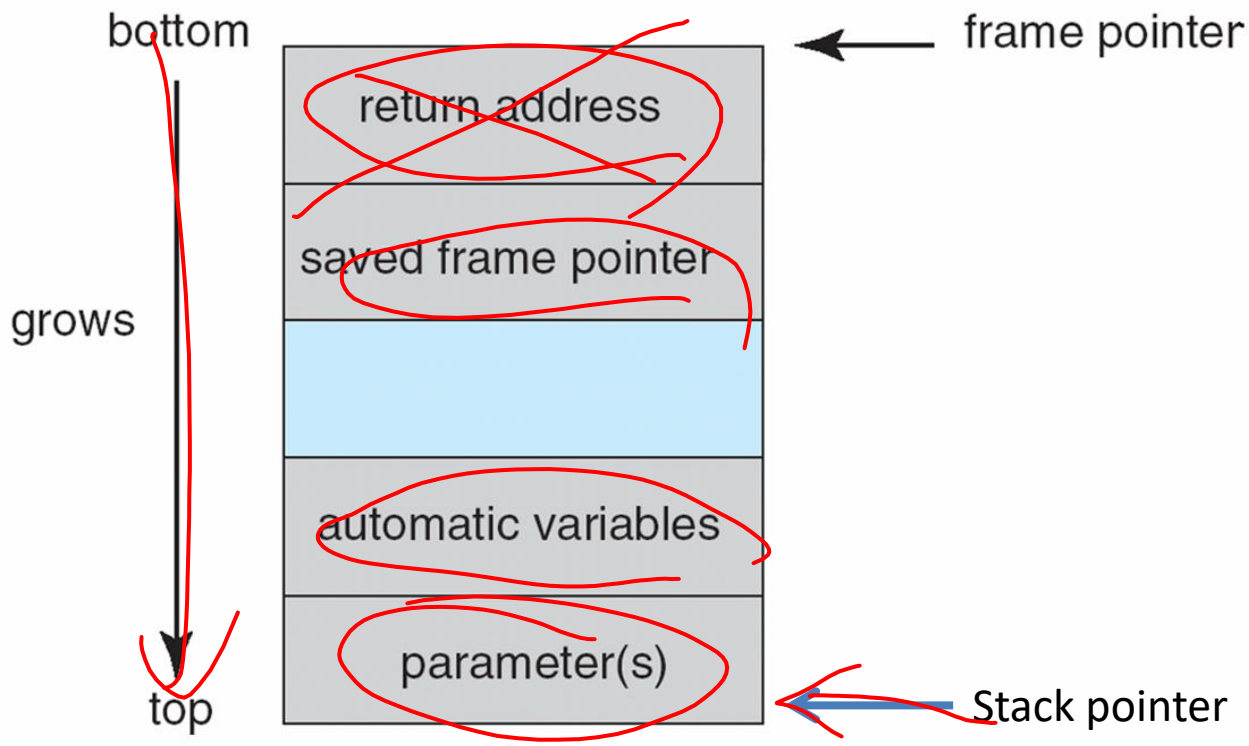
Stack Overflow



Stack Overflow

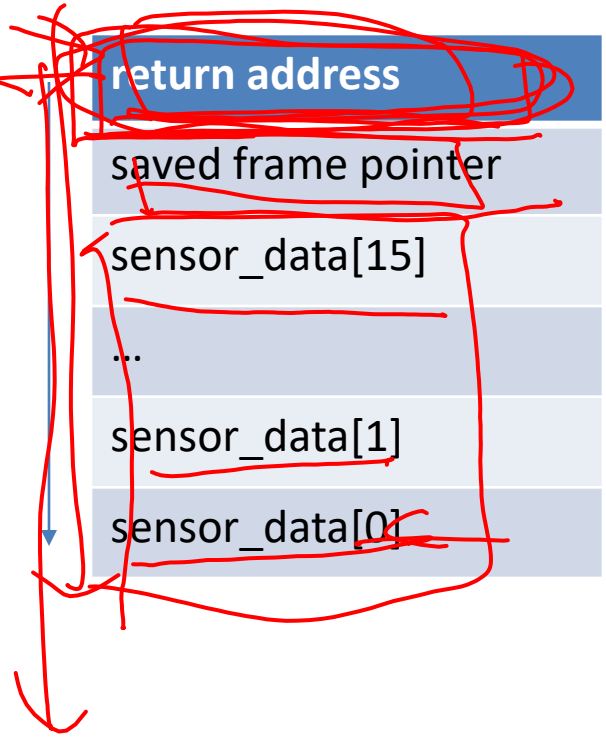
```
1  int sensor_flags[4];
2
3  void process_sensor_data() {
4    int i = 0;
5    char sensor_data[16];
6
7    // more_data returns 1 if there is more data,
8    // and 0 otherwise
9    while(more_data()) {
10     sensor_data[i] = get_next_byte();
11     i++;
12   }
13
14   // some code here that sets sensor_flags
15   // based on the values in sensor_data
16
17   return;
18 }
```

Stack Frame Layout



Stack Overflow

```
1  int sensor_flags[4];
2
3  void process_sensor_data() {
4    int i = 0;
5    char sensor_data[16];
6
7    // more_data returns 1 if there is more data,
8    // and 0 otherwise
9    while(more_data()) {
10     sensor_data[i] = get_next_byte();
11     i++;
12   }
13
14   // some code here that sets sensor_flags
15   // based on the values in sensor_data
16
17   return;
18 }
```



What would happen when more than 16 bytes are received?

Buffer Overflow

```
1  char sensor_data[16];
2  int secret_key;
3
4  void read_sensor_data() {
5    int i = 0;
6
7    // more_data returns 1 if there is more data,
8    // and 0 otherwise
9    while(more_data()) {
10     sensor_data[i] = get_next_byte();
11     i++;
12   }
13
14   return;
15 }
```

What would happen when more than 16 bytes are received?

Use after Free

```c
#include <stdlib.h>
#include <stdio.h>
struct auth{
    char name[32];
    int priv;
};

int main() {
    struct auth *auth_ptr;
    char *service;
    auth_ptr = malloc(sizeof(struct auth));
    free(auth_ptr);
    service = malloc(36);
    printf("[auth = %p, service = %p]\n",
        auth_ptr, service);
    free(service);
    return 0;
}
```

```
$ ./use_after_free
[auth = 0x716010, service = 0x716010]
```

- Freed but uninitialized pointers can be exploited

Linux Kernel: Buffer Overflow

6	CVE-2010-2521 119	DoS Exec Code Overflow	2010-09-07	2012-03-19	10.0	None	Remote	Low	Not required	Complete	Complete	Complete

Multiple buffer overflows in fs/nfsd/nfs4xdr.c in the XDR implementation in the NFS server in the Linux kernel before 2.6.34-rc6 allow remote attackers to cause a denial of service (panic) or possibly execute arbitrary code via a crafted NFSv4 compound WRITE request, related to the read_buf and nfsd4_decode_compound functions.

9	CVE-2009-0065 119	Overflow	2009-01-07	2012-03-19	10.0	Admin	Remote	Low	Not required	Complete	Complete	Complete

Buffer overflow in net/sctp/sm_statefuns.c in the Stream Control Transmission Protocol (sctp) implementation in the Linux kernel before 2.6.28-git8 allows remote attackers to have an unknown impact via an FWD-TSN (aka FORWARD-TSN) chunk with a large stream ID.

10	CVE-2008-5134 119	Overflow	2008-11-18	2012-03-19	10.0	None	Remote	Low	Not required	Complete	Complete	Complete

Buffer overflow in the lbs_process_bss function in drivers/net/wireless/libertas/scan.c in the libertas subsystem in the Linux kernel before 2.6.27.5 allows remote attackers to have an unknown impact via an "invalid beacon/probe response."

11	CVE-2008-3915 119	Overflow	2008-09-10	2012-03-19	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete

Buffer overflow in nfsd in the Linux kernel before 2.6.26.4, when NFSv4 is enabled, allows remote attackers to have an unknown impact via vectors related to decoding an NFSv4 acl.

12	CVE-2008-3496 119	Overflow	2008-08-06	2012-03-19	10.0	None	Remote	Low	Not required	Complete	Complete	Complete

Buffer overflow in format descriptor parsing in the uvc_parse_format function in drivers/media/video/uvc/uvc_driver.c in uvcvideo in the video4linux (V4L) implementation in the Linux kernel before 2.6.26.1 has unknown impact and attack vectors.

13	CVE-2008-1673 119	DoS Exec Code Overflow	2008-06-09	2012-11-26	10.0	None	Remote	Low	Not required	Complete	Complete	Complete

http://www.cvedetails.com/vulnerability-list/vendor_id-33/product_id-47/cvssscoremin-9/cvssscoremax-/Linux-Linux-Kernel.html

Linux Kernel: Use-after-free

drivers/net/wireless/rsi/rsi_91x_usb.c in the Linux kernel through 5.2.9 has a Double Free via crafted USB device traffic (which may be remote via usbip or usbredir).

4	CVE-2019-15292	416		2019-08-21	2019-09-02	10.0	None	Remote	Low	Not required	Complete	Complete	Complete

An issue was discovered in the Linux kernel before 5.0.9. There is a use-after-free in atalk_proc_exit, related to net/appletalk/atalk_proc.c, net/appletalk/ddp.c, and net/appletalk/sysctl_net_atalk.c.

5	CVE-2019-11815	362		2019-05-08	2019-06-07	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete

An issue was discovered in rds_tcp_kill_sock in net/rds/tcp.c in the Linux kernel before 5.0.8. There is a race condition leading to a use-after-free, related to net namespace cleanup.

6	CVE-2019-11811	416		2019-05-07	2019-05-31	10.0	None	Remote	Low	Not required	Complete	Complete	Complete

An issue was discovered in the Linux kernel before 5.0.4. There is a use-after-free upon attempted read access to /proc/ioports after the ipmi_si module is removed, related to drivers/char/ipmi/ipmi_si_intf.c, drivers/char/ipmi/ipmi_si_mem_io.c, and drivers/char/ipmi/ipmi_si_port_io.c.

7	CVE-2019-11683	399	DoS Mem. Corr.	2019-05-02	2019-06-14	10.0	None	Remote	Low	Not required	Complete	Complete	Complete

udp_gro_receive_segment in net/ipv4/udp_offload.c in the Linux kernel 5.x before 5.0.13 allows remote attackers to cause a denial of service (slab-out-of-bounds memory corruption) or possibly have unspecified other impact via UDP packets with a 0 payload, because of mishandling of padded packets, aka the "GRO packet of death" issue.

8	CVE-2019-10125	94		2019-03-27	2019-06-14	10.0	None	Remote	Low	Not required	Complete	Complete	Complete

An issue was discovered in aio_poll() in fs/aio.c in the Linux kernel through 5.0.4. A file may be released by aio_poll_wake() if an expected event is triggered immediately (e.g., by the close of a pair of pipes) after the return of vfs_poll(), and this will cause a use-after-free.

9	CVE-2018-20961	415	DoS	2019-08-07	2019-08-27	10.0	None	Remote	Low	Not required	Complete	Complete	Complete

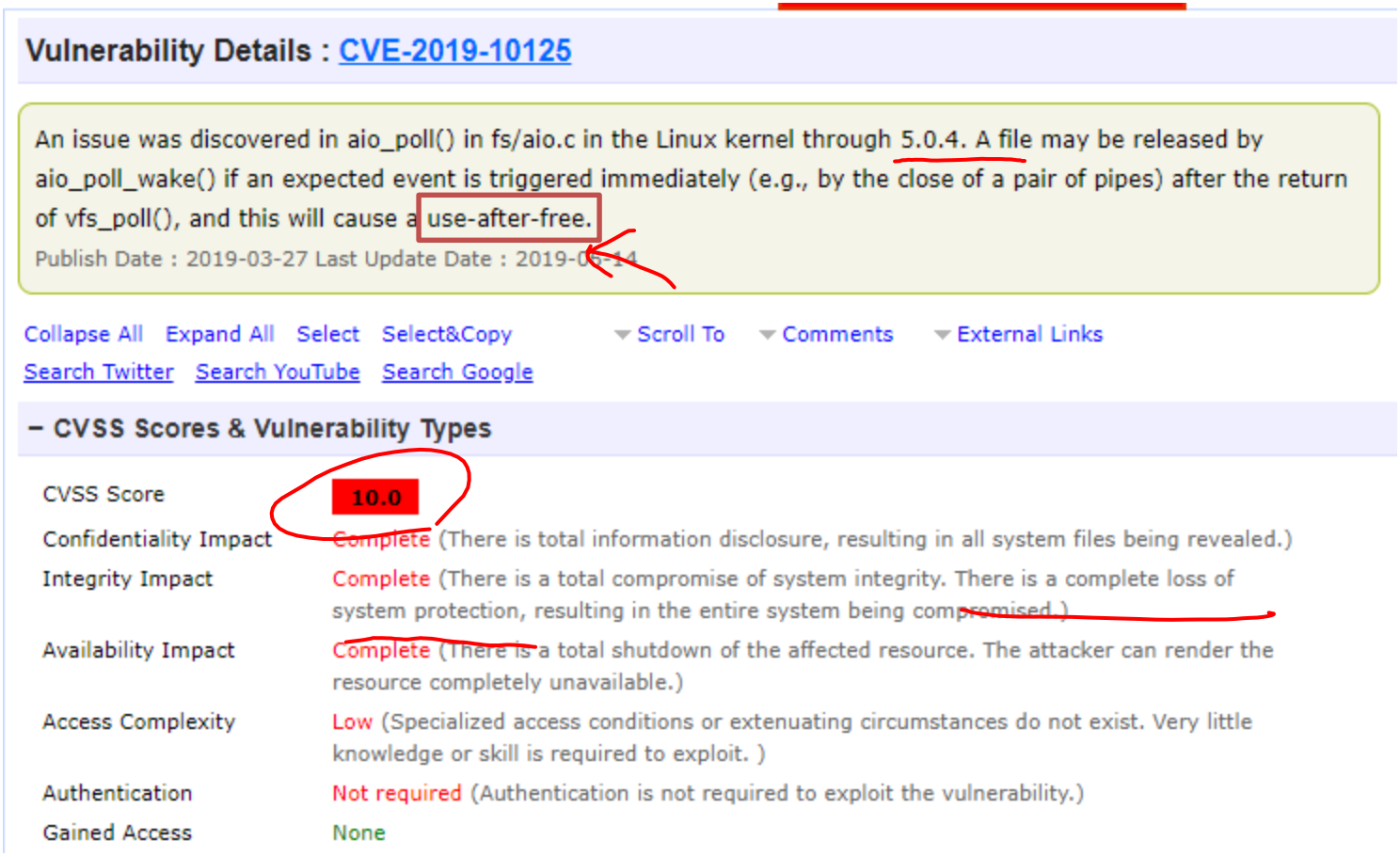
In the Linux kernel before 4.16.4, a double free vulnerability in the f_midi_set_alt function of drivers/usb/gadget/function/f_midi.c in the f_midi driver may allow attackers to cause a denial of service or possibly have unspecified other impact.

10	CVE-2018-20836	416		2019-05-07	2019-05-08	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete

An issue was discovered in the Linux kernel before 4.20. There is a race condition in smp_task_timedout() and smp_task_done() in drivers/scsi/libsas/sas_expander.c, leading to a use-after-free.

http://www.cvedetails.com/vulnerability-list/vendor_id-33/product_id-47/cvssscoremin-9/cvssscoremax-/Linux-Linux-Kernel.html

Linux Kernel: Use-after-free



Vulnerability Details : CVE-2019-10125

An issue was discovered in aio_poll() in fs/aio.c in the Linux kernel through 5.0.4. A file may be released by aio_poll_wake() if an expected event is triggered immediately (e.g., by the close of a pair of pipes) after the return of vfs_poll(), and this will cause a use-after-free.

Publish Date : 2019-03-27 Last Update Date : 2019-05-14

Collapse All Expand All Select Select&Copy Scroll To Comments External Links

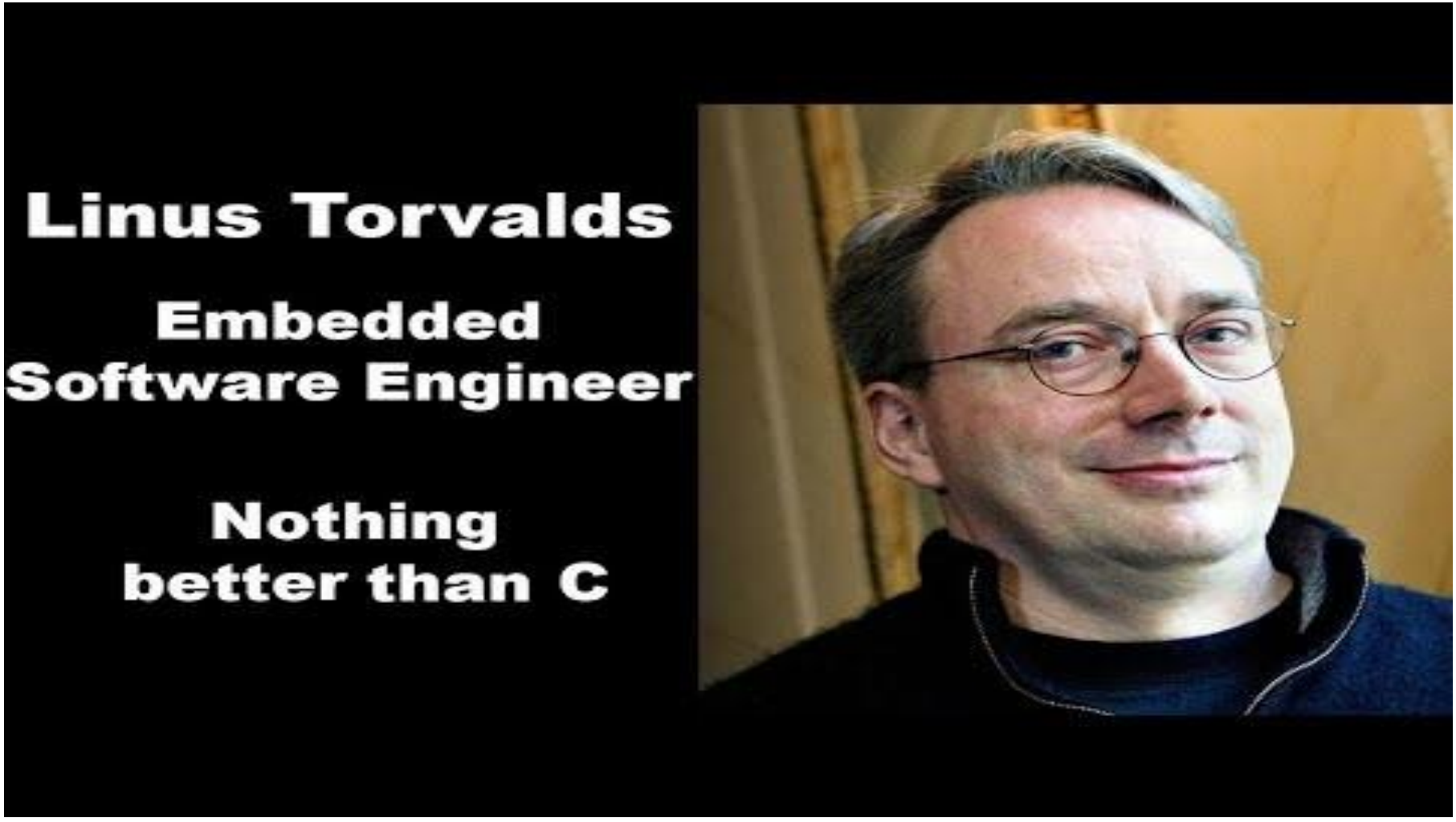
Search Twitter Search YouTube Search Google

– CVSS Scores & Vulnerability Types

CVSS Score	10.0
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None

http://www.cvedetails.com/vulnerability-list/vendor_id-33/product_id-47/cvssscoremin-9/cvssscoremax-/Linux-Linux-Kernel.html

Linus Torvalds: "Nothing better than C"



https://www.youtube.com/watch?v=CYvJPra7Ebk

Recall: C is popular but …

- Why popular?
  - Fast, efficient, and portable
  - Close to machine (assembly-like control)
  - Pointer, minimal type checking
- Problems
  - Pointer, minimal type checking
  - Require manual control of dynamic memory
  - **Unsafe (memory leak, undefined behavior, ..)**
  - Difficult to write correct, safe, secure code

“C is assembly, Rust is future”

Intel and Rust: the Future of Systems Programming: Josh Triplett