CS165 – Computer Security

Other topics

Nov 30, 2021

Other Topics

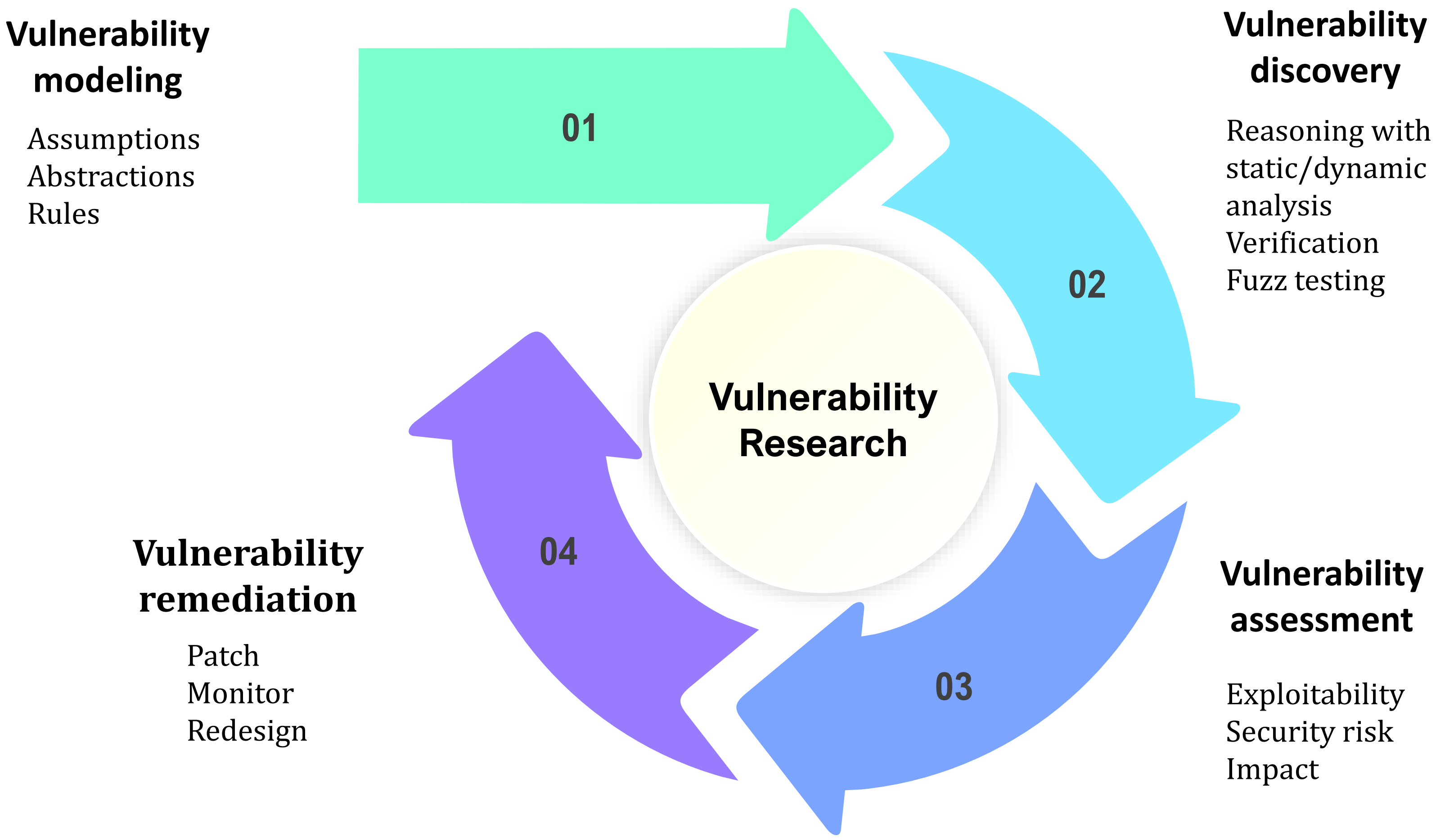
- Vulnerability research
- Forensics
- IoT
- Underground market

Other Topics

- Vulnerability research
- Forensics
- IoT
- Underground market

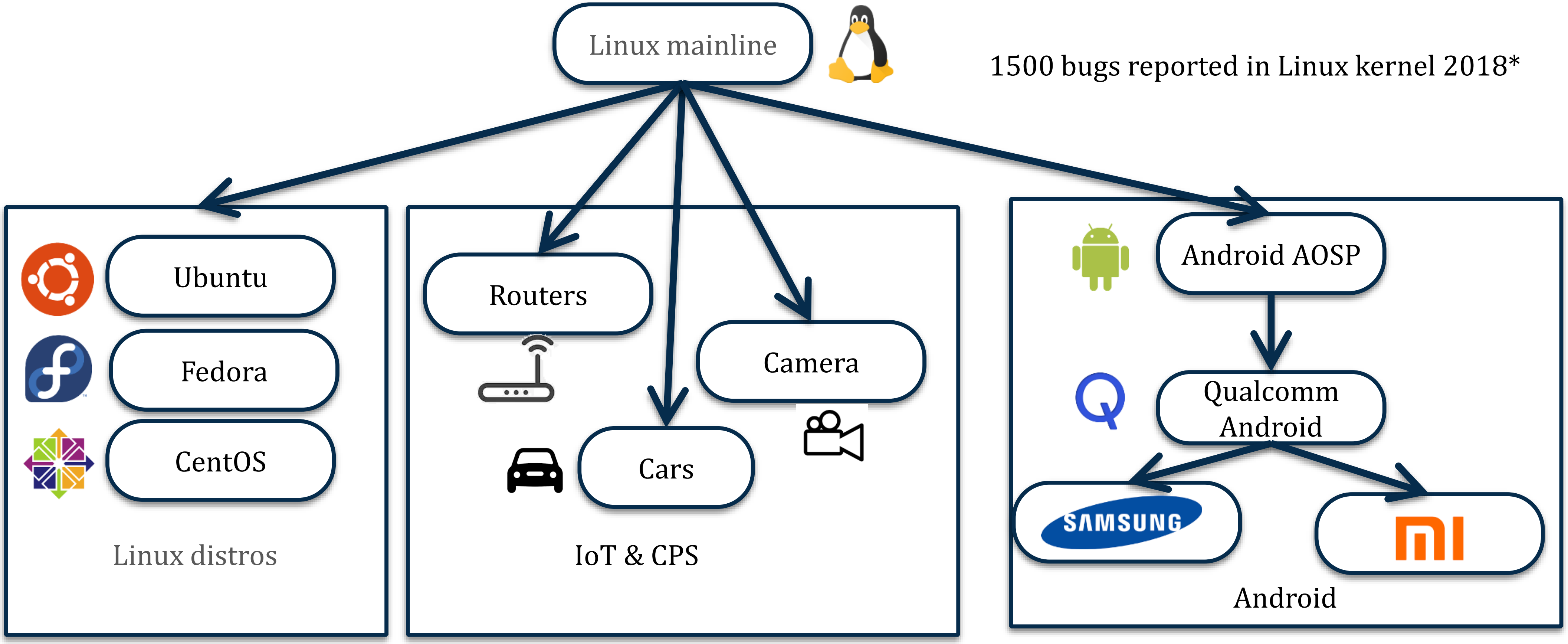
NEXT

Vulnerability Research Cycle



Linux vulnerability research - ecosystem

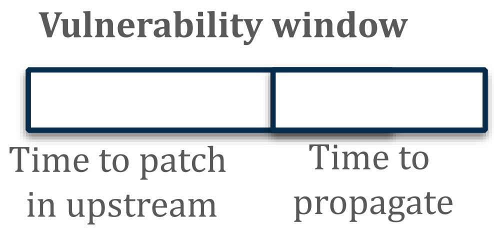
- Open system



* Syzbot and the Tale of Thousand Kernel Bugs - Dmitry Vyukov, Google, 2018

Linux ecosystem

- Transparent: Continuous fuzz testing by Google
  - Bugs displayed automatically on Syzbot

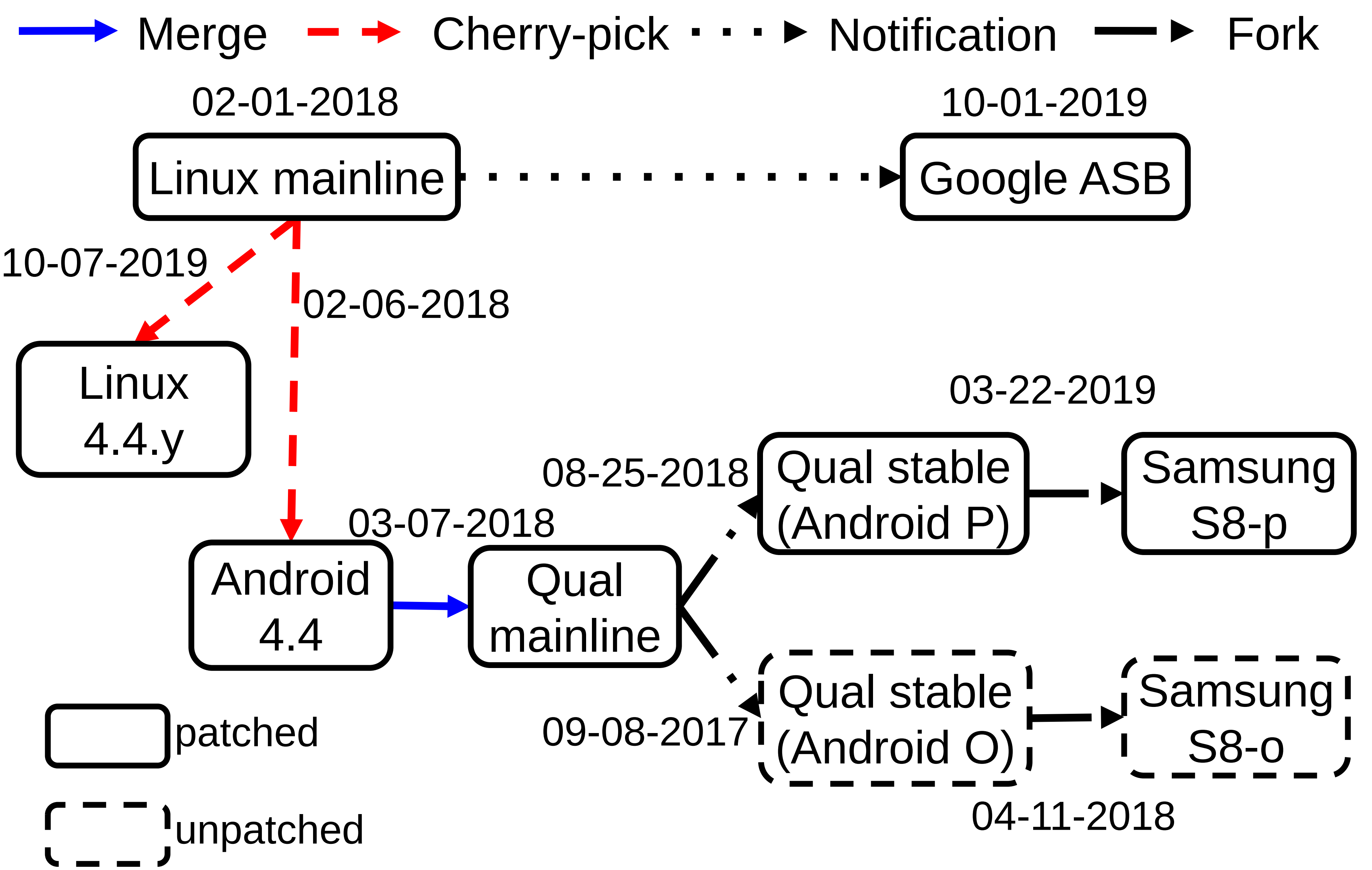



```c
// https://syzkaller.appspot.com/bug?id=6fbb32225787f789f5ce49000ac86713a6c24588
// autogenerated by syzkaller (https://github.com/google/syzkaller)

#define _GNU_SOURCE

#include <endian.h>
#include <stdint.h>
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <sys/syscall.h>
#include <sys/types.h>
#include <unistd.h>

uint64_t r[1] = {0xffffffffffffffff};

int main(void)
{
  syscall(__NR_mmap, 0x20000000ul, 0x1000000ul, 3ul, 0x32ul, -1, 0);
  intptr_t res = 0;
  memcpy((void*)0x200017c0, "/selinux/enforce\000", 17);
  res = syscall(__NR_openat, 0xffffffffffffff9cul, 0x200017c0ul, 2ul, 0ul);
  if (res != -1)
    r[0] = res;
  *(uint64_t*)0x20000000 = 0x20000100;
  memcpy((void*)0x20000100, " 8", 2);
  *(uint64_t*)0x20000008 = 2;
  *(uint64_t*)0x20000010 = 0;
  *(uint64_t*)0x20000018 = 0;
  syscall(__NR_writev, r[0], 0x20000000ul, 2ul);
  memcpy((void*)0x20000000, "/sys/kernel/debug/bluetooth/6lowpan_enable\000",
         43);
  syscall(__NR_openat, 0xffffffffffffff9cul, 0x20000000ul, 2ul, 0ul);
  return 0;
}
```

Title	Reported
BUG: unable to handle kernel paging reque	17h52m
WARNING in do_dentry_open (2)	1d19h
KASAN: use-after-free Read in vgem_gem	2d07h
WARNING: ODEBUG bug in process_one	2d11h
INFO: task hung in rxrpc_release	2d11h
KMSAN: uninit-value in batadv_interface_	3d09h
INFO: rcu detected stall in do_iter_write	3d16h
WARNING in default_device_exit_batch	3d19h
WARNING in nsim_fib6_rt_nh_del	3d19h
possible deadlock in lookup_one_len_unloc	4d03h
KMSAN: uninit-value in udp_tunnel6_xmit	4d12h

As of Feb 2, 2020

Case study: CVE-2019-2215



Process to Manage and Track Bugs

Is it a security bug?

Does it affect a specific downstream?

Bug → Triage → Security bug → Applicability Analysis

Triage:

- UAF -> Likely security impact
- NULL pointer dereference -> likely little security impact

SyzScope, USENIX Security 2022

Triggerable and exploitable from a regular app (no root or special selinux context required)

KOOBE, USENIX Security 2020

Applicability Analysis:

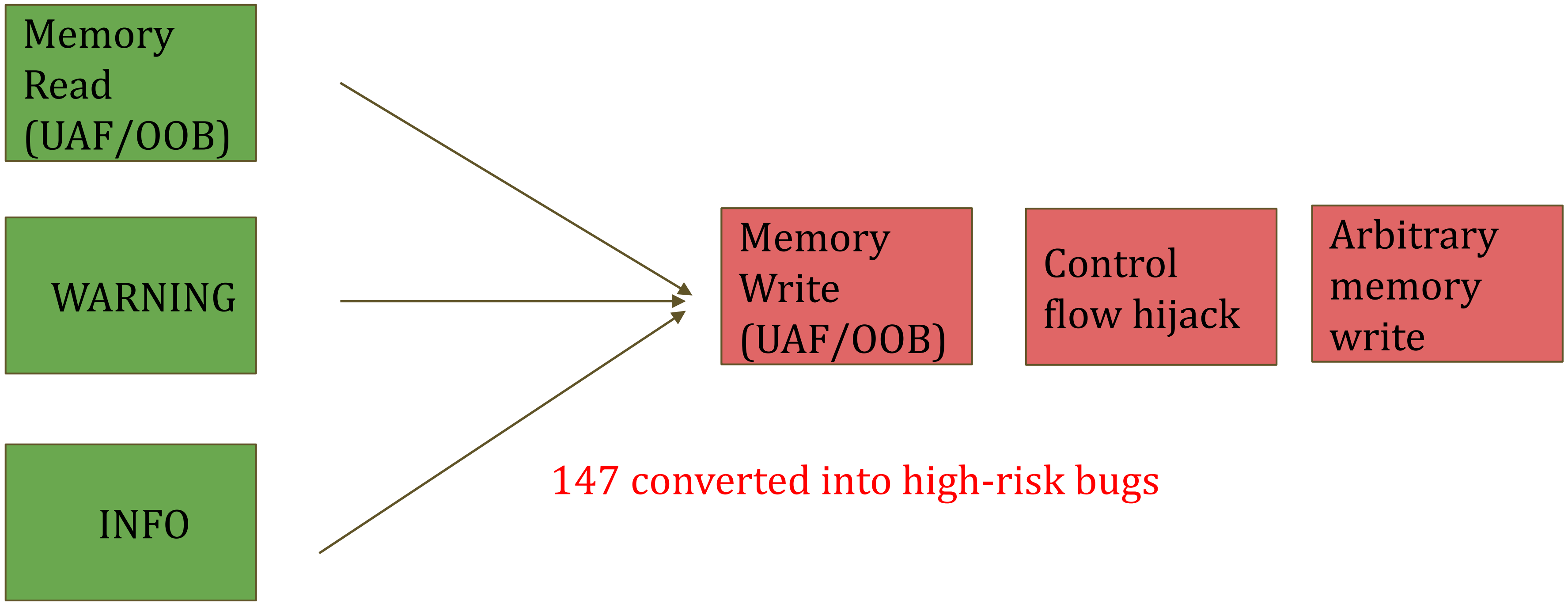
OEM kernel has the vulnerable code / logic (unpatched)

FIBER, USENIX Security 2018, 2021

Still triggerable and exploitable from a regular app (security policy customization)

Ongoing

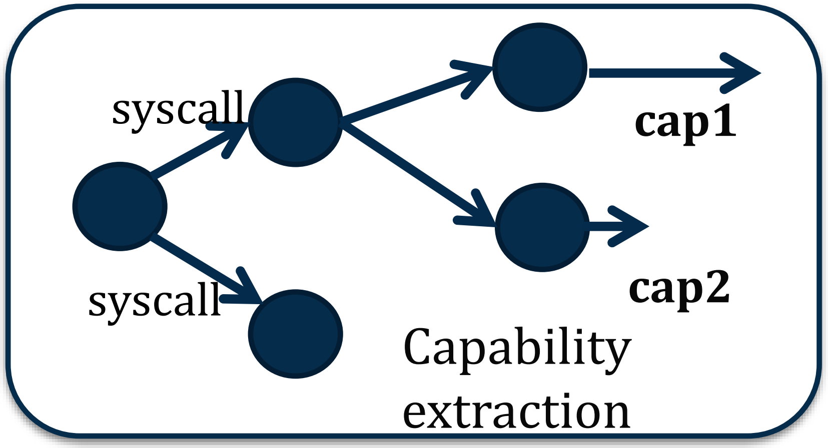
SyzScope: Revealing High-Risk Security Impacts of Fuzzer-Exposed Bugs in Linux kernel

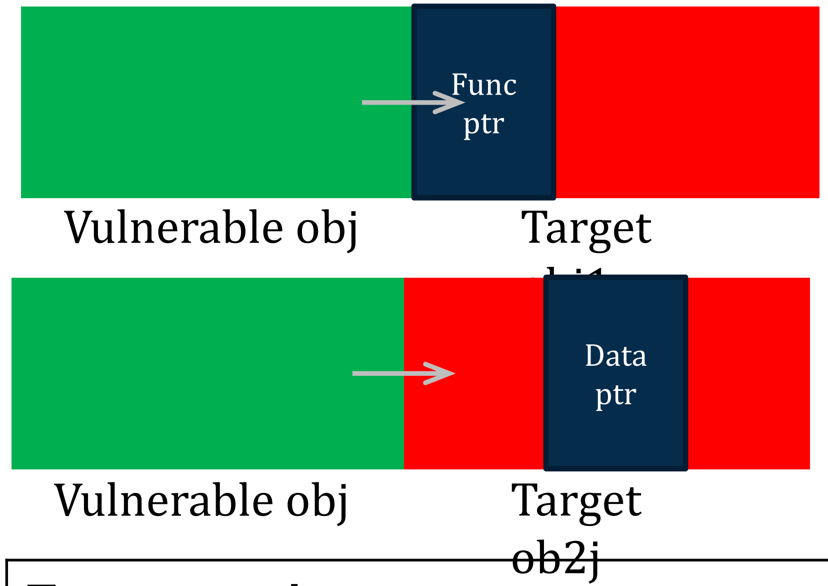


1173 low-risk bugs

KOOBE: Towards Facilitating Exploit Generation of Kernel Out-Of-Bounds Write Vulnerabilities

Capability extraction vs. Target object matching





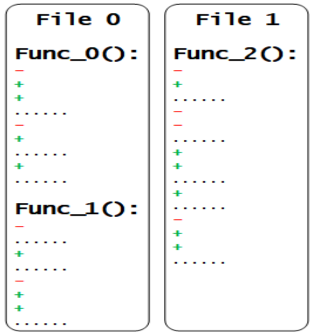
Capability
offset = 128
length = 1 : 100
value[0:99] = 0 ~ 0xffffffffffffffff

$\wedge$

Target requirement
M[0:7] = …
M[8:15] = diverted address
…

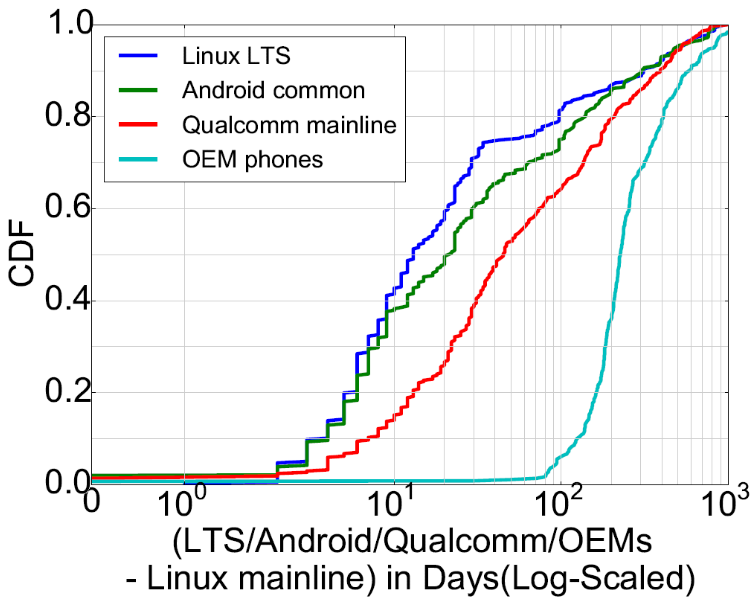
FIBER: Precise and Accurate Patch Presence Test for Binaries

Source-level patch (CVE)



Binary OEM Android kernel

Patch applied?



Other Topics

- Linux vulnerability research
- Forensics

NEXT

- IoT
- Underground market

Digital forensics

Digital forensics is the process of preserving, identifying, extracting, documenting, and interpreting data in order to investigate past actions or obtain legal evidence. Used to **investigate crimes**, **recover from attacks**.

Four stages of forensic analysis:

1. Identification

Identify specific objects that store important data for the case analysis.

2. Collection

Preserve evidence, establish chain of custody, ensure data stays intact and unaltered.

3. Analysis

Examine the information stored on digital evidence and conduct an analysis of the incident.

4. Reporting

Interpret findings, prepare and deliver an expert report and/or testimony.

Identification

You are the investigator, which objects do you think will be useful for investigations?

Computer (case and power supply)

Just the hard drive (without computer)

Monitor

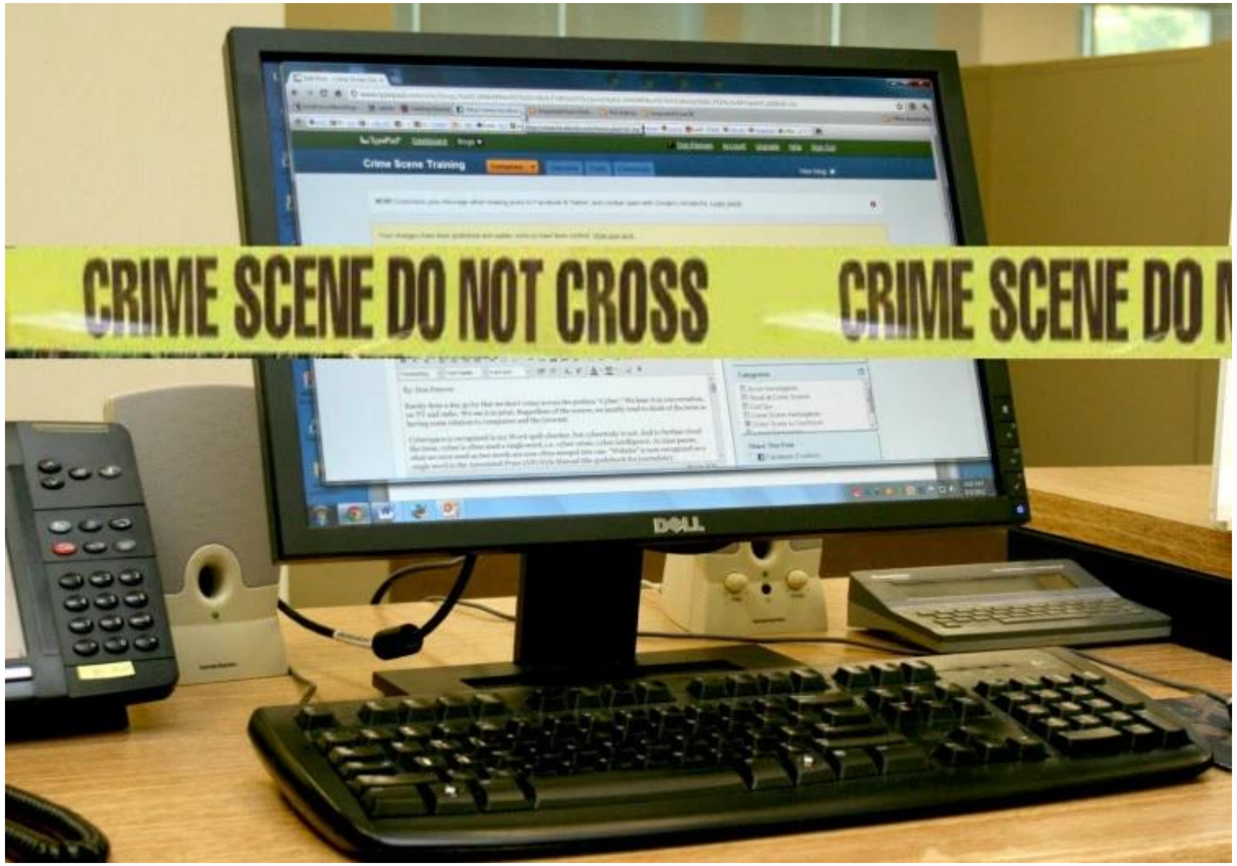
Keyboard and mouse

Media (CD, DVD, USB drives, etc.)

Printer

Answer: All of the above!

Digital forensics does not replace traditional forensic analysis.



Collection

When collecting evidence, must take care not to *change* the evidence.

- Information on digital media is easily changed. Once altered, impossible to prove the original state.
- Computer or media is the "crime scene." Once evidence is contaminated, it can't be decontaminated.
- Examining a live file system changes state of the evidence.
- Instead, work with a **forensic image** (carefully created copy) or the data.

Principles for collecting evidence:

Maintain a **chain of custody:**

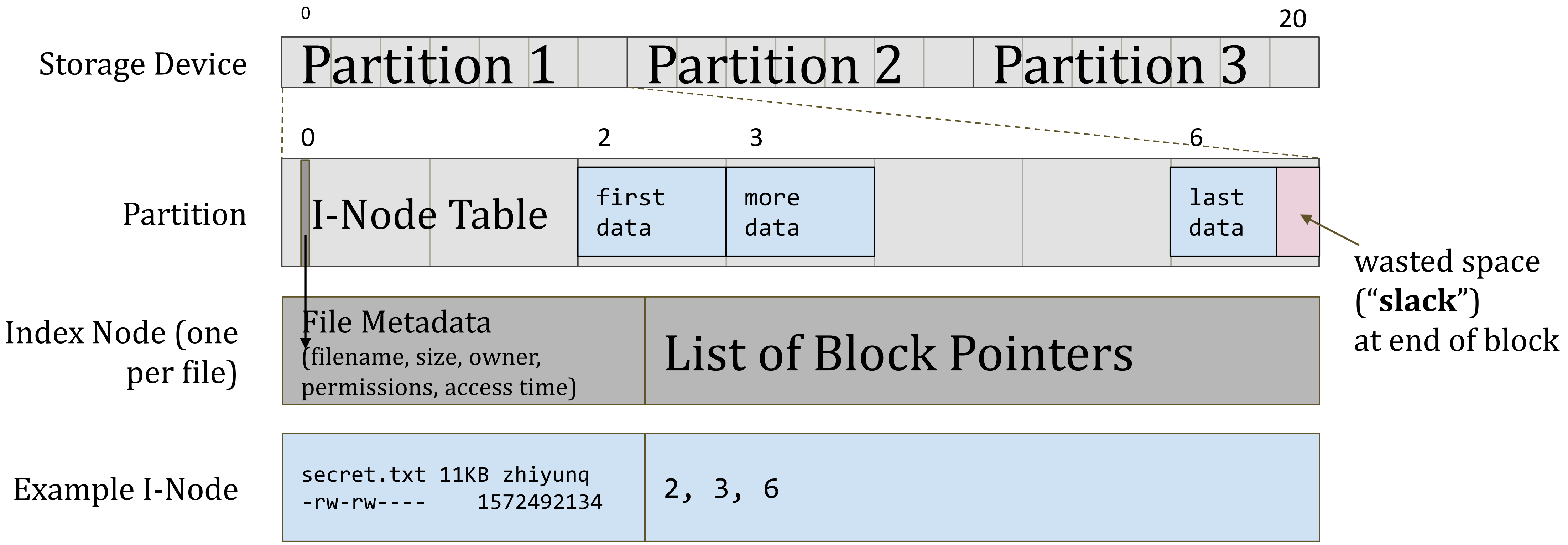
- Physically secure items of evidence.
- Track possession step-by-step.
- Keep documentation (e.g., hash of image) to allow you to trace evidence back to the source.

Prioritize collection by **volatility:**

- Some data is more **volatile**.
- **RAM > disk > external media**
- General idea: Capture more volatile evidence first. **[Why?]**

How Data is Stored on a Disk

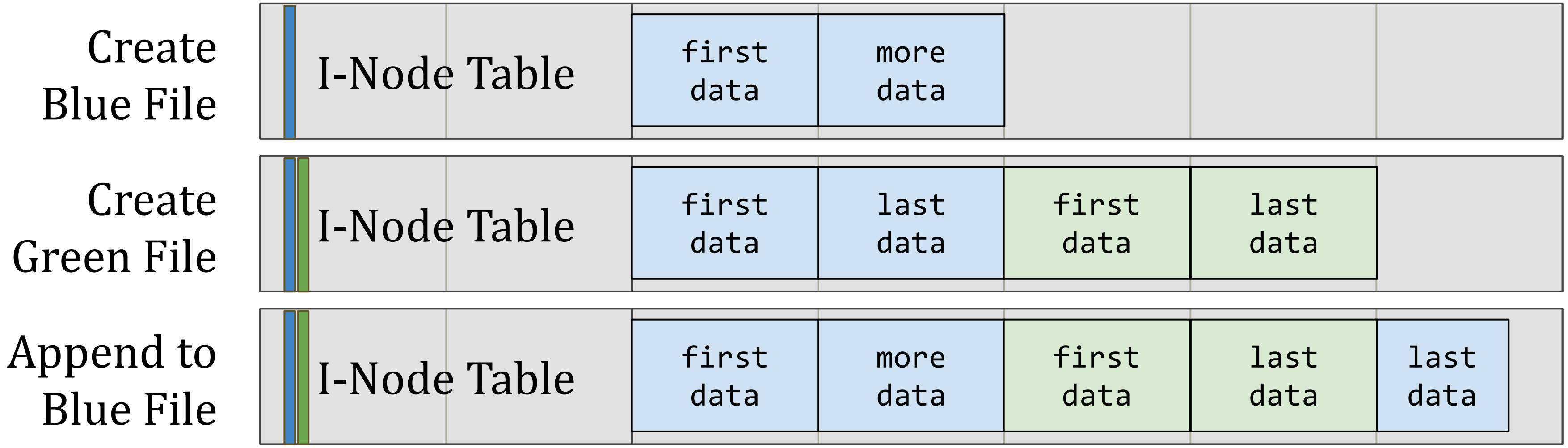
Low-level storage devices are essentially arrays of fixed-sized **blocks** (typically 4 KB).
A **filesystem** organizes these blocks to provide abstractions like files and directories.



(Greatly simplified. Details vary by OS and kind of filesystem.)

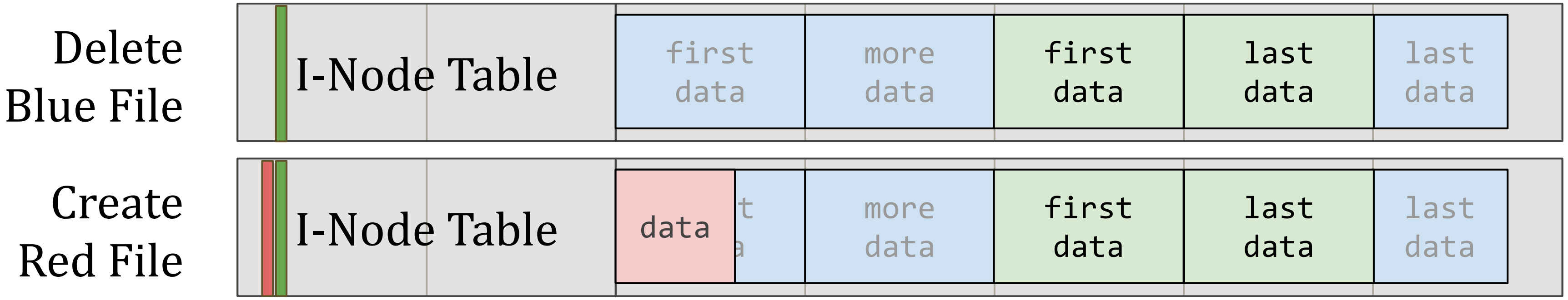
Forensic Clues in Low-Level Data

Low-level filesystem layout often contain important forensic clues.



Fragmentation shows some other data was there first.

Deleting file removes only the i-node! Residual data remains until overwritten by new files.



All blocks of deleted file still fully intact.

Part of first block still recoverable in slack space.

Flash contains even more low-level residual data, which can be read with special hardware.

Collection: Imaging RAM

Live-memory forensics also considers the contents of RAM.

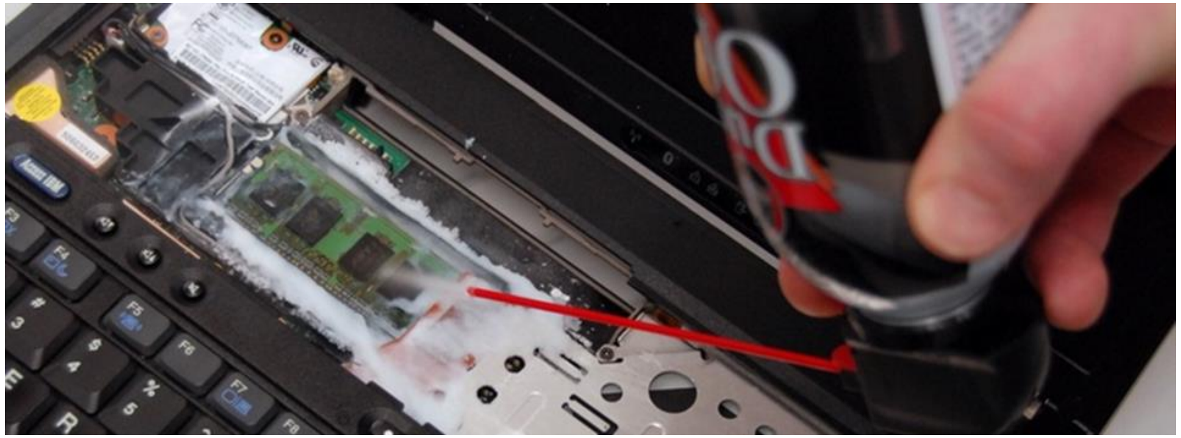
- Can be essential for decrypting data on disk, recovering passwords, or spotting in-memory malware.

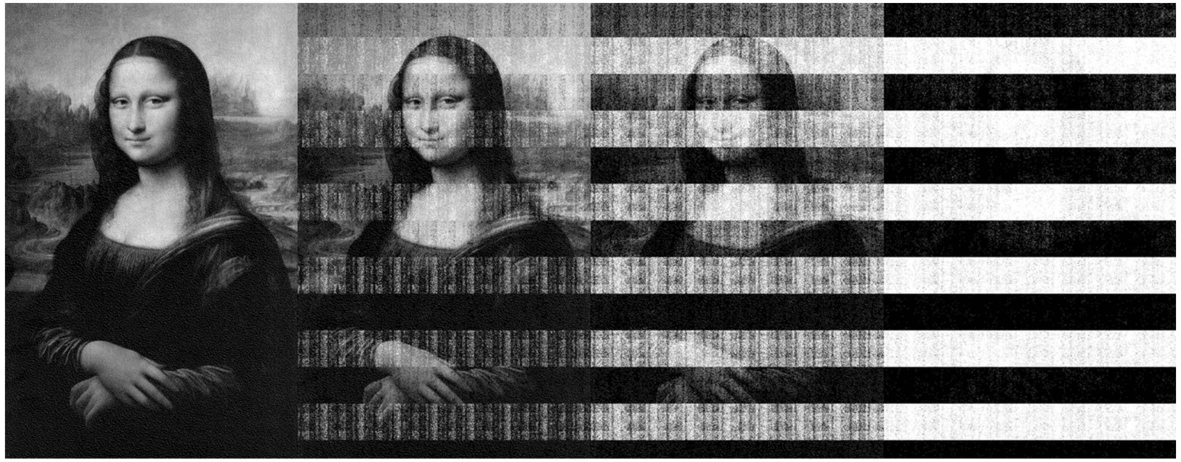
Specialized devices can image RAM by exploiting vulnerabilities in Thunderbolt.

Virtual machines can be snapshotted to image RAM and disk simultaneously.

Cold-boot attack: Many systems can be reset and booted into a special-purpose OS designed to image RAM. (Typically, RAM not erased except when the normal OS loads.)

If unable to boot special OS, freeze memory chips and move them to different machine.





5 secs | 30 secs | 60 secs | 300 secs

Collection: Mobile Devices

Mobile devices present special forensics challenges, due to radio connectivity and advanced security features.

Defeat remote wiping by placing device in a Faraday bag to shield RF signals.

Arms race: Mobile device makers implementing strong encryption, hardware-backed security.

Forensics companies make specialized devices to exploit vulnerabilities and recover data.
(e.g., Cellebrite, GrayKey).

Latest device models/firmware may be unrecoverable, but probably not for long…

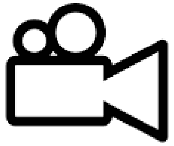
Other Topics

- Linux vulnerability research
- Forensics
- IoT
- Underground market

NEXT

IoT devices

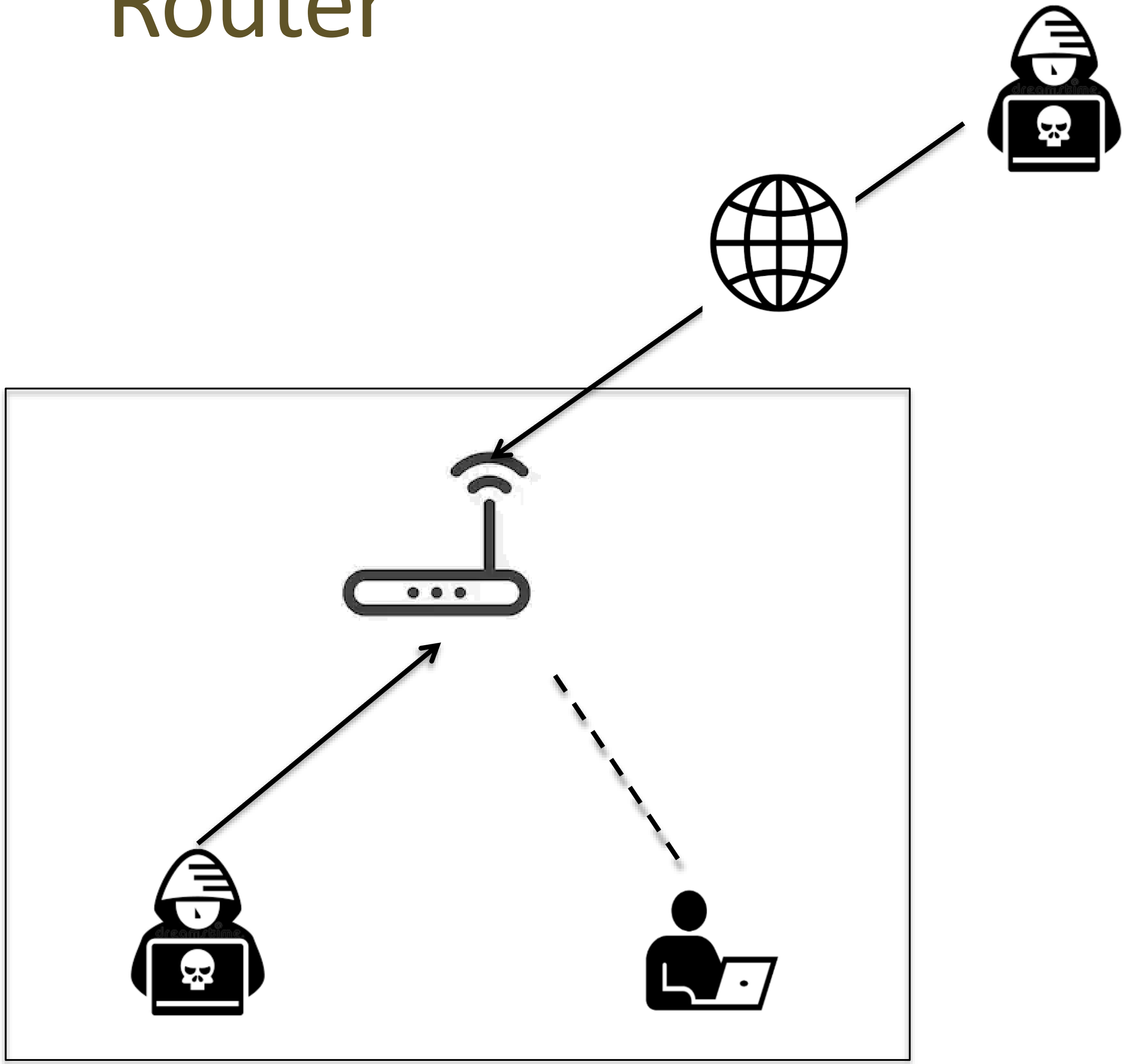




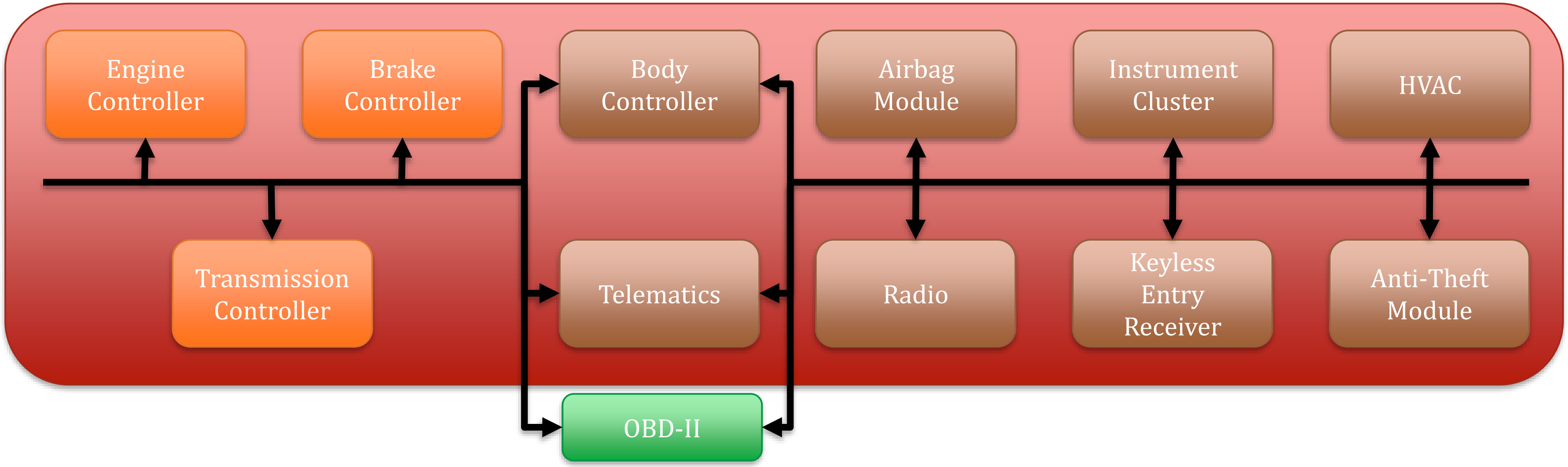
Attack surface?

Router

- Internet facing
- Local network facing



Cars' system



- ECU(Electronic Control Unit) :
  - Ubiquitous computer controller
- ECU interconnection driven by safety, efficiency, and capability requirements
- But, also has some fatal shortcomings

Oakland 2010, they showed…

- Safety-critical systems can be compromised
  - Selectively enable/disable brakes
  - Stop engine
  - Control lights
- Owning one ECU = total compromise
- ECUs can be reprogrammed (while driving!)

- Limit: Need physical access

[Oakland'10] koscher et al. Experimental Security Analysis of a Modern Automobile.

Threat model

- Technical (theoretical) Capabilities
  - Capabilities in analyzing the system
  - Focuses on making technical capabilities realistic

- Operational (real-time) capabilities
  - Show how malicious payload is delivered
  - Attack vector
    - Indirect physical access
    - short-range wireless access
    - long-range wireless access

Indirect physical

- Definition:
  - Attacks over physical interfaces
  - Constrained: Adversary may not **directly** access the physical interfaces herself
- OBD(stands for On Board Diagnostic)

Port

Scanner

PassThru

Indirect physical

- Definition:
  - Attacks over physical interfaces
  - Constrained: Adversary may not **directly** access the physical interfaces herself
- Extends attack surface to the device

Short-range wireless

- Definition: Attacks via short-range wireless communication (meters range or less)

Bluetooth

TPMS

Remote key

Immobilizer

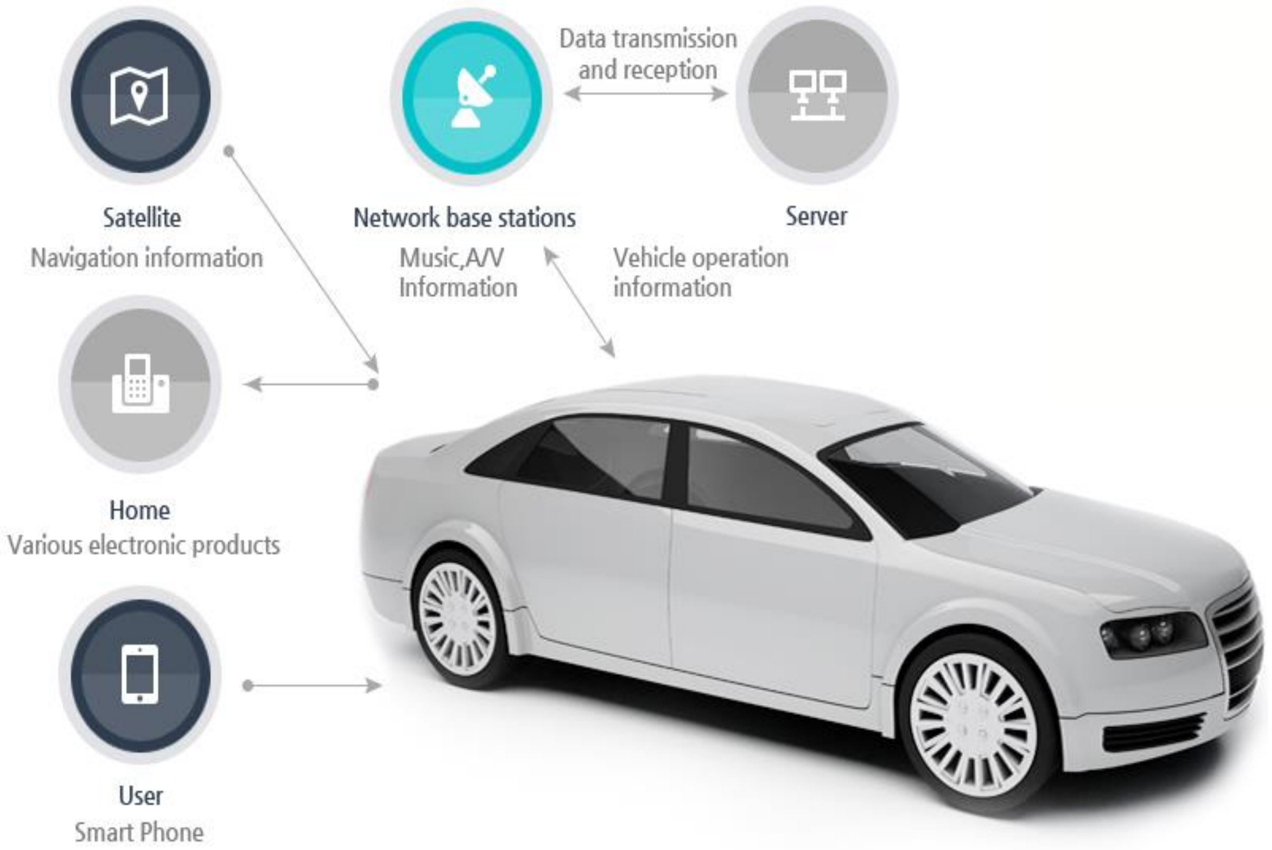
Long-range wireless

- Definition: Attacks via long-rage wireless communication (miles, global-scale)
- Broadcast channel
  - Satellite Radio, GPS, RDS

Satellite Radio

Long-range wireless

- Definition: Attacks via long-rage wireless communication (miles, global-scale)
- Addressable channel
  - Telematics



Other Topics

- Linux vulnerability research
- Forensics
- IoT
- Underground market

NEXT

Underground market

- Compromised hosts/infrastructure reselling
- Click fraud
- Spam
- Cyber weapon