ECE458/ECE750T27: Computer Security

Programming Security

Dr. Kami Vaniea,
Electrical and Computer Engineering
kami.vaniea@uwaterloo.ca

First, the news...

- First 5 minutes we talk about something interesting and recent
- You will not be tested on the news part of lecture
- You may use news as an example on tests
- Why do this?
    1. Some students show up late for various good reasons
    2. Reward students who show up on time
    3. Important to see real world examples

MALWARE DETECTION

No-fault

- Areas like aviation and nautical take a “no fault” view towards incident management
- The sectors consider it more important to learn from problems than to blame and punish

Boeing Plane Incidents Timeline: Full List of 9 Issues in 3 Months

Published Mar 25, 2024 at 10:54 AM EDT | Updated Mar 25, 2024 at 11:15 AM EDT

By Thomas Kika
Weekend Staff Writer

FOLLOW

The Boeing aviation company announced on Monday that current CEO Dave Calhoun intends to step down by the end of the year.

This move came after months of incidents involving the company's planes have created a bruising PR nightmare, causing widespread uncertainty among the general public about the quality of Boeing planes and air travel in general. Larry Kellner, chairman of the board for Boeing, will also not be seeking reelection and will be replaced by Steve Mollenkopf, the former CEO of Qualcomm and a Boeing board member since 2020, with the search ongoing for a replacement for Calhoun.

While the company has weathered incidents and accidents with its planes at various points in the past, its current troubles flared up after a January incident involving an Alaska Airlines flight that went viral online. Every incident involving troubles with a Boeing craft since then has received renewed and intense public scrutiny.

Newsweek reached out to Boeing via email on Monday morning for comment.

Here is a look at the incidents on Boeing planes since January.

Alaska Airlines, January 5

On this date, a Boeing 737 Max 9 craft operated by Alaska Airlines was forced to make an emergency landing shortly after departing Portland International Airport after a shoddily installed door plug flew off in midair. Images from inside the craft showing the sizable opening that had been left in the craft went viral online, causing widespread alarm, though no one on board had been injured.

Think-pair-share

- Why is no-fault not used in computer security?

Collaboration

- Defenders do need to collaborate
- No one likes viruses, malware, or phishing, so these are “safe” to share
- So organizations like VirusTotal and APWG collect together examples of such bad things and share those examples with everyone
- Company privacy costs money:
  “By submitting data [you agree] to the sharing of your Sample submission with the security community.”

Attacking from the inside

- Not all attacks are from external, some are from employees
- Castle security thinking does not work well with insider attacks
- Boundaries can sometimes be bypassed

Salami Attacks

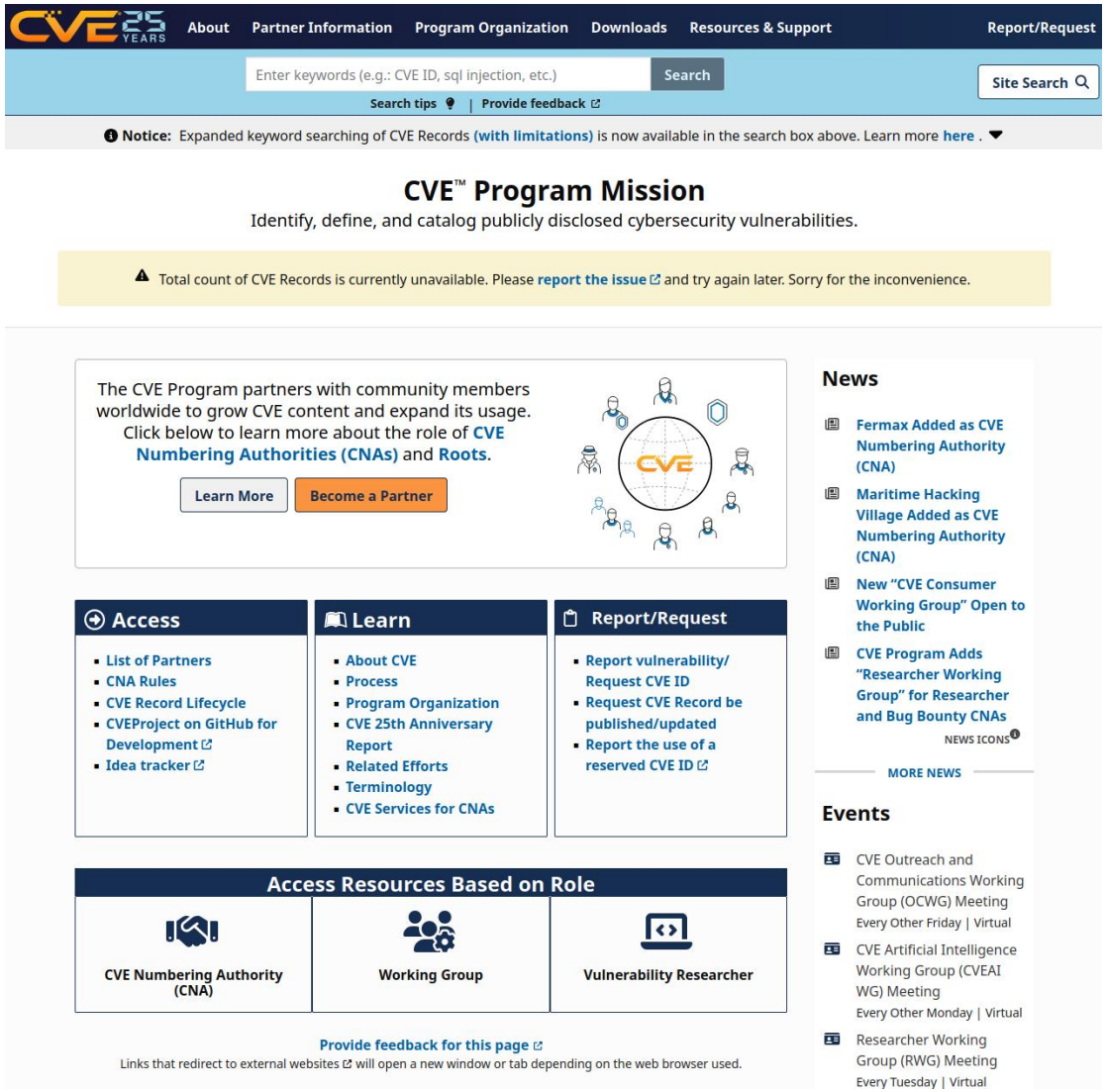
- Attack that takes only a small amount of the resource each time to avoid being noticed

- Program bank software so that money that is rounded off is moved to a bank account

COMMON VULNERABILITIES AND EXPOSURES (CVE)

Common Vulnerabilities and Exposures (CVE)

- Launched in 1999, maintained by Mitre
- Assigns numbers to reported vulnerabilities in publicly released software



Common Weaknesses Enumeration (CWE)

- Similar to CVE but tracks common problems at a more abstract level
- CVEs and CWEs often refer to each other

Reference	Description
CVE-2022-20141	Chain: an operating system kernel has insufficent resource locking (CWE-413) leading to a use after free (CWE-416).
CVE-2022-2621	Chain: two threads in a web browser use the same resource (CWE-366), but one of those threads can destroy the resource before the other has completed (CWE-416).
CVE-2021-0920	Chain: mobile platform race condition (CWE-362) leading to use-after-free (CWE-416), as exploited in the wild per CISA KEV.
CVE-2020-6819	Chain: race condition (CWE-362) leads to use-after-free (CWE-416), as exploited in the wild per CISA KEV.
CVE-2010-4168	Use-after-free triggered by closing a connection while data is still being transmitted.
CVE-2010-2941	Improper allocation for invalid data leads to use-after-free.
CVE-2010-2547	certificate with a large number of Subject Alternate Names not properly handled in realloc, leading to use-after-free
CVE-2010-1772	Timers are not disabled when a related object is deleted
CVE-2010-1437	Access to a "dead" object that is being cleaned up
CVE-2010-1208	object is deleted even with a non-zero reference count, and later accessed
CVE-2010-0629	use-after-free involving request containing an invalid version number

CWE Common Weakness Enumeration
A community-developed list of SW & HW weaknesses that can become vulnerabilities

Top 25 | Top HW CWE | New to

Home > CWE List > CWE-416: Use After Free (4.17) ID Lookup:

Home | About ▼ | Learn ▼ | Access Content ▼ | Community ▼ | Search ▼

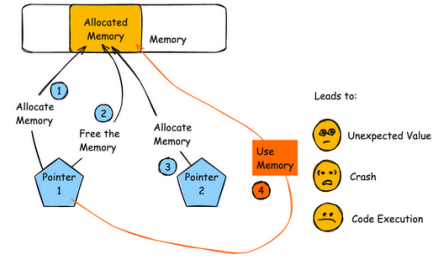
CWE-416: Use After Free

Weakness ID: 416
Vulnerability Mapping: ALLOWED
Abstraction: Variant

View customized information: Conceptual | Operational | Mapping Friendly | **Complete** | Custom

Description

The product reuses or references memory after it has been freed. At some point afterward, the memory may be allocated again and saved in another pointer, while the original pointer references a location somewhere within the new allocation. Any operations using the original pointer are no longer valid because the memory "belongs" to the code that operates on the new pointer.



Alternate Terms

Dangling pointer	a pointer that no longer points to valid memory, often after it has been freed
UAF	commonly used acronym for Use After Free
Use-After-Free	

Common Consequences

Impact	Details
Modify Memory	**Scope: Integrity** The use of previously freed memory may corrupt valid data, if the memory area in question has been allocated and used properly elsewhere.
DoS: Crash, Exit, or Restart	**Scope: Availability** If chunk consolidation occurs after the use of previously freed data, the process may crash when invalid data is used as chunk information.
Execute Unauthorized Code or Commands	**Scope: Integrity, Confidentiality, Availability** If malicious data is entered before chunk consolidation can take place, it may be possible to take advantage of a write-what-where primitive to execute arbitrary code. If the newly allocated data happens to hold a class, in C++ for example, various function pointers may be scattered within the heap data. If one of these function pointers is overwritten with an address to valid shellcode, execution of arbitrary code can be achieved.

Common Weaknesses Enumeration (CWE)

- Similar to CVE but tracks common problems at a more abstract level
- CVEs and CWEs often refer to each other

Reference	Description
CVE-2022-20141	Chain: an operating system kernel has insufficent resource locking (CWE-413) leading to a use after free (CWE-416).
CVE-2022-2621	Chain: two threads in a web browser use the same resource (CWE-366), but one of those threads can destroy the resource before the other has completed (CWE-416).
CVE-2021-0920	Chain: mobile platform race condition (CWE-362) leading to use-after-free (CWE-416), as exploited in the wild per CISA KEV.
CVE-2020-6819	Chain: race condition (CWE-362) leads to use-after-free (CWE-416), as exploited in the wild per CISA KEV.
CVE-2010-4168	Use-after-free triggered by closing a connection while data is still being transmitted.
CVE-2010-2941	Improper allocation for invalid data leads to use-after-free.
CVE-2010-2547	certificate with a large number of Subject Alternate Names not properly handled in realloc, leading to use-after-free
CVE-2010-1772	Timers are not disabled when a related object is deleted
CVE-2010-1437	Access to a "dead" object that is being cleaned up
CVE-2010-1208	object is deleted even with a non-zero reference count, and later accessed
CVE-2010-0629	use-after-free involving request containing an invalid version number

8.8 HIGH

CVE-2010-1772

"WebKit Google Chrome Use-after-free in Geolocation"

⌘ Overview | Vulnerability Timeline | Exploitability Score History | Knowledge Base

Description

Use-after-free vulnerability in page/Geolocation.cpp in WebCore in WebKit before r59859, as used in Google Chrome before 5.0.375.70, allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted web site, related to failure to stop timers associated with geolocation upon deletion of a document.

Affected Products

The following products are affected by CVE-2010-1772 vulnerability. Even if cvefeed.io is aware of the exact versions of the products that are affected, the information is not represented in the table below.

ID	Vendor	Product	Action
1	Canonical	ubuntu_linux	
1	Redhat	enterprise_linux	
1	Fedoraproject	fedora	
1	Google	chrome	
1	Opensuse	opensuse	

USE-AFTER-FREE

Use-After-Free (CWE-416)

- Basic idea:
  - P1: Creates a pointer to memory address A, and allocate memory there
  - P1: Free the memory, but keep the pointer
  - P2: Allocates memory and gets memory address A
  - P1: Reads from memory address A using its still-existing pointer

Example Language: **C**

```
char* ptr = (char*)malloc (SIZE);
if (err) {
  abrt = 1;
  free(ptr);
}
...
if (abrt) {
  logError("operation aborted before commit", ptr);
}
```

https://cwe.mitre.org/data/definitions/416.html

Use-After-Free (CWE-416)

- Creates a race condition for read and write between the two programs
- Possibly allow a low-security program to read memory of a high-security program
- Possibly allows a low-security program to write code to memory that a high-security program might later execute

Example Language: **C**

```
char* ptr = (char*)malloc (SIZE);
if (err) {
  abrt = 1;
  free(ptr);
}
...
if (abrt) {
  logError("operation aborted before commit", ptr);
}
```

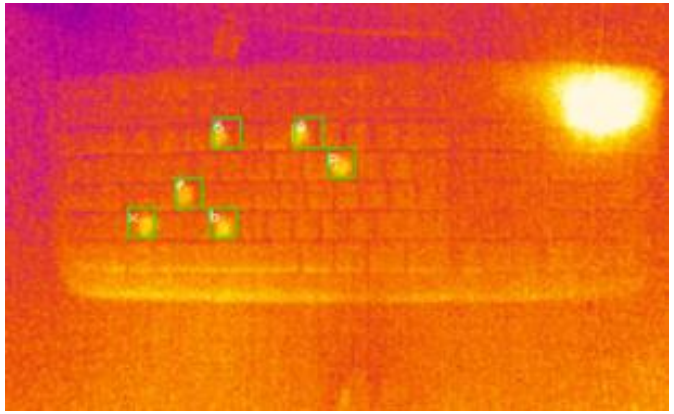
https://cwe.mitre.org/data/definitions/416.html

SIDE CHANNELS

Examples of Side Channels

Side Channels are an exercise in creativity:

- Timing
  - A command doing ‘more’ will take longer
  - E.g., Square and multiply problem
- Temperature
  - Relies on the processor heating up when it’s working hard
- Radio waves
  - More power being transmitted over a wire will emit more RF
- Power
  - A command doing ‘more’ will consume more power
- Many more…

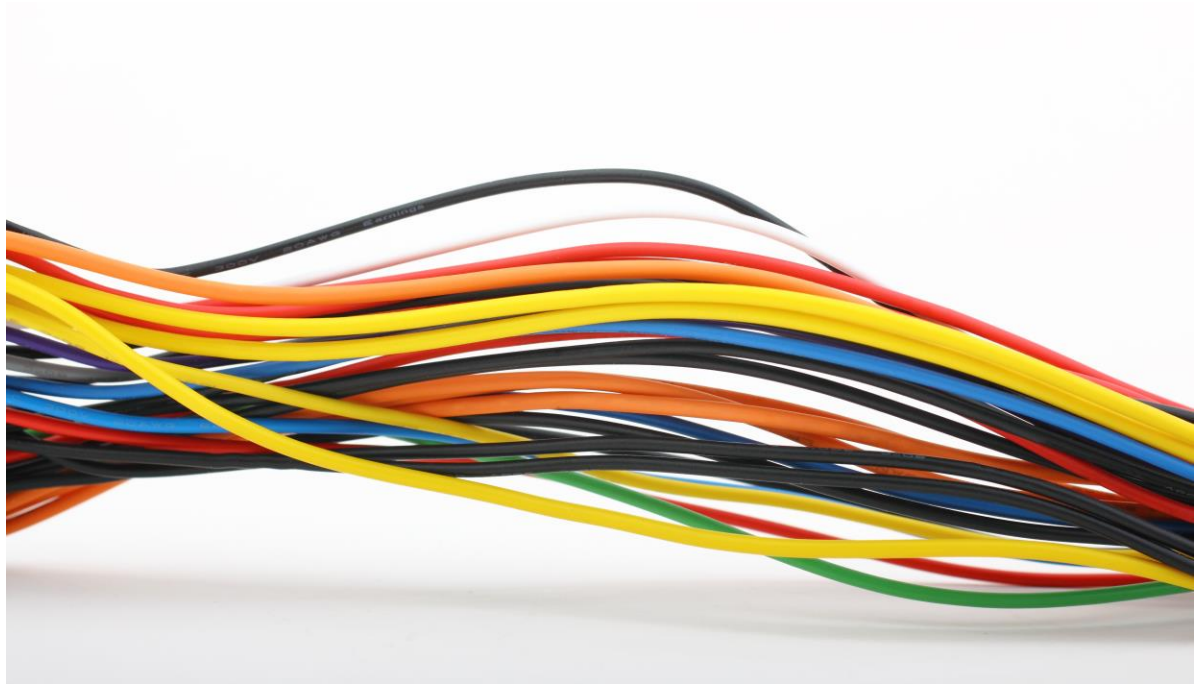


Side channels allow us to acquire information about a target in unexpected ways

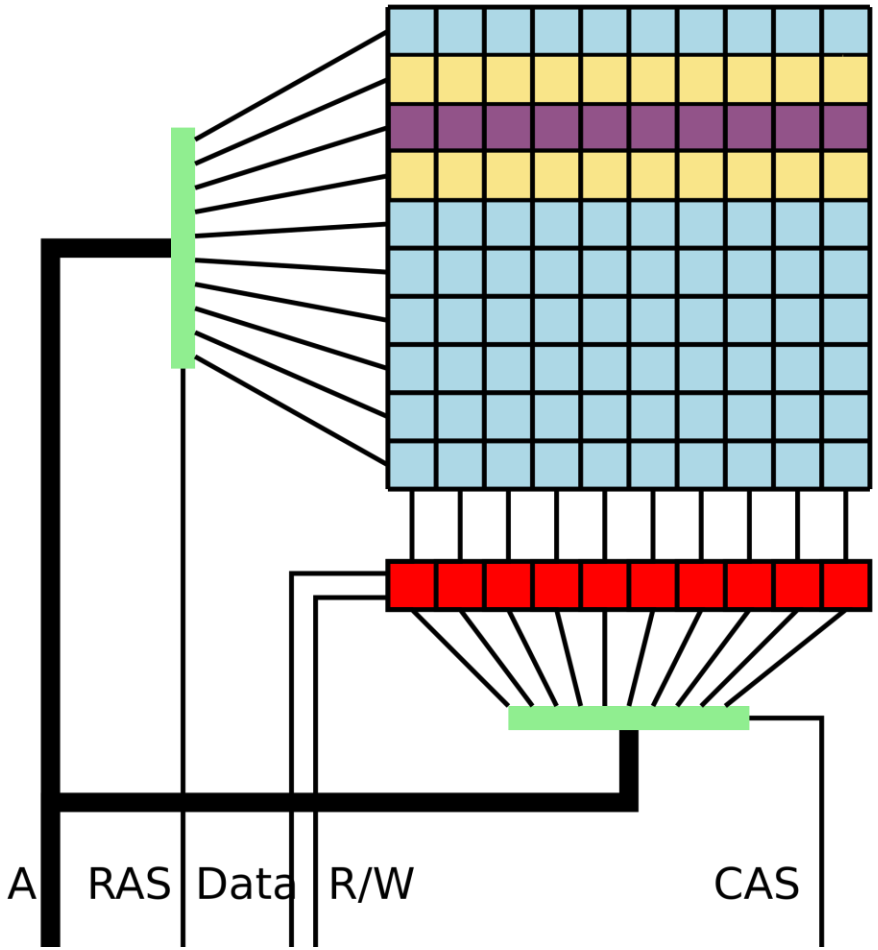
E.g., A thermal image of the keyboard for a user who has just logged in…

Electronic resonance

- Two wires that are physically close to each other resonate; they pick up each other's signals
- One easy way to "steal" data is just run a wire next to your target wire



RowHammer (2014)



By Dsimic - Own work, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=38868341

- Repeated activation of rows can cause bits in neighboring rows to change
- Happens because DRAM is becoming more compact and with lower noise margins
- A low-access process could in theory overwrite bits in a high-access process

```
hammer:
  mov (X), %eax  // read from address X
  mov (Y), %ebx  // read from address Y
  clflush (X)    // flush cache for address X
  clflush (Y)    // flush cache for address Y
  jmp hammer
```

A snippet of x86 assembly code that induces the row hammer effect (memory addresses `X` and `Y` must map to different DRAM rows in the same memory bank)[1]:3[4][18]:13–15

https://en.wikipedia.org/wiki/Row_hammer

Flip Feng Shui (2016)

- Memory deduplication allows an attacker to reverse-map any physical page into a virtual page she owns as long as the page's contents are known. Rowhammer, in turn, allows an attacker to flip bits in controlled (initially unknown) locations in the target page.

Flip Feng Shui: Hammering a Needle in the Software Stack

Kaveh Razavi, Ben Gras, and Erik Bosman, *Vrije Universiteit Amsterdam;*
Bart Preneel, *Katholieke Universiteit Leuven;* Cristiano Giuffrida and Herbert Bos, *Vrije Universiteit Amsterdam*

https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/razavi

This paper is included in the Proceedings of the
25th USENIX Security Symposium

August 10–12, 2016 • Austin, TX

ISBN 978-1-931971-32-4

Open access to the Proceedings of the
25th USENIX Security Symposium
is sponsored by USENIX

Flip Feng Shui (2016)

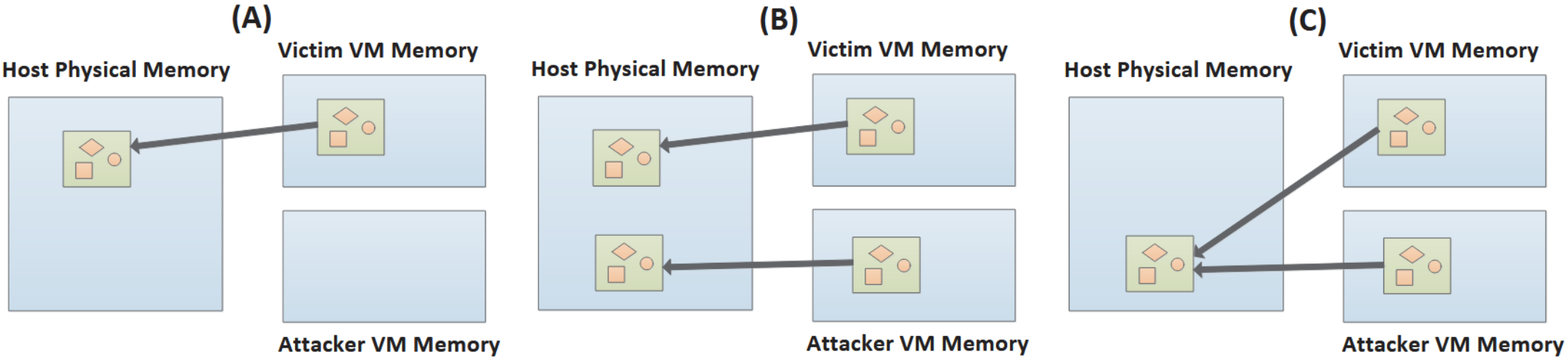
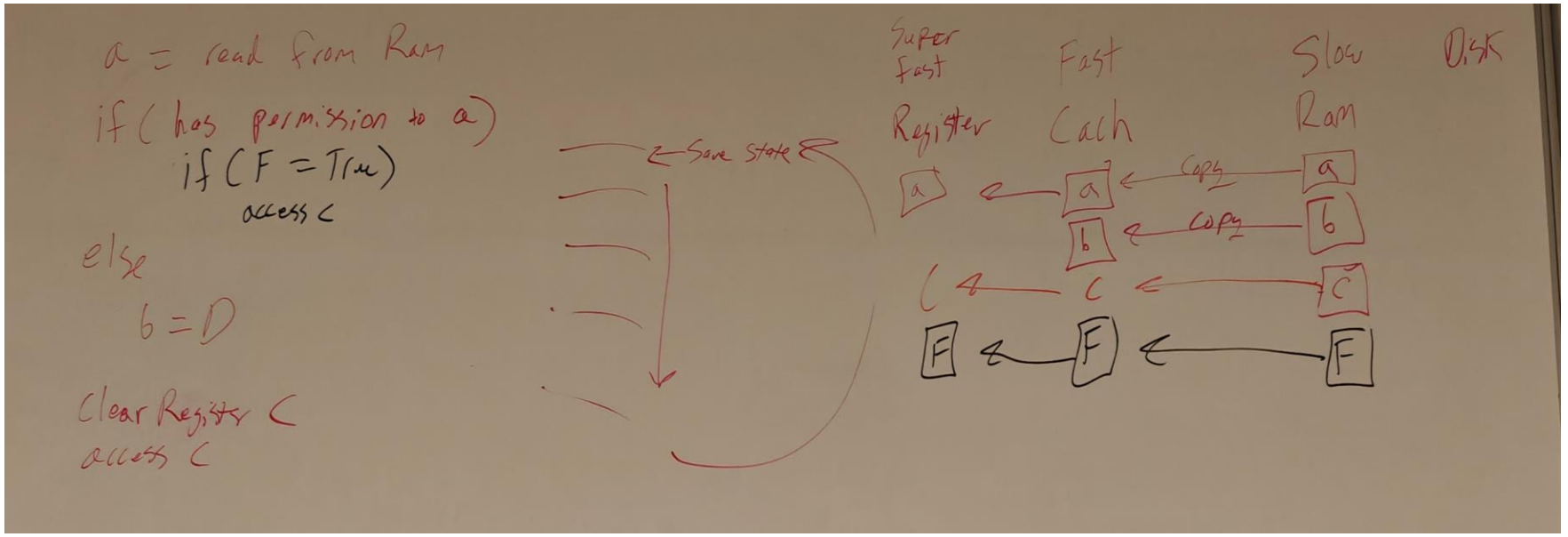
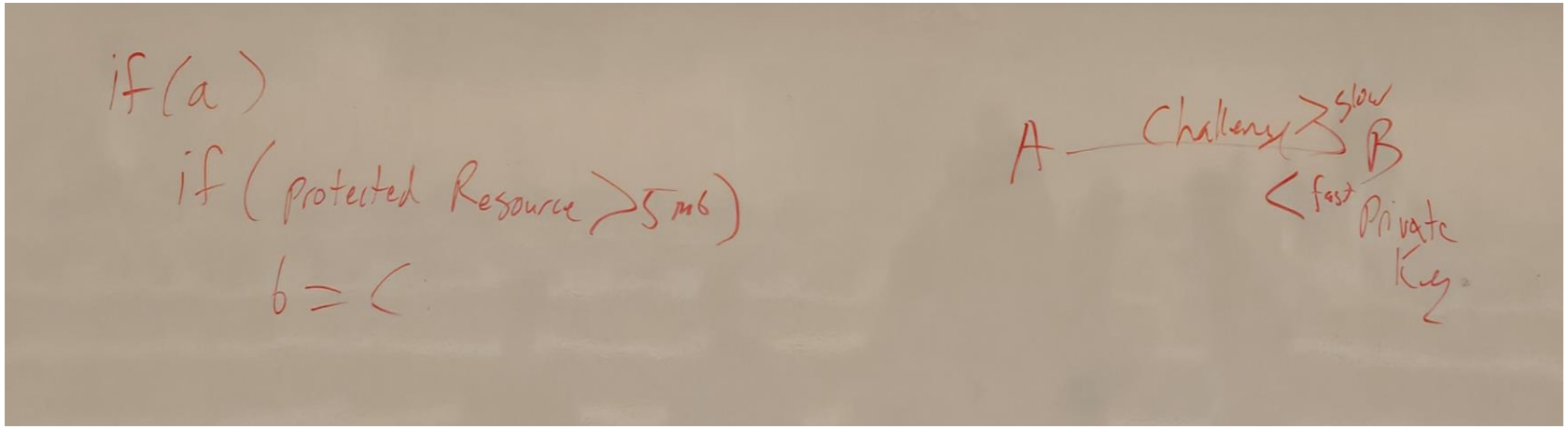


Figure 1: Memory deduplication can provide an attacker control over the layout of physical memory.

- Memory deduplication – efficiency feature in hypervisors (VMs) to only store one copy of identical pages.
- Attack: Create an attack VM on the same physical host as victim. RowHammer victim to make pages identical. Hypervisor helpfully merges pages. Attacker now has access to victim page

Spectre and Meltdown (photo of final white board)





Spectre (2017/2018)

- Timing attack using speculative execution in the CPU
- "[induces] a victim to speculatively perform operations that would not occur during strictly serialized in-order processing of the program's instructions, and which leak victim's confidential information via a covert channel to the adversary."

Kocher, Paul, et al. "Spectre attacks: Exploiting speculative execution." *Communications of the ACM* 63.7 (2020)

Meltdown (2017/2018)

- Race condition attack between memory access and privilege level check

1. Attacker chooses a memory location inaccessible to them and gets it loaded into a register
2. A transient instruction access a cache line based on that register
3. Attacker uses Flus+Reload (timing) to determine the accessed cache line

HACKING CAR KEYS

Car thefts in Canada are on the rise.

Thefts in Ontario nearly doubled in 2022.

MACLEAN'S

Car thefts have reached crisis levels across Canada. How did we get here?

A car is now stolen every six minutes in Canada, and organized crime rings are largely to blame

KATIE UNDERWOOD

SEPTEMBER 7, 2023

In the last two years, the country's car-theft rates graduated from a simmering problem to a full-blown crisis. In 2022 alone, the number of stolen cars nearly doubled in Ontario and Quebec and rose by a third in Alberta and 20 per cent in Atlantic Canada. The total annual financial damage? A billion dollars in losses. Life has been especially cruel to owners of Honda CR-Vs, a model that now holds the dubious honour of being the country's most commonly stolen vehicle.

We can't simply boil down this stealing spree to Canadians mindlessly leaving their passenger doors unlocked at night, or even the widespread car-manufacturing shortage set off by the pandemic. Michael Rothe, president and CEO of the Canadian Finance and Leasing Association, says a large majority of thefts are actually being orchestrated by organized crime rings, who use the profits to finance illegal activities like drug and gun trafficking and human smuggling. Canada is quickly becoming known as a "donor country" for vehicles because, according to Rothe, we make getting away with it easy. Here, Rothe explains how this crisis reached its current

Car thefts in Canada are on the rise.

Thefts in Ontario nearly doubled in 2022.

MACLEAN'S

Car thefts have reached crisis levels across Canada. How did we get here?

"Another new trend targets cars with push-button starts. Some criminals will sit at the end of your driveway and intercept the radio signal from your fob, program their own key with it and steal the car. It's called a "relay attack," and it can happen in a matter of seconds."

stolen cars nearly doubled in Ontario and Quebec and rose by a third in Alberta and 20 per cent in Atlantic Canada. The total annual financial

If you own a push-start vehicle, a very simple tip is to buy a Faraday bag. They're roughly $20 on Amazon and block wireless signals from entering or leaving your car, which prevents hacking.

president and CEO of the Canadian Finance and Leasing Association, says a large majority of thefts are actually being orchestrated by organized crime rings, who use the profits to finance illegal activities like drug and gun trafficking and human smuggling. Canada is quickly becoming known as a "donor country" for vehicles because, according to Rothe, we make getting away with it easy. Here, Rothe explains how this crisis reached its current

Hyundai and Kia vehicles do not use engine immobilizers. As a result, they can be started using an USB cable.

New York sued because stolen cars were becoming a public nuisance. Companies settled for $200 million.

Reuters

My News

Legal | Product Liability | Public Policy | ADAS, AV & Safety | Litigation

New York City sues Hyundai, Kia over vehicle thefts

By **Jonathan Stempel**

June 6, 2023 8:59 PM EDT · Updated a year ago

NEW YORK, June 6 (Reuters) - New York City on Tuesday sued Hyundai Motor Co (005380.KS) and Kia Corp (000270.KS), accusing the South Korean automakers of negligence and creating a public nuisance by selling vehicles that are too easy to steal.

The most populous U.S. city joined several other major cities that have sued Hyundai and Kia over the thefts, including Baltimore, Cleveland, Milwaukee, San Diego and Seattle.

In a complaint filed in Manhattan federal court, New York faulted the automakers' failure from 2011 to 2022 to install anti-theft devices called immobilizers on most of their cars, making them "nearly unique" among automobile manufacturers.

New York said this has "opened the floodgates to vehicle theft, crime sprees, reckless driving, and public harm," exacerbated by TikTok videos showing how to steal cars that lack push-button ignitions and immobilizers.

The city said the number of reported stolen Hyundais and Kias doubled last year, followed by a "virtual explosion of thefts" in the first four months of 2023 with 977 reported thefts, up from 148 in the same period in 2022.

Hyundai and Kia vehicles do not use engine immobilizers. As a result, they can be started using an USB cable.

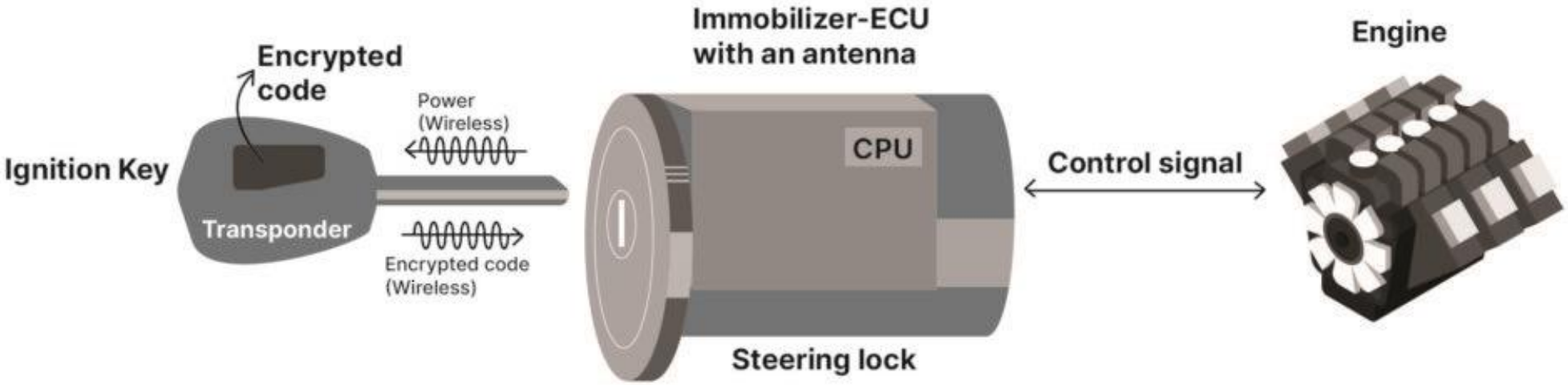
New York sued because stolen cars were becoming a public nuisance. Companies settled for $200 million.

thedrive.com

Tour of car security history heavily drawn from “Security Engineering” v3 by Ross Anderson

Engine immobilizer: challenge response protocol

- Simple idea: use cryptography to verify that the real key is present
- Engine (E) sends a random number (N) to the key transponder (T). Transponder then encrypts N using the shared key K and sends back to the Engine.
  - $E \rightarrow T: \ N$
  - $T \rightarrow E: T, \{T, N\}_K$



https://www.sic.co.th/whatisimmobilizer/

- Older key transponders only worked if the metal key was inserted as well.
- Close proximity mean low signal strength needed
- Key powered using signal power sent by car

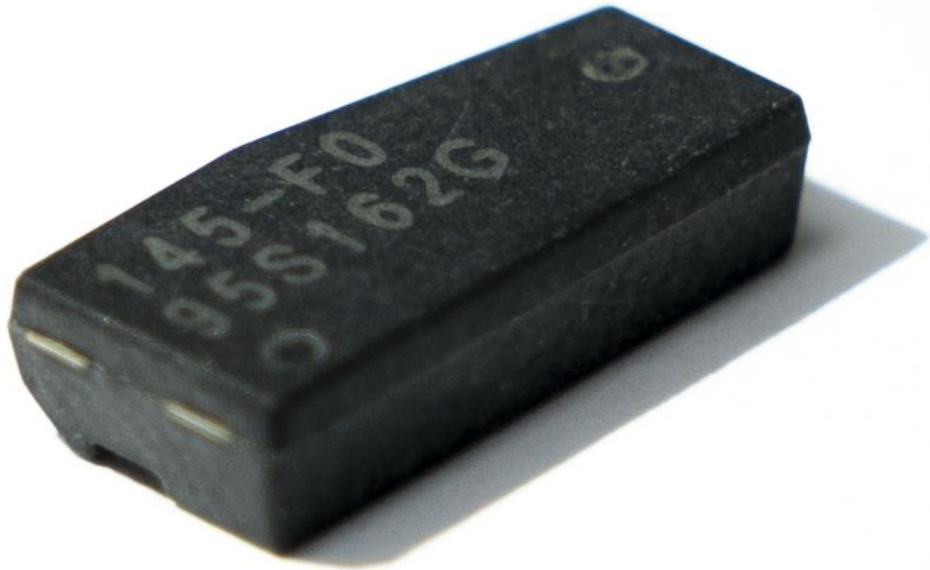
Lots of ways to mess up implementation....

- Key length – too short and it can be guessed
- Same cryptographic keys for many cars
- Poor cryptographic implementation
- Pretend to be owner/mechanic and duplicate the key
- Relay attacks
- Replay attack

https://www.sic.co.th/whatisimmobilizer/

Texas Instrument's DST transponder

- Used by large car companies
- Basis for the SpeedPass Toll payments
- Used 40-bit key
- It was so short because of US export controls (see crypto wars)
- Key could be brute force computed based on two observed challenge/response pairs (offline attack)



https://en.wikipedia.org/wiki/Digital_signature_transponder

Succeeded by the DST80

- Serious implementation problems with key management
  - Hundai keys only have 3 bytes of entropy
  - Toyota keys derived from device serial number that attacker can read (Tesla also did this)

We discovered that Kia and Hyundai immobiliser keys have only three bytes of entropy and that Toyota only relies on publicly readable information such as the transponder serial number and three constants to generate cryptographic keys. Furthermore, we present several practical attacks which can lead to recovering the full 80-bit cryptographic key in a matter of seconds or permanently disabling the transponder.

Image from service that will duplicate car key fobs for you. If such a service exists for your car, be concerned.

https://sumokey.com/collections/rfid-duplicate-by-serial-number

Wouters, Lennert & Van den Herrewegen, Jan & Garcia, Flavio & Oswald, David & Gierlichs, Benedikt & Preneel, Bart. (2020). Dismantling DST80-based Immobiliser Systems.

Volkswagon used a fixed "master" key

- "we show that the security of the keyless entry systems of most VW Group vehicles manufactured between 1995 and [2016] relies on a few, global master keys. We show that by recovering the cryptographic algorithms and keys from electronic control units, an adversary is able to clone a VW Group remote control and gain unauthorized access to a vehicle by eavesdropping a single signal sent by the original remote"

Valid use of master key: pacemakers. A surgeon needs to be able to interact with any pacemaker, even if they did not install it.

Heartteam.com

Lock It and Still Lose It – On the (In)Security of Automotive Remote Keyless Entry Systems. by Garcia et al. in USENIX

QUESTIONS