Cyber-Security (of Cars)

Zhenkai Zhang
CPS Summer Camp

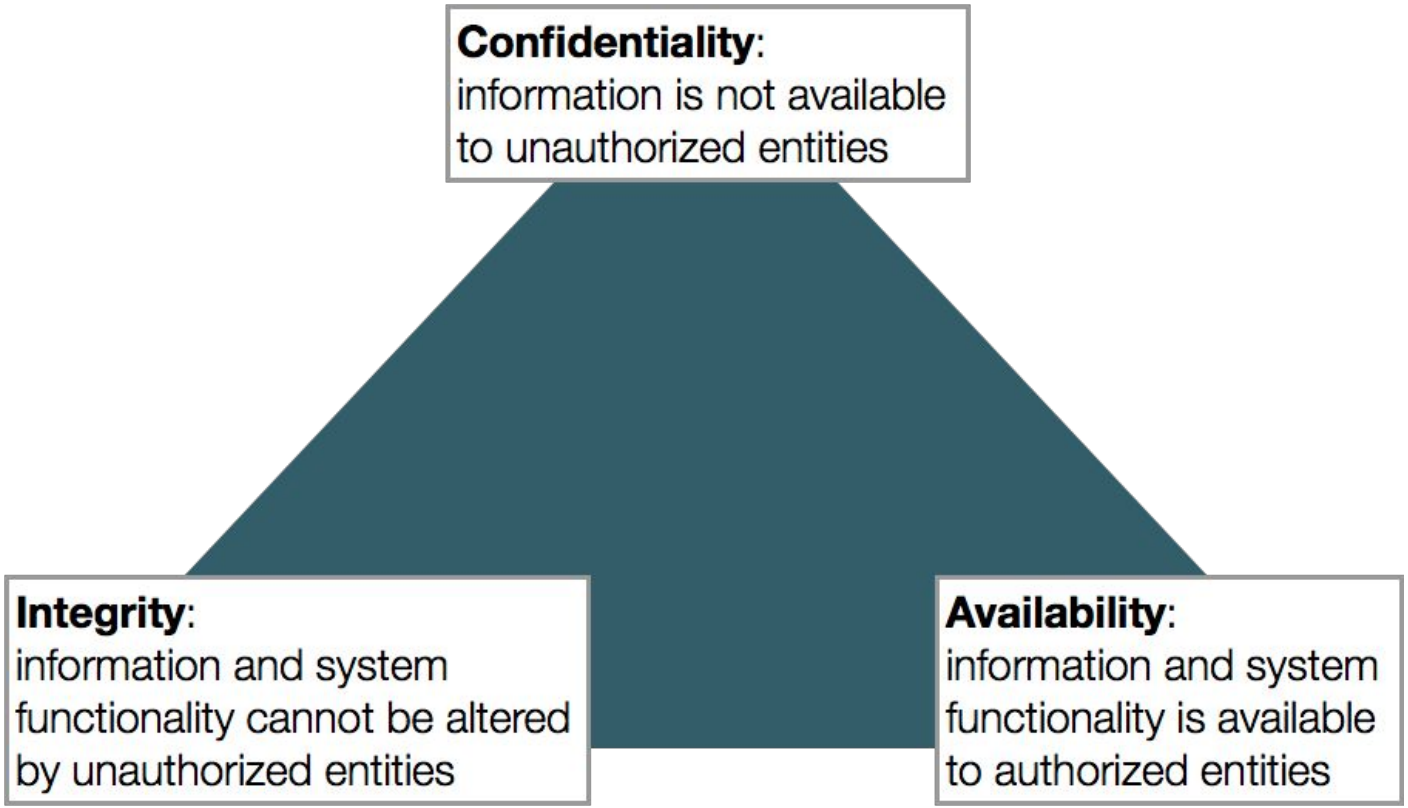
Disclaimer: This presentation is based on “Survey on Security Threats and Protection Mechanisms in Embedded Automotive Networks” by I. Studnia et al.

What is cyber-security?

NIST (National Institute of Standards and Technology) Computer Security Handbook gives a well-accepted definition:

> The protection afforded to an automated information system in order to attain the applicable objectives of preserving the **integrity**, **availability**, and **confidentiality** of information system resources (includes hardware, software, firmware, information/data, and telecommunications).

CIA triad -- three objectives of cyber-security



Examples in reality

1. In 2000, a 15-year-old Canadian known as Mafiaboy launched one of the first huge DoS attack on websites including Amazon, Yahoo, eBay and CNN, causing an estimated $1.3 billion in lost business
2. In 2011, a US Lockheed RQ-170 drone was captured by Iran. It has been suggested that Iran used spoofed GPS signals to bring it down
3. From December 2012 to January 2013, more than 20 US banks suffered DoS attack, banks including Chase, Bank of America, Capital One and Citibank were disrupted
4. In 2013, Target was hacked and millions of customers' credit card numbers were disclosed. Target says the cost is more than $162M
5. In 2013, the Emergency Alert System on Montana station KRTV broadcasted a message with an alert that "the bodies are rising from their graves and attacking the living"
6. In 2016, two hackers obtained names, email addresses, and mobile phone numbers of 57 million Uber users and driver license numbers of 600,000 Uber drivers
7. In 2016, the DoS attack against the DNS provider Dyn caused millions of users failing to connect numerous websites

Cars of the future

https://www.deccanchronicle.com/140601/technology-science-and-trends/article/have-you-seen-suitcase-scooter-yet

Your car runs on code

- ECUs (Electronic Control Units) are the embedded computers in your car which monitor and control your car
  - Modern vehicles usually have up to 70 ECUs
  - ECUs are interconnected to form an internal network of the car
  - Previously, ECUs could not be easily accessed from outside
    - The implementation of security mechanisms into ECU network was not a major concern
- Modern cars are able to communicate with outside through wired or wireless interfaces, such as USB, Bluetooth, WiFi, or even 3G
  - The trend keeps increasing with the future deployment of vehicle-to-vehicle and vehicle-to-infrastructure communications
  - ECU network can not be considered as *closed*
    - Such interfaces may expose the internal network to an attacker
    - They are seen as entry points for cyber-attacks

Automotive network examples

- CAN (Controller Area Network) is a serial bus designed for automotives
  - A node can start transmitting if no message is currently being transmitted on the bus
  - Data transmission rate can go up to 1Mbps
  - CAN is the most used protocol in automotive networks
- LIN (Local Interconnet Network) uses a master-slave model
  - A slave can only send a message if asked to by the master
  - Data transmission rate can only go up to 20kbps (low-cost solution to connect ECUs)
  - LIN is usually used for controlling a car's comfort elements (window lifts or windshield wipers)
- FlexRay arises as a successor to CAN
  - Data transmission rate can go up to 10Mbps
  - Such rates enable X-by-wire -- to electrically control these currently mechanical controlled systems like steering wheel (steer-by-wire) or the brakes (brake-by-wire)
- MOST (Media Oriented Systems Transport) is used to carry multimedia data
  - It offers rates up to 24Mbps

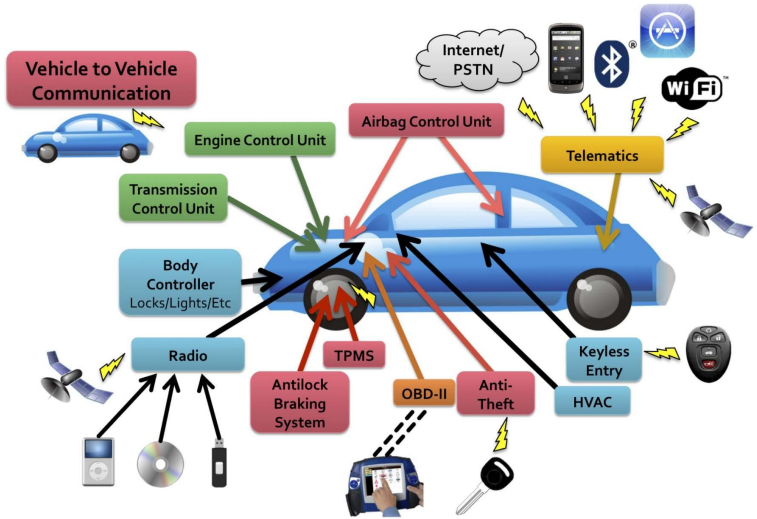
SAE classification of automotive networks

SAE (Society of Automotive Engineers) classified communication protocols in four categories, ranging from A to D, according to their rates and offered features

Class	Rate	Use	Examples
A	<10kb/s	Body control	LIN
B	10kb/s $\rightarrow$125kb/s	Non critical generic data transfer	CAN-B (Low-speed CAN)
C	125kb/s $\rightarrow$1Mb/s	Critical real-time communications	CAN-C (High-speed CAN)
D	>1Mb/s	Multimedia or X-by-wire	MOST, FlexRay

Possible connections of a modern car

As mentioned earlier, a car's internal networks are not complemented by means of communication with external devices

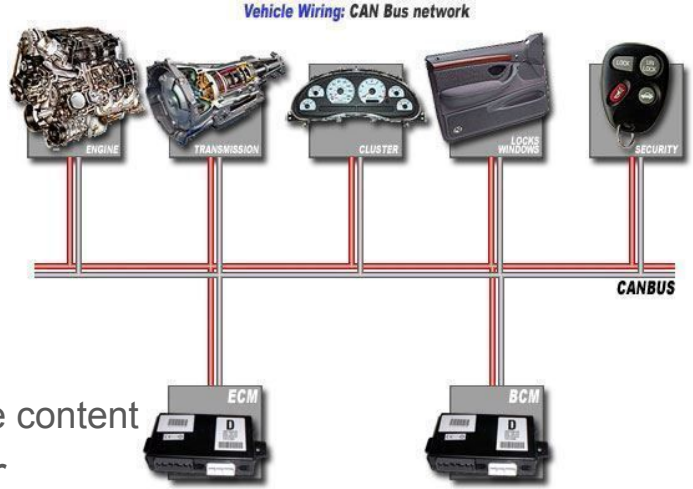


S. Checkoway et al., "Comprehensive experimental analyses of automotive attack surfaces, " in Proc. 20th USENIX Security, San Francisco, CA, 2011.

Attack goals

- Theft: this is the most obvious motivation at the first glance
  - For example, an attacker can exploit a vulnerability in a wireless communication protocol to quietly unlock the targeted car and then deactivate the immobilizer or a potential alarm
- Electronic tuning: this gathers all the situations where the attacker is also the owner of the car -- his goal is to make unauthorized modifications
  - For example, Tesla is selling a 70kWh battery that is secretly a 75kWh battery, and an attacker may try to unlock this feature without paying
- Sabotage: this contains all the attacks aimed at damaging the vehicle through the deactivation of ECUs, the alternation of their software, or DoS
  - Consequences range from minor inconveniences to potentially deadly accidents
- Privacy breach: this is to obtain personal information stored on the car
  - For example, an attacker can retrieve the driver's phone directory and call history, GPS coordinates history, or favorite radio frequencies
- Intellectual property theft: this is to obtain confidential information about the design of the car
  - For example, an attacker can reverse engineer the code running on the ECU or a proprietary bus protocol

Vulnerabilities on the bus



Let’s focus on vulnerabilities on CAN bus

- Confidentiality: CAN broadcasts every message
  - A malicious node can eavesdrop on the bus and read the content
- Authenticity: CAN doesn’t authenticate its sender
  - Any node can potentially send messages that should only be sent by some other nodes
- Integrity: CAN uses CRC to check if bits are flipped during transmission
  - A CRC can be easily forged if a message is changed by an attacker
- Availability: CAN naively arbitrates messages
  - An ECU can flood the CAN bus with high priority frames to cause a DoS
- Non-repudiation: CAN has no way to prove who did what
  - An ECU can’t prove it has not sent or received a given message

https://canbuskits.com/what.php

Threats posed by OBD port

OBD (On Board Diagnostics) port is implemented in every car sold in the US (since 1996) and the EU (since 2001 for gas-powered vehicles and 2004 for diesel-powered ones)

- OBD port is used to retrieve diagnostic data of the car through CAN bus
- OBD dongles are used to interface a computing device with the OBD port
  - It can be legally by anyone
- Many documented attacks based on OBD port are available
  - Some ECUs can be updated and reflashed
  - Automotive virus can infect the car, which is triggered only under certain conditions

Attacks on CD player

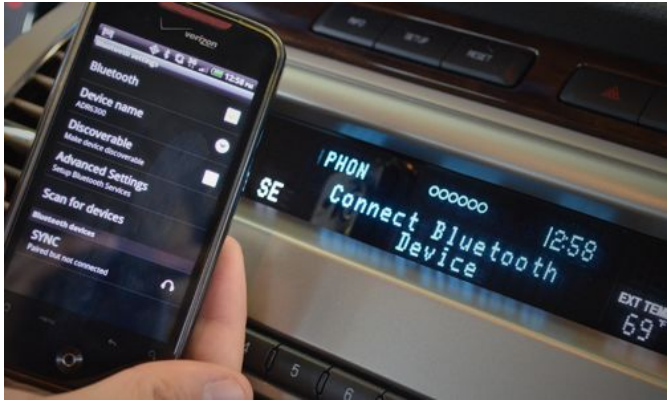
Two attacks have been identified in some CD players

- The insertion of a CD containing a file with a certain name tricked the player into believing it to be a firmware update
  - Malicious software can be installed
- An playable WMA file can even be created to cause the player to emit messages on the bus while reading it

http://www.azoft.ru/blog/razrabotka-ui-dlya-mediapleera/

Security issues in wireless pairing of mobile devices

- Modem vehicles can sometimes be paired with mobile devices
  - For example, the driver can connect his phone via Bluetooth and use his car's sound system as a hands free kit
- The implementation of such wireless protocols into the car can be faulty
- Exploiting such vulnerabilities can lead to
  - the retrieval of data stored into the communication unit
  - the ability to eavesdrop on the conversations (like phone calls or conversations between the passengers), or even
  - the compromission of the ECU (and therefore the network)

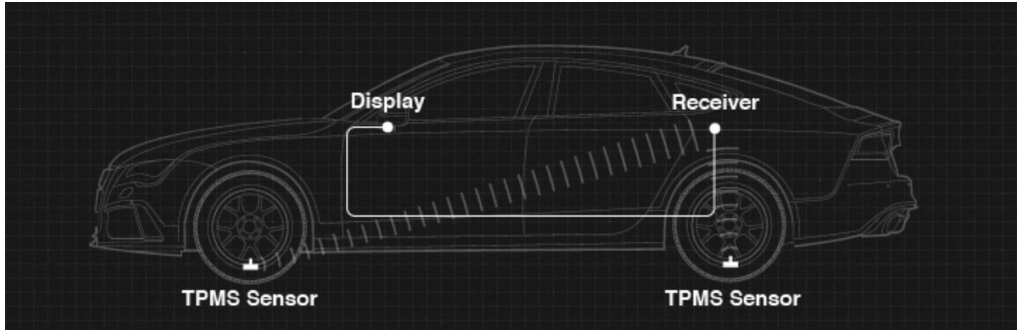


http://cars.phototourismbg.com/how-to-connect-phone-to-ford-sync/

Attacks on TPMS

TPMS (Tire Pressure Monitoring System) is composed of a pressure sensor inside the tire that sends its data to a dedicated ECU located on the CAN via a radio frequency emitter

- TPMS are now mandatory in the US, in Europe and soon in Japan
- Attacks against a TPMS allowed an attacker to eavesdrop on it from up to 40 meters and send spoofed messages to the monitoring ECU, causing it to turn on tire pressure warning lights at inappropriate times



http://autoexpress.com.pk/2018/03/29/my-tpms-light-came-on-what-does-it-mean/

Attacks on wireless unlocking

- Many cars now implement a remote unlocking of their doors or alarms
  - While some encryption is applied to such instructions sent over the air, it can be cracked
    - For example, attacks against KeeLoq, a block cipher used by several manufacturers, have been described in the literature
- Passive Keyless Entry and Start (PKES) systems allow the drivers to unlock and start their cars while keeping their keys in their pockets
  - A team was able to perform relay attacks on PKES systems of ten different car models
    - By placing an antenna close to the key holder (within a 8m radius) and another near the targeted car, they were able to unlock it then start its engine while the keys were actually 50 meters from the car
- New car models may also allow the owner to remotely control the vehicle from a mobile device (e.g., OnStar RemoteLink app)
  - Samy Kamkar found a vulnerability that can exploited to remotely control OnStar-enabled GM cars

Long-range attacks

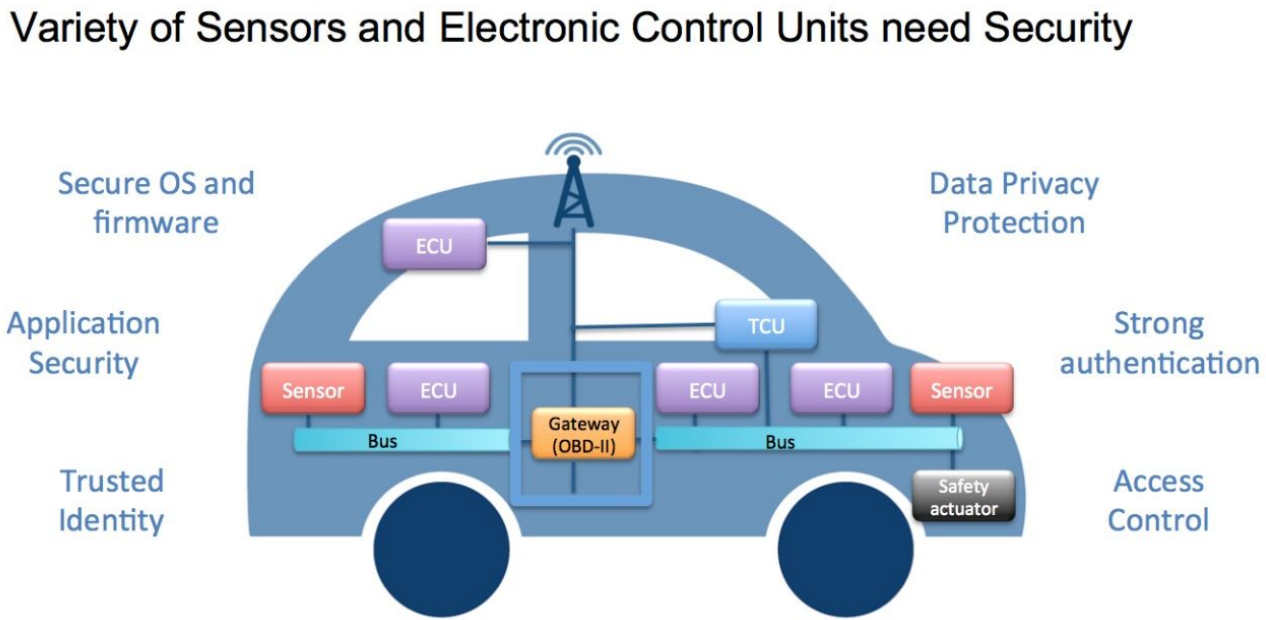
- Telephony: Following the discovery of several vulnerabilities in the telematic unit, Checkoway et al. successfully made it execute custom code downloaded through the 3G network, effectively compromising the vehicle
- Web browsing: In the event that a vehicle embeds a web browser, possible exploits similar to those found on traditional computers and mobile devices are to be considered (e.g., buffer overflow, code injection, etc.)
- App store: In a trend similar to what can be found on the smartphones, some car manufacturers already provide, via the firm online store, a selection of downloadable applications for the multimedia unit of their cars. A successful attack against the online store, or a program sold on such a store actually containing a trojan horse would have serious large scale consequences

Relay attack against PKES demonstration

Locate, unlock, and remote start vehicles…

Hackers remotely kill a Jeep on the highway …

More security is needed



http://telematicsnews.info/2015/09/23/ibm-and-giesecke-devrient-team-up-on-connected-car-security_s6234/

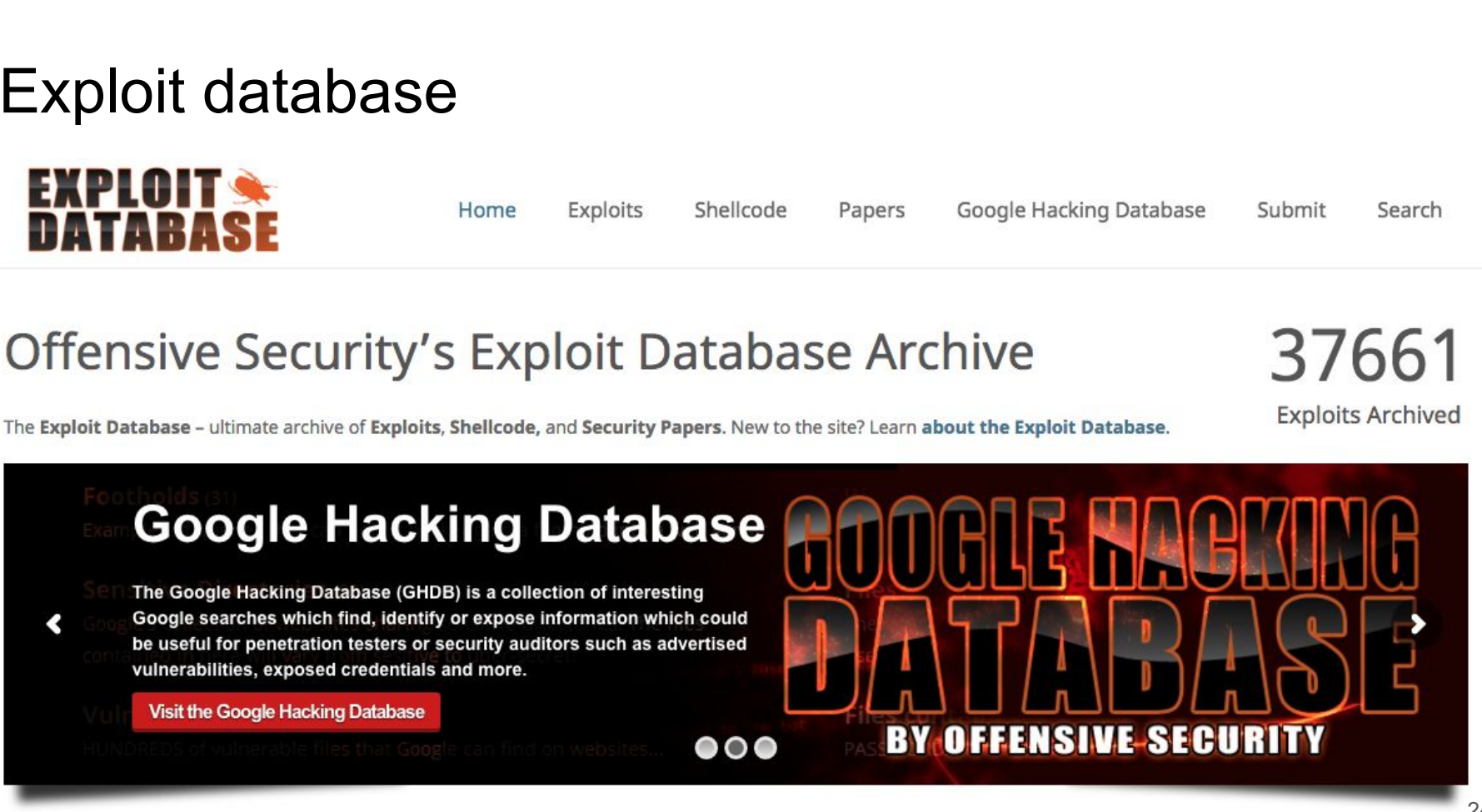
Protection mechanism examples

- External
  - Design secure communication architectures for V2V and/or V2I communications
  - Strictly follow existing security recommendations about communication protocol
  - Integrate additional defense mechanism to secure the communication
- Internal
  - Apply cryptographic technique to encrypt the message transmitted
  - Monitor the data transmission to detect anomalies occurring in the system
  - Ensure the ECU software integrity

Black Hat & DEF CON

Black Hat (USA, Asia, Europe) and DEF CON are the two major annual security conventions that many hackers, security researchers, industrial practitioners, executives, government agents, and non-technical individuals would attend

Exploit database



Why you want to delve into cybersecurity later on?

According to Forbes, there were one million cybersecurity job openings in 2016

“

… the burgeoning cybersecurity market which is expected to grow from $75 billion in 2015 to $170 billion by 2020 …

… a career can mean a six-figure salary, job security, and the potential for upward mobility…

… more than 209,000 cyber-security jobs in the U.S. are unfilled, and postings are up 74% over the past five years, according to a 2015 analysis of numbers from the Bureau of Labor Statistics by Peninsula Press, a project of the Stanford University Journalism Program …

”

Questions?

Thank you for your attention!