Electronic Carjacking

Alexander Pires

March 7, 2012

Example, please?

Example, please?

- In February 2010, an employee is fired from a Texas car dealership that uses GPS devices for repossession purposes.

Example, please?

- In February 2010, an employee is fired from a Texas car dealership that uses GPS devices for repossession purposes.
- He uses an old colleague's password to remotely shut down more than 100 vehicles.

That wasn't really carjacking...

Around the same time, Toyota is starting to look into this "unintended acceleration" issue in some of their vehicles.

That wasn't really carjacking...

Around the same time, Toyota is starting to look into this "unintended acceleration" issue in some of their vehicles.

- A year later, independent investigation placed the blame on drivers and mechanical defects, not electronics.

That wasn't really carjacking...

Around the same time, Toyota is starting to look into this "unintended acceleration" issue in some of their vehicles.

- A year later, independent investigation placed the blame on drivers and mechanical defects, not electronics.
- A team of researchers used this opportunity to publish their findings on the security of vehicle electronics.

...And?

They found multiple vectors of attack on vehicle systems.

...And?

They found multiple vectors of attack on vehicle systems.

1. Physical access via the OBD-II port all newer vehicles have.

...And?

They found multiple vectors of attack on vehicle systems.

1. Physical access via the OBD-II port all newer vehicles have.
2. "PassThru" devices that serve as an interface between this port and Windows-based machines.

...And?

They found multiple vectors of attack on vehicle systems.

1. Physical access via the OBD-II port all newer vehicles have.
2. "PassThru" devices that serve as an interface between this port and Windows-based machines.
3. Buffer overflows and authentication failures in onboard Wifi and Cellular devices.

...And?

They found multiple vectors of attack on vehicle systems.

1. Physical access via the OBD-II port all newer vehicles have.
2. "PassThru" devices that serve as an interface between this port and Windows-based machines.
3. Buffer overflows and authentication failures in onboard Wifi and Cellular devices.
4. Playing corrupted music files in the CD player.

Wait, CDs?

All of these exploits granted full control over every system in the vehicle.

Wait, CDs?

All of these exploits granted full control over every system in the vehicle.

- Modern vehicles can have 70 or more different Electronic Control Units (ECU).

Wait, CDs?

All of these exploits granted full control over every system in the vehicle.

- Modern vehicles can have 70 or more different Electronic Control Units (ECU).
- These all communicate over a special networking system known as a Controller Area Network (CAN).

Wait, CDs?

All of these exploits granted full control over every system in the vehicle.

- Modern vehicles can have 70 or more different Electronic Control Units (ECU).
- These all communicate over a special networking system known as a Controller Area Network (CAN).
- When compromised, it can grant full control over every electronic system in the car.

Why so vulnerable?

- Modern vehicle systems "need" to be very interconnected for desired functionality.

Why so vulnerable?

- Modern vehicle systems "need" to be very interconnected for desired functionality.
- Many of the interfaces between ECUs are custom-built, and use unsafe C functions like strcpy.

Why so vulnerable?

- Modern vehicle systems "need" to be very interconnected for desired functionality.
- Many of the interfaces between ECUs are custom-built, and use unsafe C functions like strcpy.
- Programs like telnetd, ftp, and vi still installed in the OS of some PassThru and Bluetooth devices.

So...when can we panic?

The researchers say nobody should panic.

So...when can we panic?

The researchers say nobody should panic.

- It took 10 of them nearly 2 years to develop these exploits for one brand of car.

So...when can we panic?

The researchers say nobody should panic.

- It took 10 of them nearly 2 years to develop these exploits for one brand of car.
- Vehicle software often differs based on manufacturer and model.

So...when can we panic?

The researchers say nobody should panic.

- It took 10 of them nearly 2 years to develop these exploits for one brand of car.
- Vehicle software often differs based on manufacturer and model.
- Because of this, attacks aren't necessarily cost-effective at the moment.

Down the road...

- The interfaces between ECUs need to be shored up.

Down the road...

- The interfaces between ECUs need to be shored up.
- Some systems should only work if the user is physically in the car.

Down the road...

- The interfaces between ECUs need to be shored up.
- Some systems should only work if the user is physically in the car.
- Inbound cellular connections don't need data transfer.

Down the road...

- The interfaces between ECUs need to be shored up.
- Some systems should only work if the user is physically in the car.
- Inbound cellular connections don't need data transfer.

- Every news story I found said that the industry is working on this.

Questions?

http://www.huffingtonpost.com/2010/03/17/omar-ramoslopez-car-hacke_n_503163.html

http://www.technologyreview.com/computing/35094/?ref=rss&a=f http:

//blogs.discovermagazine.com/80beats/2011/03/16/scientists-can-now-wirelessly-hack-your-car/

http://www.usatoday.com/tech/news/story/2011/08/Cars-vulnerable-to-theft-by-hacking/50057610/1

http://en.wikipedia.org/wiki/CAN_bus http://www.autosec.org/pubs/cars-usenixsec2011.pdfl