

Car Hacking



EECS 3482 Intro to
Computer Security

Team 11:
Najiba, Mike, Edward

Computers have become a necessary part of every car.



A vehicle can have upwards of 35 computer controllers

- engine, steering, doors, braking system, sensors, navigation...



Today these controllers are increasingly interconnected to a central control unit.

Drawback



- Like computers, cars are vulnerable to software attacks and unauthorized access
- The more wireless connections a car offers, the greater the opportunity for intrusions

The background of the slide is a photograph of a car's interior, showing the steering wheel, dashboard, and center console. The image is dimly lit, with a semi-transparent dark overlay that serves as a background for the text.

Updating/patching software currently involves:

- Tracking down owners and notifying them
- Transmitting security patch at car dealerships, via USB key
- Infrequent OTA firmware updates

Components you can control with central ECU (electronic control unit):

A dark-colored Audi car is shown from a front-facing perspective. The car's headlights are illuminated, and the Audi logo (four interlocking rings) is visible on the front grille. The background is dark, making the car stand out.

- Doors, lights, windows, dashboard, horn, engine, steering, braking systems...
- Once access is gained, incorrect data may be fed to central CU: false temperatures, tire pressures, speed, collision distance

Wired Access:

- connect a computer to the ECU



Wireless Access:

- access central ECU through wireless entry point like OnStar





What is the industry doing to ensure
“connected” vehicles are safe?

Making safe cars doesn't just apply
to the mechanical technology
but also to data security.

Mercedes-Benz

- Cloud firewall

Tesla

- White hat hackers

Hyundai

- Long distance communication technologies



Mercedes-Benz

A wide-angle, top-down view of the front interior of a Mercedes-Benz vehicle. The dashboard is dark with wood trim, featuring a central infotainment screen and two air vents. The steering wheel is black with the Mercedes-Benz logo in the center. The seats are light-colored leather with dark stitching. The center console is visible between the seats. The overall lighting is bright and even.

- Enabling people in vehicle to control their data
- Drivers can erase information after they exit vehicle

Tesla



- Hires hackers from all over the world to test information security
- Hires specialists to hack on-board systems in three month projects

Hyundai

Developing technology to use long distance communication to remote access vehicles



Texas Auto Center

More than 100 customers found their cars disabled or the horns honking out of control after disgruntled ex-employee wreaked havoc on dealership's online repo-system



DARPA — Defense Advanced Research Projects Agency

DARPA security experts remote hack a vehicle by sending complex radio message to OnStar system then inserting code to ECU



Award Winning Journalist, Michael Hastings' Death Raises Concerns About Vehicle Hacking

THIS WAS
AN Not
Accident
FBI SURVEILLANCE



“What evidence is available publicly is consistent with a car cyber-attack. And the problem with that is you can't prove it.”

—Richard Clarke, Cybersecurity advisor to George W. Bush



Why should we be concerned?

A black presidential limousine (Cadillac stretch) is the central focus, parked on a street. The car has an American flag and a presidential seal on the hood. Several men in dark suits are standing around the car. In the foreground, there are several people in dark clothing, some wearing balaclavas, and a person in a tan uniform. The background shows a crowd of people behind metal barricades.

- Wireless technology in cars is relatively new
- Vehicles with vulnerabilities will remain on roads for years
- Exploits can have devastating or life threatening consequences

How can consumers safeguard against hacking?



- Prevent others using physical connections with your car
- Prevent others using on-board diagnostics interface
- Do not use remote controller apps
- Understand your vehicle's wireless functions
- Uninstall wireless functions

What implementations can actively protect against software attacks?

The image shows the interior of a modern car, likely a Lexus, with a focus on the steering wheel and dashboard. The steering wheel is black with a silver Lexus logo in the center and features several control buttons. The instrument cluster behind the wheel is digital, displaying a speedometer, tachometer, and navigation information. The central console has a large, curved digital display showing a driver's seat and various control icons like A/C, OFF, and S/M. The interior is finished with dark leather and orange accents.

Software attacks are possible because on board computers are not as sophisticated as personal computers. Intrusion detection as well as malicious code detection will add a crucial security layer to vehicles as they become more “connected”.

Sources

<http://www.cbsnews.com/news/car-hacked-on-60-minutes/>

<http://www.forbes.com/sites/centurylink/2015/01/02/3-hurdles-standing-in-the-way-of-the-internet-of-things-2/>

http://ca.norton.com/yoursecurityresource/detail.jsp?aid=car_computer

<http://money.cnn.com/2015/02/09/technology/security/car-hack/>

<http://www.techtimes.com/articles/14637/20140902/tesla-motors-hiring-hackers-to-improve-security-systems.htm>

<http://www.extremetech.com/extreme/91306-hackers-can-unlock-cars-and-meddle-with-traffic-control-systems-via-sms>

<http://www.scribd.com/doc/236073361/Survey-of-Remote-Attack-Surfaces>