Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study

Presenter: Wenyuan Xu

Ishtiaq Rouf, Rob Miller, Hossen Mustafa, Travis Taylor, Sangho Oh

Wenyuan Xu, Marco Gruteser, Wade Trappe, Ivan Seskar

Dept. of CSE, University of South Carolina

WINLAB, Rutgers University

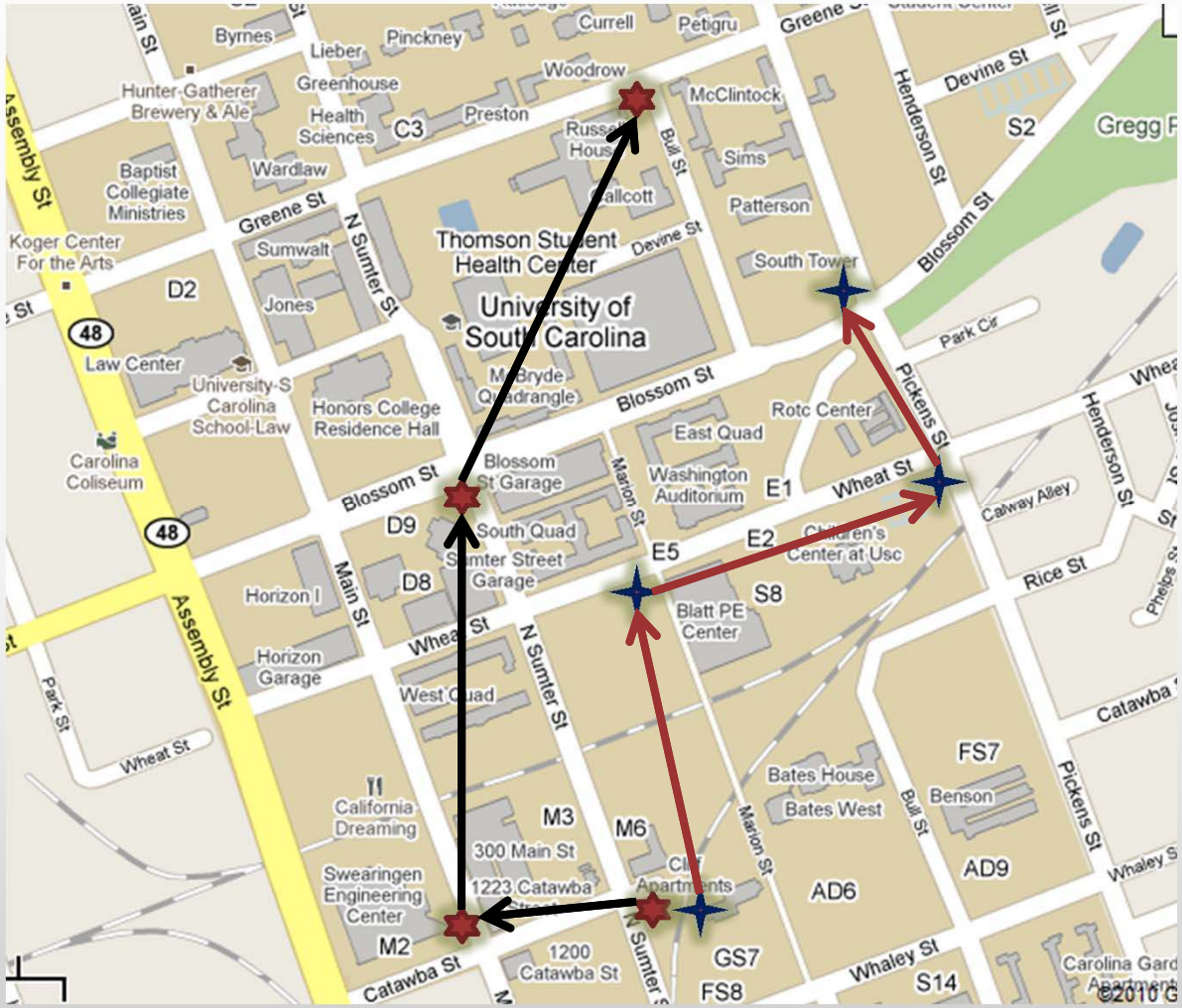
Wireless in Automobiles

- Wireless increasingly connected to CAN bus in automobiles
  - Web-based vehicle-immobilization system
  - MyRate from insurance companies to collect data
  - "iChange" controls the car via an iPhone
  - More in-car wireless sensor networks

Tire Pressure Monitoring System (TPMS)

- What is TPMS?
  - Monitors tire-pressure in real time
  - Alerts drivers if underinflated
  - To increase safety and fuel economy
  - Indirect TPMS vs. direct TPMS
- National Highway Transportation Safety Administration (NHTSA) ***mandates*** TPMS. Virtually, all new cars sold or manufactured after ***2007*** in US are equipped with wireless TPMS.

Misuse 1: Car Tracking



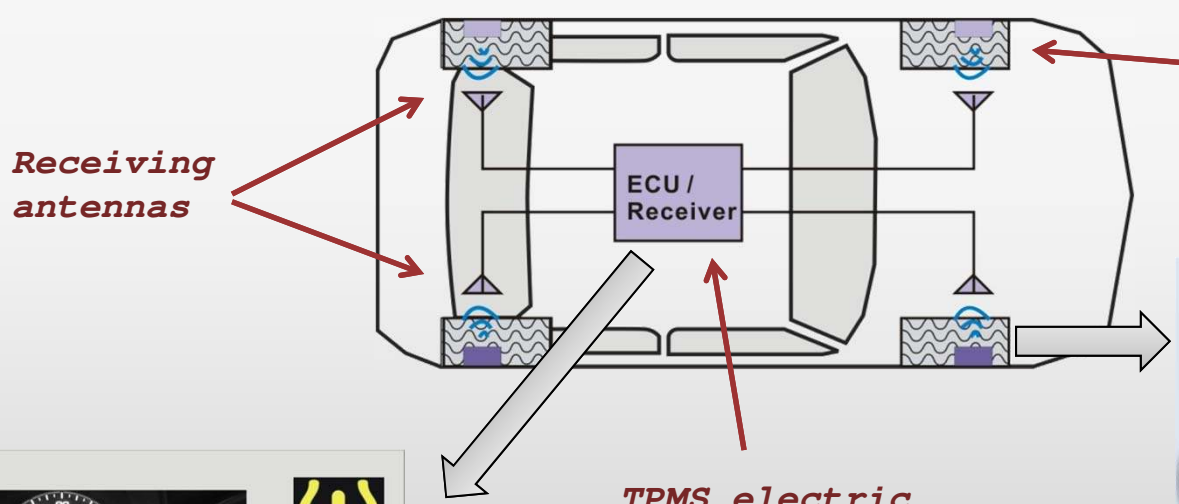
Misuse 2: Trick The Driver To Stop

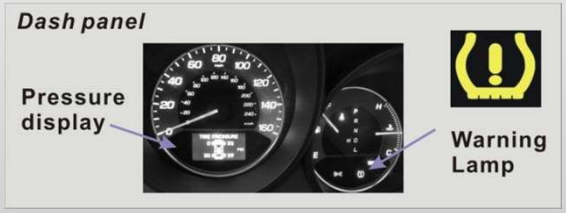
TPMS – To Be Discovered

- What are the communication protocol details?
  - How difficult to reverse engineer?
  - Messages encrypted? Authenticated?
- How easy to eavesdrop TPMS communication?
  - What is the *range*?
  - Travel speeds, car's metal body, message rate, transmission power
- How easy to spoof TPMS communication?
  - What is the *range*?
  - ECU filters/rejects suspicious packets?
  - How much damage can spoofing accomplish?
- What can be done to protect TPMS communication?

TPMS – From the Public Domain

- Communication protocols
  - Link Sensor IDs with TPMS ECU
  - Sensors → ECU **315/433Mhz**
    - ECU filters packets based on IDs
  - Sensors can be waken up by
    - ECU → sensors **125kHz**
    - Travel at high speeds (>40 km/h)





Security and Privacy Analysis
Step 1: Reverse-engineering

- Proprietary protocols
  - Security through obscurity?
- Equipment
- Goal
  - Modulation schemes
  - Encoding schemes
  - Message formats (encrypted?)

ATEQ VT55

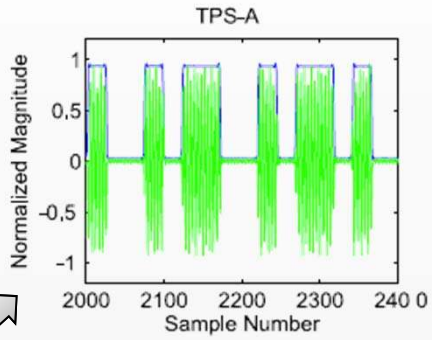
Sensors: TPS-A and TPS-B

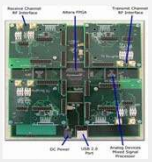
Universal Software Radio Peripheral (USRP)

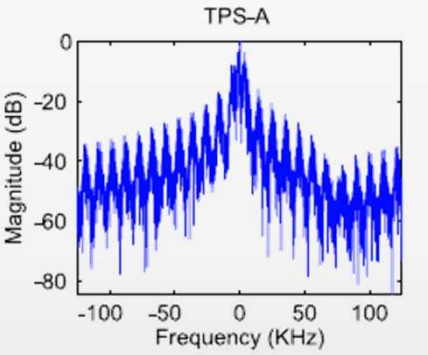
Agilent Vector Signal Analyzer (VSA)

Reverse-Engineering Walk-Through

- Reverse engineering steps
  - Capture packet transmission
  - Demodulate and decode data
  - Determine packet format
- Observations
  - Reverse engineering possible
  - No encryption



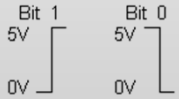




Triggered sensors at 125 kHz → **Responded at 315 MHz** → **Captured RF transmission at 315 MHz** → **Determined Modulation ASK** → **Encoding Scheme Manchester** → **Determined Message Format**

32-bit or 28-bit

preamble	Sensor ID	Pressure	Temperature	Flags	Checksum



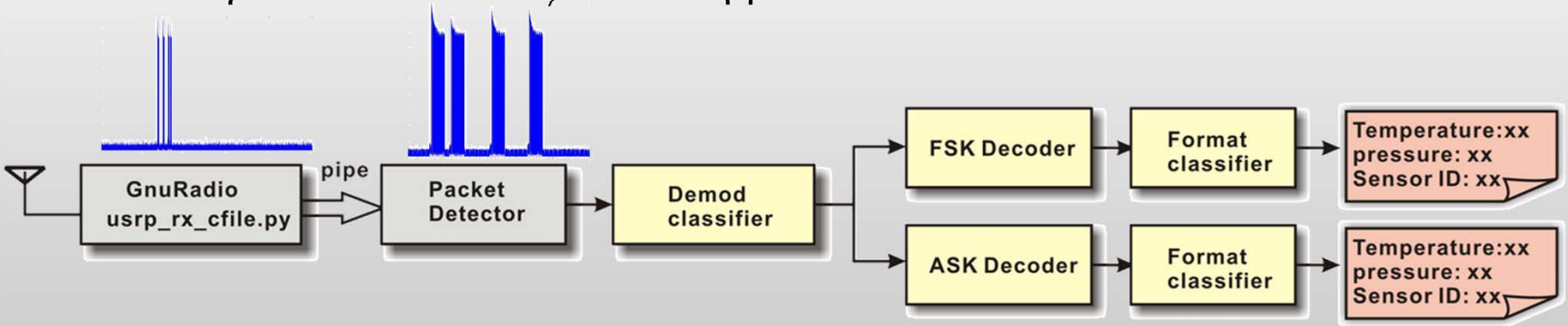
How likely that two cars have the same ID?

→ 10^{15} cars with P_c = 1%.

Security and Privacy Analysis
Step 2: Eavesdrop capability

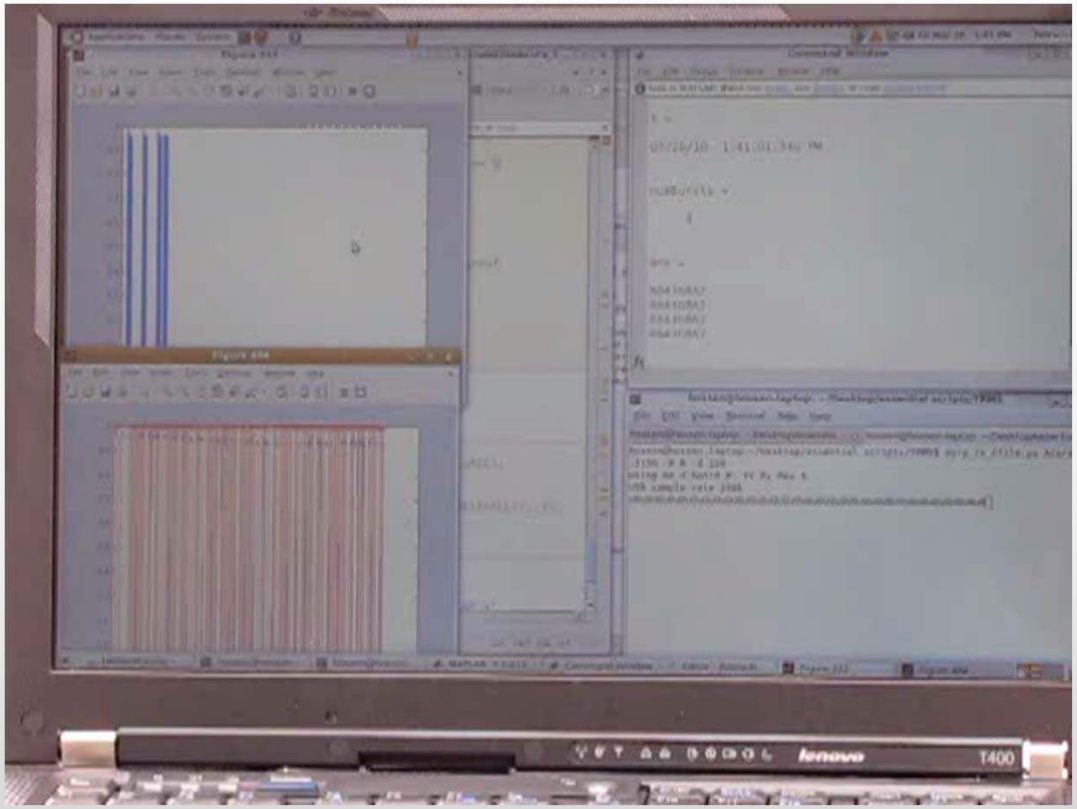
- How likely to eavesdrop?
  - Cars travel at high speeds
  - Cars' metal bodies shield RF
  - TPMS message rate (1 per 60s-90s)
  - Low transmission power (battery)
- Eavesdropping System
  - Used USRP only, no VSA
  - Used low noise amplifier (LNA)
  - Reused decoders from RE
  - Developed a live decoder/eavesdropper

Low noise amplifier (LNA)



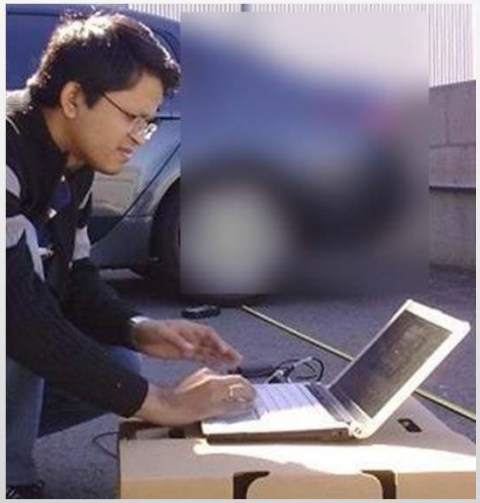
Demonstration of Live Eavesdropping

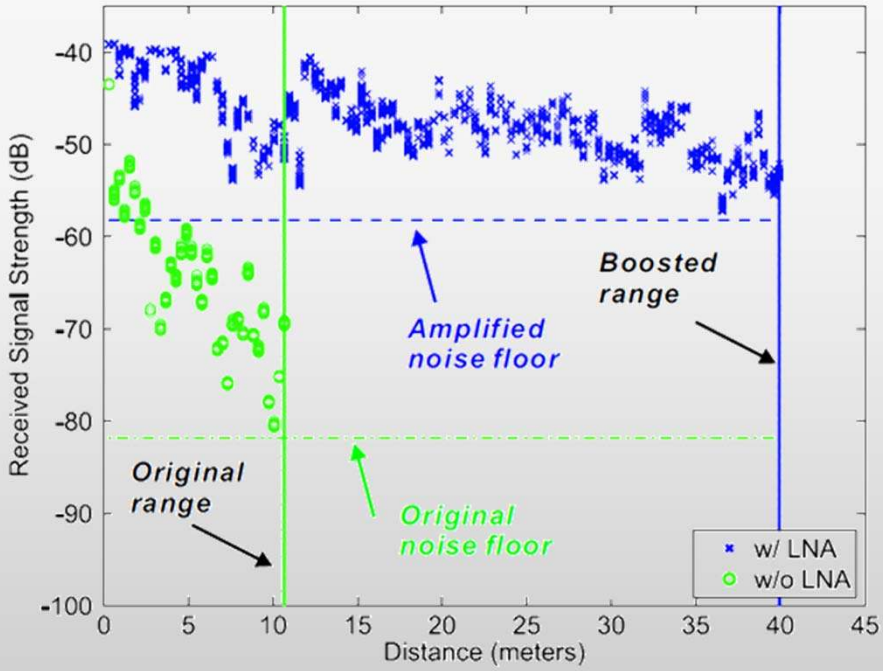
Sensor ID 884368A2



Exp. 1: Eavesdropping Distance

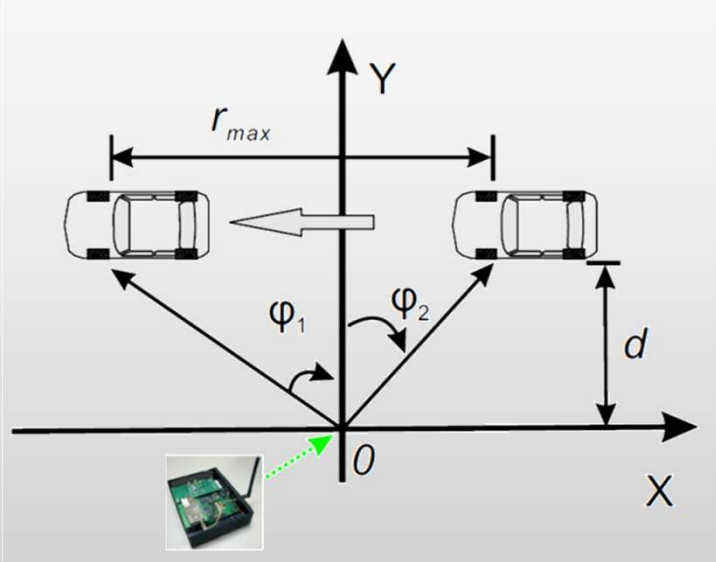
- Scenarios
  - USRP + cheap antenna
  - USRP + LNA ($75) + cheap antenna
- Observations
  - Able to decode packets, if RSS (received signal strength) > Ambient noise floor
  - LNA boosts the decoding range from 10.7m to **40m**

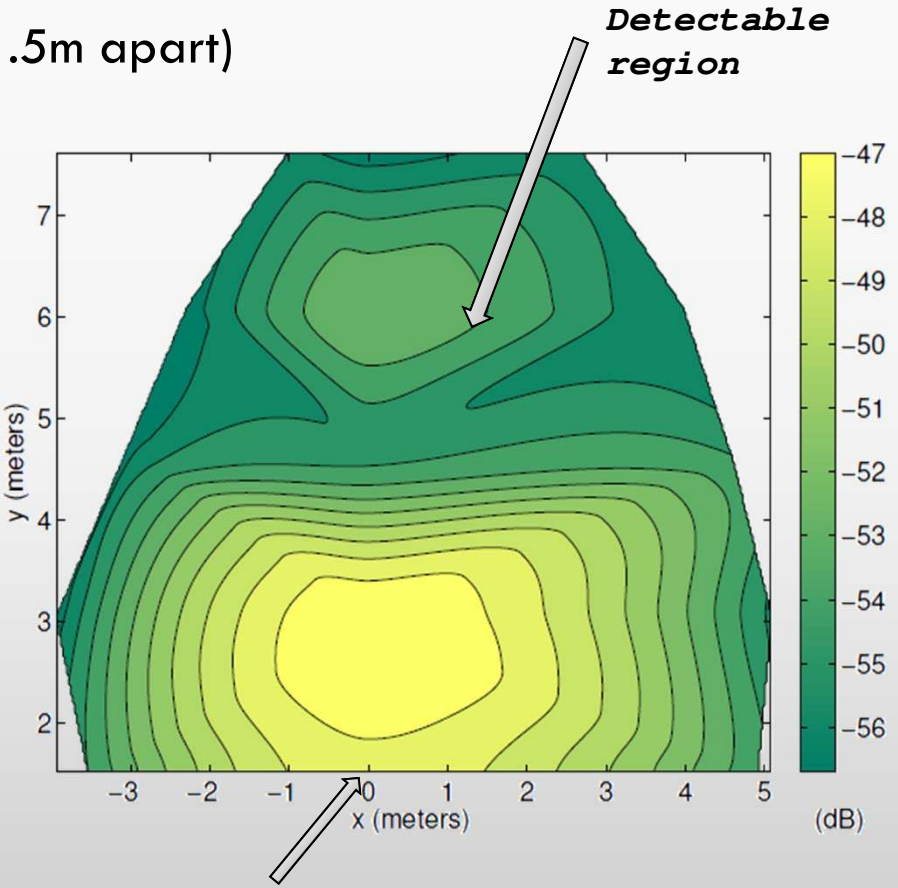




Exp. 2: Eavesdropping Distance and Angle

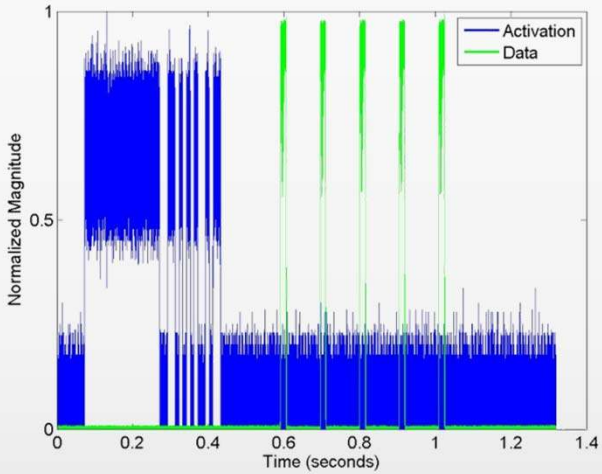
- Setup
  - USRP at origin
  - Car moved parallel to the x-axis (1.5m apart)
- Observations
  - The widest range is 9.1 meters
  - Sniffed at over 70mph speed





Feasibility of Tracking

- Passive tracking
  - Complete location tracking is difficult
  - Given: 1 packet per 60 seconds, eavesdropping range 9 meters
  - A car at 60km/h → 110 sniffers
- Active tracking
  - Activation signal makes the tracking easier
  - Send the activation signal at 125kHz
  - The sniffer places down the road
  - Experiments
    - Obtained timing data: USRP + TVRX (315MHz) + LFRX (125kHz)
    - Validation: ATEQ VT55 (activator) + USRP (sniffer);



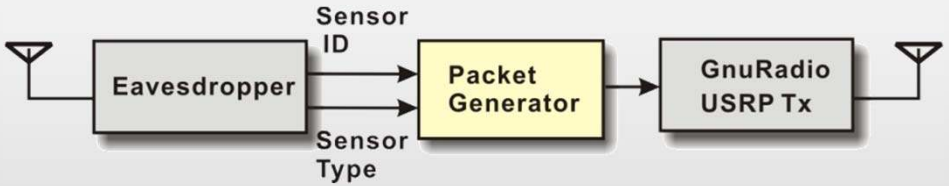
Tracking via TPMS
- Independent of LOS → hidden
- Higher technical requirement to deactivate TPMS

Tracking via License Plate Capture Cameras (LPCC)
- Requires LOS → visible camera mounting location
- Affected by weather
- Less technical sophistication to hide license plates

Security and Privacy Analysis Step 3: Packet Spoofing

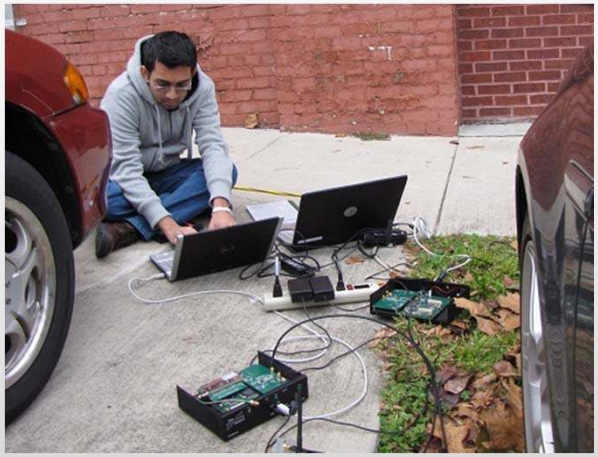
- How likely to spoof TPMS communication?
  - Is the in-car radio able to pick up spoofing packets from outside the vehicle or a neighboring vehicle?
  - Security mechanisms in ECU?
    - Will ECU filter/reject suspicious packets?
    - How long will ECU recover from the spoofing?
- Spoofing System
  - Frequency mixer
  - Reused eavesdropper from step 2
  - Developed a packet generator
    - Include a proper checksum
    - Contain the alarm flag

Frequency mixer



Spoofing Validation

- Tested on two equipment:
  - ATEQ VT55 validates packet structure
  - A car (TPS-A) validates ECU's logic
    - 40 packets per minute



Spoofing Validation

- Tested on two equipment:
  - ATEQ VT55 validates packet structure
  - A car (TPS-A) validates ECU's logic
    - 40 packets per minute

- Observations
  - No authentication
  - **No input validation**
  - Warning lights only depend on the alarm flag, not the real pressure
  - Large range: 38 meters with a cheap antenna without any amplifier
  - Inter-vehicle Spoofing is feasible; travel speed 55 km/h and 110 km/h

TPMS-LPW light

Vehicle's warning light

Disabled TPMS ECU

- Timer and window-based filtering opens vulnerabilities
- *Broke TPMS ECU purely by spoofing! Replaced the ECU at the dealership.*

Recommendations

- Reliable software design
  - Cross-check pressure reading with flag
  - Detect conflict messages
  - Set packet delivery rate limit

??

- Cryptographic solutions:
  - Use encryption and key-establishment protocols
  - Include sequence number in packets
  - Use cryptographic checksum (e.g., MAC)

- Preventing spoofed activation

Conclusions

- Tracking risks
  - (i) The TPMS messages contain fixed sensor IDs in plaintext
  - (ii) TPMS packets can be intercepted up to **40 meters** using USRP with an LNA
  - (ii) Active tracking is possible while cars are travelling
- Spoofing risks
  - (i) Spoofing attacks are possible to a car traveling at high speeds from a nearby car
  - (ii) **No input validation and weak filtering**
  - (iii) **Permanently disabled the TPMS ECU** by spoofing attacks only
- Raise awareness before more serious security and privacy vulnerabilities emerge
- Many of these issues can be addressed by reliable software design and cryptographic algorithms

Thank you & Questions?

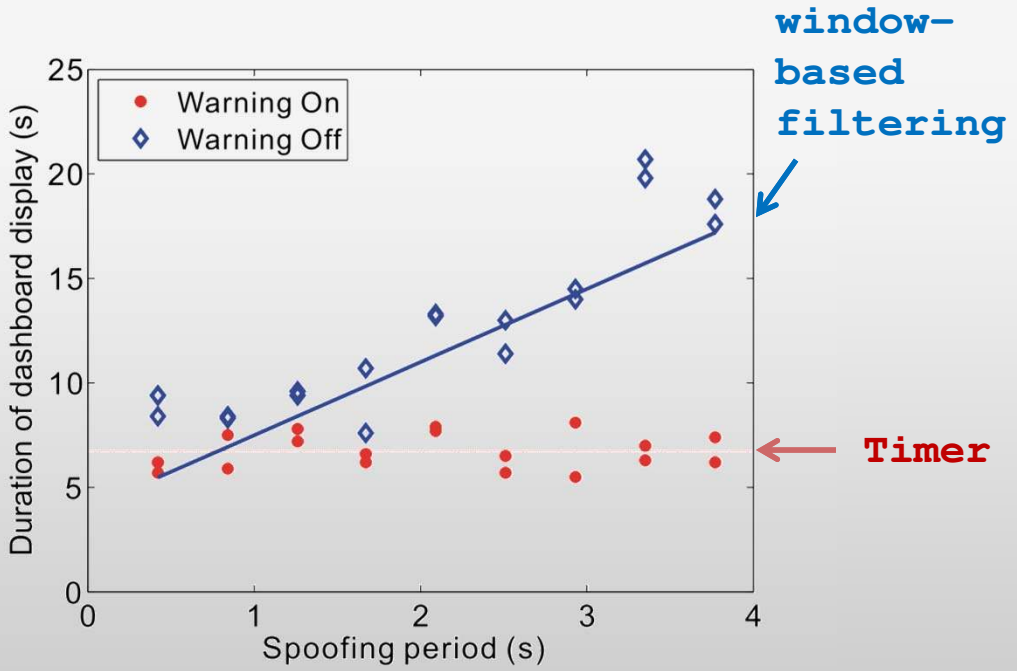
Exploring the Logic of ECU Filtering

- Sustainability of the spoofing attacks
  - Q: Minimum number of packets to trigger the TPMS warning light once

    A: Trigger requirement: 4 pkts (240ms apart)
  - Q: Minimum spoofing rate to keep the TPMS warning light on

    A: Sustain requirement: 1 pkt per 4 seconds
  - Q: Can we permanently illuminate warning lights even after stopping the spoofing attack?

- Explored TPMS-LPW Light
  - Change the number of packets
  - Change the rate of packets



Related Work

- Security and privacy analysis of other wireless systems
  - RFID systems [Koscher2009], [Molnar2004], [Weis2004]
  - UbiComp devices [Saponas2007]
  - Implantable medical devices [Halperin2008]
  - House robots [denning2009]
- Location privacy
  - Monitoring radiometric signatures [Brik2008]
  - Leveraging link- and application-layer information [Grutesers2003]
  - Pseudonym-based defense [Jiang2007]
  - Identifier-free-based defense [Greenstein2008]
- Security and privacy in sensor networks
  - SPIN and random key predistribution [Perrig2001] [Chen2003]
- Security analysis of a modern car [Koscher2010]
  - Directly mounting into a car's internal network via the On Broad Diagnostics (OBD) port