1. V2I Cyber-Security

- V2V cyber-security and privacy requires supporting infrastructure
  - Renew security credentials in OBUs
  - Receive information about revoked devices
  - Send misbehavior reports
- Communication channel might be RSUs, built-in modem, etc.
- Communication channel must be available to/from every vehicle
V2I Cyber-Security

- V2I applications can use the same communication channel.
- Security credential management for V2I applications can be plugged into existing V2V security systems.
  - Requires additional functionality
V2I Cyber-Security

- V2I applications introduce a variety of vulnerabilities
- V2I applications introduce clear motivations for hackers, e.g.
  - Disturb traffic flow for fun/curiosity
  - Gain advantage to find parking spot
  - ...
- Need a secure framework rather than case-by-case consideration
V2I Privacy

- V2V safety communication privacy is well understood and handled
- V2I applications have different privacy implications and require different solutions
  - E.g., an OBU might give away its profile because it always contacts the same service providers
- Solution approaches
  1. Provide baseline technical privacy solutions
  2. Add case-by-case solution, offered by service provider
  3. Use trustworthy anonymizer proxy, similar to TOR
2. Infrastructure Vulnerability

- What happens if a hacker shuts down all bridges and tunnels to/from Manhattan?
- What is if hackers manipulate traffic light controllers in a metropolitan area?
  - E.g. switch all traffic lights to red
- Hackers could also eavesdrop all traffic surveillance cameras
Infrastructure Vulnerability

- Infrastructure can be used to spread local attacks
  - E.g. vehicle injects malware to dealership infrastructure which in turn spreads it to all serviced vehicles
- Hacker uses existing infrastructure to push forged firmware to vehicles and/or traffic controllers
  - Even if devices do not accept new firmware, might result in large-scale denial-of-service, and technicians might have to fix vehicles and traffic controllers
Contact

Dr. André Weimerskirch
University of Michigan
Transportation Research Institute

2901 Baxter Road, Ann Arbor, MI 48109
Email: andrewmk@umich.edu
Office: 734-936-1046
Mobile: 734-474-5255