Leadership in Embedded Security

Breakout 2 -
Automotive/Drone/Transportation

CCC
Computing Community Consortium
Catalyst

Identify 3 Key Trends in the Application Area

- Increasing connectivity and attacks
- Increasing autonomy
- Consolidation of many components into a smaller number of processors (Tesla model) → a single point of failure?
- Traditional IT security techniques are increasingly adopted in

CCC
Computing Community Consortium
Catalyst

Identify 3 Key Challenges in the Application Area

- What is the threat model?
  - There are many ways to cause an accident. Remote attacks. Privacy concerns.
- Security and privacy of data coming off the vehicle (who owns the data? policy?)
- Key management
  - Inter-operation among multiple car vendors (V2V) and V2I
- Securely obtain locations and other (physical) properties
  - Gap between what sensors see and what humans see. Easy to spoof sensor inputs
- Long lifetime
- Patching, testing. (require patching with a regulation?)
  - Challenge: huge diversity of vehicles. what is the patching process? Who's responsible for updates?
- How to provide economic incentives for security?
- Switch between manual and autonomous operations

CCC
Computing Community Consortium
Catalyst

Identify 3 Key Challenges in the Application Area

- No security in RTOS
- When to allow exceptions? (emergency?)
- What is the platform architecture that we can ensure both safety and security properties?

CCC
Computing Community Consortium
Catalyst

Identify 3 Potential Novel Solutions in the Application Area

- Methodology (including formal methods) and tools to incorporate security from beginning and reason about multiple layers with different assumptions (control, software, hardware)
- Leverage interactions among multiple layers or physical properties to provide system-level security (actuation to verify sensor inputs)
  - Attack resilient control algorithms
- Platform with stronger isolation including timing
- Benchmarks and metrics to evaluate security and safety
- Automatic detection of software vulnerabilities in embedded systems
- Analysis and securing of new emerging platform architecture
- Security regulation and economic incentives

CCC
Computing Community Consortium
Catalyst

Extra Slide

- Nam qui officiminis dolorrovit fugitatecum ipsaperru quost
- Vellab illenim agnati quisciis alignam ululique nonseria vollige nditas nisl zzril
- Ulparem re simendi gnatiorae doloresti tecta nam qui
- Nam qui officiminis dolorroovit
- Asdfasdf
- Asdfadf

CCC
Computing Community Consortium
Catalyst