Securing Connected Vehicles:
Challenges and Opportunities

Tao Zhang, Ph.D, IEEE Fellow

Cisco Systems, Inc.

tazhang2@cisco.com

December 2015

Three Basic Questions

1. What security challenges in connected vehicles are so unique that they cannot be adequately addressed by the existing security paradigm?

2. What fundamental changes will be necessary?

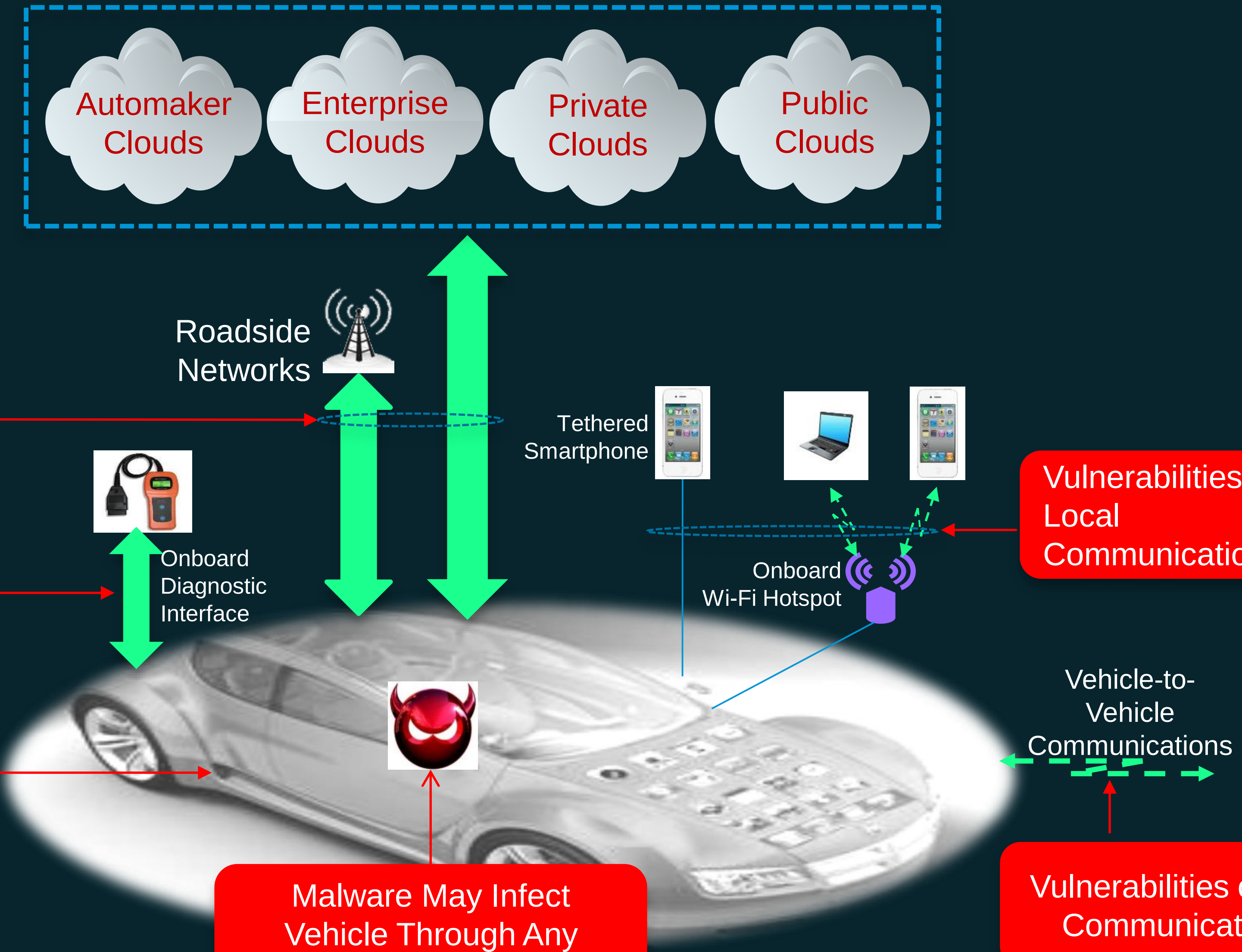
3. What opportunities will result from these changes?

Existing Cyber Security Paradigm in a Nutshell

Cyber security technologies have evolved tremendously, and have been following the following paradigm:

1. We build firewalled gardens, with firewalls and intrusion detection/prevention mechanisms, seeking to keep threats outside
   - We even do preemptive strikes to try to keep threats away, but that is not yet in wide spread use
2. When security compromises are detected, we shut the compromised systems down, clean them up, then start them again
3. Then, we try to learn from what have happened to improve our future defense

Connected Vehicles Have Many Security Vulnerabilities



Vulnerabilities of Vehicle-to-Infrastructure/Cloud Communications

Vulnerabilities of Onboard Diagnostic Interface

Vulnerabilities of Onboard Networks, Devices, and Applications

Malware May Infect Vehicle Through Any Communication Channel

Vulnerabilities of Local Communications

Vulnerabilities of V2V Communications

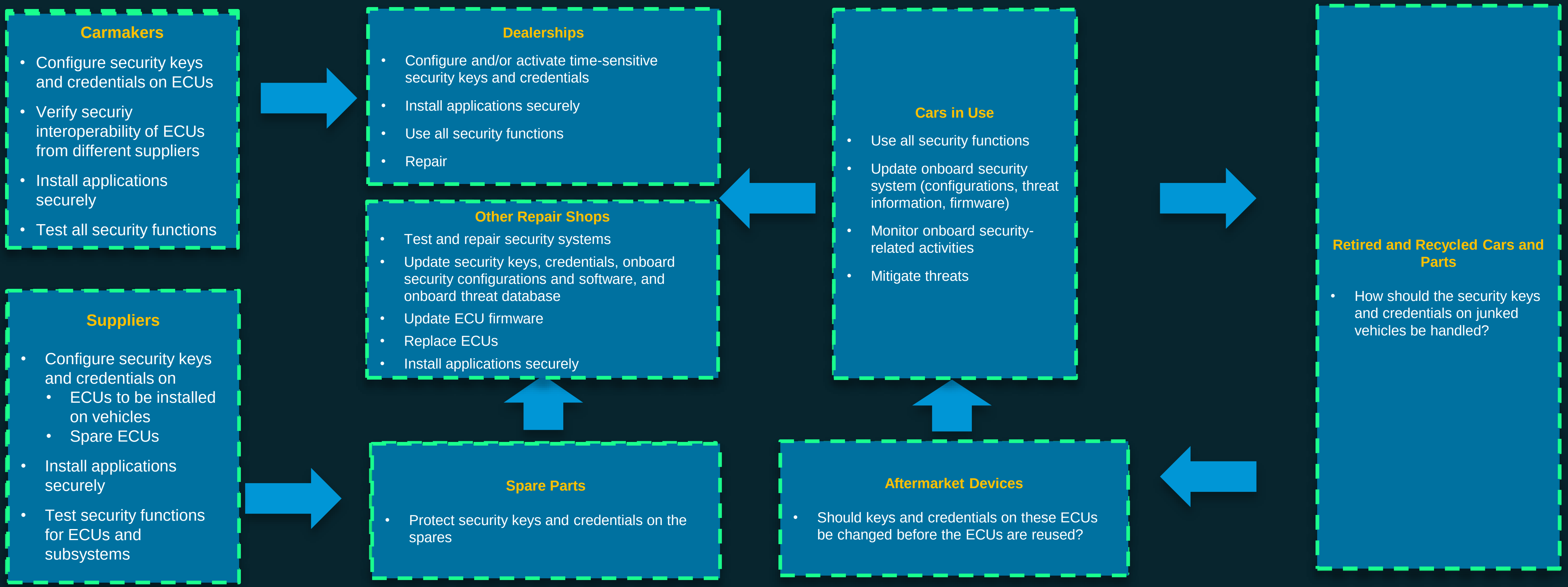
What’s Unique about Securing Connected Vehicles?

Vehicles	Vehicles have long lifespans and yet highly constrained resources that cannot be upgraded or replaced easily	**Vehicles will need external help/services for adequate security**
Environment	Vehicles operate in highly vulnerable or completely unprotected environments	**Existing “Firewalled Garden” security paradigm no longer sufficient**
Vehicle Operations	Vehicles have little tolerance for down times	**Existing “Shutdown-Cleanup-Restart” incident response paradigm no longer adequate**
Security Operations	Vehicles are not managed by IT experts, and sending them to repair shops can cause intolerable disruption/inconvenience to users	**Security operations must be significantly more automated and manageable** **Remote online threat mitigation will be essential**

The Challenges Continue …

Challenges	Implications
Standard OBD interfaces allow everyone to access vehicle’s internal networks and even update ECU firmware	How to defend a vehicle when virtually anyone can access its internal networks?
Attackers can compromise a vehicle to use its valid security credentials to mount security attacks	How to handle such potentially prevalent “insider attacks”?
Information from vehicles is necessary for threat detection but can be untrustworthy	How to determine the trustworthiness of information from vehicles?
Spare ECU’s security credentials must interoperate with every authorized vehicle	How to manage security credentials for the huge number of spare ECUs while preventing successful attacks from scaling?
Security compromises can have serious consequences	How to respond to critical compromises?
In-vehicle devices have widely varying capabilities and use a multitude of legacy networks	How to secure in-vehicle devices, software, and applications?
Solutions must be highly scalable: Secure connections, security credential management	How to support, for one carmaker, 10+ millions of vehicles, each with 10s of ECUs and requiring many spare parts?

Vehicle Lifecycle Security Needs



Carmakers

- Configure security keys and credentials on ECUs
- Verify securiy interoperability of ECUs from different suppliers
- Install applications securely
- Test all security functions

Suppliers

- Configure security keys and credentials on
  - ECUs to be installed on vehicles
  - Spare ECUs
- Install applications securely
- Test security functions for ECUs and subsystems

Dealerships

- Configure and/or activate time-sensitive security keys and credentials
- Install applications securely
- Use all security functions
- Repair

Other Repair Shops

- Test and repair security systems
- Update security keys, credentials, onboard security configurations and software, and onboard threat database
- Update ECU firmware
- Replace ECUs
- Install applications securely

Spare Parts

- Protect security keys and credentials on the spares

Cars in Use

- Use all security functions
- Update onboard security system (configurations, threat information, firmware)
- Monitor onboard security-related activities
- Mitigate threats

Aftermarket Devices

- Should keys and credentials on these ECUs be changed before the ECUs are reused?

Retired and Recycled Cars and Parts

- How should the security keys and credentials on junked vehicles be handled?

Manufacturing

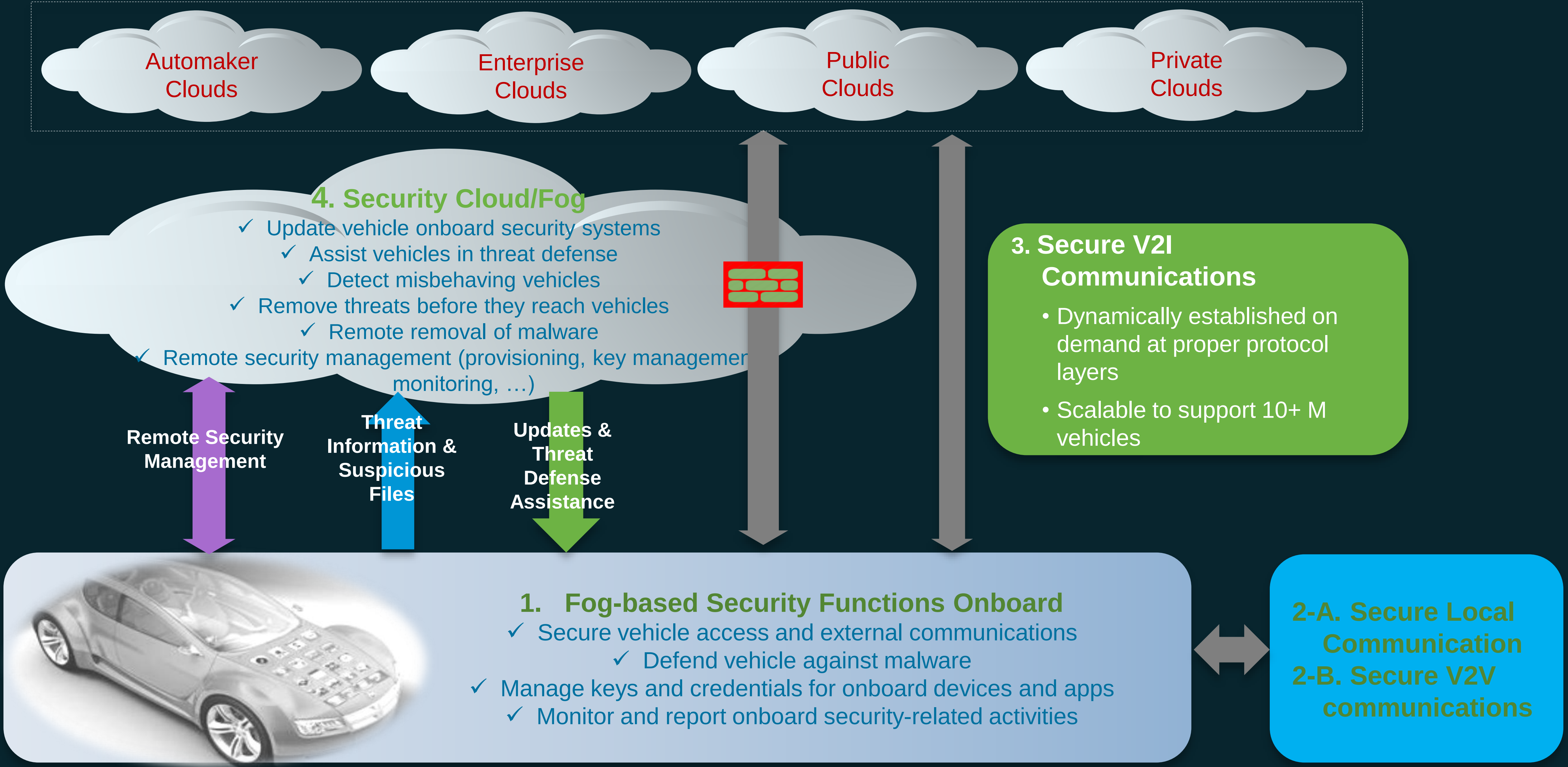
Sales/Maintenance/Repair

Registered/Use

Alternation

Recycle

Fog/Cloud-Assisted Vehicle Security Architecture



Automaker Clouds
Enterprise Clouds
Public Clouds
Private Clouds
Remote Security Management
Threat Information & Suspicious Files
Updates & Threat Defense Assistance

4. Security Cloud/Fog

- ✓ Update vehicle onboard security systems
- ✓ Assist vehicles in threat defense
- ✓ Detect misbehaving vehicles
- ✓ Remove threats before they reach vehicles
- ✓ Remote removal of malware
- ✓ Remote security management (provisioning, key managemen monitoring, …)

3. Secure V2I Communications

- Dynamically established on demand at proper protocol layers
- Scalable to support 10+ M vehicles

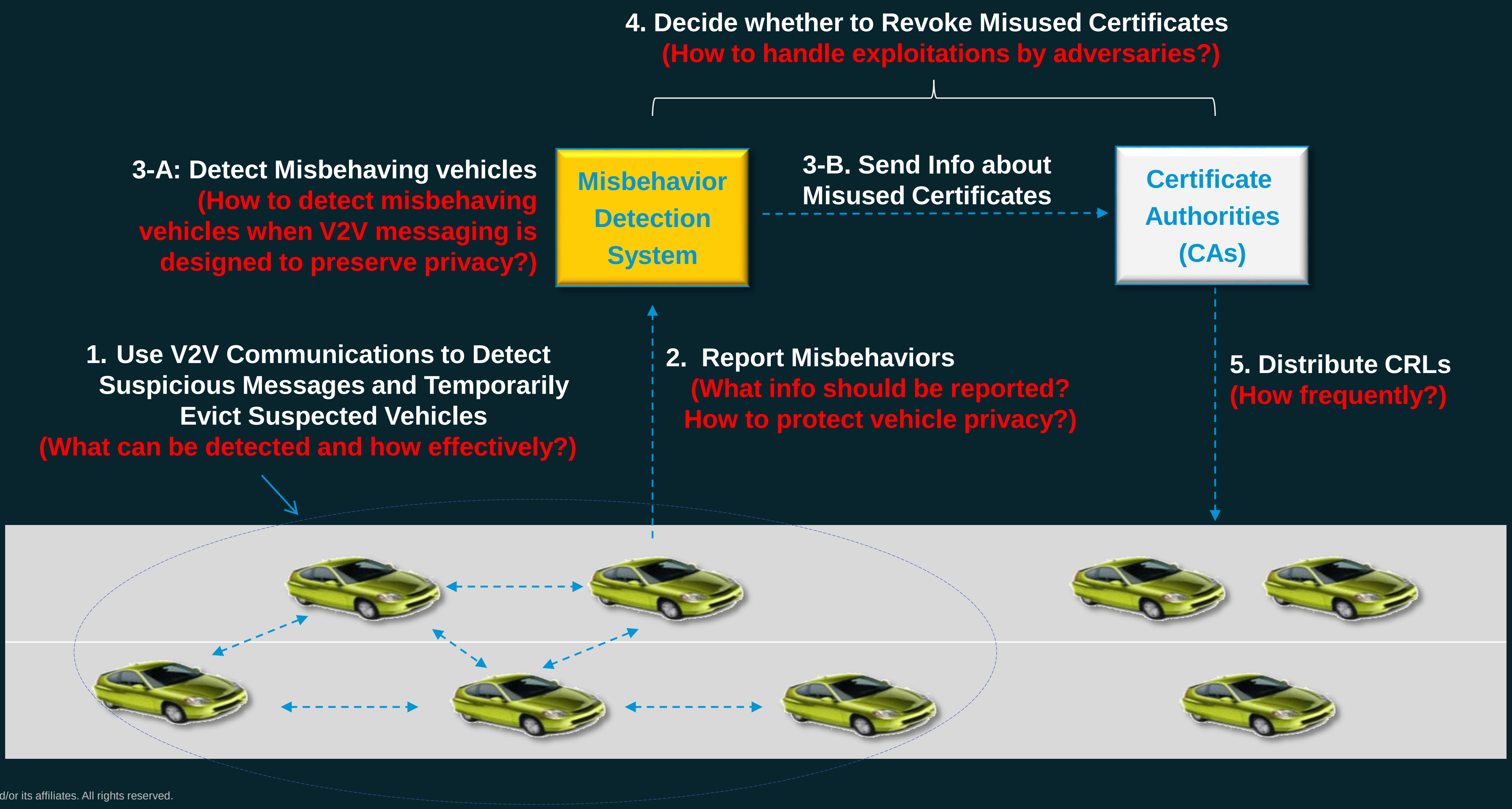
1. Fog-based Security Functions Onboard

- ✓ Secure vehicle access and external communications
- ✓ Defend vehicle against malware
- ✓ Manage keys and credentials for onboard devices and apps
- ✓ Monitor and report onboard security-related activities

2-A. Secure Local Communication

2-B. Secure V2V communications

Example of V2V Communication Security Challenges: How to Handle Misbehaving Vehicles?



4. Decide whether to Revoke Misused Certificates
(How to handle exploitations by adversaries?)

3-A: Detect Misbehaving vehicles
(How to detect misbehaving vehicles when V2V messaging is designed to preserve privacy?)

Misbehavior Detection System

3-B. Send Info about Misused Certificates

Certificate Authorities (CAs)

1. Use V2V Communications to Detect Suspicious Messages and Temporarily Evict Suspected Vehicles
(What can be detected and how effectively?)

2. Report Misbehaviors
(What info should be reported? How to protect vehicle privacy?)

5. Distribute CRLs
(How frequently?)

Going Forward, Need Joint Industry-Academia-Government Efforts To

- Build eco-system necessary to combat automotive security threats
- Identify new security threats to connected and autonomous vehicles
- Develop an open framework/platform for automotive security and for supporting end-to-end automotive security services
- Test automotive security technologies

Thank you.

CISCO TOMORROW starts here.