

Vehicle Safety Communications – Applications (VSC-A) Project: Security for Vehicle Safety Messages

Sue Bai

Honda Research Americas, Inc.



CAMP

Vehicle Safety Communications 2

Mercedes-Benz
Research & Development North America, Inc.



TOYOTA

HONDA
Honda R&D Americas, Inc.



Intelligent Transportation Systems

A rectangular box containing logos and text for the CAMP Vehicle Safety Communications 2 project. At the top, the word 'CAMP' is written in a stylized, italicized font. Below it, the project name 'Vehicle Safety Communications 2' is also in an italicized font. The logos for Mercedes-Benz (with 'Research & Development North America, Inc.' below it), GM, and TOYOTA are arranged in a row. Below that, the logos for HONDA (with 'Honda R&D Americas, Inc.' below it) and Ford are arranged in a row. At the bottom of the box, the phrase 'Intelligent Transportation Systems' is written in an italicized font.

Security for V2V Safety Messages

- **Overall objective:** Improve existing *vehicle-to-vehicle* (V2V) communication security schemes
 - Efficient authentication of V2V safety communications (>1000 received messages per second)
 - Dealing with privacy concerns due to periodic V2V safety communications (10 messages per second)
- Extend IEEE 1609.2 and VII-C results regarding V2V safety communication security
- Conform to IEEE 1609.2 and rely on VII-C results regarding infrastructure and management

Activities

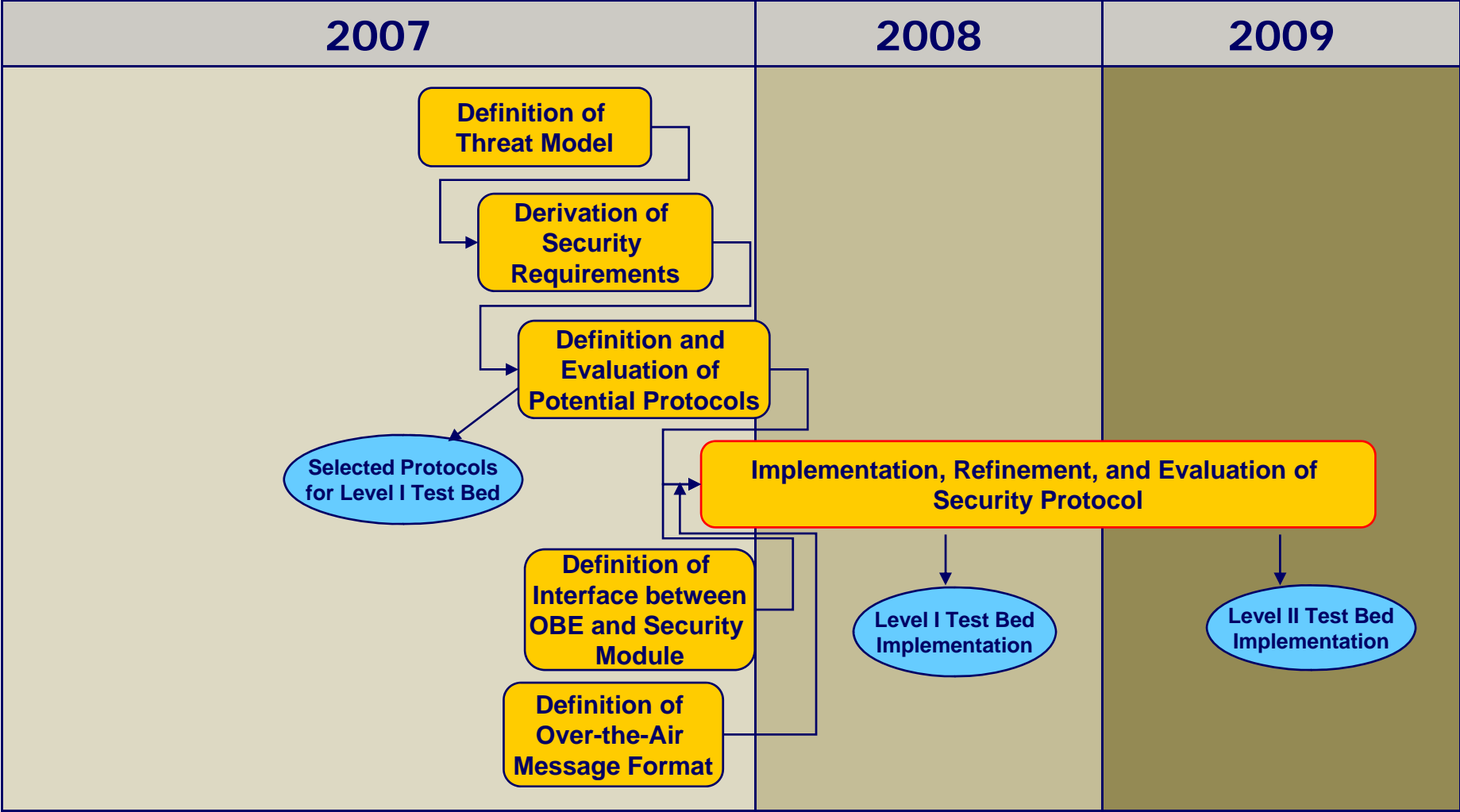
- Cost / run-time performance
 - Avoid dedicated hardware
 - Cost handicaps market penetration
 - Security updates are cumbersome
 - Potentially piggy-back on existing processor to run security solution
- Over-the-air (OTA) bandwidth overhead
 - Bandwidth is an issue, even regardless of security
 - Can bandwidth overhead due to security be reduced without loss of security and reliability ?

Activities (continued)

Privacy protection

- Adapt privacy protecting mechanisms for V2V safety applications
- Utilize VII-C solutions
- Potentially, consider deployment without supporting infrastructure (RSEs)

Time Schedule



Implemented Security Protocols

- Certificate distribution
 - Do not attach certificate to each message
 - Balance availability of certificates and OTA bandwidth
- Authentication protocols:
 - Reference protocol: IEEE 1609.2 / ECDSA1
 - TESLA2 [3, 4, 5, 6]
 - TADS (TESLA Authentication and Digital Signatures) [1]
 - Verify-on-Demand [2]

¹*ECDSA: Elliptic Curve Digital Signature Algorithm*

²*TESLA: Timed Efficient Stream Loss-tolerant Authentication*

Implemented Security Protocols

	ECDSA (IEEE 1609.2)	TESLA	TADS	Verify-on- Demand
Properties	Standardized	<ul style="list-style-type: none"> Two-step protocol Time-dependent 	Combination of ECDSA and TESLA	Only verify messages that have actual impact
Computation	Demanding	Highly efficient	Highly efficient	Efficient
Time delay	Medium / Deterministic	Varies (very low – higher than ECDSA)	Reasonable / Adjustable	Reasonable / Deterministic
OTA overhead	Reasonable	Varies	Slightly higher	Reasonable

Next Steps

- Evaluate performance/scalability of potential protocols through extensive network simulations
- Adapt security module software to run on same CPU as safety applications
- Bring in expertise and results to IEEE 1609.2 (DSRC Security Standard)
- Decide on one security protocol
- Perform third-party evaluation of protocol



Open Issues

- Public Key infrastructure
 - How to organize the keys
 - Detection of malicious vehicles
 - Revocation of vehicles
- Privacy
 - Technical challenges
 - Governance issues

Thank You