Center for Education and Research in Information Assurance and Security

Secure Dissemination of Data in Vehicle-to-Vehicle Systems

Presentation for:
ADI (Sypris), Feb 22nd, 2017

B. Bhargava[1], D. Ulybyshev[1], M. Villarreal-Vasquez[1], R. Ranchal[1], G. Izera M.[1] L. Lilien[2]

[1]Computer Science Department/CERIAS, Purdue University, West Lafayette, IN, USA

[2]Department of Computer Science, Western Michigan University, Kalamazoo, MI, USA

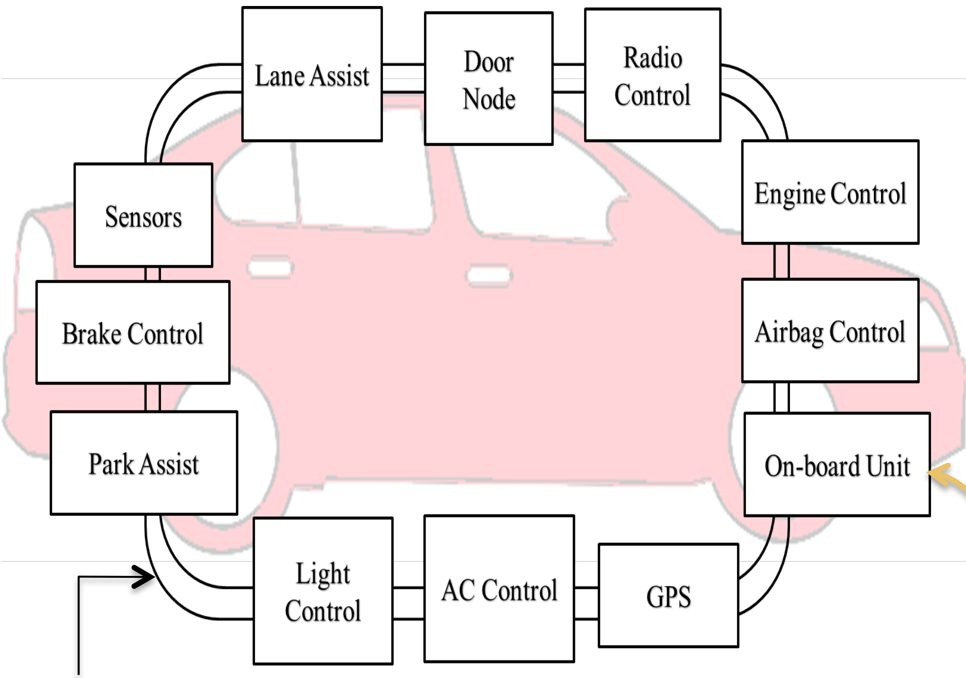
PURDUE UNIVERSITY

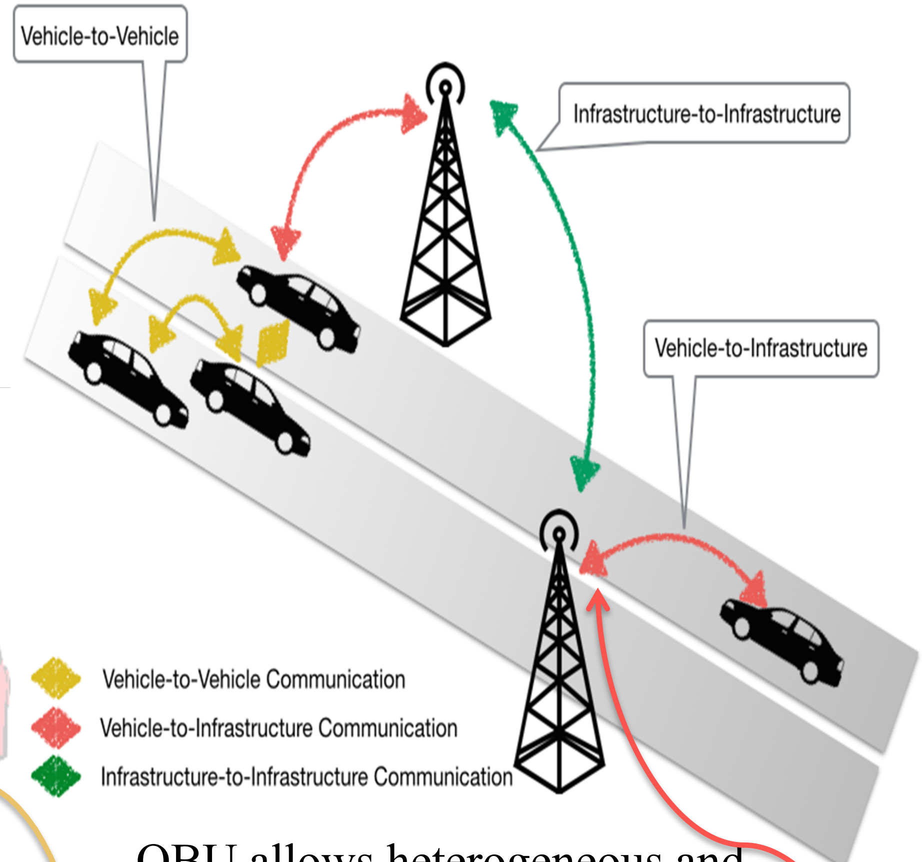
Outline

1. Motivation
2. Objectives
3. Deliverables
4. Related Work
5. Impact of Attacks on Safety
6. Impact of Implementing Security Features
   6.1 Case of Study: Security vs. Safety
7. Active Bundle Core Design
   7.1. Key Generation / Encryption
   7.2. Tamper – resistance
8. Lightweight encryption
9. Encrypted Search over Encrypted Data
10. References

Motivation

Vehicle has more than 60 sensors and 30 or more Electronic Control Units (ECUs), i.e. Brake Control, Engine Control, GPS, Airbag Control, etc [6]





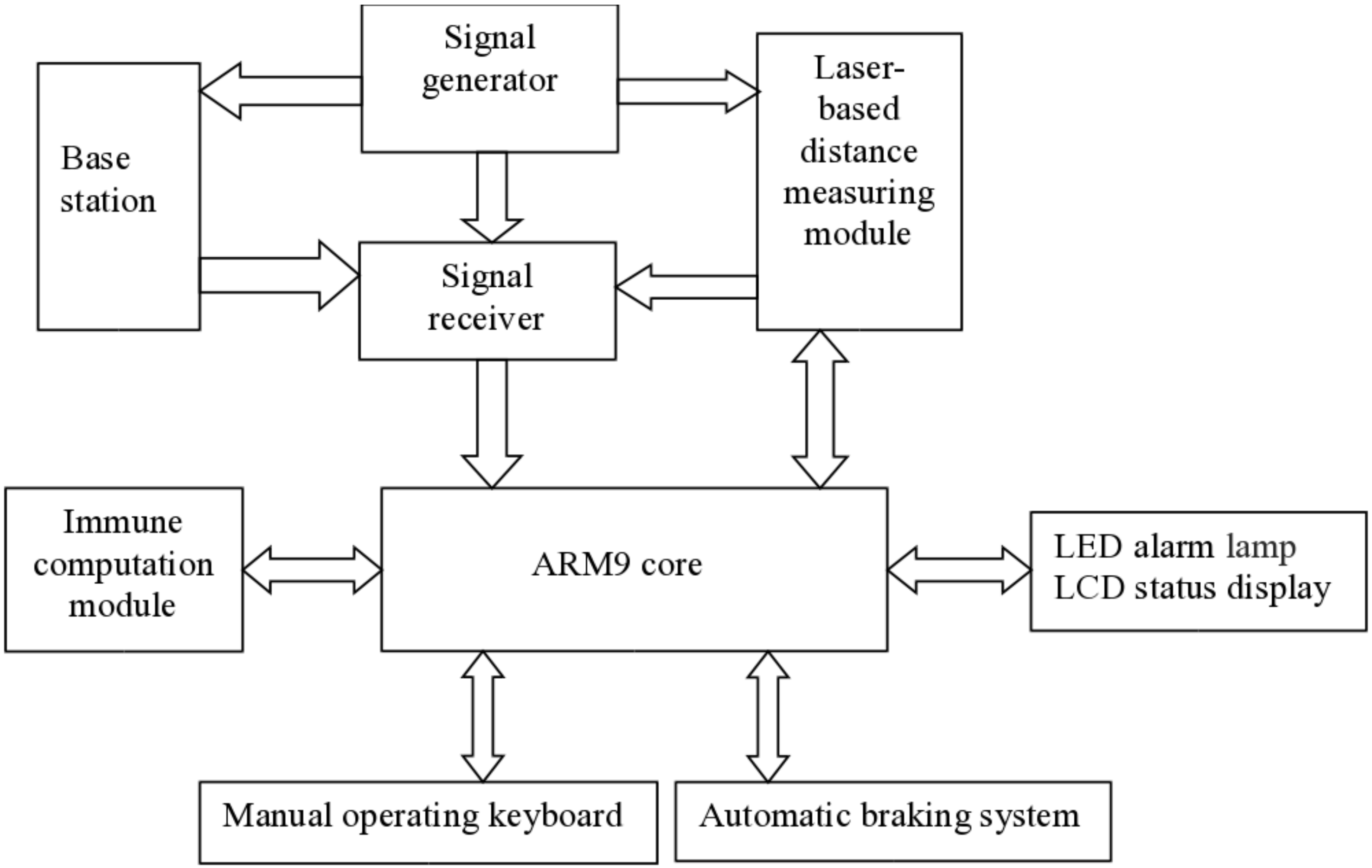
OBU allows heterogeneous and homogenous communications between vehicles and infrastructures (roadside equipment)

CAN (Control Area Network) Bus

Radio Interface or On-Board Unit (OBU) enables short-range wireless ad hoc networks to be formed

Motivation

ARM9 – based intelligent immune system for avoiding rear-end collision [14]



Communications between modules and ARM9 core need to be secure !

Motivation

- Connected vehicles deploy signals to communicate with other vehicles, roadside units, personal devices and cloud services
  - Goal: provide assistance to drivers and prevent collisions

- Connected vehicle consists of electronic control units (ECUs) communicating via CAN (Controller Area Network) bus to transfer messages and execute queries sent from other ECUs

- Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications are prone to security threats

- Lightweight encryption – based protection mechanisms:
  - Active Bundle [5], [9], [10], [11], [12], [13]
  - Digital Signature
  - HMAC

Objectives

1. Provide vehicle collision avoidance

2. Ensure data security and privacy

3. Measure the cost/overhead associated with proving security in V2V communication and its impact on safety

4. Provide system's self-backup, the software fault detection and the software system repairing

Deliverables

1. Prototype demonstrating the evaluation of schemes to avoid collisions

2. Evaluation of tradeoff between ensuring security and safety

3. Evaluation of using cloud for computing versus dedicated chip

Related Work

- Research report "Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application" [3] by National Highway Traffic Safety Administration
  => What policy should V2V system contain in order to minimize the likelihood of unauthorized access to insider information that could impose risks to privacy, e.g. facilitate tracking?

- EVITA [4] project (developed in EU):
  => Identified and evaluated security requirements for automotive on-board networks based on a set of use cases and an investigation of security threat (dark-side) scenarios

Impact of Attacks on Safety

- Threats
  - Denial of Service Attack
  - Masquerade Attack
  - Malware Attack
  - Message Tampering

- Mitigation Schemes
  - Active Bundle
  - Digital Signatures
  - HMAC
- Cost of Deployment
  - Detection and mitigation of attack require the following costs:
    - Performance overhead
    - Memory overhead
    - CPU and energy usage

Impact of Attacks on Safety

Miller and Valasek demonstrated in DEF CON 21 a set of attacks [7], [8], including very serious attacks.

- Hard braking/ no braking attack
  - Locked brake
  - Sudden stop
  - Braking distance increase
- Acceleration attack
  - Sudden uncontrollable acceleration
- Steering wheel attack
  - Sudden uncontrollable rotation of a steering wheel
- Engine shutdown
- Light out attack
  - Dashboard indication is misrepresented
  - Dashboard indication is off

Impact of Deploying Security

Mechanism	Security	Safety
Digital Signature	Data comes from a known trusted node	Delay: validating undetected data
Encryption	Security depends on the key size	Delay: Undetected modifications can compromise safety
Active Bundle	Privacy–preserving policy-based and context-based data dissemination	Delay: validating undetected data
Levels of operation	Need to override access control for log and subsystems to handle emergencies	Way to bypass security and keep normal behavior

Impact of Implementing Security Features

V2V		Security	Safety
No security features	No attacks	Do nothing	
	Under attacks	Misleading dashboard and gps; firmware and data wiped out; compromised vehicle's sensors, part of botnet framework	Human damage, collisions, delays in traffic
With security features	No attacks	Power consumption and computation overhead	Do nothing
	Under attacks	Isolate intruder, warn other nodes about attack, deviate attacks to targets with less damage	Faster response time

CASE OF STUDY: SECURITY VS SAFETY

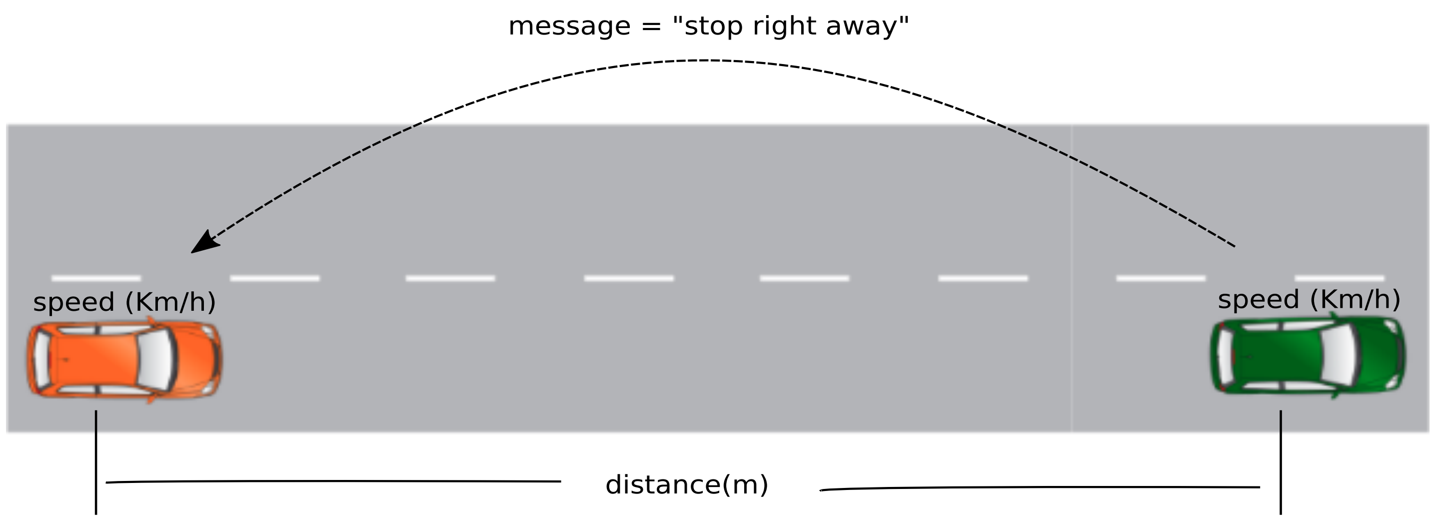
Category of traffic messages:

- *Traffic information messages*: Used to disseminate the current conditions of specific areas and they indirectly affect safety
- *General safety messages*: Used for cooperative driving a  collision avoidance, and require an upper bound on the delivery delay of messages
- *Liability-related messages*: Exchanged after an accident occurs

CASE OF STUDY: SECURITY VS SAFETY

Scenario 1: Sudden stop on a highway

- Vehicles move to same speed on the highway
- Pre-determined distance between them
- Reaction time with and without V2V
- Reaction time with secured V2V



High way scenario with only two vehicles involved

CASE OF STUDY: SECURITY VS SAFETY

Stopping distance:

- Driver's perception time
- Driver's reaction time
- Vehicle's reaction time
- Vehicle's braking capability

Speed (Km/h)	Minimum Reaction Distance (m)	Minimum Braking Distance (m)	Minimum Stopping Distance (m)
30	6	6	12
40	8	10	18
50	10	15	25
60	12	21	33
80	16	36	52
100	20	50	70
120	24	78	102

Table 1 *– The RSA recommended minimum stopping distance under dry conditions*

CASE OF STUDY: SECURITY VS SAFETY

System Model:

- Network:
  - ✓ IEEE 802.11a compliant
  - ✓ 6Mbps minimum

- Security mechanism on V2V:
  - ✓ PKI infrastructure
  - ✓ Every vehicle is assigned a public and private key
  - ✓ Public key distributed through a certificated signed by the CA
  - ✓ Authenticated message:

CASE OF STUDY: SECURITY VS SAFETY

System Model:

- Security costs on V2V:

✓ Processing cost

Public Key Cryptosystem	Generation (ms)	Verification (ms)
ECDSA	3.255	7.617

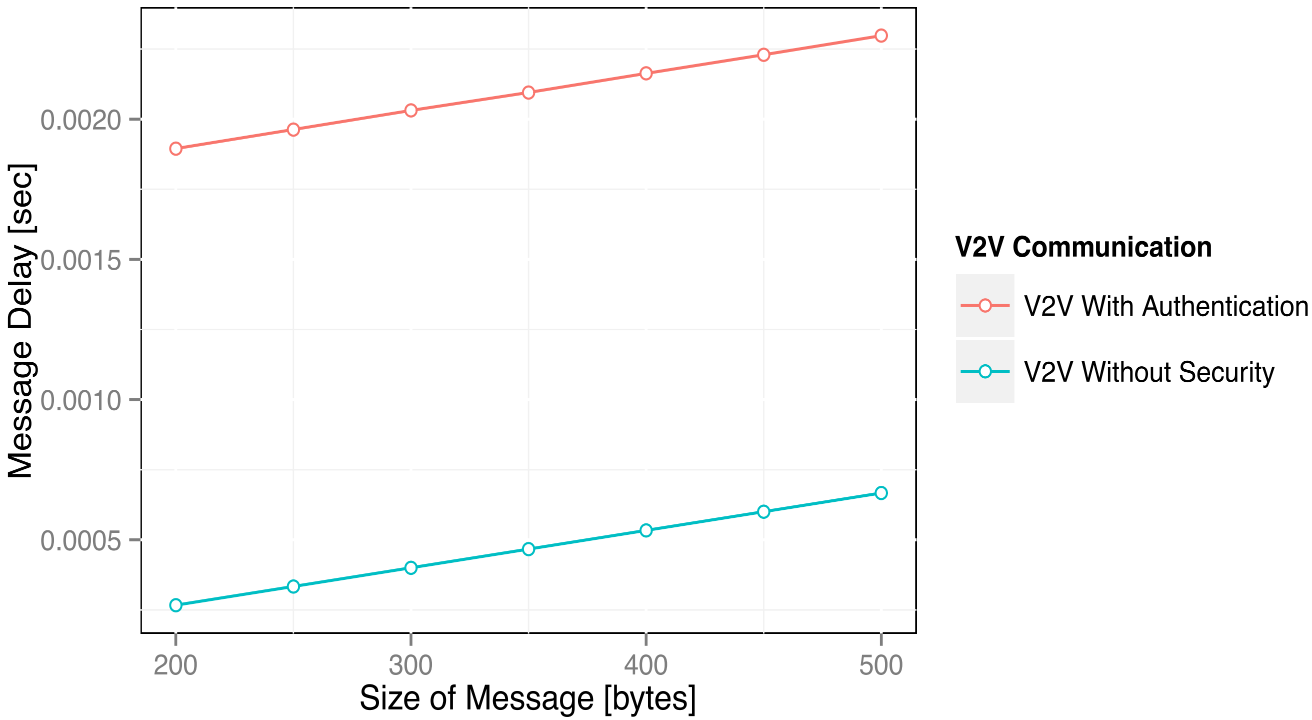
✓ Communication cost:

$$d_{com} = d_{transmission} + d_{propagation} + d_{queueing}$$

- Distance: 120m
- Bandwidth: 6Mbps
- Speed of communication link: 3x10^8m/s

CASE OF STUDY: SECURITY VS SAFETY

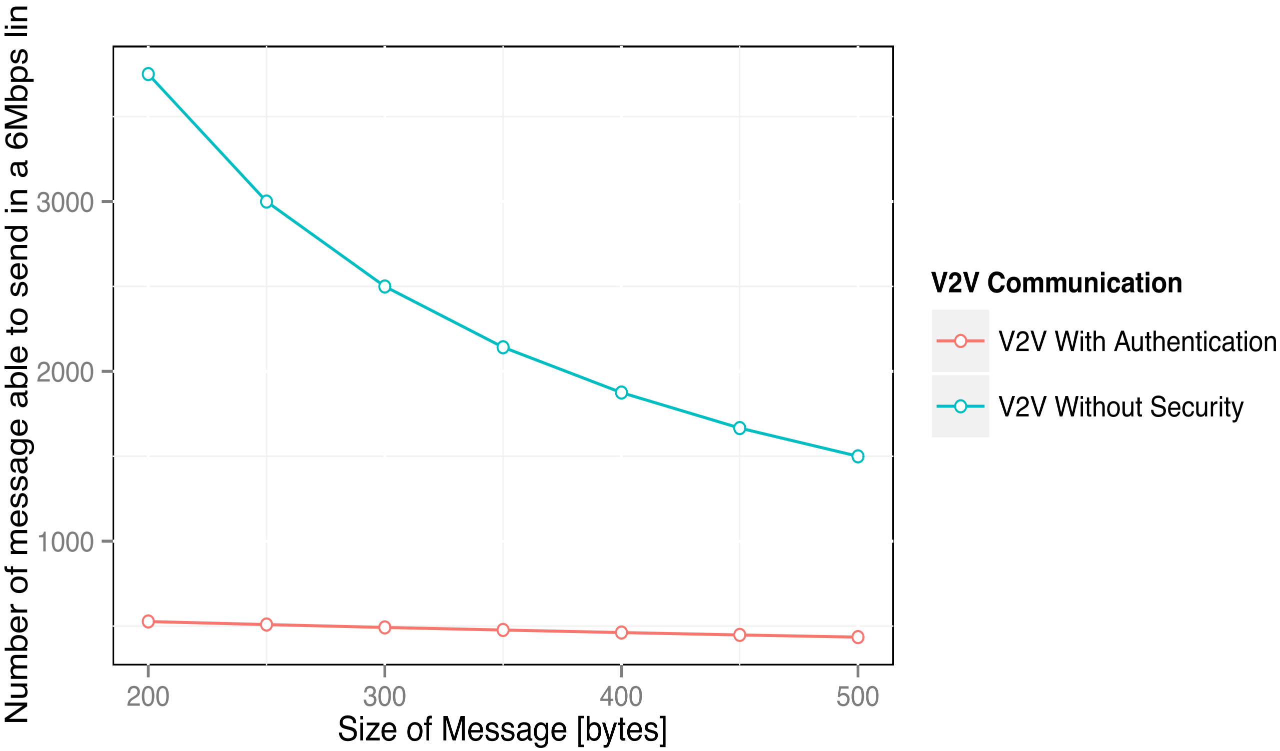
- **Experiment 1**: Measurement of delays of V2V messages with and without securitv



- ✓ Speed: 120Km/h
- ✓ Distance: 120m

CASE OF STUDY: SECURITY VS SAFETY

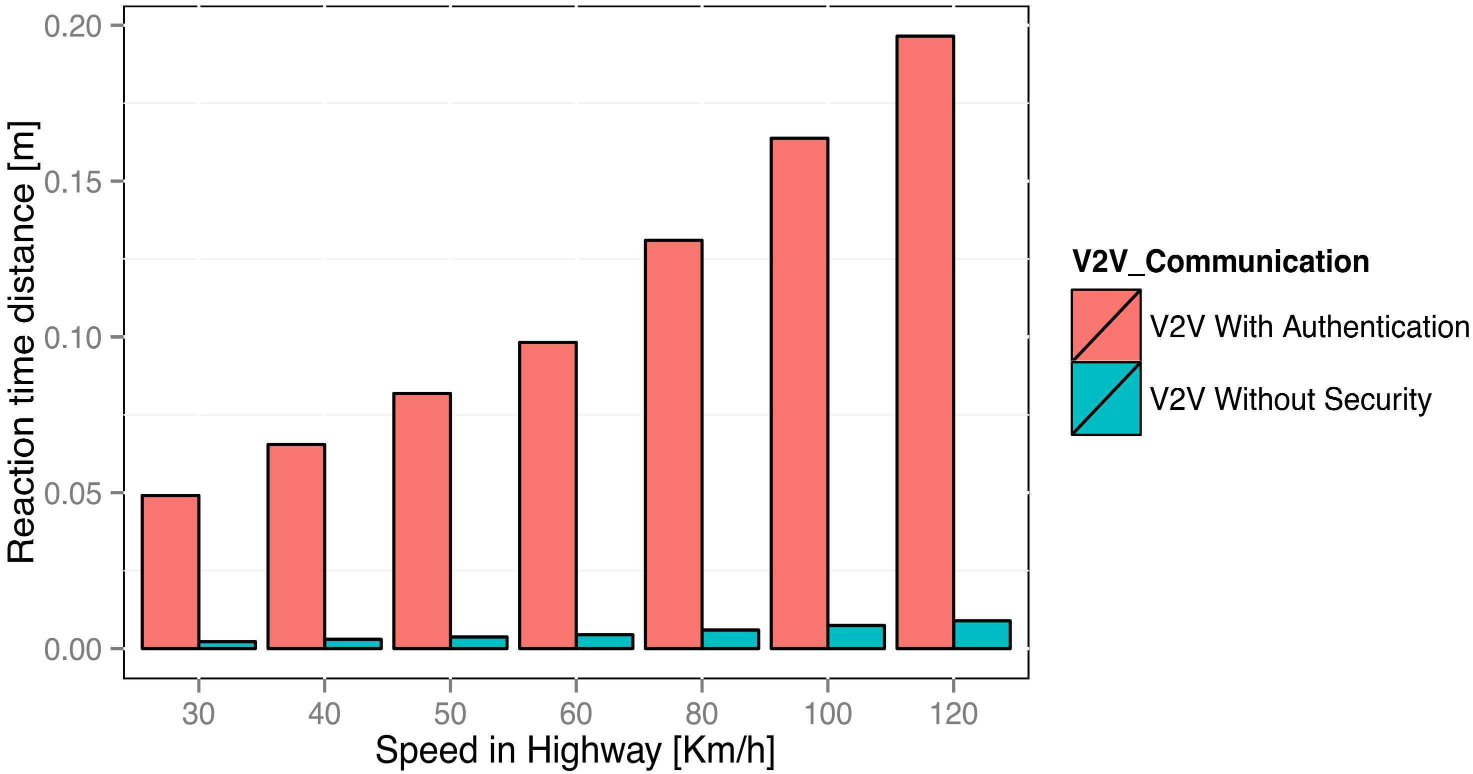
- **Experiment 2**: Measurement of the capacity of the link



✓ Speed: 120Km/h
✓ Distance: 120m

CASE OF STUDY: SECURITY VS SAFETY

- **Experiment 3**: Reaction time with V2V



✓ Size of the message: 200 bytes

✓ Distance: 120m

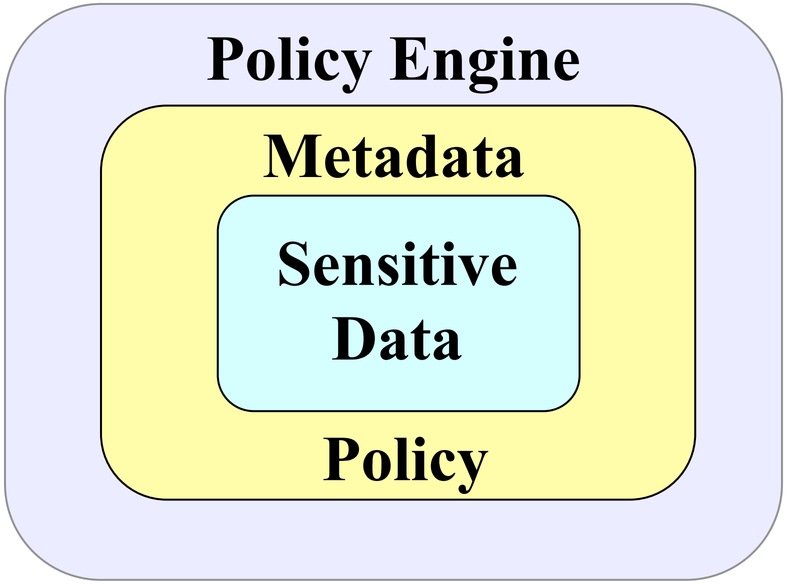
CASE OF STUDY: SECURITY VS SAFETY

Conclusion:

- ✓ Vehicular networks strictly require integrity and authentication but not confidentiality.
- ✓ Reaction times achieved via V2V (with or without security) are significantly smaller than a those of systems without V2V.
- ✓ V2V without security allows shorter reaction times than V2V with security.
- ✓ Lightweight cryptography must be applied to speed up processing.
- ✓ Alternative mechanisms for key management need to be explored.

AB Core Design

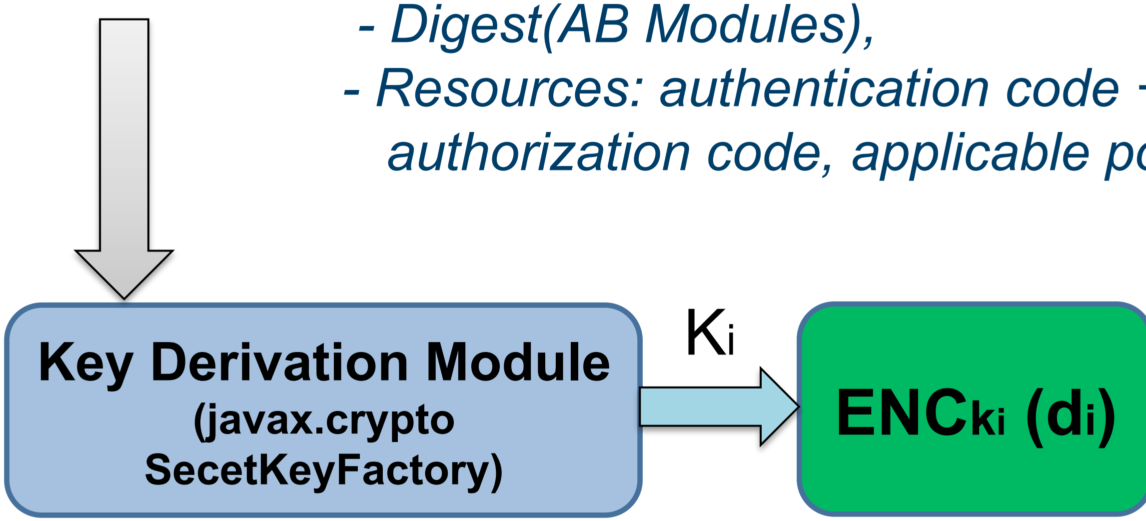
Active Bundle (AB) consists of:



- *Sensitive data*: encrypted data items => applicable policy of AB ensures secure distribution of the corresponding data item
- *Metadata*: describes AB and its policies which manage AB interaction with services and hosts
- *Policy Engine:* enforces policies specified in AB
  - Additionally, provides tamper-resistance of AB

Key Generation

Aggregation{d_i} (*- Generated AB modules execution info;*
- Digest(AB Modules),
- Resources: authentication code + CA certificate, authorization code, applicable policies + evaluation code)



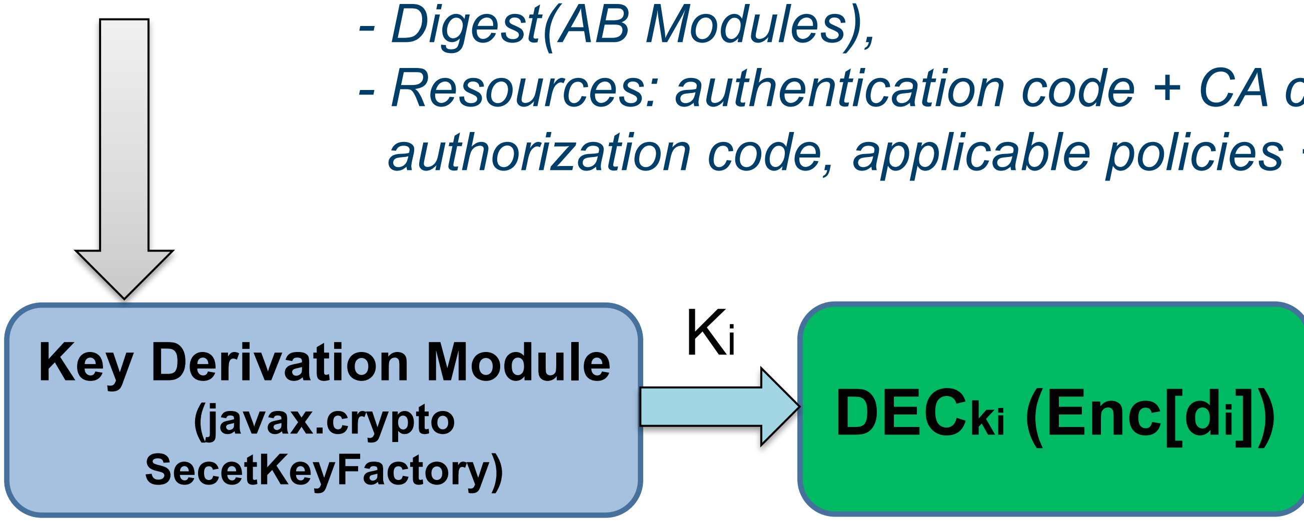
- AB Template [5] used to generate new ABs with data and policies (specified by data owner)
- AB Template includes implementation of invariant parts (monitor) and placeholders for customized parts (data and policies)
- AB Template is executed to simulate interaction between AB and service requesting access to each data item of AB

Key Generation

- Info generated during the execution and digest (modules) and AB resources are collected into a single value
- Value for each data item is input into a Key Derivation module (such as ***SecretKeyFactory, PBEKeySpec, SecretKeySpec*** from ***javax.crypto*** library)
- Key Derivation module outputs the specific key relevant to the data item
- This key is used to encrypt the related data item [5]

Key Derivation

Aggregation{d_i} (- *Generated AB modules execution info;*
- Digest(AB Modules),
- Resources: authentication code + CA certificate, authorization code, applicable policies + evaluation code)



- AB receives data item request from a service
- AB authenticates the service and authorizes its request (evaluates access control policies)

"Cross-Domain Data Dissemination and Policy Enforcement", R. Ranchal, PhD Thesis, Purdue University, Jun. 2015.

Decryption Key Derivation

- Info generated during the AB modules execution in interaction with service, and digest (AB modules) and AB resources are aggregated into a single value for each data item [5]

- Value for each data item is input into the Key Derivation module

- Key Derivation module outputs specific key relevant to data item

- This key is used decrypt the requested data item

- If any module fails (i.e. service is not authentic or the request is not authorized) or is tampered, the derived key is incorrect and the data is not decrypted

Other key distribution methods

- Centralized Key Management Service
  - TTP used for key storage and distribution
  - TTP is a single point of failure

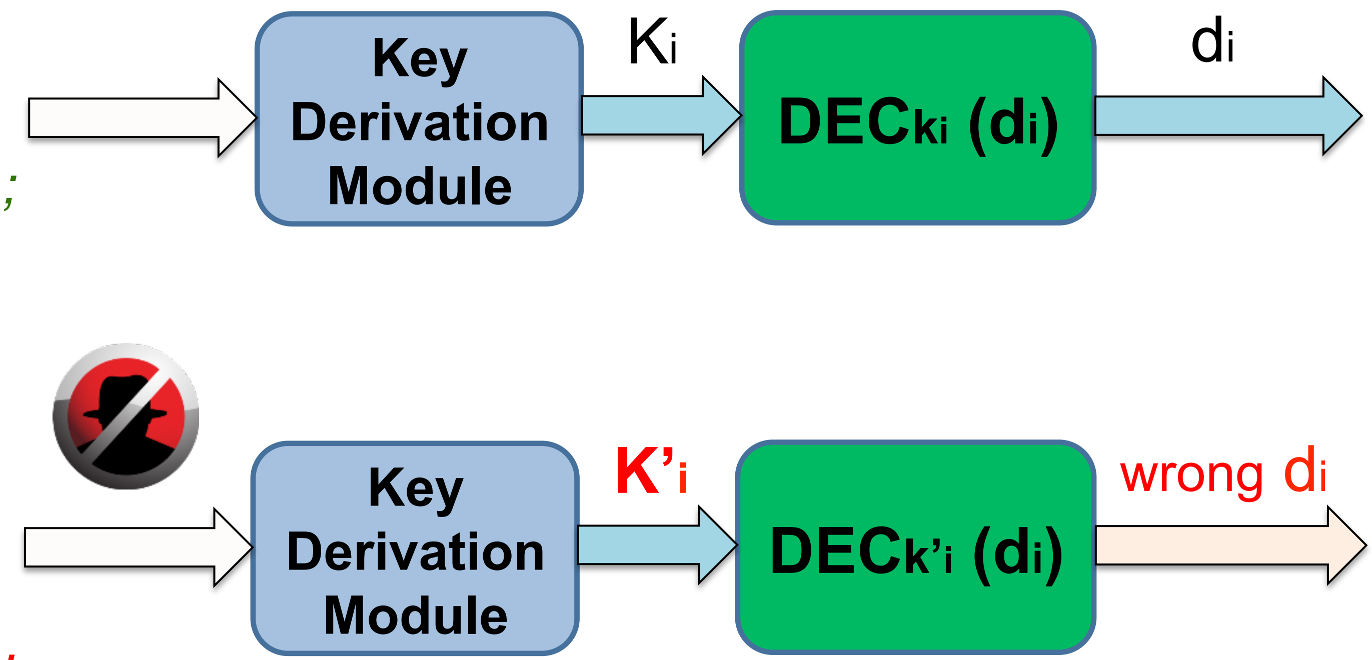
- Key included inside AB
  - Prone to attacks!

Tamper Resistance of AB

- Key is not stored inside AB
- Separate symmetric key is used for each separate data value
- Ensure protection against tampering attacks

Aggregation{d_i}
(*Execution info;*
Digest(AB Modules);
Resources)

Aggregation{d_i}
(***Tampered (***
Execution info;
Digest(AB Modules);
Resources ***)***)



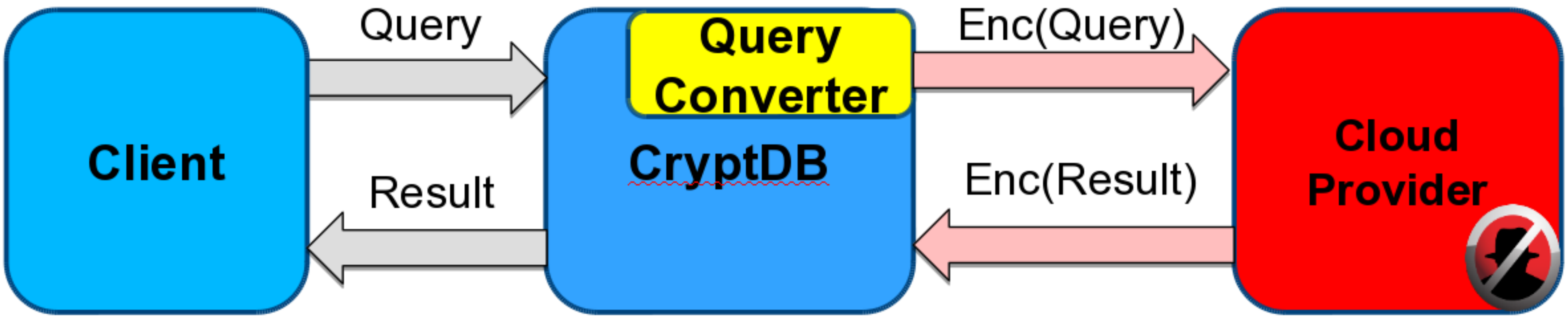
Lightweight encryption

- Can be used in Active Bundle instead of regular AES [1]

Cipher	Key size [bits]	Block size [bits]	Throughput at 4 MHz [kbit/sec]	Relative Throughput (% of AES)
Hardware-oriented block ciphers				
DES	56	64	29.6	38.4
DESXL	184	64	30.4	39.3
Hight	128	64	80.3	104.2
Software-oriented block ciphers				
AES	128	128	77.1	100.0
IDEA	128	64	94.8	123

Encrypted Search over Encrypted Data

- Cloud provider hosts database of Abs
- AB contains vehicle data in encrypted form



- Query example:
  select video from Vehicle_DB where description LIKE %highway%;
- Converted query:
  select c1 from Alias1
  where ESRCH (Enc(description), Enc(highway));

Advantages

1. Data dissemination mechanism works in untrusted environments
2. Data owner (source) availability is not required
3. Independent from trusted third parties
4. Agnostic to policy language and evaluation engine
5. On-the-fly key generation
6. Light-weight encryption is supported
7. Encrypted search over encrypted data is supported

References

[1] T. Eisenbarth, C. Paar, A.Poschmann, S. Kumar, L. Uhsadel, "A Survey of Lightweight-Cryptography Implementations", IEEE Design and Test of Computers, 2007

[2] The OpenCV Library Dr. Dobb's Journal of Software Tools (2000) by G. Bradski

[3] J. Harding, G. Powell, R. Yoon, J. Fikentscher, C. Doyle, D. Sade, M. Lukuc, J. Simons, J. Wang, "Vehicle-to-vehicle communications: Readiness of V2V technology for application," Report No. DOT HS 812 014, National Highway Traffic Safety Administration, Washington, DC, August 2014

[4] A. Ruddle, D. Ward, B. Weyl, S. Idrees, Y. Roudier, M. Friedewald, T. Leimbach, A. Fuchs, S. Grgens, O. Henniger, R. Rieke, M. Ritscher, H. Broberg, L. Apvrille, R. Pacalet, G. Pedroza,"Deliverable d2.3: Security requirements for automotive on-board networks based on dark-side scenarios," 2009

[5] R. Ranchal, "Cross-Domain Data Dissemination and Policy Enforcement", PhD Thesis, Purdue University, Jun. 2015.

[6] G. Izera M., and B. Bhargava."Security Protection Methods in Vehicle-to-Vehicle Systems." Computer Science Department Poster Showcase, Purdue University. Sept 2015.

[7] C. Miller and C. Valasek, "Adventures in automotive networks and control units," DEF CON 21 Hacking Conf., 2013. Accessed in Mar. 2014, http://www.youtube.com/watch?v=n70hIu9lcYo.

[8] C. Miller and C. Valasek. Adventures in automotive networks and control units. Technical White Paper, IOActive, 2014

References

[9] P. Angin, B. Bhargava, R. Ranchal, N. Singh, L. Lilien, L. Othmane and M. Linderman. "An entity-centric approach for privacy and identity management in cloud computing." 29th IEEE Symp. on Reliable Distributed Systems, Oct. 2010.

[10] R. Ranchal, B. Bhargava, L. Othmane, L. Lilien, A. Kim, M. Kang and M. Linderman. "Protection of identity information in cloud computing without trusted third party." 29th IEEE Symp. on Reliable Distributed Systems, Oct. 2010.

[11] B. Bhargava, P. Angin, R. Ranchal, R. Sivakumar, A. Sinclair and M. Linderman. "A trust based approach for secure data dissemination in a mobile peer-to-peer network of AVs." Intl. J. of Next-Generation Computing, vol.3(1), Mar. 2012.

[12] L. Ben Othmane and L. Lilien, "Protecting Privacy in Sensitive Data Dissemination with Active Bundles," .Seventh Annual Conf. on Privacy, Security and Trust (PST 2009), Saint John, New Brunswick, Canada, Aug. 2009, pp. 202-213.

[13] L. Ben Othmane, "Protecting Sensitive Data throughout Their Lifecycle," Ph.D. Dissertation, Dept. of Computer Science, Western Michigan University, Kalamazoo, Michigan, Dec. 2010.

[14] Lei Yao, Tao Gong, Jin Fan, Bharata Bhargava, "Research on ARM9-Based Intelligent Immune System for Avoiding Rear-End Collision", Intl. Journal of Immune Computation (IC) Vol. 1, No. 1, pp. 4-8, 2013

[15] G. Izera M., A. Johnson, B. Bhargava, "Secure protection methods in vehicle-to-vehicle networks", submitted, 2017