Secure Dissemination of Data in Vehicle-to-Vehicle Systems

Presentation for:
ADI (Sypris), Feb 22\textsuperscript{nd}, 2017

B. Bhargava\textsuperscript{1}, D. Ulybyshev\textsuperscript{1}, M. Villarreal-Vasquez\textsuperscript{1},
R. Ranchal\textsuperscript{1}, G. Izera M.\textsuperscript{1} L. Lilien\textsuperscript{2}

\textsuperscript{1}Computer Science Department/CERIAS,
Purdue University, West Lafayette, IN, USA

\textsuperscript{2}Department of Computer Science, Western Michigan University, Kalamazoo, MI, USA
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
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)

Motivation

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


  => 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

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

<table>
<thead>
<tr>
<th>V2V</th>
<th>Security</th>
<th>Safety</th>
</tr>
</thead>
<tbody>
<tr>
<td>No security features</td>
<td>No attacks</td>
<td>Do nothing</td>
</tr>
<tr>
<td></td>
<td>Under attacks</td>
<td>Misleading dashboard and gps; firmware and data wiped out; compromised vehicle’s sensors, part of botnet framework</td>
</tr>
<tr>
<td>With security features</td>
<td>No attacks</td>
<td>Power consumption and computation overhead</td>
</tr>
<tr>
<td></td>
<td>Under attacks</td>
<td>Isolate intruder, warn other nodes about attack, deviate attacks to targets with less damage</td>
</tr>
</tbody>
</table>
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 and 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

Highway scenario with only two vehicles involved

message = "stop right away"
CASE OF STUDY: SECURITY VS SAFETY

Stopping distance:
- Driver’s perception time
- Driver’s reaction time
- Vehicle’s reaction time
- Vehicle’s braking capability

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

*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

  ✓ Communication cost:

  \[ d_{com} = d_{transmission} + d_{propagation} + d_{queueing} \]

  ▪ Distance: 120m
  ▪ Bandwidth: 6Mbps
  ▪ Speed of communication link: \(3 \times 10^8\) m/s

<table>
<thead>
<tr>
<th>Public Key Cryptosystem</th>
<th>Generation (ms)</th>
<th>Verification (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ECDSA</td>
<td>3.255</td>
<td>7.617</td>
</tr>
</tbody>
</table>
CASE OF STUDY: SECURITY VS SAFETY

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

  - Speed: 120Km/h
  - Distance: 120m
CASE OF STUDY: SECURITY VS SAFETY

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

![Graph showing the relationship between message size and number of messages that can be sent in a 6Mbps link under V2V Communication and V2V With Authentication vs V2V Without Security.]

- 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 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)

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 ) )

Key Derivation Module

K_i

DECK_i (d_i)

d_i

Key Derivation Module

K'_i

DECk'_i (d_i)

wrong d_i
## Lightweight encryption

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

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

References