CERIAS

The Center for Education and Research in Information Assurance and Security

Secure Data Dissemination in Vehicle-to-Vehicle Systems

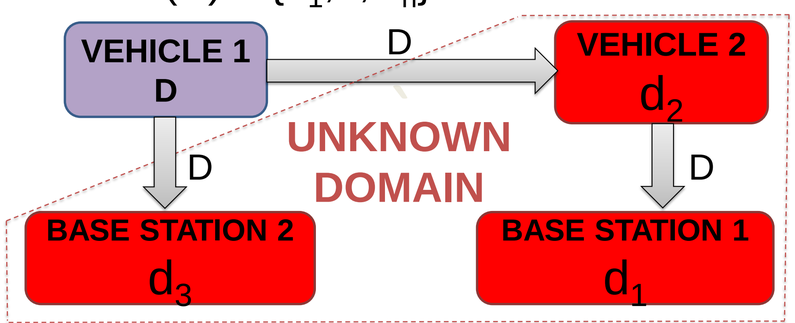
Denis Ulybyshev[1], Bharat Bhargava[1] , Chenyang Qu[1], Rohit Ranchal[2], Leszek T. Lilien[3,1]

[1] Computer Science Department and CERIAS, Purdue University; [2] IBM Watson Health Cloud

[3] Department of Computer Science, Western Michigan University

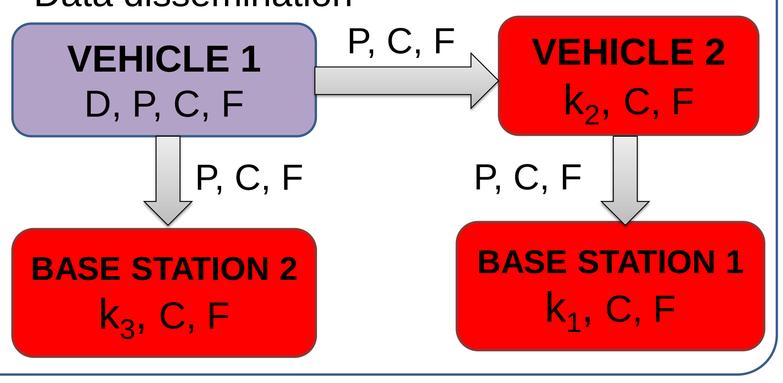
MOTIVATION

- Data (D) = {d_1,.., d_n}



REQUIREMENTS FOR F

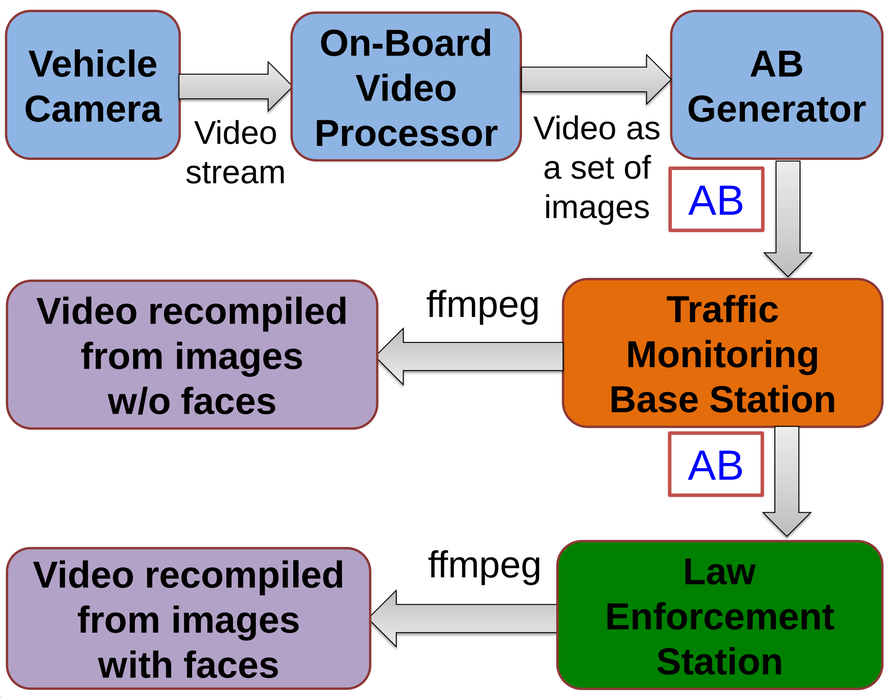
- Host (Service) Authentication
- Policy evaluation (Authorization)
- Key derivation
- Data dissemination
- Tamper Resistance



HARDWARE SETUP

- Credit-card size Raspberry Pi board (model B)
- Pi video camera

SYSTEM ARCHITECTURE



PROBLEMS

- Opaque data sharing
- Undetected data leakages
- Lack of policy infrastructure

Cyberattacks in V2V	Protection
No Brakes	Digital Signature / HMAC
False Acceleration	
Light-out attack	
Forced Steering Wheel	
Malware	Stack Protection, Antivirus, IDS
Denial-of-Service	Firewall

OBJECTIVES

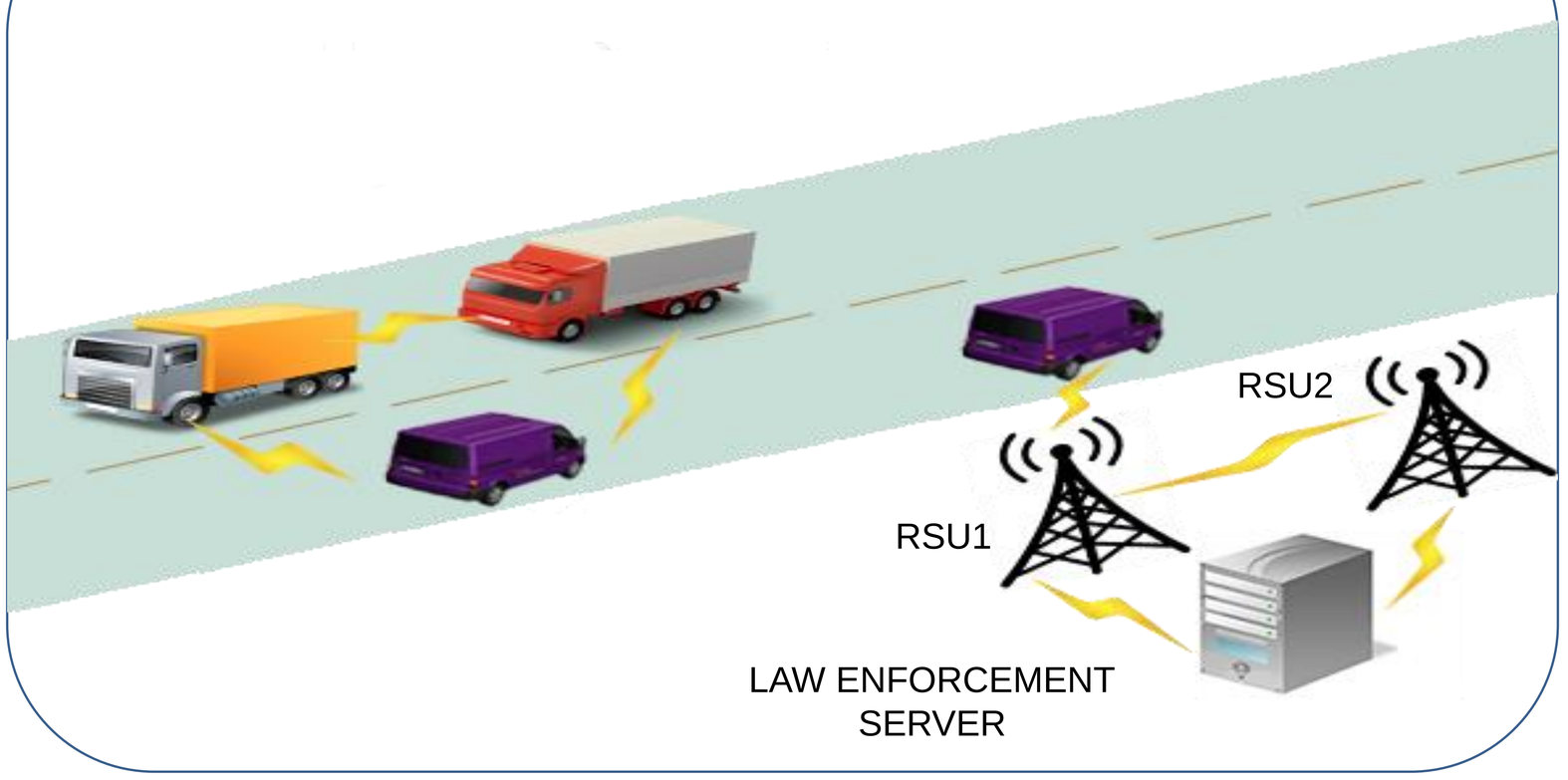
- Vehicle manufacturers, law enforcement officials and drivers should be able to define access control policies for vehicle's data items
- Authorized service (host) should only be able to access data items for which it is authorized
- Unauthorized host shouldn't be able to access any data

PROPOSED SOLUTION

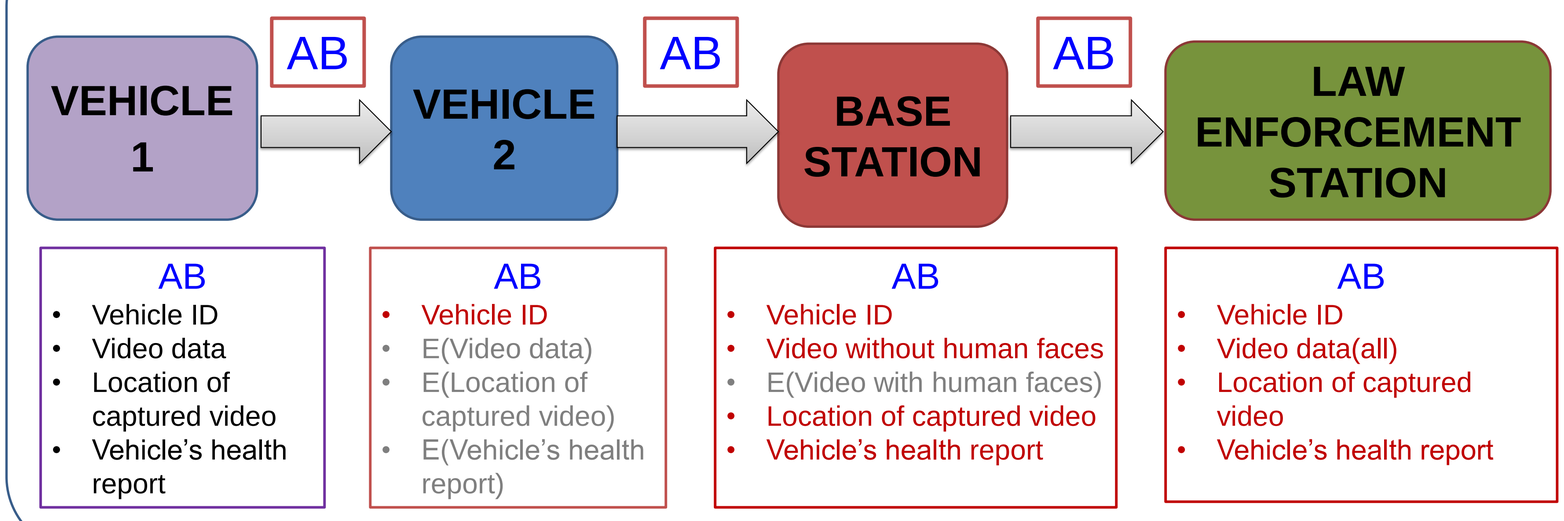
- Data item (d_i) = <k_i, v_i>
- Policies (P) = {p_1,.., p_m}
- Ciphertext (C) = {c_1,.., c_n}
- Function set (F)
- Encrypt data (C) and define function set (F)
- Share C and F with each service (host)

```
if (service.IsAuthorized)
  F(dataRequest, cipherText)= dataItem
```

V2V and V2I COMMUNICATIONS



DATA DISSEMINATION IN V2V AND V2I SYSTEMS



ACKNOWLEDGEMENT: This publication was made possible by NPRP grant # [7-1113-1-199] from the Qatar National Research Fund (a member of Qatar Foundation). The statements made herein are solely the responsibility of the authors.

CERIAS

PURDUE UNIVERSITY