Secure Dissemination of Video Data in Vehicle-to-Vehicle Systems

C. Qu[1], D. Ulybyshev[1], B. Bhargava[1], R. Ranchal[1],
G. Izera M.[1], L. Lilien[2]

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

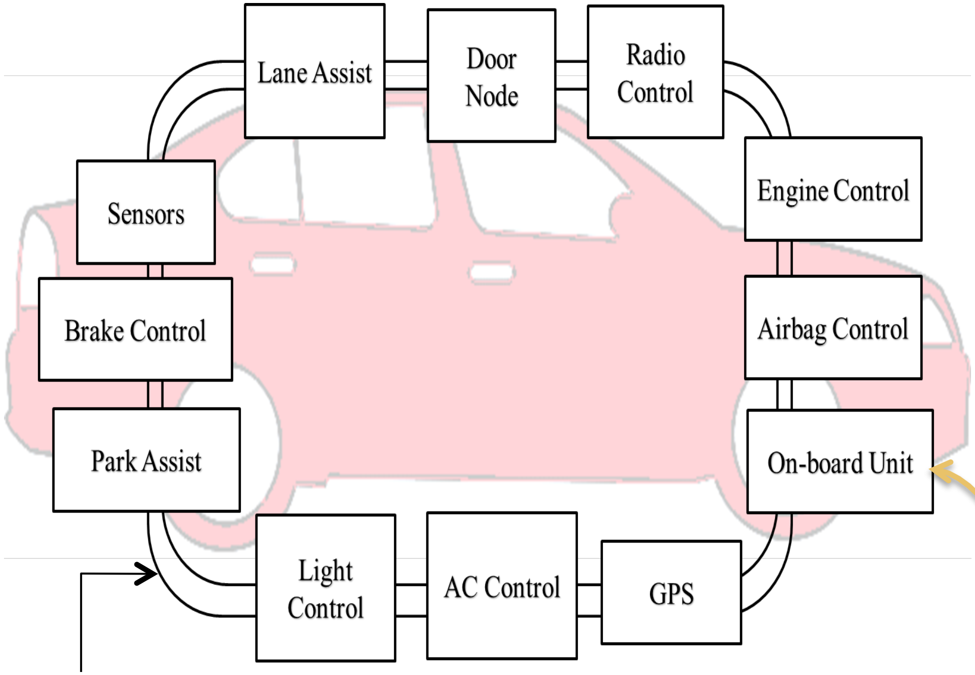
[2]Department of Computer Science,
Western Michigan University, Kalamazoo, MI, USA

Outline

1. Motivation
2. Objectives
3. Related Work
4. Core Design
   - 4.1. Active Bundle Concept
   - 4.2. System Architecture
   - 4.3. Video Recording
   - 4.4. Face Recognition
   - 4.5. Video Recreation
5. Evaluation
6. Pros and Cons
7. Conclusions

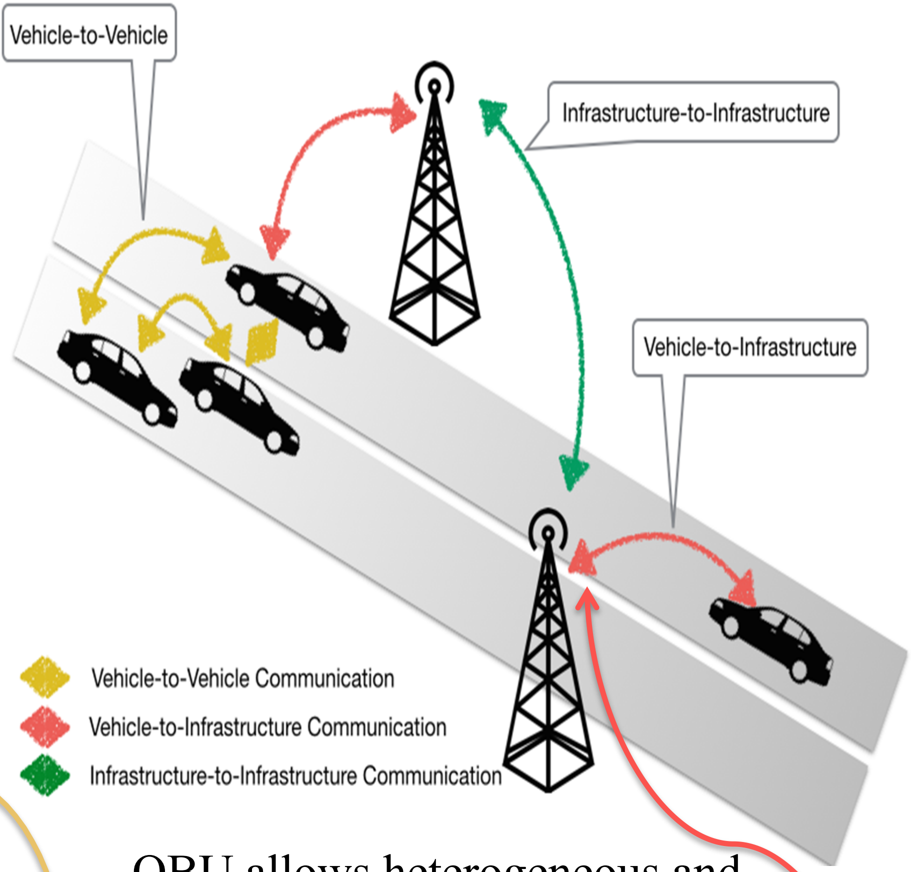
Motivation

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]



CAN (Control Area Network) Bus

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


Vehicle-to-Vehicle
Infrastructure-to-Infrastructure
Vehicle-to-Infrastructure
Vehicle-to-Vehicle Communication
Vehicle-to-Infrastructure Communication
Infrastructure-to-Infrastructure Communication

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

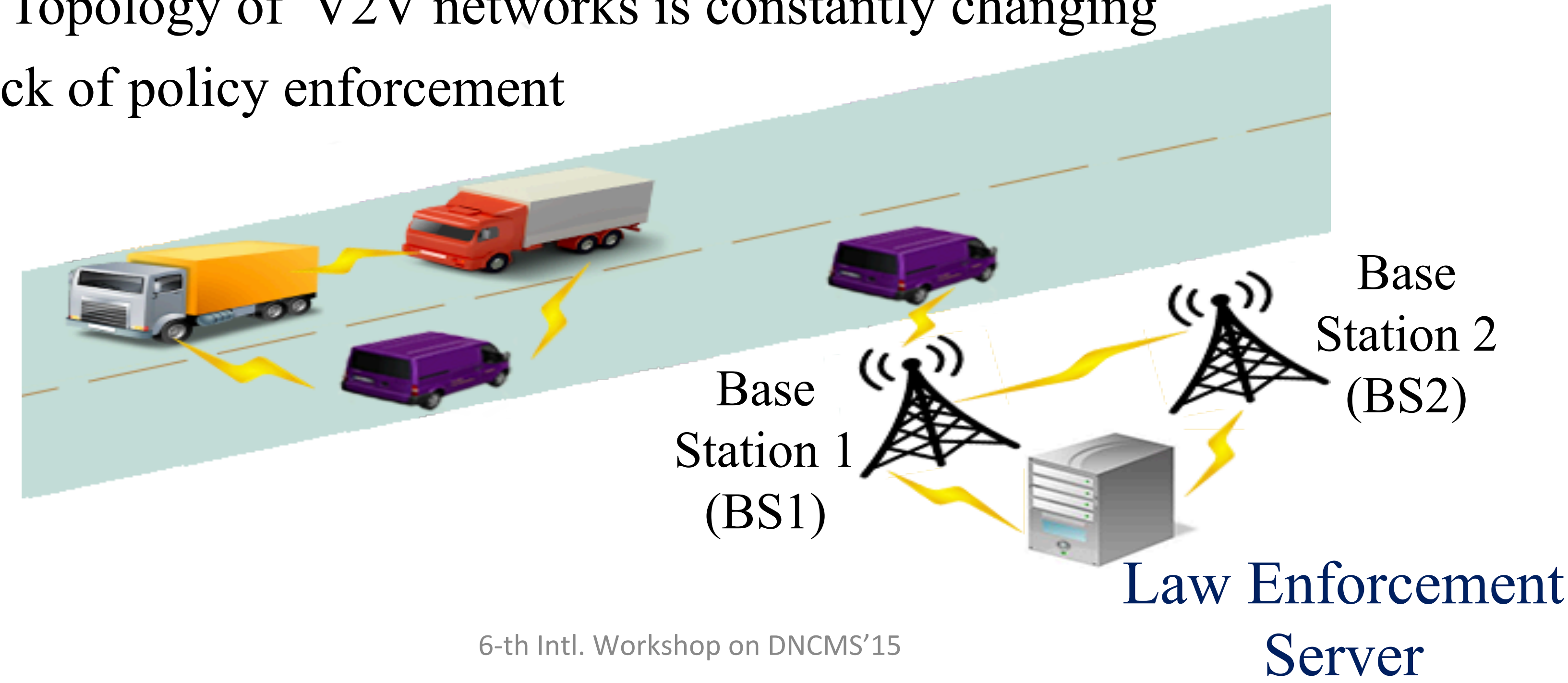
Motivation

- Connected vehicles deploy signals to communicate with other vehicles, roadside units, personal devices and cloud services
  - Goal: provide assistance to drivers and prevent accidents
- 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
- Protection mechanisms
  - Active Bundle [5], [9], [10], [11], [12], [13]
  - Digital Signature
  - HMAC

Motivation

Potential problems in vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) systems:

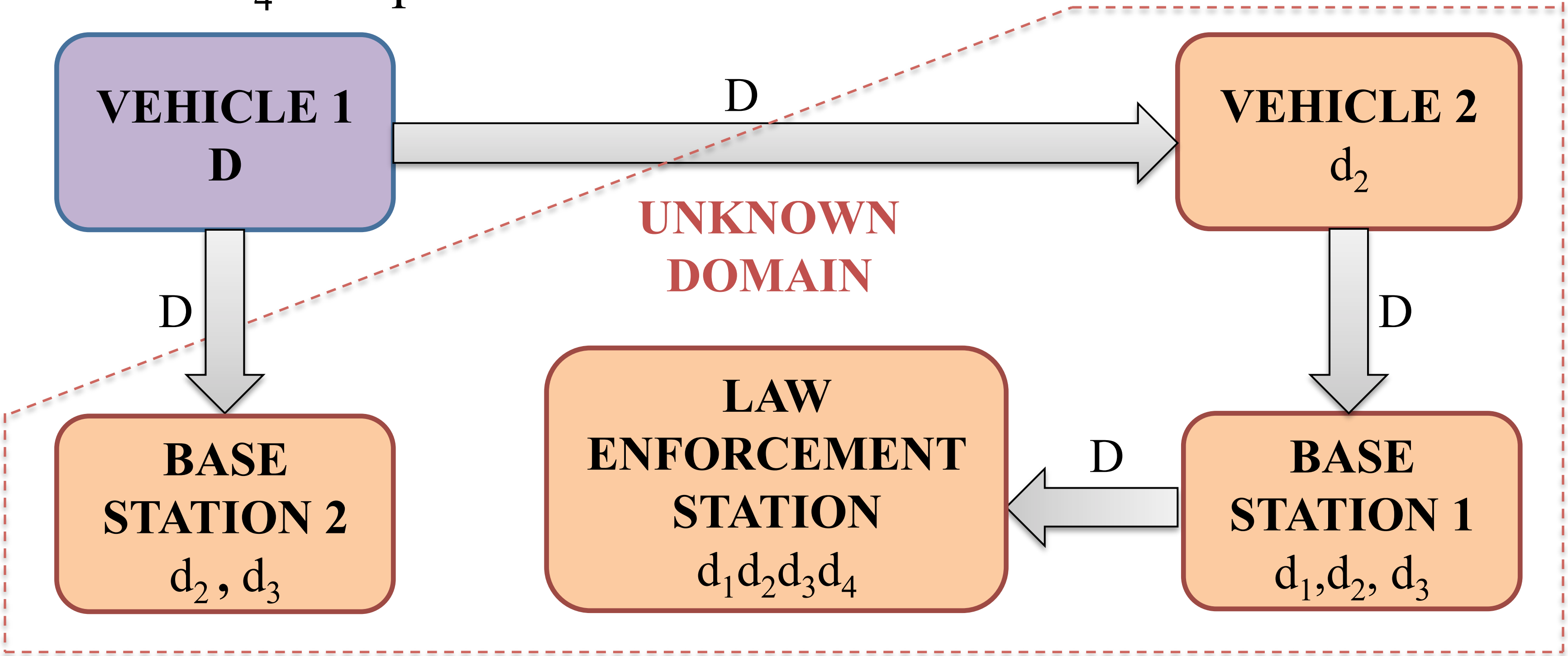
- Opaque data sharing (e.g. BS1=> BS2)
  - Owner’s data can be shared with other parties but data owner does not know about it
- Undetected privacy violations
  - Topology of V2V networks is constantly changing
- Lack of policy enforcement



Motivation

Data D = {d_1, … , d_n } where d_i is a separated data item

- Data D is sent in encrypted form
- E.g. d_1 is captured video data without human faces
  d_2 is a traffic information
  d_3 is vehicle's health report
  d_4 is captured video data with human faces



Objectives

1. Develop a mechanism for privacy-preserving data dissemination in V2V and V2I systems, such that:

    1.1. Each node is only able to access data items for which it is authorized

    1.2. Vehicle manufacturers, law enforcement and drivers are able to define access control policies for vehicle's data items

    1.3. Secure data dissemination in untrusted V2V and V2I environments is provided

    1.4. Message authenticity and integrity is provided

2. Analyze existing sets of regulations for data security policies in V2V and V2I systems in the U.S. and in EU

3. Develop a framework for detecting whether human face is present in video data captured by vehicle's camera

    - Face detection result is used in policies

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 signature
  - HMAC
  - Checksums
- 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

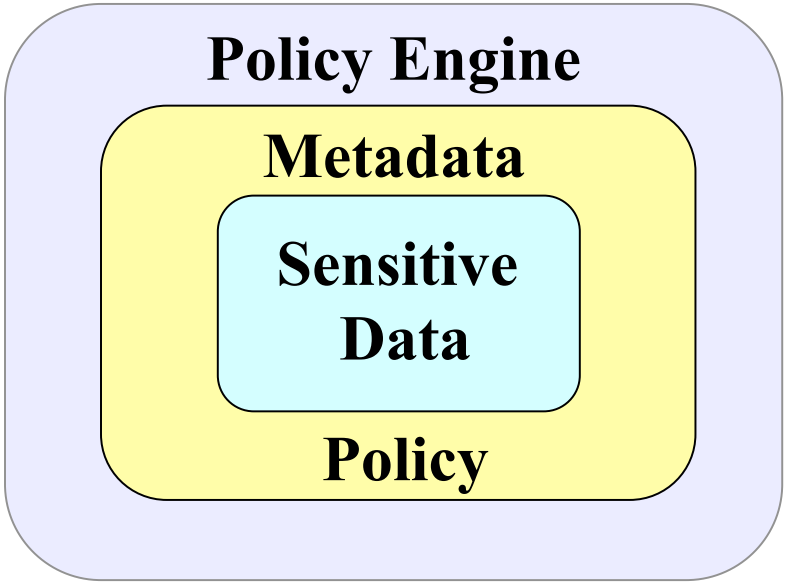
Miller and Valasek demonstrated in DEF CON 21 a set of attacks [7], [8], including very serious attacks.

- ➢ 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

Core Design

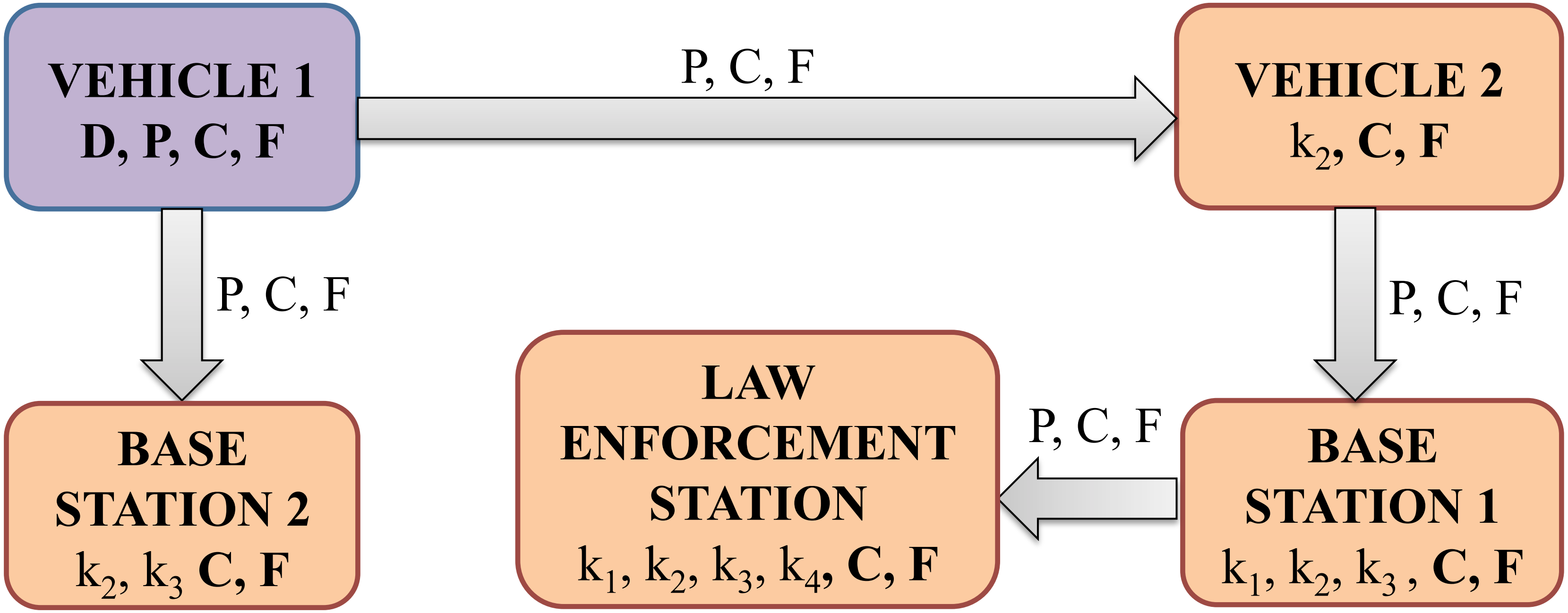
Active Bundle (AB) consists of:

- *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



Proposed Solution

- Data item (D) = $<k_i, v_i>$
- Policies (P) = $\{p_1,.., p_m\}$
- Ciphertext (C) = $\{c_1,.., c_n\}$
- Function set (F)
  - F encapsulates AB and maps C to D considering P



Key Generation

- AB Template [5] is used to generate new ABs with data and policies specified by a user
  - AB Template includes the implementation of invariant parts (monitor) and placeholders for customized parts (data and policies)

- User-specified data and policies are included in AB Template

- AB Template is executed to simulate the interaction process between an AB and a service requesting access to each data item of AB

- Collect and aggregate into a single value for each data item the information generated during the execution of different AB modules and the digests of these modules and their resources such as:
  - Authentication: authentication code, CA certificate that it uses
  - Authorization: authorization code, applicable policies, policy evaluation code

Key Generation

- Value for each data item is input into a Key Derivation module (such as SecretKeyFactory, PBEKeySpec, SecretKeySpec provided by 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]

Decryption Key Derivation

- AB receives access request to a data item from a service
- AB authenticates the service and authorizes its request
- Information generated during the execution of different AB modules and the digests of these modules and their resources (authentication (authentication code, CA certificate that it uses), authorization (authorization code, applicable policies, policy evaluation code)) are collected and aggregated into a single value for each data item [5]
- Value for each data item is input into the Key Derivation module (such as SecretKeyFactory, PBEKeySpec, SecretKeySpec provided by javax.crypto library)

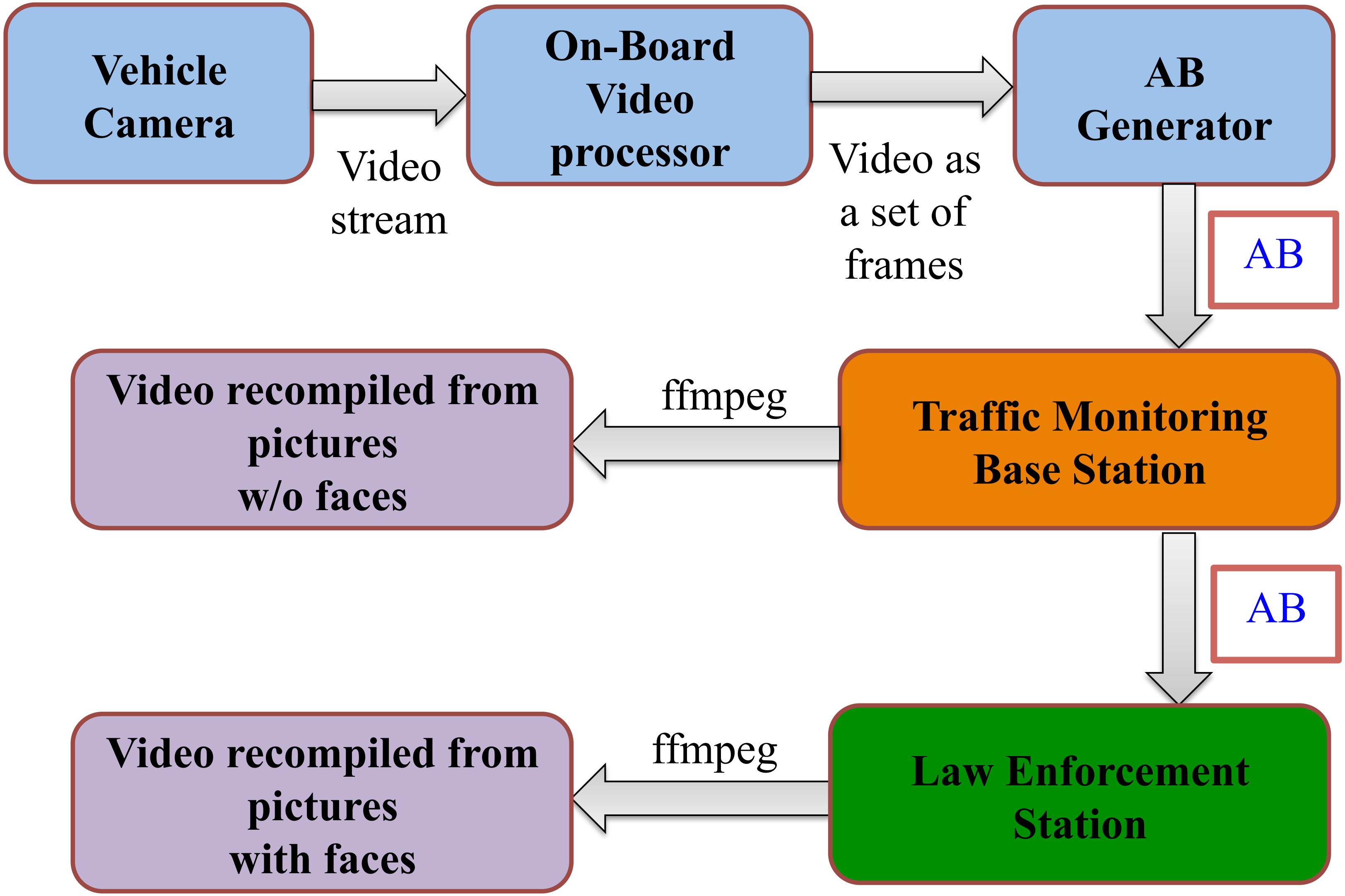
Decryption Key Derivation

- Key Derivation module outputs the specific key relevant to the data item [5]
- 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 methods for key distribution

- Centralized Key Management Service
  - TTP used for key storage and distribution
- Key included inside AB
  - Prone to attacks!

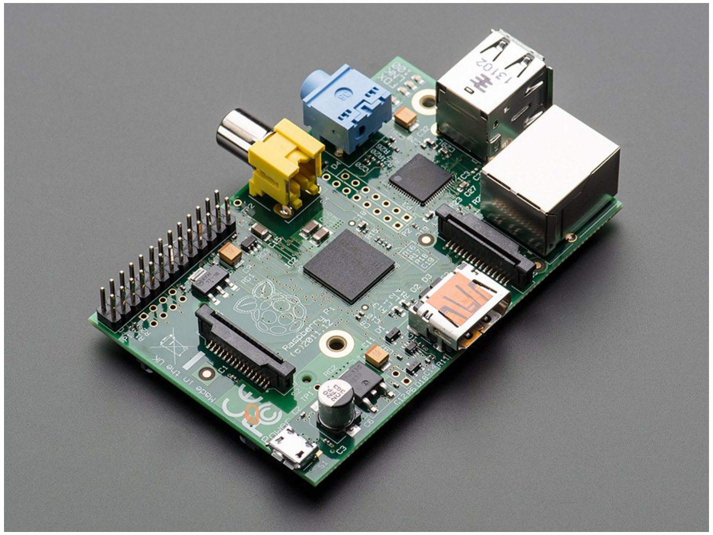
System Architecture

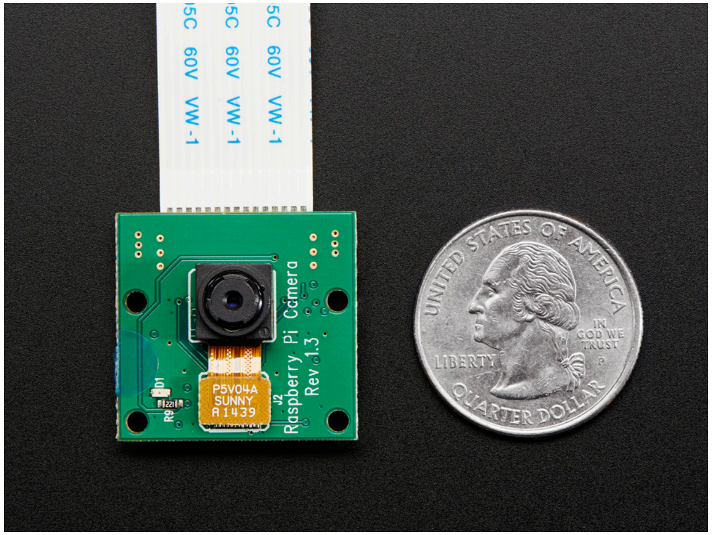


Hardware Setup

Hardware Setup to record and process video data

- Raspberry Pi (model B)
  - 4” x 3” x 1.5” credit-card size development board
  - 5V of DC power
  - 700 MHz ARM CPU
  - 512 MB RAM
- Pi camera
  - Up to 2592 x 1944 pixels for static frames
  - Up to 1080p for video recording





Software application

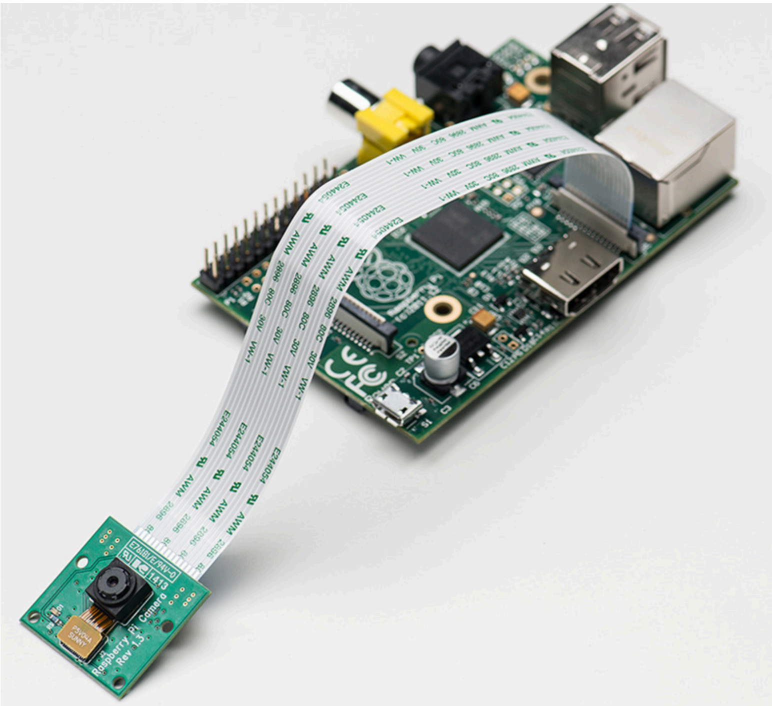
- Developed C++ application running on Raspberry Pi board.

  Goals:

  - Specify parameters for camera configuration (video resolution, video length and frame rate)
  - Restore video data as an array of "Mat" objects from OpenCV[2] library
  - Apply existing face recognition algorithms (cascade classifiers) from OpenCV [2] library
  - According to the result of face recognition function, separate frames into two groups ("frames with human faces" and "frames without human faces")
  - Use "ffmpeg" [1] to recreate videos from different groups of frames

Video Recording

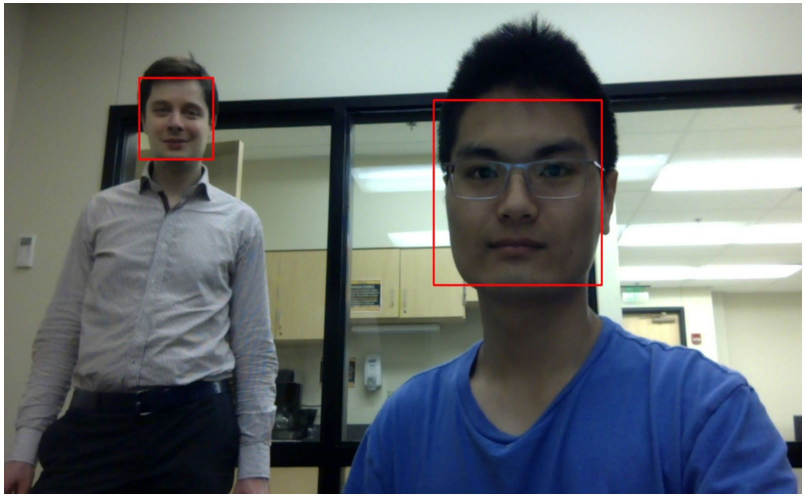
- CSI (Camera Serial Interface) bus between Pi camera and CPU
  - High-speed communication (up to 1 Gbits/s data rate)[1]
- C++ application for video recording
  - User-specified resolution, video length and frame rate
  - Restore image as an array of “Mat“ objects



[1] Online Source: http://www.electronicproducts.com/Digital_ICs/Communications_Interface/Camera_Serial_Interface_CSI-2_sensors_in_embedded_designs.aspx

Face Recognition

- 4 face recognition algorithms (cascade classifiers) from OpenCV [2] library:
  - haarcascade_frontalface_alt
  - haarcascade_frontalface_alt2
  - haarcascade_frontalface_default
  - lbpcascade_frontalface



- C++ application for face recognition
  - Process all frames of video data
  - Apply face recognition algorithm to each frame
  - Report whether human face was detected

Video Recreation

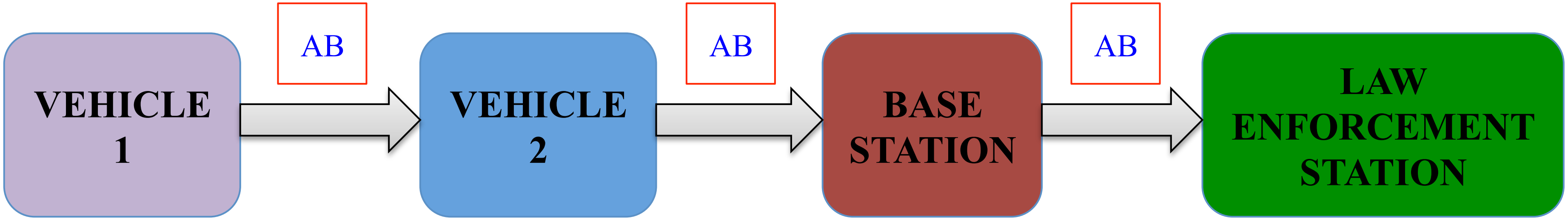
- Frames with human faces are sensitive data
  => their privacy must be ensured in untrusted environments

- Result of face recognition is used in policies

- Every node is able to extract from AB only those frames for which it is authorized

- Use “ffmpeg [1]” to recreate video from a set of accessible frames at receiver’s side
  - Frame rate can be specified

Scenario of AB Transfer



VEHICLE 1

AB

VEHICLE 2

AB

BASE STATION

AB

LAW ENFORCEMENT STATION

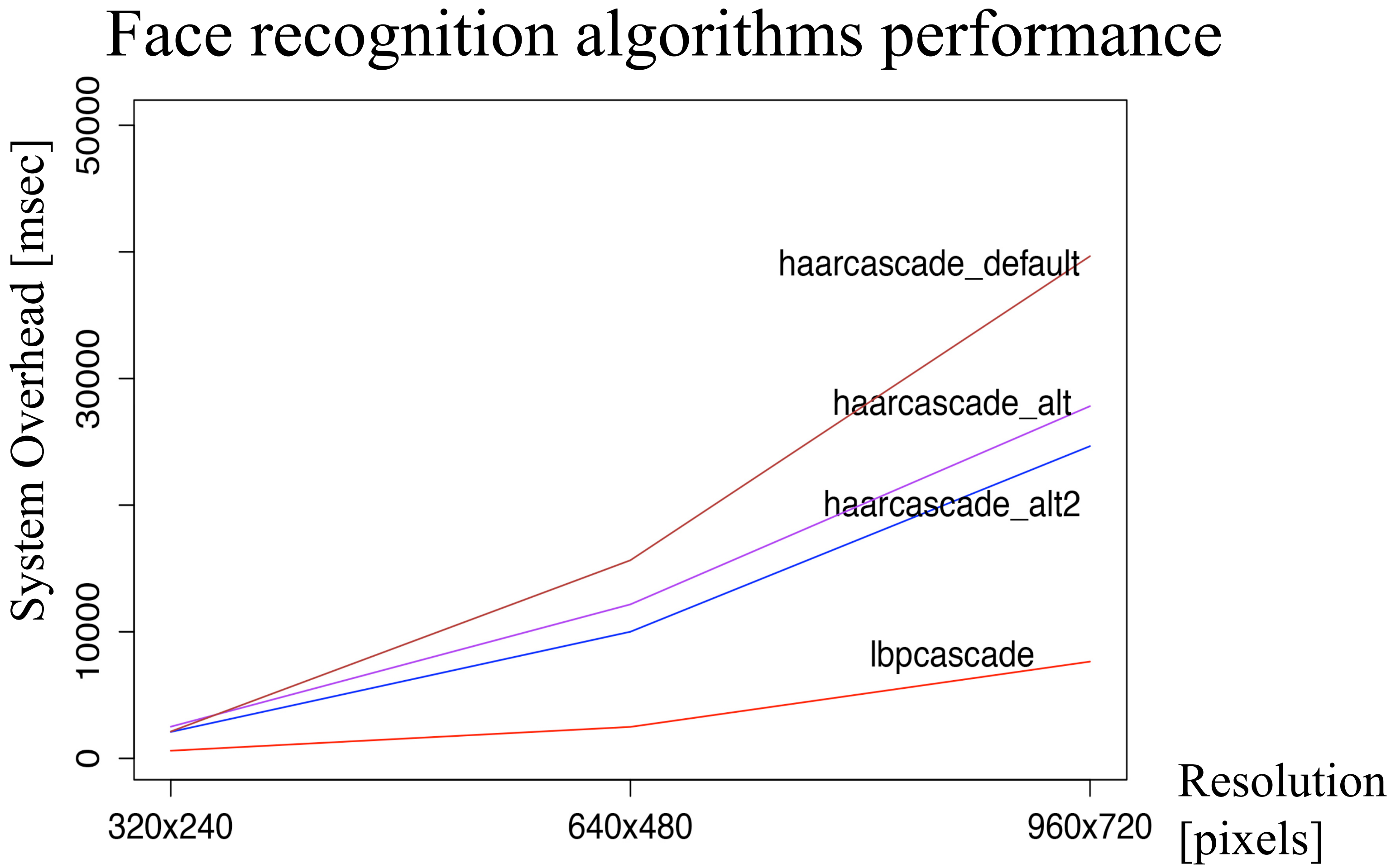
AB
- Traffic Info
- Video with human faces
- Video w/o human faces
- Vehicle's health report
- Location of captured video

AB
- Traffic Info
- E(Video with human faces)
- E(Video w/o human faces)
- E(Vehicle's health report)
- E(Location of captured video)

AB
- Traffic Info
- E(Video with human faces)
- Video w/o human faces
- Vehicle's health report
- Location of captured video

AB
- Traffic Info
- Video with human faces
- Video w/o human faces
- Vehicle's health report
- Location of captured video

Evaluation



- ➢ "Haar Cascade Alternative 2" has the highest detection rate with the second lowest overhead

Pros and Cons

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. Four face recognition algorithms are supported

Pros and Cons

Disadvantages:

1. Interaction time between service and AB is more than 1 sec (in case of only one policy) => currently not applicable for vehicle's critical systems

Future Work:

- ➢ Currently a set of policies is defined once by data owner => allow other parties to add new policies to AB
- ➢ Need a mechanism to merge policies added by different parties, e.g. to resolve contradicting policies

Conclusions

- Developed a policy-based approach for controlled and secure video data dissemination in untrusted environments in V2V and in V2I communication systems by means of *Active Bundles* [5]

- Approach is illustrated on secure dissemination of video data captured by vehicle's camera

- Among 4 face recognition algorithms - "*Haar Cascade Alternative 2*" has the highest detection rate with the second lowest overhead

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.

References

[1] ffmpeg http://www.ffmpeg.org

[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] 1. 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.

References

[8] C. Miller and C. Valasek. Adventures in automotive networks and control units. Technical White Paper, IOActive, 2014
http://www.ioactive.com/pdfs/IOActive_Adventures_in_Automotive_Networks_and_Control_Units.pdf

[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.