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

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

[1] Computer Science Department, Purdue University, West Lafayette, IN 47907
{qu10, dulybysh, bbshail, rranchal}@purdue.edu
[2] Department of Computer Science, Western Michigan University, Kalamazoo, MI 49008
{leszek.lilien}@wmich.edu

Abstract — Data exchange between vehicles and base stations may contain information on traffic accidents, traffic jams, road constructions etc. Risks to data privacy in vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) systems need be minimized. We present a policy-based solution that provides controlled and privacy-preserving dissemination of video data in V2V and V2I. This policy-based solution relies on Active Bundle (AB), which incorporates policy enforcement mechanism and policies that describe access to video data. The usage of ABs ensures privacy of actors during disclosure of captured video in untrusted environment.

Face recognition algorithm is used to identify sensitive data in videos and it is used in policies. We use four algorithms to process images that are captured by a vehicle's camera.

Keywords—active bundle, vehicle-to-vehicle system, video dissemination, face recognition

I. Introduction

Vehicles can exchange different types of useful information among each other in (V2V) and (V2I) systems. This information is transmitted in V2V and V2I systems to prevent accidents and provide assistance to drivers. Video captured by vehicle's cameras can be shared in V2V and V2I systems to make reports on traffic accidents and to request emergency assistance.

V2V and V2I communications introduce risks to privacy of sensitive data. A video captured by dashed camera can be shared among multiple parties (vehicles and base stations). For example, if the direct communication between a vehicle and a base station can not be established, this vehicle may transfer a video or another information to a base station through a chain of other base stations and driving vehicles. Video fragments containing human faces are considered as sensitive data and its privacy must be ensured in untrusted environments. Every party involved in data exchange should access only those data that it is authorized to see. We present a policy-based approach that provides secure data dissemination in untrusted environments by means of Active Bundles (AB) [5], [6], [7], [11], [20], [21], [22].

There is a need to extend existing sets [14], [15] of regulations for policies that can be specified by vehicle manufacturers, by law enforcement officials and by the driver (data owner). These policies must provide controlled and secure data dissemination [19].

Section II contains a brief overview of related work, Section III outlines a proposed solution, Section IV evaluates performance overhead for different face recognition algorithms. Section V concludes the paper.

II. Related Work

Miller and Valasek demonstrated in DEF CON 21 a set of attacks on two cars [16], [17], including very serious attacks that can take control over brakes, accelerator, engine and steering wheel. Authors succeeded in reverse engineering the code of an Electronic Control Units (ECU), and provided a list of keys/passwords used by ECUs internally for cryptographic operations. In contrast, in AB the key for encryption/decription operations on AB's data is derived from the execution flow and is stored neither inside AB nor at sending/receiving site.

Ben Othmane showed that connected vehicles are prone to cyberthreats [18]. The research report "Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application" [14] made by National Highway Traffic Safety Administration, assesses the readiness for application of V2V communications, a system designed to transmit basic safety information between vehicles to deliver warnings to drivers in order to prevent impending crashes. This report addresses the following question: What policy or organizational controls 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 [14]? This report includes the description of privacy policies framework and lists the requirements for V2V security system. We extend this privacy policies framework with concrete policies that can be specified by vehicle manufacturers. Shared video fragments containing human faces should only be accessed by law enforcement officials. This policy when included into AB will control distributed dissemination of data captured by vehicle's camera.

EVITA project [15], developed in European Union, has identified and evaluated security requirements for automotive on-board networks based on a set of use cases and an investigation of security threat scenarios (dark-side scenarios). In Section 3.2.8, the project report says "The personal information stored within the car shall remain confidential even during exchange of ECUs" or "The seat position information for a driver shall remain confidential, even during exchange of data with a mobile device" [15]. The report further states "Users shall be able to determine by themselves the disclosure of information acceptable for various applications regarding their private profile or their car profile, providing it is lawful."

III. Proposed Solution

A. Active Bundles for secure data dissemination

Active Bundle (AB) is a data structure that contains three following parts:

1) *Sensitive data*: They may include documents, messages and multimedia content. This content may contain several data items with different security levels. An applicable policy of AB must ensure controlled and secure distribution of the corresponding data item.

2) *Metadata*: They describe the AB and its policies. AB description includes information on AB identifier, AB creator and owner, creation time and lifecycle. Policies, such as access control policies, dissemination policies and privacy policies, manage AB interaction with services and hosts.

3) *Policy engine (Virtual Machine):* It provides AB operations and enforces policies specified in AB. Implementation of the policy enforcement engine provides AB's tamper-resistance, which ensures the integrity of sensitive data and metadata

Fig. 1 illustrates the structure of AB. Sensitive data includes captured video. Policy evaluation [20] is done by means of WSO2 Balana open-source policy engine, which enforces policies. Policy specification is supported in JSON and in XACML specification language. Here is the example of the policy:

if frame (image) contains human face
then it's available only to law enforcement official

Sensitive data is encrypted and decryption key derivation is based on the AB execution control flow. AB is implemented as a JAR – file. Details on AB implementation can be found in [20].

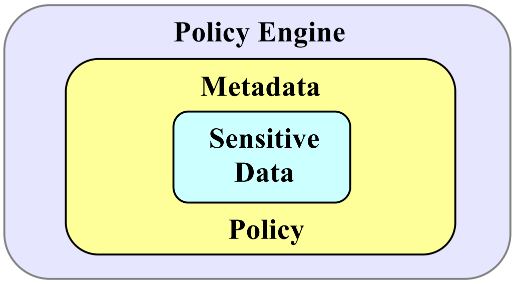

Fig.1. Example of AB structure

Details on AB concept are discussed in [21], [22].

B. System architecture

Video captured by vehicle's dashed camera are transfered to base stations and to other vehicles by means of AB. This data transfer may involve a chain of other base stations and driving vehicles. Each party executes received AB to get access only to the data for which it is authorized and then sends AB further, if necessary. In the current implementation, which is written in C/C++ and runs on a Unix kernel operating system named *Raspbian* [3], we focus on secure dissemination of video. Video is captured by camera, which is connected to a development hardware board named *Raspberry Pi* [2]. The unit of video data is an image (frame). We split the video into a set of images according to the frame rate (e.g. 24 frames per second) and apply face recognition algorithm to each frame. The result of face recognition can be used in AB policies. As an example of policy, specified in AB, law enforcement official has the authority to see images/videos with human faces. Everybody else with lower authorization level, e.g. for a journalist, images and, thus, video fragments with human faces will be unavailable. Our solution supports four face recognition algorithms: *lbpcascade, haarcascade_default, haarcascade_alt, haarcascade_alt2.* Face recognition is implemented by using an open-source library *openCV* [1].

After processing all the frames of a captured video with face recognition algorithm, AB with video, represented as a set of images (frames), is created and then AB can be transferred to base stations and other vehicles. After AB arrives at the base station or to other vehicle, only those images for which the base station or vehicle is authorized are extracted from AB and video is recreated from this set of accessible images. To recreate video at receiver's side we use *ffmpeg* software.

This process is illustrated in Fig.2. Traffic monitoring base station gets access only to frames without human faces. Law enforcement station can get access to all the frames. Thus, video recompiled from all accessible frames will contain fragments with human faces.

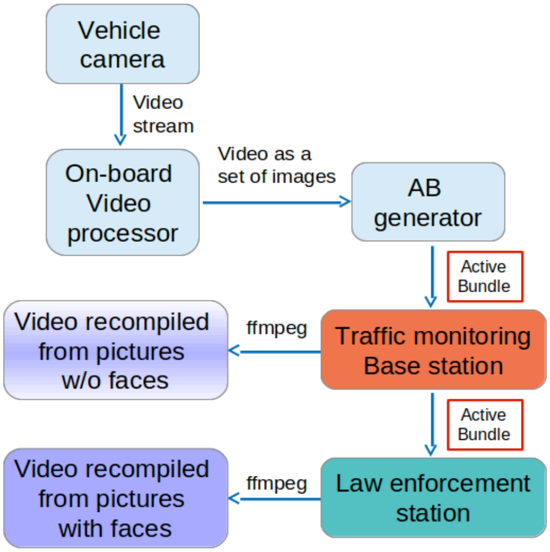

Fig.2. Example of architecture

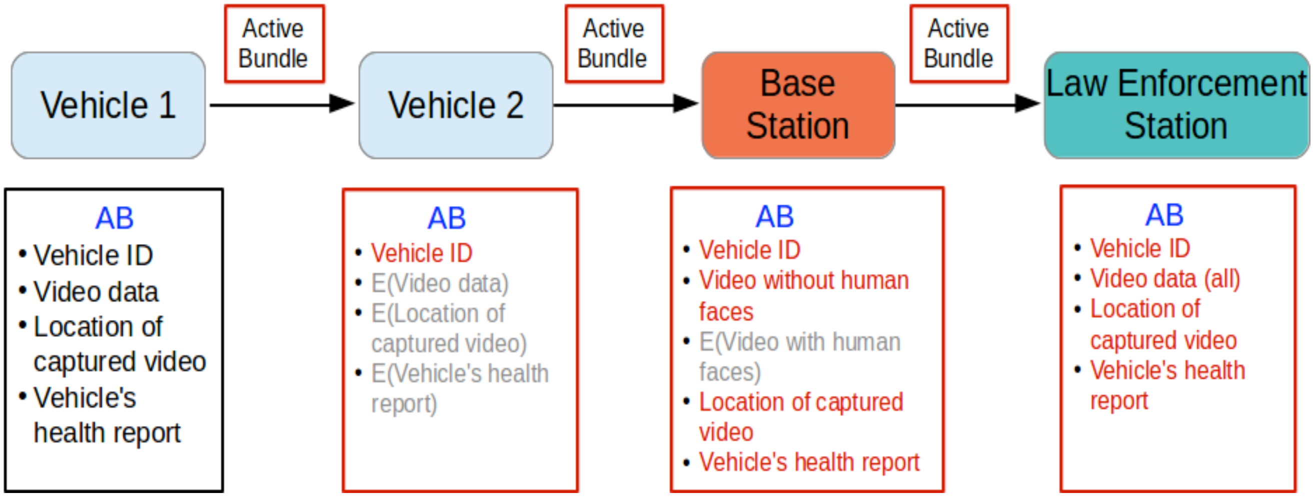
Vehicle 1
Active Bundle
Vehicle 2
Active Bundle
Base Station
Active Bundle
Law Enforcement Station
AB
• Vehicle ID
• Video data
• Location of captured video
• Vehicle's health report
AB
• Vehicle ID
• E(Video data)
• E(Location of captured video)
• E(Vehicle's health report)
AB
• Vehicle ID
• Video without human faces
• E(Video with human faces)
• Location of captured video
• Vehicle's health report
AB
• Vehicle ID
• Video data (all)
• Location of captured video
• Vehicle's health report

Fig.3. AB transfer from vehicle to other parties

In the next example in Fig.3, a vehicle captures video of a traffic accident which happened before and involved other cars driving in the opposite direction. The goal is to create AB containing video of the traffic accident and to transfer it to the nearest base station and to police. If there is no base station in a closed proximity, AB is transferred to the base station through a chain of other vehicles. AB may contain vehicle's health report, including the status of main systems (engine, brakes, battery, tires, transmission, fuel etc.). Fig. 3 illustrates what type of data from AB can be accessed by different nodes. E(data) denotes that data is encrypted and not accessible by the node. Policy engine provides policy enforcement and thus every party gets access only to those data of AB for which the party is authorized. The rest of the data remains encrypted and cannot be decrypted.

Policies for AB can be specified by vehicle manufacturers, by law enforcement officials and by the driver (data owner). E.g. policy for human faces appeared in video or in images can be pre-determined and specified by vehicle manufacturer. Other sensitive data such as status of vehicle satelite protection from hi-jacks (on/off), health report, details of a technical problem etc. could be also protected from unauthorized disclosures by specifying the corresponding policies by vehicle manufacturers. We extend existing sets of regulations [14], [15] for privacy-related policies in V2V and V2I, similar to HIPAA [12] in health care and to FERPA [13] in educational system used in the United States.

C. Video recording

Our system operates in a vehicle, assuming space and power limitations. An embedded solution with a microcomputer and video camera is needed. We use a credit-card size development board *Raspberry Pi* [2] and a Pi camera as an infrastructure. It requires a DC power supply with voltage 5V. The size of the board is only 4-inch long, 3-inch wide and 1.5-inch high. Fig. 4 demonstrates the Raspberry Pi with video camera connected.

The model of Raspberry Pi contains a Broadcom BCM2835 SoC, which includes an ARM1176JZF-S 700 MHz processor, VideoCore IV GPU, and 512 Megabytes of RAM. USB Wi-Fi adapter is used to provide wireless communication. Detailed data sheet can be found in [8]. The camera is directly connected to the BCM2835 processor via CSI bus, a high bandwidth link, which carries pixel data from the camera back to the processor. The sensor in this camera itself has a native resolution of 5-megapixel, and has a fixed focus lens on board. The camera supports 2592 x 1944 pixel static images and 1080p, 720p and 480p videos. With this hardware installed in a vehicle we are able to record high-resolution real-time video.

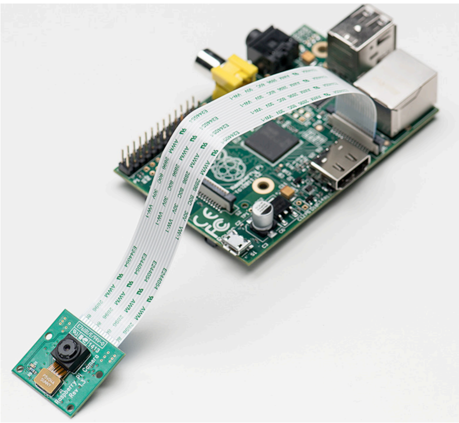

Fig.4. Raspberry Pi with a Pi – camera

However, after installation it was not possible to use directly the default video capturing An API named *VideoCapture* from *openCV*. The reason is that this API captures an image from a USB or web – based camera. The used camera is communicating with the CSI bus. In order to solve this problem, it is required to recompile the source code of our Pi camera driver and add it as a function to *openCV*. After that, we can run our program to capture video and process it on the Raspberry Pi.

D. Face recognition

There are four major *Cascade Classifiers* in openCV library [1] we can be used to detect human faces:

1) *haarcascade_frontalface_alt.xml*
2) *haarcascade_frontalface_alt2.xml*
3) *haarcascade_frontalface_default.xml*
4) *lbpcascade_frontalface.xml.*

Some of the work on geometric face recognition was carried out in [10]. Different *Cascade Classifiers* have different performance. When a user runs the program, she can specify a particular *Cascade Classifier* for the face recognition function. Resolutions are a key point for the system performance overhead. Higher resolutions impose higher overheads but provide higher quality of video. Evaluation details of the algorithms are presented in section IV.

After setting a proper algorithm for face recognition process, we feed this function with a gray-version image captured by the Pi camera. Multiple faces can be detected on one image. Detected faces are highlighted with red rectangles. Name of the image file contains current time stamp of the system. If the image contains detected face(s) then the image is saved to *picwithface* directory. Otherwise, it is saved to *picwithoutface* directory. As a result, we have two separated groups of images in corresponding directories: *picwithface* and *picwithoutface*. Then AB is created with these images as sensitive data. Currently data owner specifies policies for AB which will be enforced to provide video dissemination. Face recognition results are used in AB policies.

E. Video recreating

AB containing a set of images with and without human faces can be transferred among vehicles, base stations and other nodes. At the destination site, policies are enforced so that the destination site is able to access only those data for which the site is authorized. As shown in Fig.3, a host with law enforcement status will get access to all images, including images with human faces. Regular base station will get access only to images, which don't contain human faces. Other vehicles will not get access to any images. After enforcing the policy, a video from accessible images will be recreated at receiver's site.

There are several software tools that can be employed to create a video from a set of images. Image similarity and delta changes between images constitute another important research issue not discussed here. In our implementation video is created from a set of images by using *ffmpeg* software. An example of usage is shown below:

```
ffmpeg -i images%d.jpg -r rates output.mp4
```

The argument *images%d.jpg* will let *ffmpeg* automatically take *images1.jpg*, *images2.jpg* and so on. The argument *rates* is the frame rate per second, which is defined by the user. The ”-r” argument has a significant influence on the *output.mp4* resulting video. Higher frame rate means smaller latency in the video. If there are only a few images and user specifies a large frame rate argument, *ffmpeg* simply duplicates an image to reach that argument.

IV. Evaluation

This section focuses on performance overhead and detection rates for different face recognition algorithms. Detection rate is defined as a percentage of correct detections of true human faces. Our evaluation involves the running time cost of each classifier (on the specific hardware *Raspberry Pi*), no matter whether it detects human faces or not. We run several test cases for different resolutions with different Cascade Classifiers in order to make a comparison. Fig.5 represents experimental results.

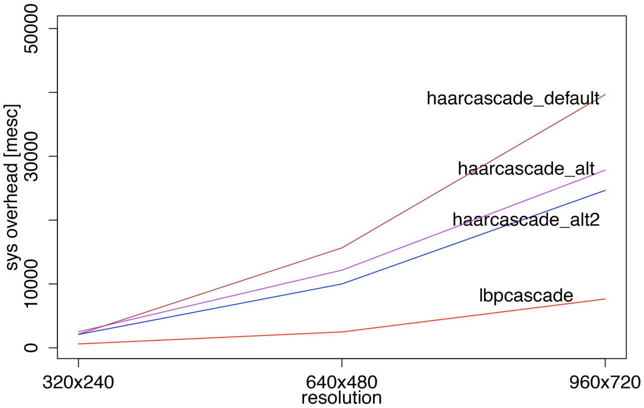

Fig. 5. Cascade Classifier Performance

Castrillón-Santana et al. [9] identified detection rate for different *haar* classifiers in 2008. As it can be seen from [9], among three haar classifiers, haarcascade_alt2 has the highest detection rate. For example, the detection rate for 400 false detections is about around 73%. Fig.5 shows that *haarcascade_alt2* imposes the lowest overhead among three haar classifiers.

As for LBP classifier, Yuan presented result in [23] claiming that there is a 71% detection rate for LBP face detection algorithm based on a YALE face database, which contains 165 gray images for 15 people.

V. Conclusions

This paper presented a policy-based approach that provides controlled and secure data dissemination in untrusted environments in V2V and in V2I communication systems by means of Active Bundles. AB consists of sensitive data, metadata including policies and policy engine, which provides policy enforcement. Policy enforcement mechanism ensures that all the parties involved in communication in V2V and V2I systems can get access only to the data they are authorized for.

Our approach is illustrated on secure dissemination of video data captured by camera installed in a vehicle. Video containing human face(s) is a sensitive data and privacy for those humans appeared in the video can be preserved by specifying policies of AB. After enforcing the policy at a receiver, a video from accessible images is recreated at receiver's site.

Our system is deployed on a credit-card size hardware platform, based on Raspberry Pi board and Pi camera. The implementation in C/C++ is available in the repository [4].

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] *Dr. Dobb's Journal of Software Tools* (2000) Key: citeulike:2236121

[2] Raspberry pi. [Online]. Available: https://www.raspberrypi.org

[3] Raspbian. [Online]. Available: http://www.raspbian.org

[4] Vehicle-to-vehicle source code repository. [Online]. Available: https://chenyangqu@bitbucket.org/chenyangqu/v2v.git

[5] 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.

[6] 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.

[7] 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.

[8] Broadcom2835. [Online]. Available: http://www.farnell.com/datasheets/1521578.pdf

[9] M. Castrillón-Santana, O. Déniz-Suárez, L. Antón-Canalís, and J. Lorenzo-Navarro. "Face and facial feature detection evaluation performance evaluation of public domain haar detectors for face and facial feature detection." (2008).

[10] R. Brunelli and T. Poggio. "Face Recognition through Geometrical Features." *European Conf . on Comp. Vision (ECCV)* 1992, pp.792–800.

[11] R. Ranchal, D. Ulybyshev, P. Angin and B. Bhargava. "PD3: Policy-based Distributed Data Dissemination". *16-th CERIAS Symp.,* Mar. 2015.

[12] Health Insurance Portability and Accountability Act (HIPAA) of Privacy: http://www.hhs.gov/ocr/privacy/HIPAA

[13] Family Educational Rights and Privacy Act (FERPA): http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

[14] 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.

[15] 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. http://evita-project.org/Deliverables/EVITAD2.3.pdf

[16] 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.

[17] 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

[18] L. Othmane, R. Fernando, R. Ranchal, B. Bhargava, E. Bodden. "Likelihoods of Threats to Connected Vehicles." *International Journal of Next-Generation Computing*, Nov. 2014

[19] L. Lilien and B. Bhargava, "A Scheme for Privacy-preserving Data Dissemination," *IEEE Trans. on Systems, Man and Cybernetics, Part A: Systems and Humans*, vol. 36(3), May 2006, pp. 503-506.

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

[21] 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.

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

[23] Yuan, Bao-Hua, Huan Wang, and Ming-Wu Ren. "Face recognition based on completed local binary pattern." *Jisuanji Yingyong Yanjiu* 29, no. 4, 2012: pp. 1557-1559.