

CAMP

Vehicle Safety Communications 3

Mercedes-Benz
Research & Development North America, Inc.



HONDA

Honda R&D Americas

NISSAN

UMTRI



HYUNDAI · KIA MOTORS
Hyundai · Kia America Technical Center, Inc.

VOLKSWAGEN

GROUP OF AMERICA

Intelligent Transportation Systems

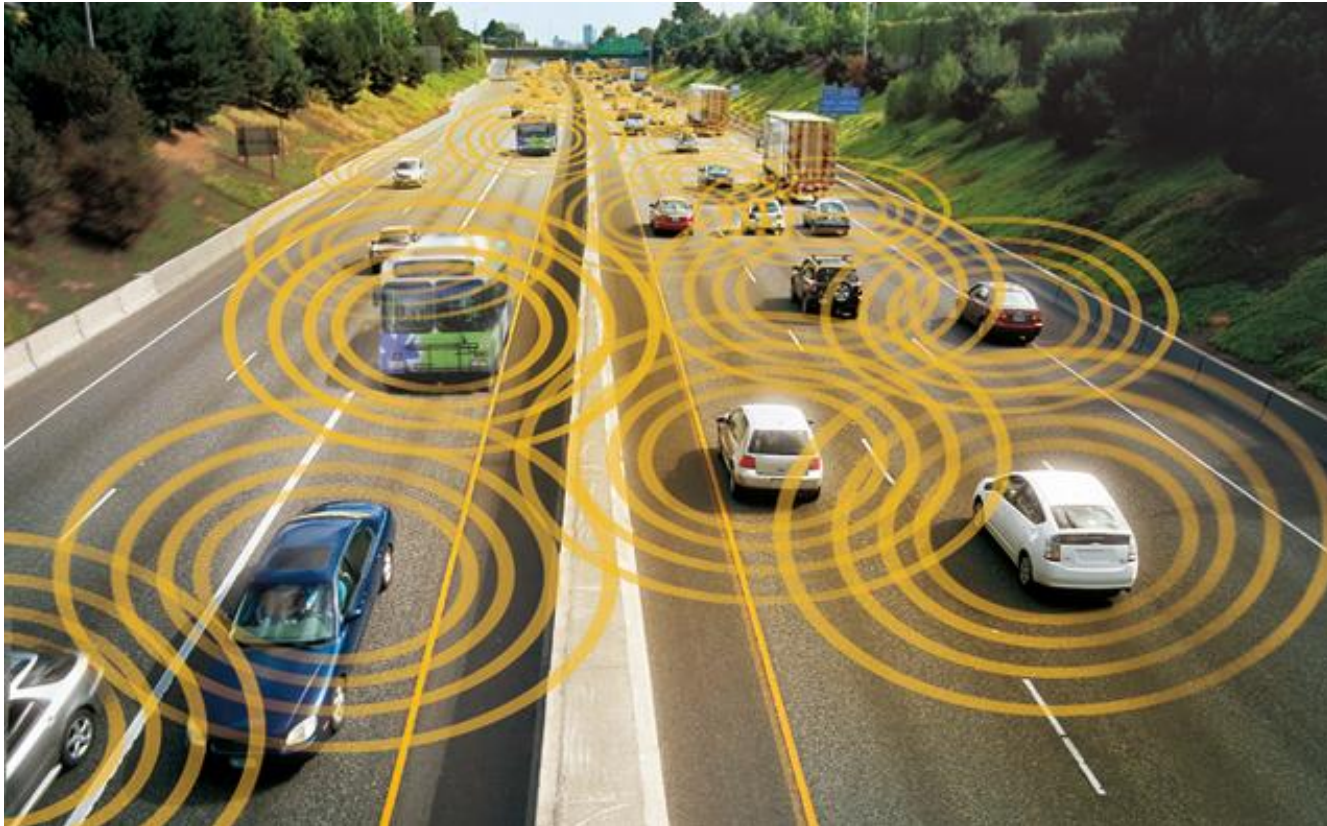
V2V Communication Security: A Privacy Preserving Design for 300 Million Vehicles

André Weimerskirch

Disclaimer

- Much of this work was conducted under Cooperative Agreements with the United States Department of Transportation. However, the opinions, findings, and conclusions in this presentation are those of the authors and not necessarily those of the United States Department of Transportation.
- Much of this work was supported by the Crash Avoidance Metrics Partnership (CAMP) VSC3 project, and in particular by Ford, GM, Honda, Hyundai-Kia, Mercedes-Benz, Nissan, Volkswagen/Audi, and the United States Department of Transportation.

Connected Vehicles – V2X




Introduction

- 32,000 deaths on the road in the US in 2012
- Day-1 applications will likely be:
 - USA: V2V driver notifications safety applications
 - Europe: mobility applications, supported by infrastructure (e.g. temporary highway construction site)
- V2V wireless communications for 360° warning applications.
 - 300+ m range
- Basic Safety Message (BSM)
 - Contains position, velocity, acceleration ...
 - Transmitted up to 10 times per second
- Allows receiving unit to predict collisions and warn driver
 - The U.S. Department of Transportation estimates that V2V technology, if widely deployed, could provide warnings to drivers in as many as 76 percent of potential multi-vehicle collisions, with the level of benefit depending on the extent of deployment and the effectiveness of V2V warnings in eliciting appropriate driver responses

Deployment

- NHTSA, February 3rd 2014: “The U.S. Department of Transportation's (DOT) National Highway Traffic Safety Administration (NHTSA) announced today that it will begin taking steps to enable vehicle-to-vehicle (V2V) communication technology for light vehicles.”
- The security system in this presentation presents the leading candidate for deployment.

Add This  [A](#) [Print](#)

Cadillac to Introduce Advanced 'Intelligent and Connected' Vehicle Technologies on Select 2017 Models

Sun, Sep 7 2014

DETROIT – Cadillac will begin offering advanced “intelligent and connected” vehicle technologies on certain 2017 model year vehicles, General Motors CEO Mary Barra said Sunday during her keynote address at the Intelligent Transport System (ITS) World Congress in Detroit.


In about two years, an all-new 2017 Cadillac vehicle will offer customers an advanced driver assist technology called Super Cruise and in the same timeframe the 2017 Cadillac CTS will be enabled with vehicle-to-vehicle (V2V) communication technology.

“A tide of innovation has invigorated the global auto industry, and we are taking these giant leaps forward to remain a leader of new technology,” Barra said. “We are not doing this for the sake of the technology itself. We’re doing it because it’s what customers around the world want. Through technology and innovation, we will make driving safer.”

Super Cruise, the working name for GM’s automated driving technology, will offer customers a new type of driving experience that includes hands-off lane following, braking and speed control in certain highway driving conditions. The system is designed to increase the comfort of an attentive driver on freeways, both in bumper-to-bumper traffic and on long road trips.

V2V communication technology could mitigate many traffic collisions and improve traffic congestion by sending and receiving basic safety information such as location, speed and direction of travel between vehicles that are approaching each other. It will warn drivers and can supplement active safety features, such as forward collision warning, already available on many production cars.

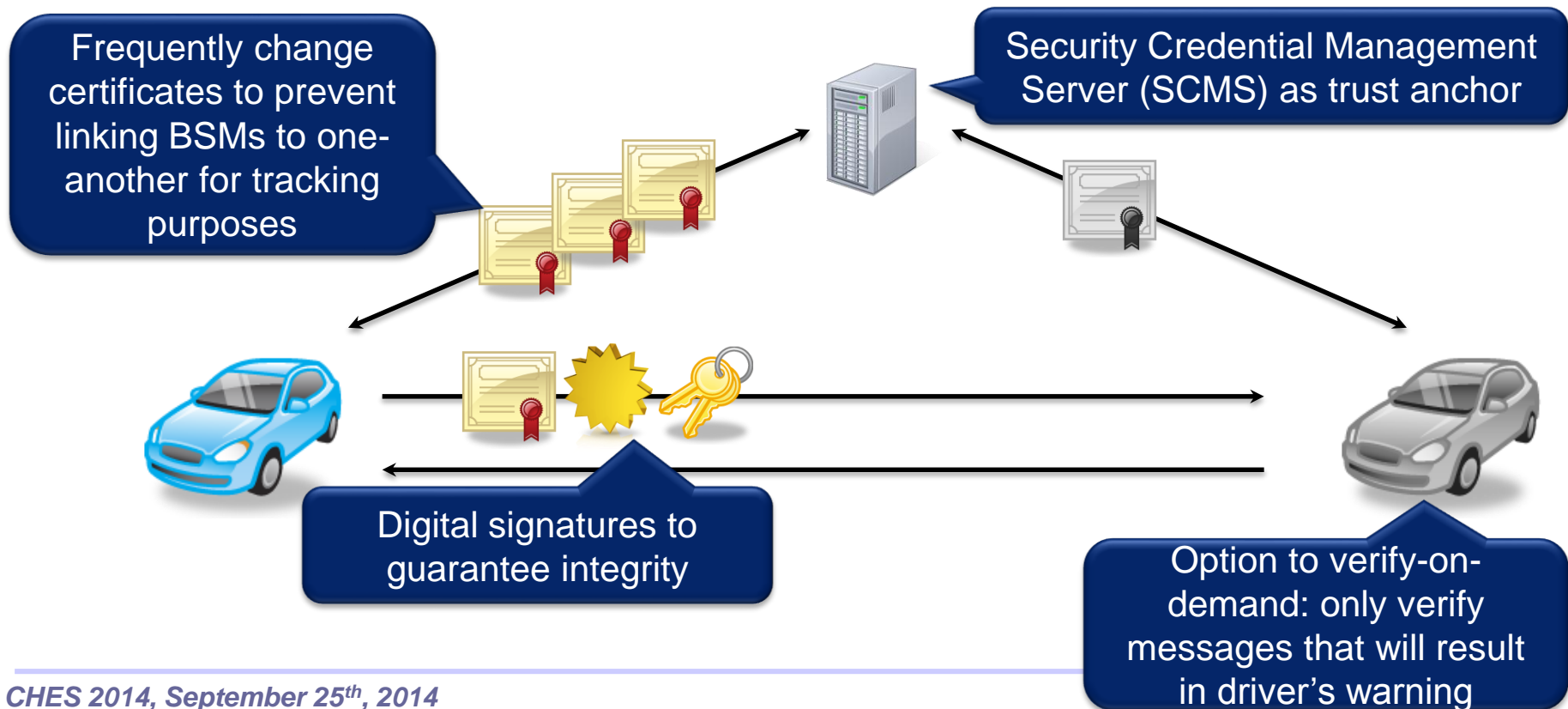
As the world becomes more congested and new populations need access to personal mobility, accidents continue to be a global concern. A recent National Highway Traffic Safety Administration study estimated that the economic and societal impact of motor vehicle crashes in the United States is more than \$870 billion per year.



Security Overview

To enforce security in V2X systems we need to ensure that

- A message originates from a trustworthy and legitimate device
- A message was not modified between sender and receiver
- Misbehaving units are removed from the system



Risk Analysis

- It can be assumed that V2X will be used for driver warnings and notifications only
 - It is reasonable to assume that V2X will only support control applications, i.e., all control applications will use V2X only as an additional sensor on top of radar or camera sensor input.
- Successful attacks do not pose a safety threat
 - However, applications must be designed in a careful manner (known from radar and camera based control applications such as assisted braking)
- Messages may affect choice of route or have other mobility/efficiency impacts (not safety-related)
 - Higher motivation for attack, however, no safety-related risk
- Actual Risk: lack of security will result in a high number of false warnings that will reduce acceptance of V2X significantly and loss of user acceptance

Security Considerations

- Impact on privacy
 - Don't want the system to be used as a tracking system
 - Prevent eavesdroppers or insiders from collecting Personally Identifiable Information (PII)
- Additional attack surface
 - New wireless interface adds another surface to hack into car (similar to Bluetooth, cellular and Wi-Fi).

Design Constraints

- *Data rate using current V2X system*: transmits at 6 Mbps under ideal conditions.
 - Typical data rates usually below theoretic optimum
- *Cost*: limits in car on processing power and storage
- *Life-cycle*: solutions designed today will be deployed in a decade and will then be used for several decades.

Design Constraints (2)

- *Connectivity*: During the early years of deployment, only limited connectivity of the vehicles to Internet available
 - Road-side units at intersections, gas stations, dealerships, etc., that allow communication for a few seconds while vehicle drives by
 - Embedded modems installed in a few cars that allow regular communication with these cars and use them as seed for epidemic spreading of data (e.g. distribution of CRLs)

V2V MESSAGE AUTHENTICATION

Acknowledgement: Many of these concepts have been developed by the CAMP VSC-A Team, the CAMP VSC3 VSCS Team, and the IEEE 1609.2 group.

V2V Authentication

- Messages are signed
 - ECDSA-256 with NISTp256 curve
- Signed messages include time and location
 - Signer adds time and location before signature
 - Allows to detect relay and replay attacks
- Optionally verify messages on demand: only verify messages that will result in a driver's warning
 - E.g. do not verify message that was broadcast from a vehicle that is 300m away

Protect Privacy

- No personal information included in broadcast messages
- Prevent tracking: “Identifiers” at application, network and other levels should be transient and change simultaneously
 - Vehicles are provisioned with three years’ worth of certs
- Vehicles have k simultaneously valid BSM certificates,
 - Dynamically choose which certificate to use to sign (e.g. rotate every 5 minutes). More research required to determine proper change strategies.
 - Baseline number of certs $k = 20$ per week (but car makers can choose to use more certificates per week)
 - For three years’ worth of certificates, at least 3,120 certificates are loaded at Day-1.
- Further approaches available, such as mix-zones
 - Vehicles change certificates in a coordinated way (e.g. at an intersection)
 - However, mix-zones seem to interfere with the idea of safety systems

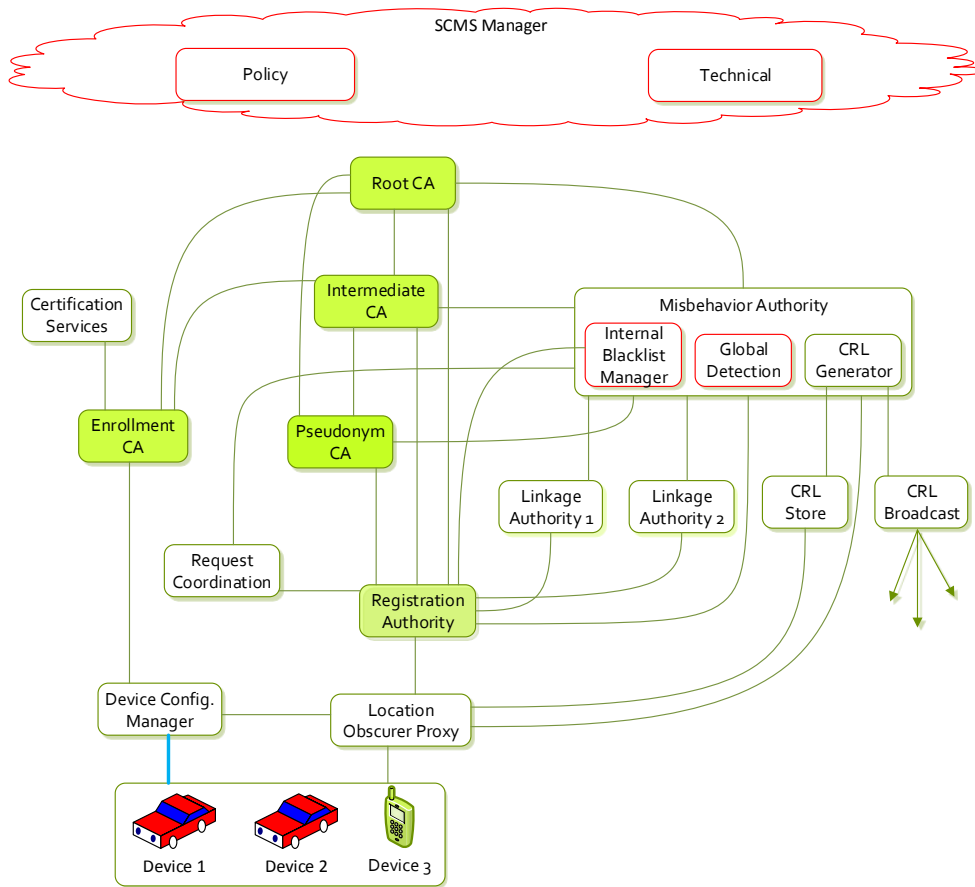
Implicit Certificates

- Messages are signed using ECDSA over the NISTp256 curve with ECQV certificates
- “Implicit” certificates replace signature with public key reconstruction value
- Save 64 bytes per certificate
- Speed up the first verification of a certificate chain

SECURITY CREDENTIAL MANAGEMENT SYSTEM (SCMS)

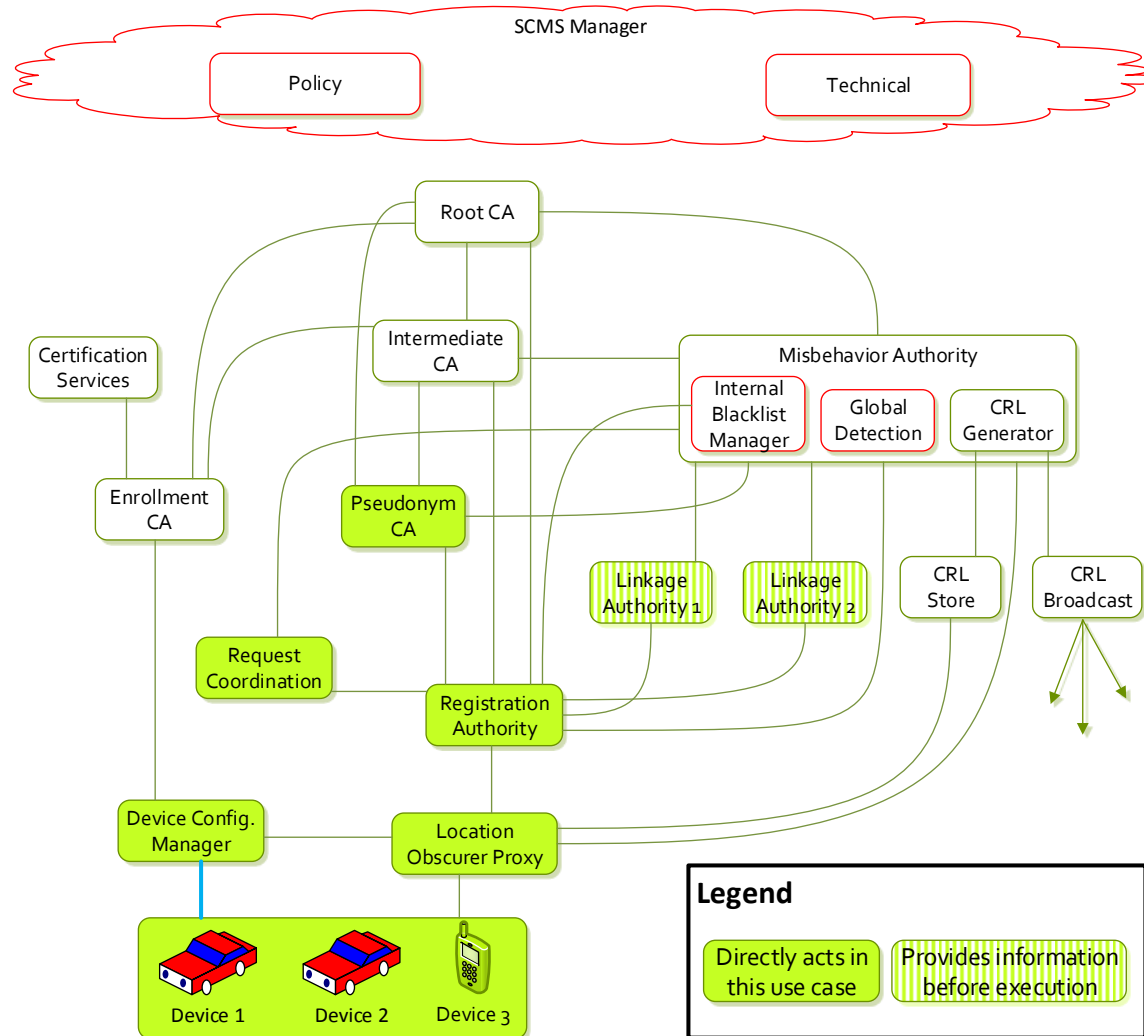
Acknowledgement: These concepts have been developed by the
CAMP VSC3 VSCS Team.

SCMS Overview



- Privacy against insiders and outsiders
 - **Separation of SCMS duties and information: a single SCMS component cannot link any two certificates to same device (no tracking)**
 - No information stored within SCMS that links certificates to a particular device, vehicle or owner
 - Registration Authority (RA) shuffles all requests from device
 - Location Obscure Proxy (LOP) acts as anonymizer proxy
- Butterfly keys to minimize effort of device
- Efficient privacy-preserving revocation

Certificate Provisioning



Shift Effort from Device to Server: Butterfly Keys

- Generating a lot of keys for requests is a burden at the OBE side
 - It might not need all of them
 - It needs to store the private keys
 - Increases request size and risk that request doesn't make it through the network
- Device generates a private/public seed value and expansion function
- Server expands public seed to create many public keys (without knowing the corresponding private keys)
- Server does most of the work, but only device knows the private keys

Butterfly Keys

- Device:
 - Generates signing keypair: a , $A = aG$ and encryption keypair: h , $H = hG$
 - Creates expansion functions $f_s(i)$, $f_e(i)$
- RA:
 - Generates signing public value $B_i = A + f_s(i) G$ and encryption public key $L_i = H + f_e(i) G$
- PCA:
 - Creates signing public key $C_i = B_i + c_i G$ for random c_i (so that RA cannot learn final public key)
 - Issues $\langle C_i \rangle$, the cert containing C_i ,
 - Encrypts $(\langle C_i \rangle, c_i)$ with L_i to Device
 - Signs encrypted value (to avoid MitM attack by RA)
- Device, and only Device, knows private key of C_i : $a + f_s(i) + c_i$
- OBE and only OBE knows private decryption key (similar argument)
- RA does not know certificate's public key and cannot link certificates

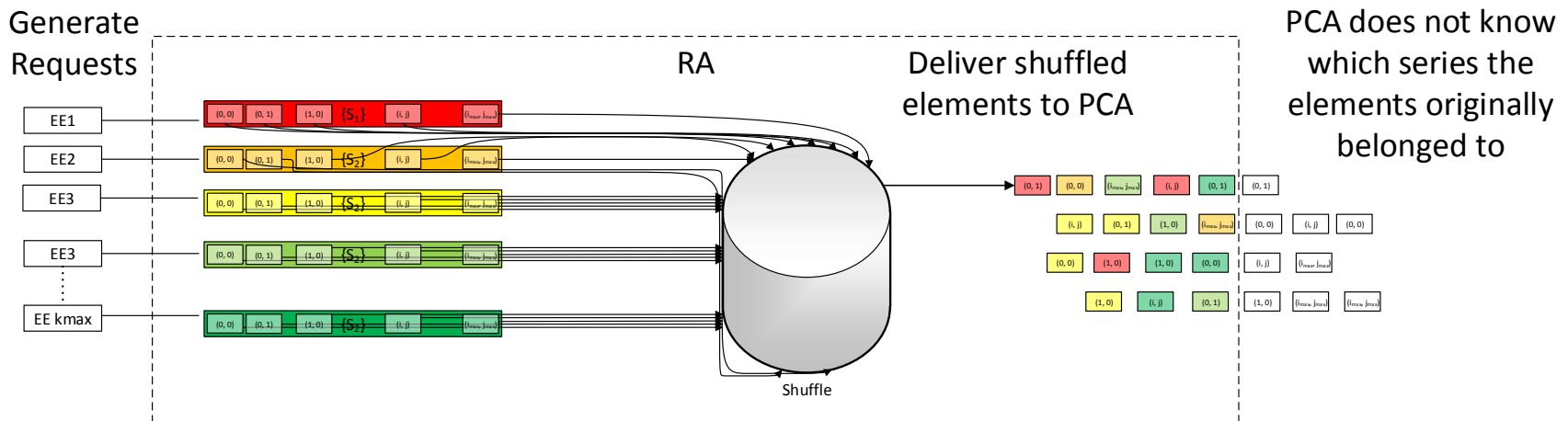
only known to OBE

in encrypted response

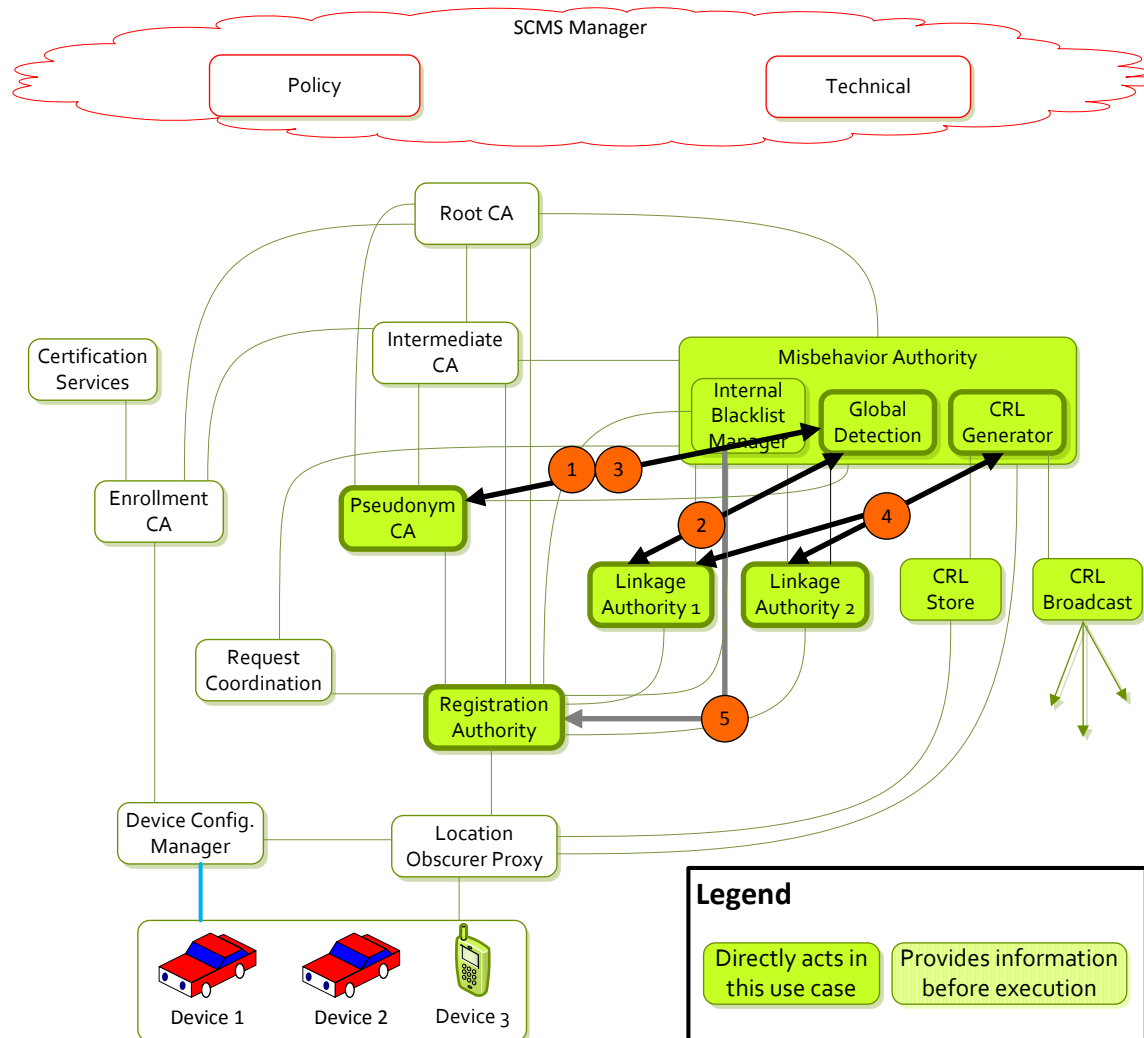
OBE knows f , can calculate this

Privacy against Insider: Shuffle at the RA

- RA receives requests from multiple end-entity devices/vehicles
- RA shuffles requests and delivers shuffled elements to PCA. PCA doesn't know to which device the request belongs.
- RA combines responses from PCA and forwards to proper device. PCA encrypts the response so that RA cannot learn certificate content.



Revocation



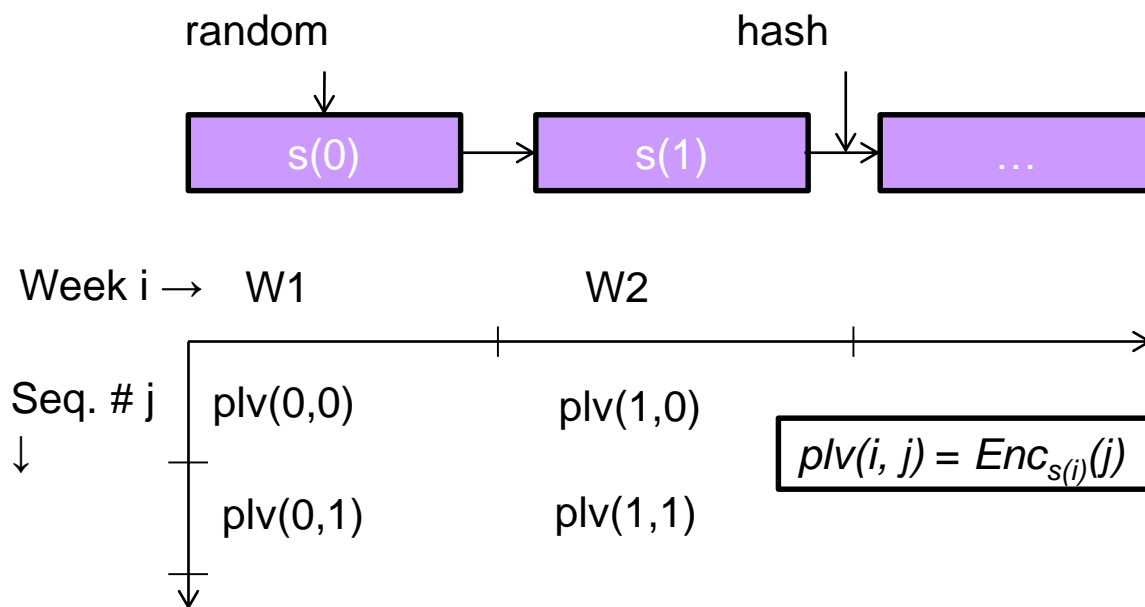
Revocation

- Two ways of revocation
 - Publish certificate revocation lists (CRL) to devices
 - Deny renewal of certificates
- Vehicles need to be provisioned with a minimum number of certs in case they are turned off for some time and turned on in an area with no coverage
 - If you have, say, a month's worth of certs, you can misbehave for a month
- Revocation by CRL must be supported to reduce potential disruption within system
- Revocation by denying renewal of certificates will be implemented on top
- Need efficient, privacy-preserving revocation

Efficient Revocation: Linkage Values

- Remember: each device holds 20 certificates per week, more than 1,000 certificates per year
- Revoke all n of a device's certificates with just one entry on the CRL
- Backwards unlinkability
 - If a device is revoked, its privacy for past events is still protected
- After revocation, privacy cannot be protected

Linkage Values



- Create one hash chain value $s(i)$ per week
- Encrypt values $j=1$ to 20 with hash chain values as key to obtain pre-linkage values:
 $plv(i,j) = Enc_{s(i)}(j)$
- Embed i and plv in certificate (i is a global unit)
- To revoke, publish current week's hash chain value $s(i)$
- Backward privacy is preserved

Linkage Values: Avoid Inside Attacks

- *Problem:* if a single entity calculates the linkage values, then this entity can link certificates.
 - Introduce Linkage Authorities LA_1 and LA_2
- LA_1 calculates pvl_1 and encrypts for PCA
- LA_2 calculates pvl_2 and encrypts for PCA
- PCA calculates $lv = pvl_1 \text{ XOR } pvl_2$

How to Revoke an OBE

- Reporter provides misbehavior report with certificate of suspicious device
 - Known: certificate with linkage value
 - PCA knows certificates that were issued. It looks up an identifier and provides identifier to RA and LAs
 - RA can link identifier to device's credentials
 - RA includes device's credentials in blacklist and will deny any further requests
 - LAs can link identifier to used hash chain value.
 - SCMS will add hash chain values to CRL
- All entities have to collaborate!

Group Revocation

- Use a mechanism similar to the above but with a public “salt” value
- Revoke all n of a device’s certs with just one entry on the CRL
- Backwards unlinkability
- Group membership is secret until revocation

What Else Was Considered?

- Group signatures for V2V message authentication
 - Large signature size (channel congestion)
 - Not standardized
 - Problematic revocation
- Group signatures for Device-SCMS requests
 - Additional program code in vehicle
 - Non-standardized

What Else Was Considered? (2)

- Blind signatures so that SCMS does not know certificate
 - High complexity and high over-the-air bandwidth requirements
 - Not standardized

SAFETY PILOT MODEL DEPLOYMENT

Acknowledgement: The underlying security design has been developed by the CAMP VSC3 VSCS Team. Safety Pilot Model Deployment has been conducted by UMTRI.

Safety Pilot Model Deployment

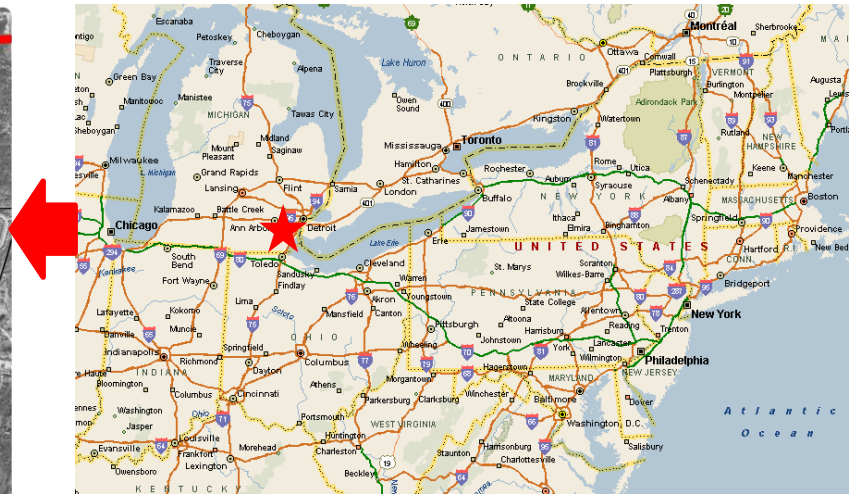
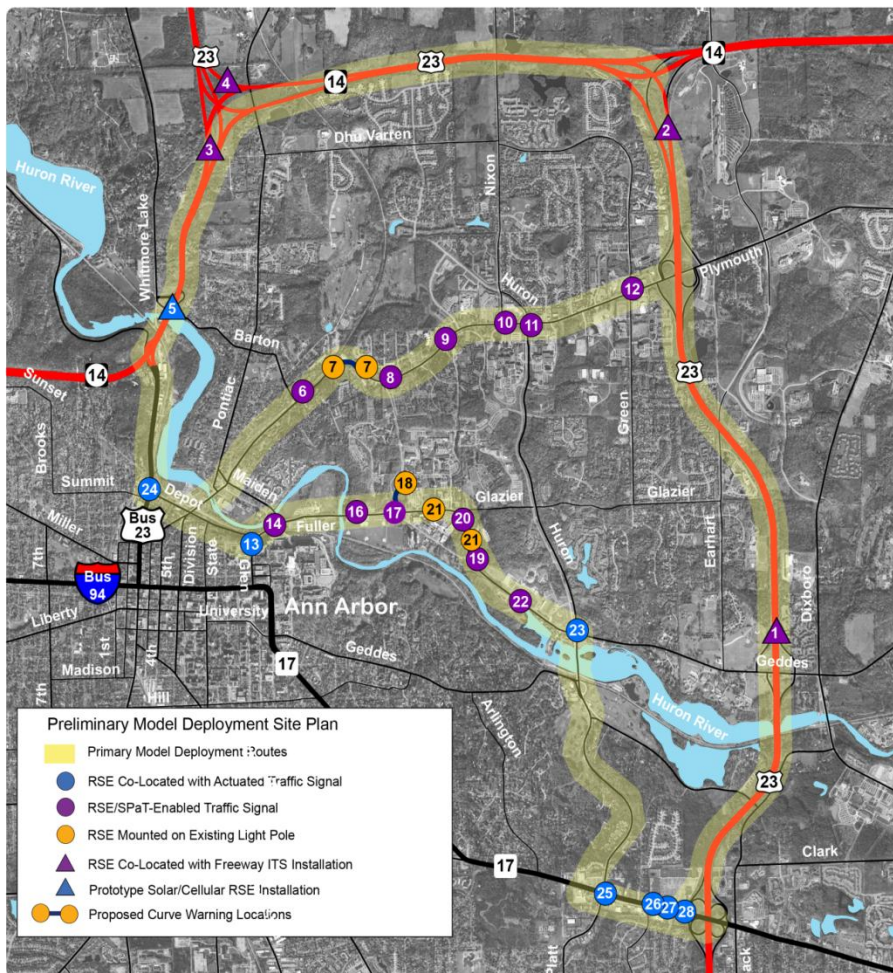


- Conducted by UMTRI
- 2,836 vehicles equipped with DSRC wireless communication devices in a concentrated geographic area (Ann Arbor)
- August 2012 – February 2014
- One year deployment period.
- Equipped roadside units.



Model Deployment Geographic Area

- Ann Arbor, Michigan



Vehicle Platform Types

Function	Integrated Systems	Retrofit / Aftermarket Devices	Vehicle Awareness Devices
Broadcasts to others	Yes	Yes	Yes
Receives broadcasts, Issues Alerts to Drivers	Yes	Yes	No
Integrated with vehicle data bus & systems; OEM interface	Yes	No	No
Vehicles in Test	67	319	2450
Source of Vehicles	Recruited drivers, USDOT-CAMP vehicles from 8 OEMs	Recruited drivers & vehicles Cars, trucks, buses	Recruited vehicles. Cars, trucks, buses, fleets.
Data Logging	Full FOT-style data acq system (DAS)	Some FOT DAS, some device logs	Device log files

Security

- 1st version of Security Credential Management Server designed in 2011 was deployed in Model Deployment, operated under a separate USDOT contract.
- 105,000 certificates per year per on-board unit (i.e., almost 300 million certificates per year were issued)
- Certificates were either loaded manually or they were updated over-the-air during road-side unit drive-by.
- Security was deployed for V2V basic safety messages and for road-side unit applications (e.g. Signal Phase and Timing broadcast messages that announce when a traffic light will turn red).
- Note: the previously presented security design is a refined version

AUTOMOTIVE SECURITY

Secure Wireless Interface

- Recent research results from various parties suggest that data security in vehicle becomes safety issue
 - Successful penetration via Bluetooth and cellular connections
- DSRC would be a standardized wireless interface
- DSRC is a safety system and requires communication with powertrain systems by design
- DSRC interface of cars must be carefully protected

Trojan-Horse MP3s Could Let Hackers Break Into Your Car Remotely, Researchers Find

By Rebecca Boyle Posted 03.14.2011 at 4:57 pm 15 Comments



Dashboard Karl Frankowski via Flickr

Last year we told you how hackers could someday [infiltrate your car's control systems](#) and install malware to take things over, as long as they had some computer skills and a laptop. Now car-hacking researchers have [done it remotely](#), using innocent tech like Bluetooth devices and even a CD.

Researchers at the University of California, San Diego, and the University of Washington are researching vulnerabilities in electronic vehicle controls, trying to warn automakers about potential security holes. Many new cars have Bluetooth wireless technology and built-in connections for cell phones and other devices, and those connections [could be exploited](#). In one example, the researchers called the car's cellular connection and uploaded malicious code using an audio file. In another test, they found out how to pair the car to a Bluetooth-enabled device, which they used to execute code.

DEVICE SECURITY

Acknowledgement: The device's security requirements have been developed by the CAMP VSC3 VSCS Team.

Secure Processing Platform

- Secure hardware
 - Message signature generation and handling of private keys only in secure hardware
 - Store certificates only encrypted and only decrypt within secure hardware
- Sending
 - Digitally sign 10 messages per second

Secure Processing Platform (2)

- Receiving
 - Digitally verify messages as required: Verify-on-Demand. Actual numbers depend on supported applications.
- Should sensor input (e.g. GPS, speed, etc.) be protected?
 - Depends on applications

Conclusions

- The US DOT announced they are moving forward with a V2V communication regulation
- The presented design is the leading candidate for deployment in the US. This will be a security system for 300 million vehicles.
- Privacy against inside and outside attackers was included in the design.
- Feedback about design highly welcome! More details available in

William Whyte, André Weimerskirch, Virendra Kumar, and Thorsten Hehn, “A Security Credential Management System for V2V Communications”, 2013 IEEE Vehicular Networking Conference (VNC 2013)

Remaining Research

- Epidemic distribution of CRLs
- Misbehavior detection algorithms (both local algorithms running in vehicle and global algorithm running in backend)
- Secure in-vehicle implementations
- Privacy models to determine proper certificate change strategies

Contact

André Weimerskirch

[Email: andrewmk@umich.edu](mailto:andrewmk@umich.edu)

APPENDIX

Standards and Projects

- V2V and V2I is specified in IEEE 1609.2
 - Latest version is from April 26th, 2013 (IEEE Std. 1609.2 – 2013)
 - 1609.2 will be further developed
- V2V security credential management
 - Specification of first version available at <http://www.priorartdatabase.com/pubView/IPCOM000210877D> (September 14th, 2011)
 - Version of 2011 was deployed in Safety Pilot Model Deployment: <http://safetypilot.umtri.umich.edu>
 - Refined design, shown in this presentation, was published at IEEE VNC 2013: W. Whyte, A. Weimerskirch, V. Kumar, T. Hehn, “A Security Credential Management System for V2V Communications“
 - The European design was published at ITS World Congress 2011: N. Bißmeyer, H. Stübbing, E. Schoch, S. Götz, J.P. Stolz, B. Lonc, „A generic public key infrastructure for securing Car-to-X communication“.

References

- [BHW09] Levente Buttyán, Tamás Holczer, André Weimerskirch, and William Whyte, “SLOW: A Practical Pseudonym Changing Scheme for Location Privacy in VANETs”, First IEEE Vehicular Networking Conference 2009 (IEEE VNC 2009), October 28-30, 2009, Tokyo, Japan
- [EVITA] <http://www.evita-project.org>
- [GVG09] Mainak Ghosh, Anitha Varghese, Arobinda Gupta, Arzad Kherani and Skanda Muthaiah, “*Misbehavior Detection with Integrated Root Cause Detection in VANETs*,” 6th ACM International Workshop on Vehicular Internetworking (in conjunction with ACM Mobicom), VANET 2009
- [HHL09] Jason J. Haas, Yih-Chun Hu, and Kenneth P. Laberteaux. Design and Analysis of a Lightweight Certificate Revocation Mechanism for VANET. *Proceedings of the Sixth ACM International Workshop on Vehicular Ad Hoc Networks*(VANET 2009). ACM, Beijing, China, September 2009, pp. 89-98.
- [HL06] Yih-Chun Hu and Kenneth P. Laberteaux. Strong VANET Security on a Budget. *Proceedings of the 4th Annual Conference on Embedded Security in Cars* (escar 2006). is-its, Berlin, Germany, November 2006.
- [KSD10] Tiffany Hyun-Jin Kim, Ahren Studer, Rituik Dubey, Xin Zhang, Adrian Perrig, Fan Bai, Bhargav Bellur, and Aravind Iyer, “VANET Alert Endorsement Using Multi-Source Filters”, In Proceedings of the Seventh ACM International Workshop on Vehicular Ad Hoc Networks (VANET’10), 2010
- [KSWL08] Frank Kargl, Elmar Schoch, Björn Wiedersheim, and Tim Leinmüller, “Secure and Efficient Beaconing for Vehicular Networks”, 5th ACM International Workshop on Vehicular Ad Hoc Networks (VANET 2008), 2008.
- [KW11] Krishnan, H. and Weimerskirch, A., “Verify-on-Demand” - A Practical and Scalable Approach for Broadcast Authentication in Vehicle-to-Vehicle Communication, SAE Technical Paper, 2011, doi:10.4271/2011-01-0584
- [LHH08] Kenneth P. Laberteaux, Jason J. Haas, and Yih-Chun Hu. Security Certificate Revocation List Distribution for VANET. Proceedings of the Fifth ACM International Workshop on Vehicular Inter-NETworking (VANET 2008). ACM, San Francisco, CA, September 2008, pp. 88-89.
- [OVERSEE] <http://www.oversee-project.org>
- [SKMW10] F. Schaub, F. Kargl, Z. Ma, and M. Weber, V-tokens for Conditional Pseudonymity in VANETs, IEEE Wireless Communications & Networking Conference (IEEE WCNC 2010), 2010.
- [SSBP09] A. Studer, E. Shi, F. Bai, and A. Perrig, “TACKing Together Efficient Authentication, Revocation, and Privacy in VANETs”, in Proceedings of the 6th Annual IEEE Communications Society Conference on Sensor, Mesh, and Ad Hoc Communications and Networks (SECON), 2009
- [VSCA] CAMP VSC-A Technical Reports, available at <http://www.nhtsa.gov/Research/Crash+Avoidance/ci.Office+of+Crash+Avoidance+Research+Technical+Publications.print>