A Security Credential Management System for Vehicle-to-Vehicle Communications

William Whyte (Security Innovation);
André Weimerskirch (University of Michigan Transportation Research Institute);
Virendra Kumar (Security Innovation); Thorsten Hehn (Volkswagen of America)

(This material has been presented at IEEE VNC 2013)
BACKGROUND
Background

• 32,000 deaths on the road in the US in 2012
• Significant reduction may be possible from V2V wireless communications for 360° warning applications.
  • 300 m range, 802.11-derived medium access
  • Basic Safety Message (BSM)
    • Contains location, velocity, steering angle…
    • Transmitted up to 10x second
• Allows receiving unit to predict collisions and warn driver
  • “Prevent 80% of unimpaired 2-vehicle accidents”
Basic Safety Message

• Spectrum reserved for these communications since 1999
  • Standards under development since 2003 selection of 802.11p MAC
  • Field trials in Michigan, scalability analysis, driver acceptance clinics
• USDOT (NHTSA) currently considering mandating this system for inclusion in new light vehicles
  • System benefit = \( p^2 \) where \( p \) is fraction of equipped vehicles, want \( p \) as large as possible
  • Decision on mandate to be made 2014
  • Everything in this presentation is in that context – this is the leading candidate for deployment, please review it!
Security considerations

• Risk of false messages
  • Reduce users’ faith in system and cause warnings to be ignored
  • (not safety-related): Messages may affect choice of route or have other mobility/efficiency impacts
  • Requirement: must be able to detect untrustworthy senders or messages and let receivers know not to trust them

• Impact on privacy
  • Don’t want the system to be used as a tracking system
    • Tracking is always possible, don’t want this option to be the cheapest
  • Prevent eavesdroppers or insiders from collecting Personally Identifiable Information (PII)
  • Conflict with requirement to detect and remove untrustworthy senders
System considerations

• Design constraints
  • Constraints on available data rate using current V2V system (6 MBps under ideal conditions)
  • Cost-sensitive suppliers: limits on processing power, storage, connectivity, number of 5.9 GHz radios, …
Authentication

- Messages are signed
  - Signed using ECDSA over the NISTp256 curve – bandwidth
  - Vehicles are provisioned with three years’ worth of certs
- No requirement to verify all messages
- Message signing certificate specifies permissions (not identity) of holder
- Misbehaving units can have their certificates identified and revoked
  - … while preserving privacy as much as possible, see later
- Use different certs for different types of operation
  - Security management, application A, application B
Protect privacy

- No personal information included in broadcast messages
- Prevent tracking: “Identifiers” at application, network and other levels should be transient
  - Attack model: Eavesdropper can record some but not all messages
- Vehicles have k simultaneously valid BSM certificates,
  - Dynamically choose which certificate to use to sign
  - Baseline number of certs = 20 per week
  - When cert changes, all other identifiers change too
- SCMS is split into a number of components
  - No individual component knows the full set of certificates that belong to a single device
  - Attack model: Eavesdropper can record some but not all messages and access database at a single SCMS component
- Policy means also possible
  - Out of scope for this presentation (and CAMP)
  - Vehicle Infrastructure Integration Consortium (VIIC) coordinates policy responses from OEMs
ARCHITECTURE
Overview / Standard PKI Hierarchy
Lifecycle
Features

- Implicit certificates
- Ability to change service providers per component
- Privacy against insiders when provisioning
  - RA shuffle
- Certificate request: Butterfly keys
- Efficient privacy-preserving revocation: Linkage authorities and linkage values
Implicit certificates

- Signed using ECDSA over the NISTp256 curve with ECQV certs
- “Implicit” certs – replace signature with public key reconstruction value
- Save 64 bytes per certificate
- Speed up the first verification of a certificate chain
Certificate Provisioning

SCMS Manager

Policy

Technical

Root CA

Intermediate CA

Pseudonym CA

Request Coordination

Registration Authority

Device Config. Manager

Location Obscurer Proxy

Certification Services

Enrollment CA

Device 1

Device 2

Device 3

Legend

Directly acts in this use case

Provides information before execution

Misbehavior Authority

Internal Blacklist Manager

Global Detection

CRL Generator

CRL Store

CRL Broadcast

Device Config. Manager

Location Obscurer Proxy

Legend

Directly acts in this use case

Provides information before execution
Shuffle at the RA

- RA receives requests from multiple end-entity devices
- Combines requests so that PCA doesn’t know that two individual cert requests received at the same time come from the same vehicle

`RA
EE1
EE2
EE3
EE kmax
{S1}(0, 0) (0, 1) (1, 0) (i, j) (ima x, jma x)
{S2}(0, 0) (0, 1) (1, 0) (i, j) (ima x, jma x)
Deliver shuffled elements to PCA
PCA does not know which series the elements originally belonged to
EE3`
Butterfly keys

• Generating a lot of keys for requests is a pain at the OBE side
  • It mightn’t 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
  • Can we do better?
• Yes, with seed key + expansion functions
  • ECC: \((a+b)G = aG + bG\)
Butterfly keys

- Device generates
  - A seed or “caterpillar” keypair
  - An expansion function
  - Cost: ~1 key generation
  - Expansion function:
    - $f(i,j) = \text{AES}_k(i,j) || \text{AES}_k(i.j \ XOR \ 1^{128})$
    - Publish expansion function by publishing $k$
Butterfly keys: concept

- Device generates
  - A seed or “caterpillar” keypair
  - An expansion function
  - Cost: ~1 key generation
- RA runs the expansion function to generate “cocoon” public keys from the caterpillar public key
  - Cocoon public keys from the same caterpillar keys are not correlated
  - Expansion function lets you generate arbitrarily many cocoon keys
  - RA submits cocoon keys to CA for certification
- Private key $b_{i,j} = a + f(i,j)$
- Public key $B_{i,j} = A + f(l,j) G$
Butterfly keys: concept

- Device generates
  - A seed or “caterpillar” keypair
  - An expansion function
  - Cost: ~1 key generation
- RA runs the expansion function to generate “cocoon” public keys from the caterpillar public key
  - Cocoon public keys from the same caterpillar keys are not correlated
  - Expansion function lets you generate arbitrarily many cocoon keys
  - RA submits cocoon keys to CA for certification
- CA randomizes each public key separately so the RA can’t recognize them
  - Certs contain the resulting “butterfly” keys
  - CA returns certs and private randomization values to the OBE
  - Private key = $a + f(i,j) + c$
  - Public key = $A + f(l,j) \cdot G + C$
Butterfly keys: summary

- Large number of certs generated from a single initial keypair
- OBE is the only device that knows private keys
- Public keys cannot be correlated by any entity
- Low computational burden on OBE at request time
- Request once, generate keys for the entire lifetime of the vehicle
Revocation and Linkage Authorities

- Why do we need revocation?
  - Why not just choose not to issue new certs to a misbehaving vehicle?
- Not all vehicles will have good data connection
  - Even vehicles that do may be out of coverage
  - 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 a month’s worth of certs, you can misbehave for a month
  - If you have three months’ worth of certs, you can misbehave for three months
  - If you have three years’ worth of certs…
- Revocation must be supported to reduce potential disruption within system, even if in practice it isn’t used.
- Need efficient, privacy-preserving revocation
Revocation and Linkage Authorities

- Revoke all $n$ of a device’s certs with just one entry on the CRL
- Multiple certs valid in one time period
- Backwards unlinkability
- No component in the SCMS knows the chain
Revocation and Linkage Authorities

- Revoke all $n$ of a device’s certs with just one entry on the CRL
  - Include linkage value $l(i) = E_k(i)$ in the cert
  - Include key $k$ on CRL; in each time period $i$, vehicles calculate $E_k(i)$ for all entries and compare to the linkage value in the cert.
Revocation and Linkage Authorities

- Revoke all $n$ of a device’s certs with just one entry on the CRL
- Multiple certs valid in one time period
Revocation and Linkage Authorities

- Revoke all $n$ of a device’s certs with just one entry on the CRL
- Multiple certs valid in one time period
Revocation and Linkage Authorities

- Revoke all $n$ of a device’s certs with just one entry on the CRL
- Multiple certs valid in one time period
- Backwards unlinkability
Revocation and Linkage Authorities

- Revoke all $n$ of a device’s certs with just one entry on the CRL
- Multiple certs valid in one time period
- Backwards unlinkability
Revocation and Linkage Authorities

- Revoke all $n$ of a device’s certs with just one entry on the CRL
- Multiple certs valid in one time period
- Backwards unlinkability
- No component in the SCMS knows the chain
Revocation and Linkage Authorities

- Revoke all $n$ of a device’s certs with just one entry on the CRL
- Multiple certs valid in one time period
- Backwardsunlinkability
- No component in the SCMS knows the chain
- LAs encrypt chain for PCA
  - Send to RA
  - RA groups, shuffles
  - PCA decrypts, XORs
Revocation

Legend
- Directly acts in this use case
- Provides information before execution

Device Config. Manager
Location Obscurer Proxy
Certification Services
Enrollment CA
Request Coordination
Root CA
Intermediate CA
Pseudonym CA
Registration Authority
Linkage Authority 1
Linkage Authority 2
CRL Store
CRL Generator
Global Detection
Internal Blacklist Manager
Misbehavior Authority
CRL Broadcast
Intermediate CA 1
Intermediate CA 2
Device 1
Device 2
Device 3

Policy
Technical

SCMS Manager
Real World Crypto

- Is the overall design good?
  - Butterfly keys?
  - Linkage authorities?
- Are we making the right tradeoffs?
  - Privacy / security / complexity
- Subjects of ongoing projects:
  - Misbehavior detection
  - CRL distribution
  - Organizational structure and relationship to USDOT
- WANTED IN THE NEXT TEN YEARS: Post-quantum signature scheme with short signatures
Questions?

- wwhyte@securityinnovation.com
- Thorsten.Hehn@vw.com
- andrewmk@umich.edu

- http://www.ieee-vnc.org/program.html