Privacy-Enhanced Capabilities for VANETs using Direct Anonymous Attestation

Jorden Whitefield Liqun Chen *Thanassis Giannetsos*
Steve Schneider *Helen Treharne*

IEEE VNC, 28th November 2017

Surrey Centre for Cyber Security
Department of Computer Science
University of Surrey
`sccs.surrey.ac.uk`

Outline

- Security & Privacy challenges of Intelligent Transportation Systems
- Trusted Computing for Automotive
- Application of DAA within VANETs
- Future Research

ITS Security & Privacy Challenges

Contradictory positions between users and infrastructure entities...

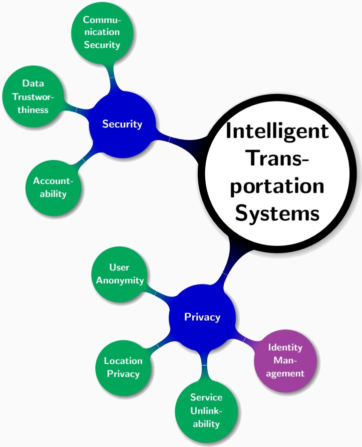
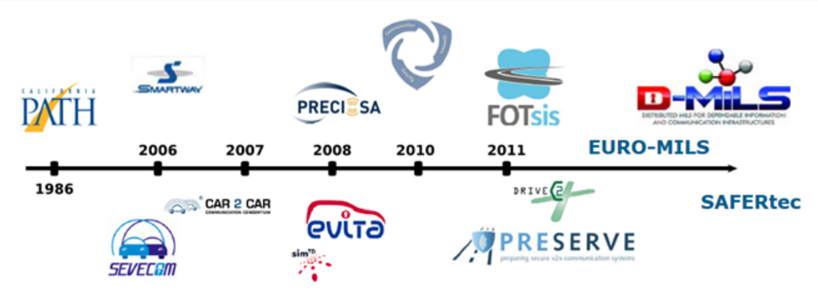


Image source: "Trustworthy People-Centric Sensing: Privacy, Security and User Incentives Road-Map"

- Protect the Users from the System (i.e., user privacy)
  - ⇒ Anonymity (conditional)
  - ⇒ Pseudonymity
  - ⇒ Unlinkability
  - ⇒ Unobservability
- Protect the System from the Users (i.e., trustworthiness)
  - ⇒ Authentication & Authorization
  - ⇒ Accountability
  - ⇒ Data Trustworthiness

- Many standardization bodies
  - ✓ Car 2 Car Communication Consortium (C2C-CC)
  - ✓ IEEE & ETSI standard specifications



But safety is the key pillar

- Vehicular Communications (VC)
- Vehicles propagate information for Safe-Driving
  - Location, Velocity, angle
  - Hazardous warnings
  - Emergency break etc.
- Cooperative awareness through beaconed status messages and event-triggered warnings
- . . . Security in VC?
  - Assure legitimate vehicles propagate information
  - Secure integrity of information

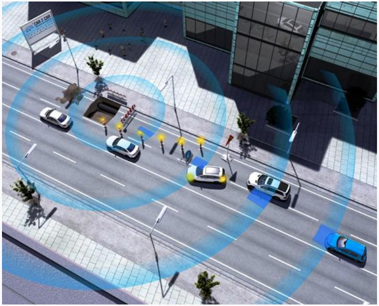


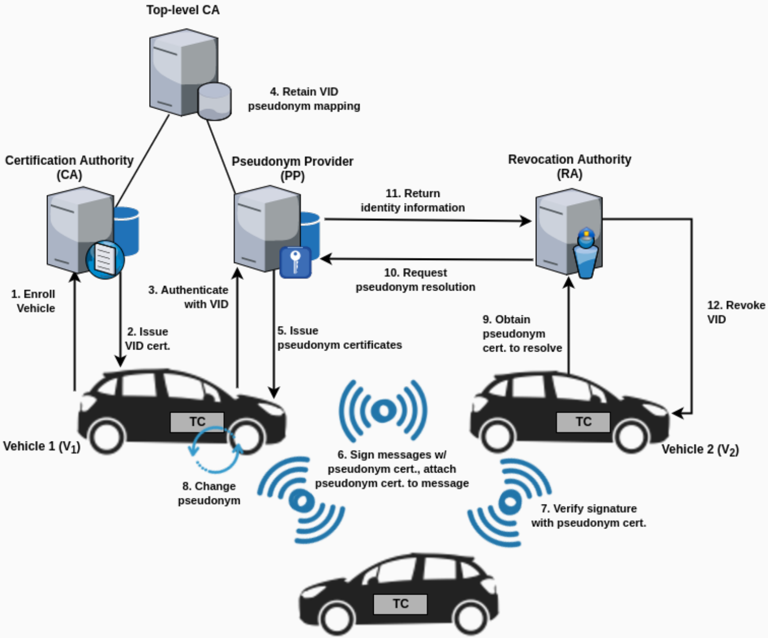
Image source: Car-2-Car Consortium

The Challenge

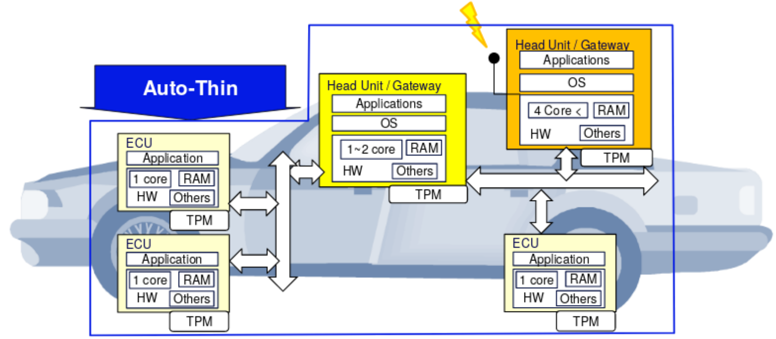
Deploy an ITS with security & privacy built-in, which is scalable providing vehicles with

- Protection from **trusted** & **colluding** third parties
- **Privacy** and **unlinkability**, while still being held **accountable**
- Scalable and dependable **authentication, authorization** & **revocation**
- Solutions that abide by the **VC standards**

State-of-the-art VPKI



Trusted Computing for Automotive



- Trusted Platform Module (TPM) provides:
  - ⇒ Isolation
  - ⇒ Protected Execution
  - ⇒ Shielded Storage
- Secure crypto processor: creates, stores, uses crypto keys
- TCG developing TPM for "Automotive Thin Profile"[1]

[1] https://trustedcomputinggroup.org/wp-content/uploads/TCG-TPM-2.0-Automotive-Thin-Profile_v1.0.pdf

Direct Anonymous Attestation

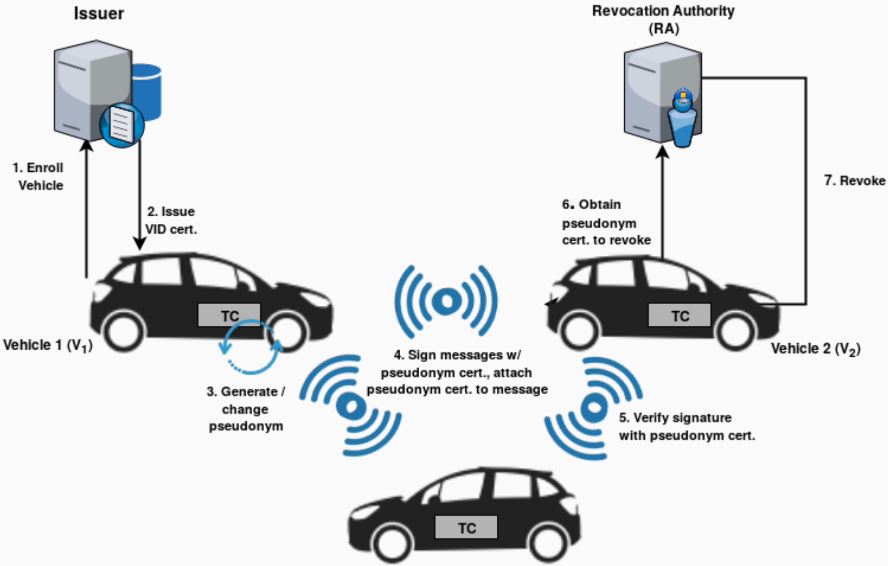
- Anonymous group signature scheme
  - ⇒ Strong, but privacy preserving authentication
- Hardware-based attestation using a TPM
- Properties of DAA include:
  - ⇒ **User-controller Anonymity/Unlinkability:**
    - → Identity of user cannot be revealed, and multiple signatures cannot be linked.
  - ⇒ **Non-Frameability:**
    - → Adversary should not be able to impersonate honest platforms.
  - ⇒ **Correctness:**
    - → Valid signatures only producible by honest platforms, and are verifiable & linkable when specified.
- Standardised in ISO/IEC 20008-2 & 11889

DAA Pseudonym Scheme - Overview

- Simplified VPKI Architecture
  - ⇒ **Issuer:** Authenticates vehicles' to ITS and issues DAA credential
  - ⇒ **Revocation Authority:** Removes misbehaving / malfunctioning vehicles'
- Decentralised ITS allows a shift-of-trust into vehicles.
  - ⇒ Vehicles responsible for self-signing pseudonyms
  - ⇒ Promotes scalability - *Certificate Revocation Lists* not required
- Timely and "*in the moment*" revocation
- Vehicles in control of privacy
- Utilises trusted hardware and uses DAA for hardware-based attestation

Trusted third parties gain no knowledge of ITS entities from colluding with one another.

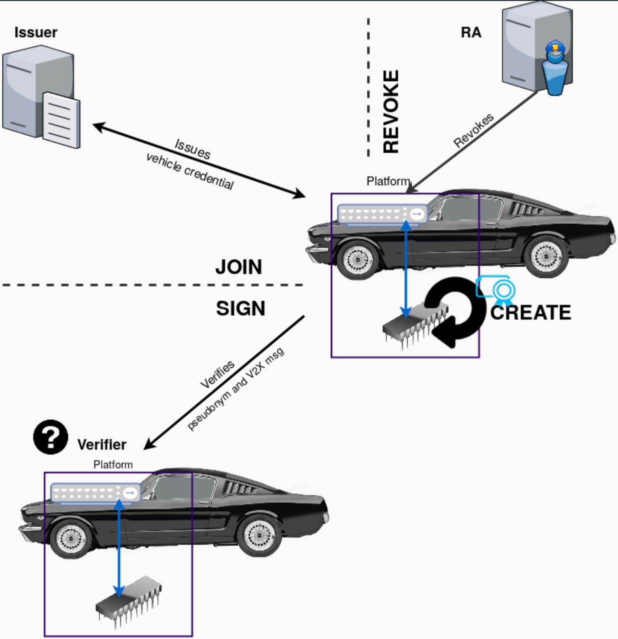
DAA Pseudonym Scheme - Architecture



DAA Protocols for VANETs

- <u>Setup:</u> TC generates fresh DAA key-pair from Issuers security parameters.
- <u>Join:</u> Attests that a vehicle has a valid TC, and produces the DAA credential from Issuer $\Rightarrow$ authenticated member of ITS.
- <u>Create:</u> Fresh self-signed pseudonyms created by TC using credential.
- <u>Sign/Verify:</u> Authenticated V2X communication that verifies pseudonym is valid.
- <u>Revoke:</u> Verifiable revocation that a vehicle has been removed from ITS. Performed without pseudonym resolution.

DAA Protocols for VANETs

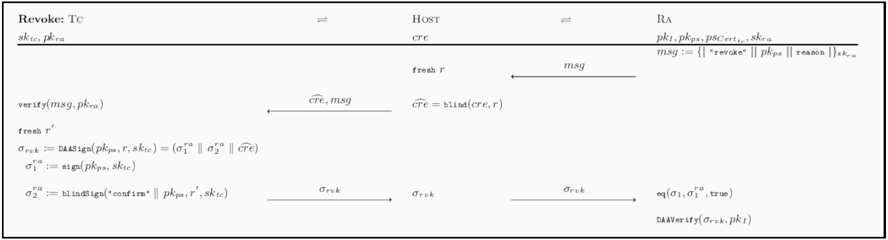


CREATE Protocol

Create: TC	⇌	HOST
sk_{tc}		cre
		fresh r
fresh sk_{ps}/pk_{ps}	← "create" $\parallel \widehat{cre}$	$\widehat{cre} := \texttt{blind}(cre, r)$
fresh r'		
$ps_{sig} := \texttt{DAASign}(pk_{ps}, r', sk_{tc}) = (\sigma_1 \parallel \sigma_2 \parallel \widehat{cre})$		
$\sigma_1 := \texttt{sign}(pk_{ps}, sk_{tc})$		
$\sigma_2 := \texttt{blindSign}(\texttt{"certified"} \parallel pk_{ps}, r', sk_{tc})$		
$ps_{Cert_{tc}} := (pk_{ps} \parallel ps_{sig})$		
$\texttt{store}(sk_{ps})$	$ps_{Cert_{tc}}$ →	$\texttt{store}(ps_{Cert_{tc}})$

1. Credential (from JOIN) is blinded by the host for privacy
2. DAASign produces two signatures: σ_1 (*deterministic*) & σ_2
3. Pseudonym is a key-pair with a DAA signature associated with a blinded credential.

REVOKE Protocol



1. Vehicle receives revocation message from RA, and TC verifies authenticity.
2. TC creates DAA signature to check if σ_1^{ra} matches σ_1
3. If match create revocation confirmation and delete all pseudonyms & DAA key-pair

Security Model

- Security & Privacy Analysis
  - ⇒ User-controlled Anonymity and Unlinkability:
    - → Pseudonym creation DAA credential blinded, not linkable to vehicle.
    - → DAA credential does not contain any PII.
  - ⇒ Non-frameability:
    - → Communication from vehicle cannot be faked or generated by adversary.
    - → SIGN/ VERIFY message is signed by TC, assured by the DAA credential of pseudonym.
  - ⇒ Assurance of revocation:
    - → Revocation requests and confirmations verified by both RA and vehicle.
    - → Confirmed revocation executes deletion of all pseudonyms and DAA credentials.

Future Research Directions

- Formal Analysis using TAMARIN
  - ⇒ Verify trace properties, e.g., security / authentication
  - ⇒ Develop theory for proving DAA in symbolic setting (General theory useful beyond vehicular use case)
  - ⇒ Analysis of V2X revocation[2]
- Implementation and Experimentation
  - ⇒ Message / signature sizes
  - ⇒ Timings for signature verification
  - ⇒ Host or TC: "Trusted VS Untrusted"
- Revocation correctness
  - ⇒ How revocation messages reach the host?
  - ⇒ Message Indistinguishability, Heartbeat?

[2] "**Formal Analysis of V2X Revocation Protocols**" by Whitefield et Al. STM 2017, Oslo, Norway

Thank You!

Q/A

Twitter: @SCCS_UniSurrey

email:

j.whitefield@surrey.ac.uk

References i

JOIN Protocol

Join: TC	$\rightleftharpoons$	Host	$\rightleftharpoons$	Issuer
$sk_{ek_{tc}}, pk_{ek_{tc}}$		$pk_{ek_{tc}}, pk_{tc}$		$pk_{ek_{tc}}, sk_I$
sk_{tc}, pk_{tc}		pk_I		
			$pk_{ek_{tc}}, pk_{tc}$ $\longrightarrow$	$\texttt{fresh}\ n_I$
	C $\longleftarrow$		C $\longleftarrow$	$C = \texttt{aenc}(n_I \parallel pk_{tc}, pk_{ek_{tc}})$
$n_I \parallel pk_{tc}$	$n_I \parallel pk_{tc}$ $\longrightarrow$		$n_I \parallel pk_{tc}$ $\longrightarrow$	$cre = \texttt{blindSign}(\ pk_{tc},\ sk_I\ )$
				$\texttt{fresh}\ key$
				$e = \texttt{senc}(\ cre, key\ )$
	d $\longleftarrow$		$d,\ e$ $\longleftarrow$	$d = \texttt{aenc}(\ key \parallel pk_{tc},\ pk_{ek_{tc}}\ )$
$key \parallel pk_{tc}$	key $\longrightarrow$	$\texttt{store}(\ cre\ )$		

CREATE Protocol

Create: TC	$\rightleftharpoons$	HOST
sk_{tc}		cre
		fresh r
fresh sk_{ps}/pk_{ps}	$\xleftarrow{\texttt{"create"} \parallel \widehat{cre}}$	$\widehat{cre} := \texttt{blind}(cre, r)$
fresh r'		
$ps_{sig} := \texttt{DAASign}(pk_{ps}, r', sk_{tc}) = (\sigma_1 \parallel \sigma_2 \parallel \widehat{cre})$		
$\sigma_1 := \texttt{sign}(pk_{ps}, sk_{tc})$		
$\sigma_2 := \texttt{blindSign}(\texttt{"certified"} \parallel pk_{ps}, r', sk_{tc})$		
$ps_{Cert_{tc}} := (pk_{ps} \parallel ps_{sig})$		
$\texttt{store}(sk_{ps})$	$\xrightarrow{ps_{Cert_{tc}}}$	$\texttt{store}(ps_{Cert_{tc}})$

SIGN/VERIFY Protocol

Sign / Verify: TC	$\rightleftharpoons$	HOST	$\rightleftharpoons$	VERIFIER
sk_{ps}		$psCert_{tc}$		pk_I
	$\xleftarrow{m_{plain}}$	$m_{plain} := \{\|\text{"70 mph"} \parallel data\,\|\}$		
$m_{sign} := \texttt{sign}(m_{plain}, sk_{ps})$	$\xrightarrow{m_{sign}}$	$msg := \{\|\, m_{plain} \parallel m_{sign} \parallel psCert_{tc}\,\|\}$	$\xrightarrow{msg}$	$\texttt{DAAVerify}(ps_{sig}, pk_I)$
				$\texttt{store}(pk_{ps})$

REVOKE Protocol

Revoke: Tc	⇌	Host	⇌	Ra
sk_{tc}, pk_{ra}		cre		$pk_I, pk_{ps}, psCert_{tc}, sk_{ra}$
				$msg := \{\Vert \texttt{"revoke"} \Vert pk_{ps} \Vert \texttt{reason} \Vert\}_{sk_{ra}}$
		$\texttt{fresh}\ r$	← msg	
$\texttt{verify}(msg, pk_{ra})$	← $\widehat{cre}, msg$	$\widehat{cre} = \texttt{blind}(cre, r)$		
$\texttt{fresh}\ r'$				
$\sigma_{rvk} := \texttt{DAASign}(pk_{ps}, r, sk_{tc}) = (\sigma_1^{ra} \parallel \sigma_2^{ra} \parallel \widehat{cre})$				
$\sigma_1^{ra} := \texttt{sign}(pk_{ps}, sk_{tc})$				
$\sigma_2^{ra} := \texttt{blindSign}(\texttt{"confirm"} \parallel pk_{ps}, r', sk_{tc})$	σ_{rvk} →	σ_{rvk}	σ_{rvk} →	$\texttt{eq}(\sigma_1, \sigma_1^{ra}, \texttt{true})$
				$\texttt{DAAVerify}(\sigma_{rvk}, pk_I)$