Privacy Preservation through Uniformity

Mohammad Khodaei, Hamid Noroozi, and Panos Papadimitratos
Networked Systems Security Group
KTH Royal Institute of Technology, Sweden
www.ee.kth.se/nss

Vehicular Communication (VC) System

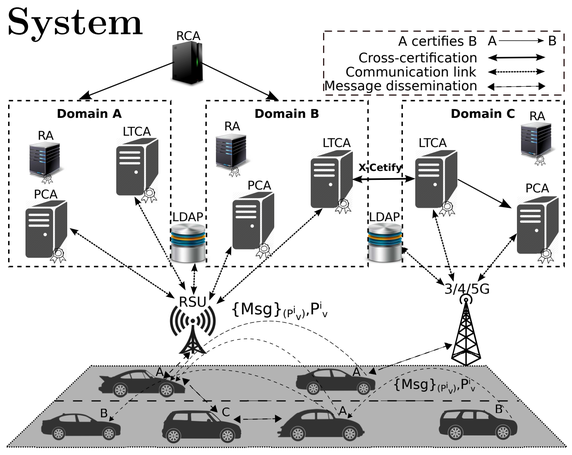

Figure 1: Vehicular Public-Key Infrastructure (VPKI) Architecture [1, 3]

Security System Entities

- Vehicles registered with one (home) **Long Term Certification Authority (LTCA)**
- **Pseudonym Certification Authority (PCA)** servers in one or multiple domains
- Vehicles can obtain pseudonyms from any **PCA** (in home or foreign domains)
- Trust across domains with the help of a **Root CA (RCA)** or cross-certification

Security & Privacy Requirements

- Authentication and communication integrity
- Authorization and access control
- Non-repudiation, accountability and eviction
- **Conditional anonymity & unlinkability**

Adversarial Model

- *Honest-but-curious* VPKI entities
- Roadside Units (RSUs), as *honest-but-curious* system entities, capture messages within their coverage range and aggregate the information

Pseudonym Acquisition Policy

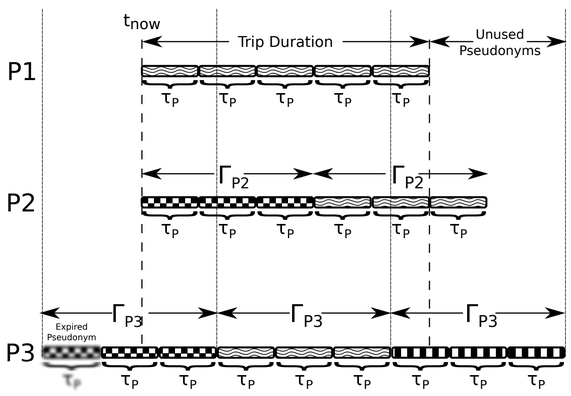

Figure 2: A Schematic Comparison of P1, P2, and P3 [3]

- P1: User-controlled (user-defined) policy
- P2: Oblivious policy
- P3: Universally fixed policy

Inferring User-sensitive Information

- Synthetically linking messages
- Semantically linking messages (time & velocity)
- **Linking based on times of pseudonym changes (cannot be obfuscated)**

Tracking Approach

τ^0	τ^1	τ^2	τ^3	τ^4	τ^5	τ^6	τ^7	τ^8	τ^9	τ^{10}
E	E	C	C	A	I	F	G	D	D	A
	C	G	H	E	A	H	A	I	F	F
		H	F	B		A	D	B	I	E

Figure 3: Pseudonym transition processes from an adversary's viewpoint.

Ground truth: [A, C, I], [F, B, G], [H, D, E]

Timing-based Inference Attack

$$(\tau^0)\quad \begin{array}{c} \\ E \end{array}\begin{array}{c} \begin{array}{c} E \end{array} \\ \begin{pmatrix} -1 \end{pmatrix} \end{array}$$

$$(\tau^1)\quad \begin{array}{c} \\ E \\ C \end{array}\begin{array}{c} \begin{array}{cc} E & C \end{array} \\ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \end{array}$$

$$(\tau^2)\quad \begin{array}{c} \\ E \\ C \\ G \\ H \end{array}\begin{array}{c} \begin{array}{cccc} E & C & G & H \end{array} \\ \begin{pmatrix} 0 & 0 & 0.33 & 0.33 \\ 0 & 0 & 0 & 0 \\ 0.33 & 0 & 0 & 0 \\ 0.33 & 0 & 0 & 0 \end{pmatrix} \end{array}$$

$$(\tau^3)\quad \begin{array}{c} \\ E \\ C \\ G \\ H \\ F \end{array}\begin{array}{c} \begin{array}{ccccc} E & C & G & H & F \end{array} \\ \begin{pmatrix} 0 & 0 & 0.33 & 0.33 & -1 \\ 0 & 0 & 0 & 0 & 0 \\ 0.33 & 0 & 0 & 0 & 0.5 \\ 0.33 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0.5 & 0 & 0 \end{pmatrix} \end{array}$$

$$(\tau^4)\quad \begin{array}{c} \\ E \\ C \\ G \\ H \\ F \\ A \\ B \end{array}\begin{array}{c} \begin{array}{ccccccc} E & C & G & H & F & A & B \end{array} \\ \begin{pmatrix} 0 & 0 & 0.33 & 0.58 & 0.25 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0.25 & 0.25 \\ 0.33 & 0 & 0 & 0 & 0.5 & -1 & -1 \\ 0.58 & 0 & 0 & 0 & 0 & 0.25 & 0.25 \\ 0.25 & 0 & 0.5 & 0 & 0 & 0.25 & 0.25 \\ 0 & 0.25 & -1 & 0.25 & 0.25 & 0 & 0 \\ 0 & 0.25 & -1 & 0.25 & 0.25 & 0 & 0 \end{pmatrix} \end{array}$$

$$(\tau^5)\quad \begin{array}{c} \\ E \\ C \\ G \\ H \\ F \\ A \\ B \\ I \end{array}\begin{array}{c} \begin{array}{cccccccc} E & C & G & H & F & A & B & I \end{array} \\ \begin{pmatrix} 0 & 0 & 0.33 & 0.58 & 0.25 & 0 & 0 & 0.5 \\ 0 & 0 & 0 & 0 & 0 & 0.25 & 0.25 & -1 \\ 0.33 & 0 & 0 & 0 & 0.5 & -1 & -1 & -1 \\ 0.58 & 0 & 0 & 0 & 0 & 0.25 & 0.25 & -1 \\ 0.25 & 0 & 0.5 & 0 & 0 & 0.25 & 0.25 & -1 \\ 0 & 0.25 & -1 & 0.25 & 0.25 & 0 & 0 & 0 \\ 0 & 0.25 & -1 & 0.25 & 0.25 & 0 & 0 & 0.5 \\ 0.5 & -1 & -1 & -1 & -1 & 0 & 0.5 & 0 \end{pmatrix} \end{array}$$

$$(\tau^6)\quad \begin{array}{c} \\ E \\ C \\ G \\ H \\ F \\ A \\ B \\ I \end{array}\begin{array}{c} \begin{array}{cccccccc} E & C & G & H & F & A & B & I \end{array} \\ \begin{pmatrix} 0 & 0 & 0.33 & 0.58 & 0.25 & 0 & 0 & 0.5 \\ 0.33 & 0 & 0 & 0 & 0.5 & -1 & -1 & -1 \\ 0.33 & 0 & 0 & 0 & 0.5 & -1 & -1 & -1 \\ 0.58 & 0 & 0 & 0 & 0 & 0.25 & 0.25 & 0.33 \\ 0.25 & 0 & 0.5 & 0 & 0 & 0.25 & 0.25 & 0.33 \\ 0 & 0.25 & -1 & 0.25 & 0.25 & 0 & 0 & 0 \\ 0 & 0.25 & -1 & 0.25 & 0.25 & 0 & 0 & 0.5 \\ 0.5 & -1 & -1 & 0.33 & 0.33 & 0 & 0.5 & 0 \end{pmatrix} \end{array}$$

$$(\tau^7)\quad \begin{array}{c} \\ E \\ C \\ G \\ H \\ F \\ A \\ B \\ I \\ D \end{array}\begin{array}{c} \begin{array}{ccccccccc} E & C & G & H & F & A & B & I & D \end{array} \\ \begin{pmatrix} 0 & 0 & 0.33 & 0.58 & 0.25 & 0 & 0 & 0.5 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0.25 & 0.25 & -1 & -1 \\ 0.33 & 0 & 0 & 0 & 0.83 & 0 & -1 & -1 & 0 \\ 0.58 & 0 & 0 & 0 & 0 & 0.25 & 0.25 & 0.33 & 0.33 \\ 0.25 & 0 & 0.83 & 0 & 0 & 0.25 & 0.25 & 0.33 & 0.33 \\ 0 & 0.25 & 0 & 0.25 & 0.25 & 0 & 0 & 0 & 0 \\ 0 & 0.25 & -1 & 0.25 & 0.25 & 0 & 0 & 0.5 & -1 \\ 0.5 & -1 & -1 & 0.33 & 0.33 & 0 & -1 & -1 & 0 \end{pmatrix} \end{array}$$

Timing-based Inference Attack (Cont'd)

$$(\tau^8)\quad \begin{array}{c} \\ E \\ C \\ G \\ H \\ F \\ A \\ B \\ I \\ D \end{array}\begin{array}{c} \begin{array}{ccccccccc} E & C & G & H & F & A & B & I & D \end{array} \\ \begin{pmatrix} 0 & 0 & 0.33 & 0.58 & 0.25 & 0 & 0 & 0.5 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0.25 & 0.25 & -1 & -1 \\ 0.33 & 0 & 0 & 0 & 0.83 & 0 & 0.33 & 0.33 & 0 \\ 0.58 & 0 & 0 & 0 & 0 & 0.25 & 0.25 & 0.33 & 0.33 \\ 0.25 & 0 & 0.83 & 0 & 0 & 0.25 & 0.25 & 0.33 & 0.33 \\ 0 & 0.25 & 0 & 0.25 & 0.25 & 0 & 0 & 0 & 0 \\ 0 & 0.25 & 0.33 & 0.25 & 0.25 & 0 & 0 & 0.5 & 0 \\ 0.5 & -1 & 0.33 & 0.33 & 0.33 & 0 & 0.5 & 0 & 0 \\ -1 & -1 & 0 & 0.33 & 0.33 & 0 & 0 & 0 & 0 \end{pmatrix} \end{array}$$

$$(\tau^9)\quad \begin{array}{c} \\ E \\ C \\ G \\ H \\ F \\ A \\ B \\ I \\ D \end{array}\begin{array}{c} \begin{array}{ccccccccc} E & C & G & H & F & A & B & I & D \end{array} \\ \begin{pmatrix} 0 & 0 & 0.33 & 0.58 & 0.25 & 0 & 0 & 0.5 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0.25 & 0.25 & -1 & -1 \\ 0.33 & 0 & 0 & 0 & 0.83 & 0 & 0.33 & 0.33 & 0 \\ 0.58 & 0 & 0 & 0 & 0 & 0.25 & 0.25 & 0.33 & 0.33 \\ 0.25 & 0 & 0.83 & 0 & 0 & 0.25 & 0.75 & 0.33 & 0.33 \\ 0 & 0.25 & 0 & 0.25 & 0.25 & 0 & 0 & 0 & 0 \\ 0 & 0.25 & 0.33 & 0.25 & 0.75 & 0 & 0 & 0.50 & 0 \\ 0.5 & -1 & 0.33 & 0.33 & 0.33 & 0 & 0.5 & 0 & 0 \\ -1 & -1 & 0 & 0.33 & 0.33 & 0 & 0 & 0 & 0 \end{pmatrix} \end{array}$$

$$(\tau^{10})\quad \begin{array}{c} \\ E \\ C \\ G \\ H \\ F \\ A \\ B \\ I \\ D \end{array}\begin{array}{c} \begin{array}{ccccccccc} E & C & G & H & F & A & B & I & D \end{array} \\ \begin{pmatrix} 0 & 0 & 0.33 & 0.58 & 0.25 & 0 & 0 & 0.83 & 0.33 \\ 0 & 0 & 0 & 0 & 0 & 0.25 & 0.25 & -1 & -1 \\ 0.33 & 0 & 0 & 0 & 0.83 & 0 & 0.33 & 0.33 & 0 \\ 0.58 & 0 & 0 & 0 & 0 & 0.25 & 0.25 & 0.33 & 0.33 \\ 0.25 & 0 & 0.83 & 0 & 0 & 0.25 & 0.75 & 0.33 & 0.33 \\ 0 & 0.25 & 0 & 0.25 & 0.25 & 0 & 0 & 0 & 0 \\ 0 & 0.25 & 0.33 & 0.25 & 0.75 & 0 & 0 & 0.50 & 0 \\ 0.83 & -1 & 0.33 & 0.33 & 0.33 & 0 & 0.5 & 0 & 0 \\ 0.33 & -1 & 0 & 0.33 & 0.33 & 0 & 0 & 0 & 0 \end{pmatrix} \end{array}$$

Potential linking solutions: [I, E, H], [G, F, B]

Mitigating Timing-based Inferences

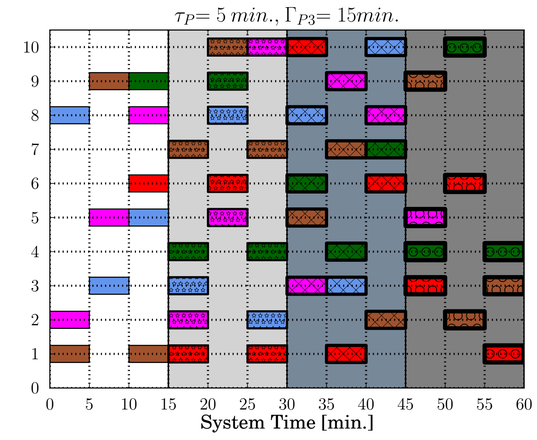

Figure 4: Universally Fixed Policy [1, 3, 5]

- Achieving highest level of privacy: anonymity set equals to the number of active vehicles
- Preventing a single *honest-but-curious* VPKI entity from linking pseudonyms

References

[1] M. Khodaei, H. Jin, and P. Papadimitratos, **"SECMACE: Scalable and Robust Identity and Credential Management Infrastructure in Vehicular Communication Systems,"** IEEE Transactions on Intelligent Transportation Systems, vol. 19, no. 5, 1430–1444, May 2018.

[2] M. Khodaei, A. Messing, and P. Papadimitratos. 2017. **"RHyTHM: A Randomized Hybrid Scheme To Hide in the Mobile Crowd,"** In IEEE Vehicular Networking Conference (VNC), Torino, Italy, Nov. 2017.

[3] M. Khodaei and P. Papadimitratos, **"Evaluating On-demand Pseudonym Acquisition Policies in Vehicular Communication Systems,"** in Proceedings of the First International Workshop on Internet of Vehicles and Vehicles of Internet, Paderborn, Germany, pp. 7–12, July 2016.

[4] M. Khodaei and P. Papadimitratos, **"The Key to Intelligent Transportation: Identity and Credential Management in Vehicular Communication Systems,"** IEEE VT Mag., vol.10, no.4, pp.63–69, Dec. 2015.

[5] M. Khodaei, H. Jin, and P. Papadimitratos. **"Towards Deploying a Scalable & Robust Vehicular Identity and Credential Management Infrastructure,"** IEEE VNC, Paderborn, Germany, Dec. 2014.