Secure and private connectivity in smart environments

Acronym: SURPRISE

Project ID: RIT17-0005

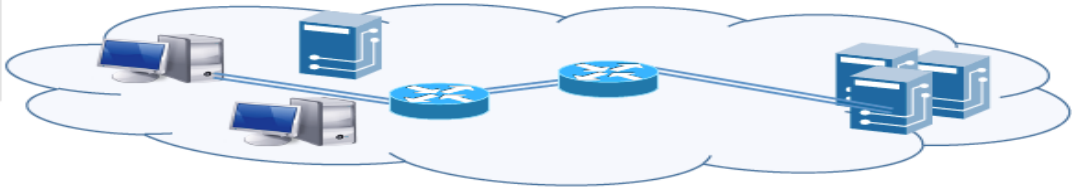
PI: Papadimitratos (KTH)

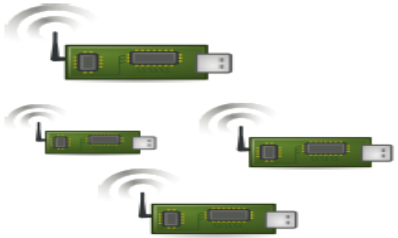
Co-PIs: Fischer-Hübner (KAU), Johansson (LTH), Larsson (LiU), Skoglund (KTH)

https://nss.proj.kth.se/surprise/

Overview

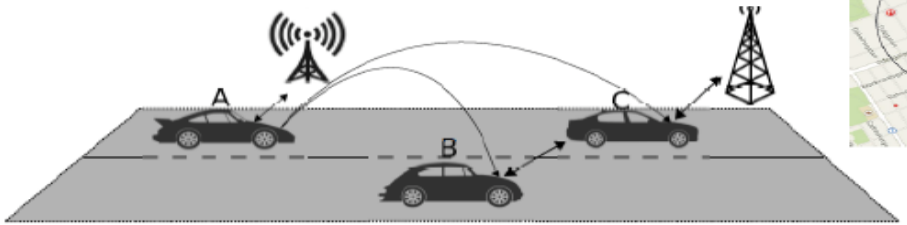
Identity and credential management





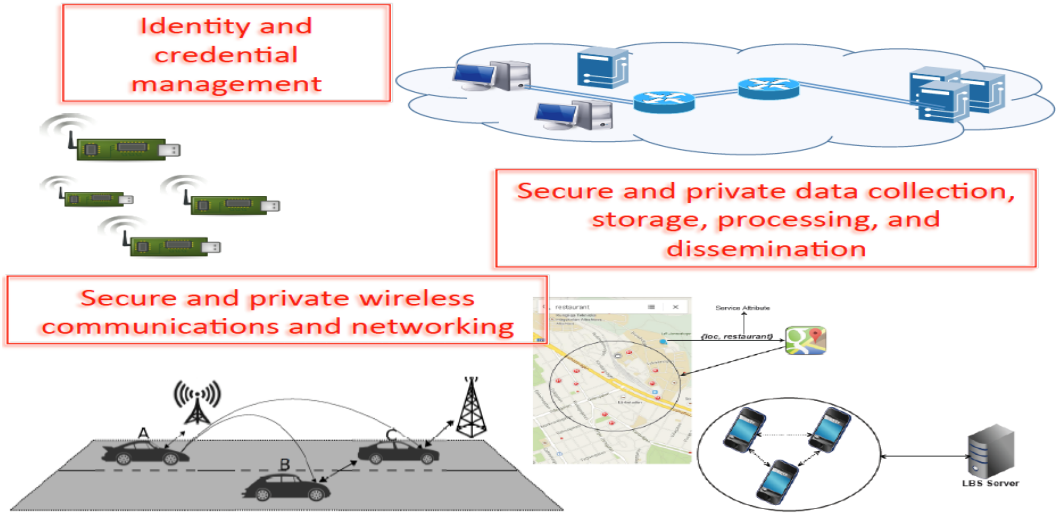
Secure and private data collection, storage, processing, and dissemination

Secure and private wireless communications and networking



Goals

- Three key security and privacy (S&P) enablers
  - Trust management, including identity and credential management for S&P
  - Lean, resilient S&P preserving communication and networking
  - Data validation and S&P preserving processing



Research environment
Consortium

NSS

ISE

Research environment
Academic collaborations

Beyond the proposal:
RISE, Digital Futures, SecurityLink & FOI

Research environment
Academic collaborations (cont'd)

Beyond the proposal: ESA, KI; several bilateral collaborations; top conference organization

Privacy Enhancing Technologies Symposium
On the Internet, 2021

South Africa
Sweden
University Forum

acm

esa
European Space Agency

Cyber Security for Europe

Young Academy of Europe

IEEE
Advancing Technology for Humanity

Karolinska Institutet

Swedish Defence University

European Commission
HORIZON 2020

Research environment
Industrial collaborations

Beyond the proposal: ICA, mozilla, einride, Google, City of Gothenburg

CAR 2 CAR
COMMUNICATION CONSORTIUM

ICA
GRUPPEN

City of Gothenburg

Google

mozilla

einride

SAAB

ERICSSON

ABB

COMBITECH

advenica

Scientific results

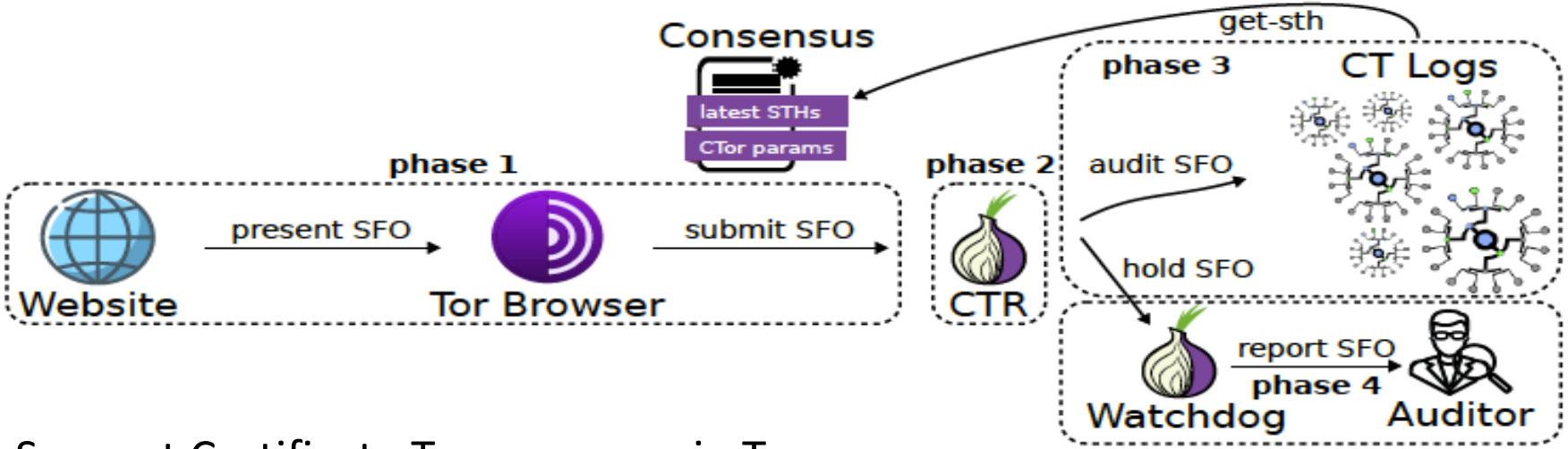
WP1: Selected paper

sciendo

Proceedings on Privacy Enhancing Technologies ; 2021 (2):194–213

Rasmus Dahlberg*, Tobias Pulls, Tom Ritter, and Paul Syverson

Privacy-Preserving & Incrementally-Deployable Support for Certificate Transparency in Tor



- Support Certificate Transparency in Tor
- Privacy-Preserving
- Incrementally-deployable

Scientific Results

WP2: Selected paper

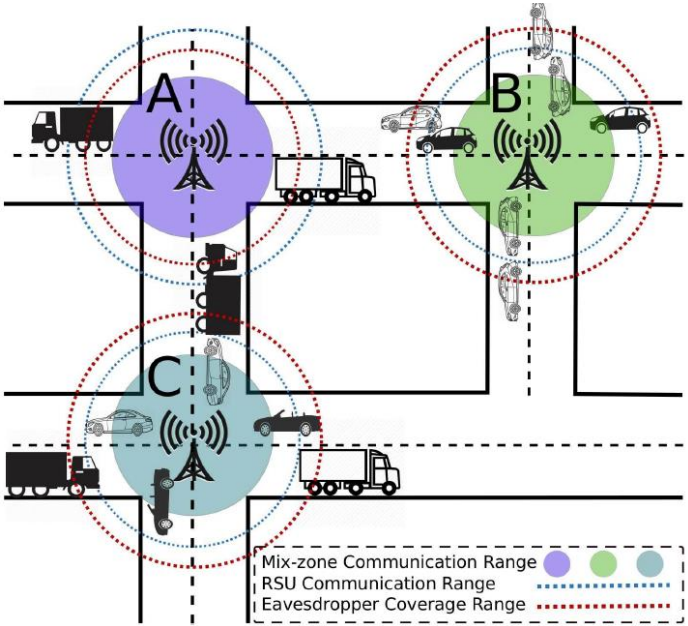


Fig. 2. Mix-zone construction with decoy traffic.

Cooperative Location Privacy in Vehicular Networks: Why Simple Mix Zones Are Not Enough

Mohammad Khodaei, *Member, IEEE*, and Panos Papadimitratos, *Fellow, IEEE*

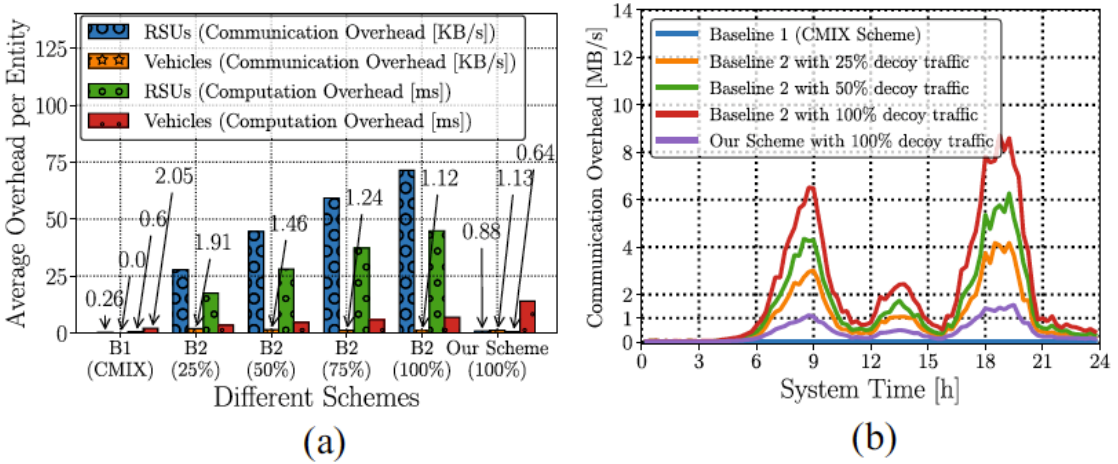


Fig. 8. Comparison among CMIX (B1) [37], chaff-based CMIX (B2) [42], and our scheme: 1K chaff pseudonyms in a CF with $\rho = 10^{-25}$; beacon frequency: $\gamma_{mz} = 0.5$, $\gamma_v = 0.2$. (a) Computation and communication overheads. (b) Communication overhead, averaged every 300 s.

Scientific Results

WP3: Selected paper

Algorithm 1. KEM.CCA.Encaps

Input: pk
Output: $\mathbf{c}$ and $\mathbf{s}$

1: pick a random $\mathbf{m}$
2: $(\mathbf{r}, \mathbf{k}) \leftarrow H_1(\mathbf{m}, \mathsf{pk})$
3: $\mathbf{c} \leftarrow \mathsf{PKE.CPA.Enc}(\mathsf{pk}, \mathbf{m}; \mathbf{r})$
4: $\mathbf{s} \leftarrow H_2(\mathbf{c}, \mathbf{k})$
5: **Return** $(\mathbf{c}, \mathbf{s})$

Algorithm 2. KEM.CCA.Decaps

Input: sk, pk, $\mathbf{c}$
Output: $\mathbf{s}'$

1: $\mathbf{m}' \leftarrow \mathsf{PKE.CPA.Dec}(\mathsf{sk}, \mathbf{c})$
2: $(\mathbf{r}', \mathbf{k}') \leftarrow H_1(\mathbf{m}', \mathsf{pk})$
3: $\mathbf{c}' \leftarrow \mathsf{PKE.CPA.Enc}(\mathsf{pk}, \mathbf{m}'; \mathbf{r}')$
4: **if** $(\mathbf{c}' = \mathbf{c})$ **then Return** $\mathbf{s}' \leftarrow H_2(\mathbf{c}, \mathbf{k}')$
5: **else Return** $\mathbf{s}' \leftarrow H_2(\mathbf{c}, \mathsf{sk}_r)$, where sk_r is a random seed in sk
6: **end if**

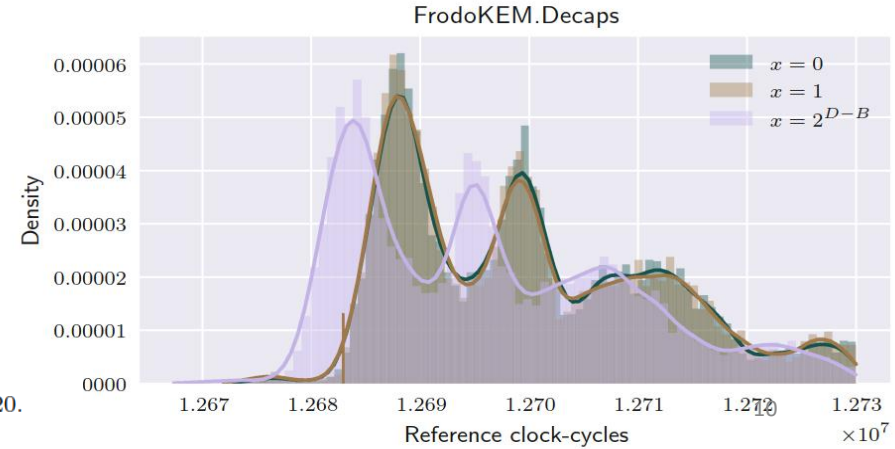
D. Micciancio and T. Ristenpart (Eds.): CRYPTO 2020, LNCS 12171, pp. 359–386, 2020.
https://doi.org/10.1007/978-3-030-56880-1_13

A Key-Recovery Timing Attack on Post-quantum Primitives Using the Fujisaki-Okamoto Transformation and Its Application on FrodoKEM

Qian Guo[1,2(✉)], Thomas Johansson[1(✉)], and Alexander Nilsson[1,3(✉)]

[1] Department of Electrical and Information Technology, Lund University, Lund, Sweden
{qian.guo,thomas.johansson,alexander.nilsson}@eit.lth.se
[2] Selmer Center, Department of Informatics, University of Bergen, Bergen, Norway
[3] Advenica AB, Malmö, Sweden

- NIST PQ project candidate
- We show how to recover the secret key by feeding the Decaps with special c and then study timing information



Scientific Results

WP4: Selected paper

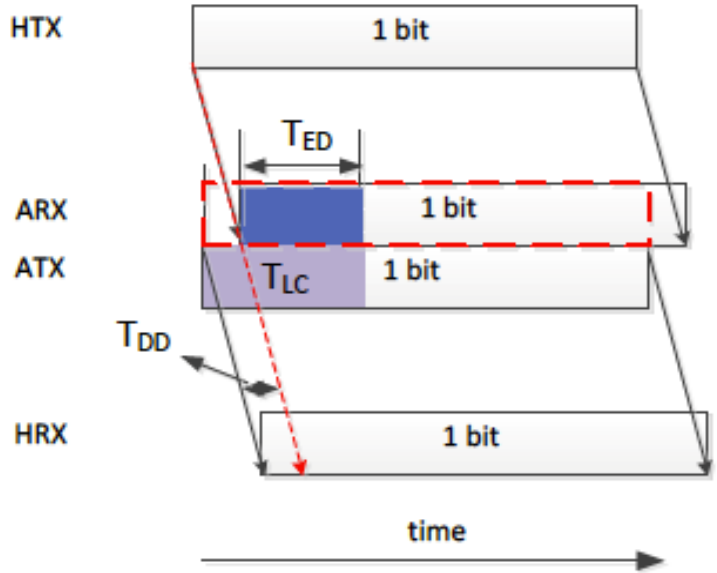
IEEE TRANSACTIONS ON AEROSPACE AND ELECTRONIC SYSTEMS, NOVEMBER 2021

Protecting GNSS Open Service Navigation Message Authentication Against Distance-Decreasing Attacks

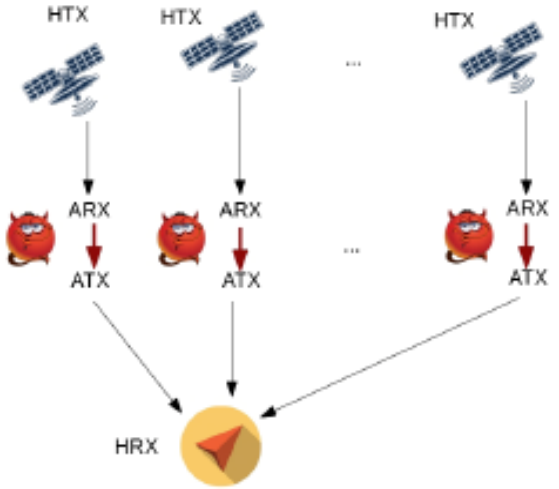
KEWEI ZHANG
KTH Royal Institute of Technology, Stockholm, Sweden

ERIK G. LARSSON, Fellow, IEEE
Linköping University, Linköping, Sweden

PANOS PAPADIMITRATOS, Fellow, IEEE
KTH Royal Institute of Technology, Stockholm, Sweden



(a) Illustration of DD attack.



(b) Adversary illustration for DD attack on GNSS.

Fig. 1: Distance-decreasing attacks on GNSS signals.

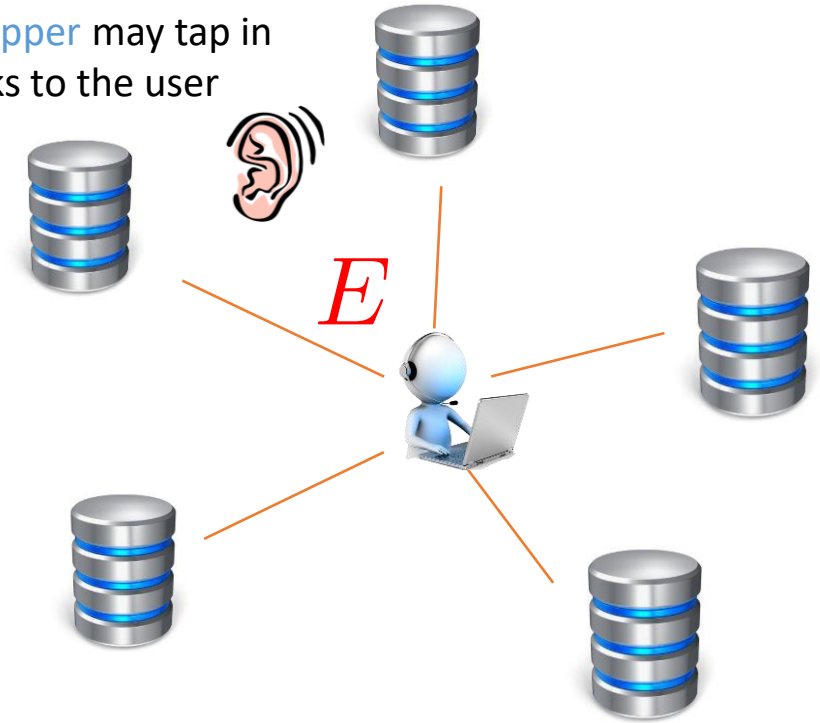
Scientific Results

WP5: Selected paper

The Capacity of Private Information Retrieval With Eavesdroppers

Qiwen Wang, *Member, IEEE*, Hua Sun, *Member, IEEE*, and Mikael Skoglund, *Fellow, IEEE*

An eavesdropper may tap in on any *E* links to the user



K messages stored at *N* servers

At most *T* servers may collude

User should be able to download any message without revealing which data is of interest

Capacity *C* = maximum number of requested message bits per downloaded bit

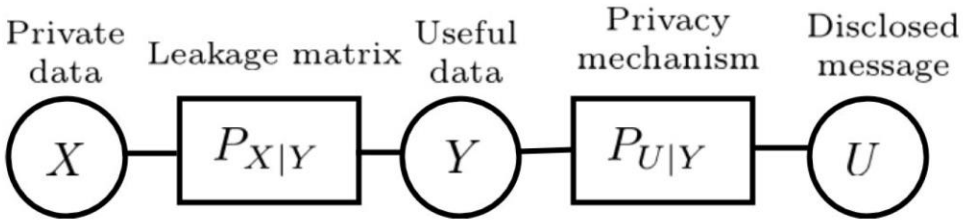
Scientific Results

WP6: Selected paper

IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 16, 2021

A Design Framework for Strongly χ^2-Private Data Disclosure

Amirreza Zamani, *Member, IEEE*, Tobias J. Oechtering, *Senior Member, IEEE*, and Mikael Skoglund, *Fellow, IEEE*



$$\sup_{P_{U|Y}} \quad I(U;Y), \tag{1a}$$

$$\text{subject to:} \quad X - Y - U, \tag{1b}$$

$$\left\| [\sqrt{P_X}^{-1}](P_{X|U=u} - P_X) \right\|^2 \leq \epsilon^2, \quad \forall u \in \mathcal{U}. \tag{1c}$$

Secure and private connectivity in smart environments

Acronym: SURPRISE

Project ID: RIT17-0005

PI: Papadimitratos (KTH)

Co-PIs: Fischer-Hübner (KAU), Johansson (LTH), Larsson (LiU), Skoglund (KTH)

https://nss.proj.kth.se/surprise/