SMARTY: Secure Software Update Deployment for the Smart City

CONTACT: MARTIN HELL (martin.hell@eit.lth.se)

Participating Parties

- Department of Electrical and Information Technology, Lund University
- Department of Computer Science, Lund University

Funding: SSF

Goals

Advance the research in topics related to **updating** devices in a Smart City context

Vulnerability analysis

A reason for updating

“Improving technical and organizational aspects of discovering, analyzing and prioritizing vulnerabilities”

Device management

Handling the devices receiving updates

“Enable management of and communication between devices, such that updates can be rolled out securely and efficiently”

Network security

Configurable and adaptable network

“Investigate new and improved techniques for security and privacy in network communication, using trusted computing and SDN”

Applications

Designing secure smart city applications

“Propose new applications based on novel cryptographic primitives that contribute to the realization of the smart city vision.”

Implement and demonstrate parts of the research in actual environments

Selected Results

Vulnerability Analysis

1

“Machine learning-based mapping of vulnerability data to affected software”

E. Wåreus, M. Hell: Automated CPE labeling of CVE summaries with Machine Learning. DIMVA 2020.

2

“Maturity model for improved organizational processes in vulnerability handling”

M. Höst, M. Hell: Evaluation of the HAVOSS software process maturity model. SEAA 2020.

3

“Call graph-based analysis detecting if the vulnerable part of software is used”

R. Hagberg, M. Hell, C. Reichenbach: Using Program Analysis to Identify the Use of Vulnerable Functions. SECRYPT 2021.

Device Management

1

“Composition language for micro-services interaction”

Alfred Akesson, Görel Hedin, Mattias Nordahl & Boris Magnusson: ComPOS: Composing Oblivious Services. PerCom 2019.

2

“Blockchain-based PKI with dynamic enrolment and revocation of devices”

Mohsen Toorani & Christian Gehrmann: A Decentralized Dynamic PKI based on Blockchain. SAC’21.

3

“Demonstrator showing how devices can be updated and managed in a use case defined by Helsingborg”

Mattias Nordahl, Boris Magnusson, Görel Hedin & Alfred Åkesson: Smart bikes: Gradual update of IoT systems. EDOC 2020.

Selected Results

Network Security

1

“Deconstructing Open vSwitch to protect flow tables using Intel SGX enclaves”

J. Medina, N. Paladi, P. Arlos: Protecting OpenFlow using Intel SGX, IEEE NFV-SDN 2019.

2

“Validation of SDN policies using property-based testing ”

LM Castro, N Paladi: Validation of SDN policies: a property-based testing perspective, Procedia Computer Science, 2019.

3

“Lightweight key provisioning with symmetric keys integrated with the SDN flow setup”

N. Paladi, M. Tiloca, PN. Bideh, M. Hell: Flowrider: Fast On-Demand Key Provisioning for Cloud Networks, SecureComm 2021

Applications

1

“Emergency traffic prioritization in an SDN application”

P. Nikbakht Bideh, N. Paladi, M. Hell: Software Defined Networking for Emergency Traffic Management in Smart Cities. IWVSC 2019.

2

“FIPS 140-3 requirements for SGX-based virtualized HSM in the cloud”

J. Brorsson, P. Nikbakht Bideh, A. Nilsson, M. Hell: On the Suitability of Using SGX for Secure Key Storage in the Cloud. TrustBus 2020.

3

“Privacy preserving deduplication of data stored in the cloud”

Daniel E. Lucani, Lars Nielsen, Claudio Orlandi, Elena Pagnin, Rasmus Vestergaard: Secure generalized deduplication via multi-key revealing encryption. SCN 2020.

Collaborations

Academia

AARHUS UNIVERSITY

KTH VETENSKAP OCH KONST

CHALMERS

BLEKINGE TEKNISKA HÖGSKOLA · BTH ·

TECHNISCHE UNIVERSITÄT DRESDEN

UNIVERSIDADE DA CORUÑA

Industry

SONY

HBG CITY

debricked

RI. SE

Chocolate Cloud

• itACiH •
DIGITALT STÖD FÖR SÄKER SJUKVÅRD I HEMMET

Happy to get more collaborations in the areas of interest