RISE SICS SECURITY LAB
A secure and competitive Sweden!

Shahid Raza, PhD
shahid.raza@ri.se

Research Institutes of Sweden
ICT
SICS
The RISE institutes Innventia, SP and Swedish ICT have merged in order to become a stronger research and innovation partner for businesses and society.
RISE SICS Security Lab at a glance

- Among the largest security groups in Sweden
  - 16 members, 3 affiliates
  - Two locations (Stockholm, Lund)
Featured research areas and projects

IoT
- EIT ACTIVE
- SIP-IoT
- CEBOT
- Celtic-plus
- CyberWI
- FP7 SEGRID

5G
- H2020 5G-ENSURE

Platform Security
- VINNOVA UDI SECONDS
- ARTEMIS EMC²
- SSF PROSPER
- VINNOVA UDI HACPOC

Cloud
- H2020 COLA
- H2020 PaaSword

Privacy
- Industry funded
  Enabling Privacy
- H2020 PaaSword

Blockchain
- Self-funded
The Reality of IoT Security

- IoT security now is like IT security in the 1990s
- IoT manufacturers have been ignoring security in the rush to get to market first
- “There is no Internet of Things, only other people's computers in your house.” -- Jacob Hoffman-Andrews
- Recent attacks are changing the mindset (security is not an add-on)
CyberWI - Cyber Security for the Wireless Industrial use cases

SEGRID - SSecurity for smart electricity GRIDs

ACTIVE - Advanced ConnecTIvity platform for VErtical segments


+ Contributing to ongoing IETF standardization

talk by Göran Selander
Secure group communication for IoT

- Protection of messages exchanged in multicast groups
  - Ensure confidentiality, integrity and source authentication
  - Binding of multicast requests and (multiple) unicast responses
  - Focus on the application layer (Group OSCOAP) – Joint standardization work with Ericsson

- Secure joining of multicast groups
  - Provisioning of group key material
  - Paired with access control enforcement
  - Flexible and suitable to different security profiles

- Management of group key material
  - Renew group keys when group members join or leave
  - Need for high efficiency and scalability with the group size

*FP7 project SEGRID and the EIT-Digital HII ACTIVE*
Counteract (DoS) attacks

- Improve robustness of secure session establishment
  - Protect (D)TLS servers from malevolent handshakes
  - Cover both versions 1.2 and 1.3 of (D)TLS protocol

- Reaction to packet-flooding attacks
  - Context-aware and self-adaptive to attack intensity
  - Preserve (best-effort) availability to serve legitimate clients

- Prevent selective jamming in wireless networks
  - Enforced at the MAC layer with negligible overhead
  - Focus on the multi-channel mode of IEEE 802.15.4e (TSCH)

FP7 project SEGRID and the EIT-Digital HII ACTIVE
The reference project for 5G Security, Privacy and Trust

- Produce a 5G Security Architecture and Use Cases
- An initial set of Security Enablers
- 5G Security test bed
- Contribute to standards bodies
- Secure storage
- Verified cloud resources
- Secure launch and execution of Cloud application
- Searchable Encryption
- Trusted 3rd party verification
- Context aware Access Control
- Optimum and secure deployment and run-time orchestration of cloud application.

Prerequisite: *minimum impact on user experience and performance*
Platform security for embedded systems and cloud
- Mainly through (high assurance) separation
  - e.g. with virtualization
- In-house open-source hypervisor for ARM (SICS Hypervisor)
- Formal verification (e.g. using interactive theorem proving)
- Also research activities on trusted computing, SGX, system-on-chip extensions, ...
Example: secure virtualization

formally verified: separation as good as in a physically distributed setting

talk by Arash Vahidi
Privacy is increasingly important in a data driven society

RISE SICS works with
- Identifying mechanisms for increasing trust for processing of personal data
- Mechanisms for creating internal awareness for how data is used
- Help companies to play a more proactive role in taking a responsibility for data collection

Ongoing projects: Engaging Privacy, DigiTrust
IoT

- Fully automated secure and sustainable security for IoT
  - PKI for battery-power IoT devices
  - Access control through trusted third part (OAuth 2.0)
  - Secure firmware/software updates
- DDoS protection
- Standardisation
- Secure IoT for Automotive (Ransomware protection)

Blockchain

- Blockchain-IoT integration with lightweight crypto
- Open source APIs and Proof-of-concept
  - Application
    - Fleet management - PostNord
    - Auto industry - Volvo

Cloud and 5G

- Slicing
- Orchestration
- Design and analysis of encrypted database schemes
- Industry 4.0

GDPR

- Enforcement in cloud-connected IoT with digital guarantees

Software security for IoT
Developing lightweight security protocols for the IoT with SICS

Connected homes, self-driving cars and automated industry – just a few of the things that come to mind when you think of the Internet of Things (IoT). Behind the scenes, however, there’s still plenty of work to be done before many IoT devices can truly become a cost-effective and efficient reality. In partnership with SICS, Ericsson Security Research is developing a key enabler of the IoT: lightweight security protocols.
Zertifikate für Dinge

Projekt CEBOT liefert ein neues „PKI-Protokoll“ für das IoT

Das schwedische Forschungsinstitut RISE SICS und der IAM-Anbieter Nexus haben ein Protokoll für die Zertifikatsverteilung im „Internet of Things“ (IoT) entwickelt, das auch ressourcenarme Geräte mit einer vertrauenswürdigen Grundlage für eindeutige Identifizierung und sichere Kommunikation versorgen soll.

Von Ralph Horner, Ettlingen

Das Internet der Dinge (IoT) verheißt Potenzial für neue Geschäftsmodelle, aber auch Einfallsreicht für Cyberangriffe. Der Zugang zu solchen Geräten muss deshalb kontrolliert, ihre Kommunikation geschützt werden – dabei sind eindeutige und vertrauenswürdige digitale Identitäten gefragt. In der Regel übernehmen Zertifikate bei solchen Aufgaben eine wichtige Rolle.

Doch eine Zertifikatsverteilung an Geräte mit beschränkten Ressourcen, etwa mit wenig Arbeitspeicher und geringer Verarbeitungskapazität, sowie an Systeme ohne kontinuierliche Energieversorgung ist problematisch. Marsche „Dinge“ müssen bis zu zehn Jahre mit nur

CEBOT


Swedish research project
CEBOT has solved one of the toughest IoT security problems

It has been hard to give resource-constrained things trusted identities, and as the internet of things (IoT) grows this has become one of the biggest security problems. “We have now solved this enrollment challenge by creating a new, super lightweight, and fully automated protocol,” says Shahid Raza, senior researcher and project manager for CEBOT.

The backbone for all security solutions is that people, software and things have trusted identities – if you do not know who or what you are communicating with, it does not matter how well-encrypted your digital connection is, or how well-guarded your facilities are.

“When it comes to the internet, the state of the art for enabling trusted identities is using public key infrastructure, PKI. But a real challenge with PKI is the enrollment process,” says Shahid Raza, senior researcher at Swedish non-profit research organization RISE SICS and project manager for
Thanks!