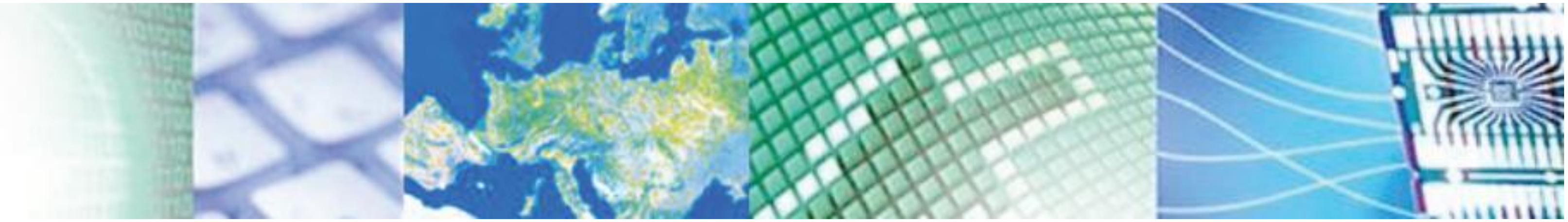
chist-era



CHIST-ERA Projects Seminar

SPTIoT

Gareth Howells

Bucharest, April 4th, 2019

Programme co-funded by the
EUROPEAN UNION

User-Centric Security, Privacy and Trust in the Internet of Things (SPTIoT)

- Methods for data anonymisation
- Technical mechanisms to increase trustworthiness when data is shared between different providers
- Intrusion detection methods
- Authentication using trusted computing (lightweight hardware and software security)
- Dynamic security to allow systems to adapt to varying users
- Data visualisation for increasing user awareness of privacy issues
- Empowering users with risk evaluation tool for their data and contacts;
- Assistive technology/techniques to encourage more secure behaviour and awareness of users

Projects of the Topic

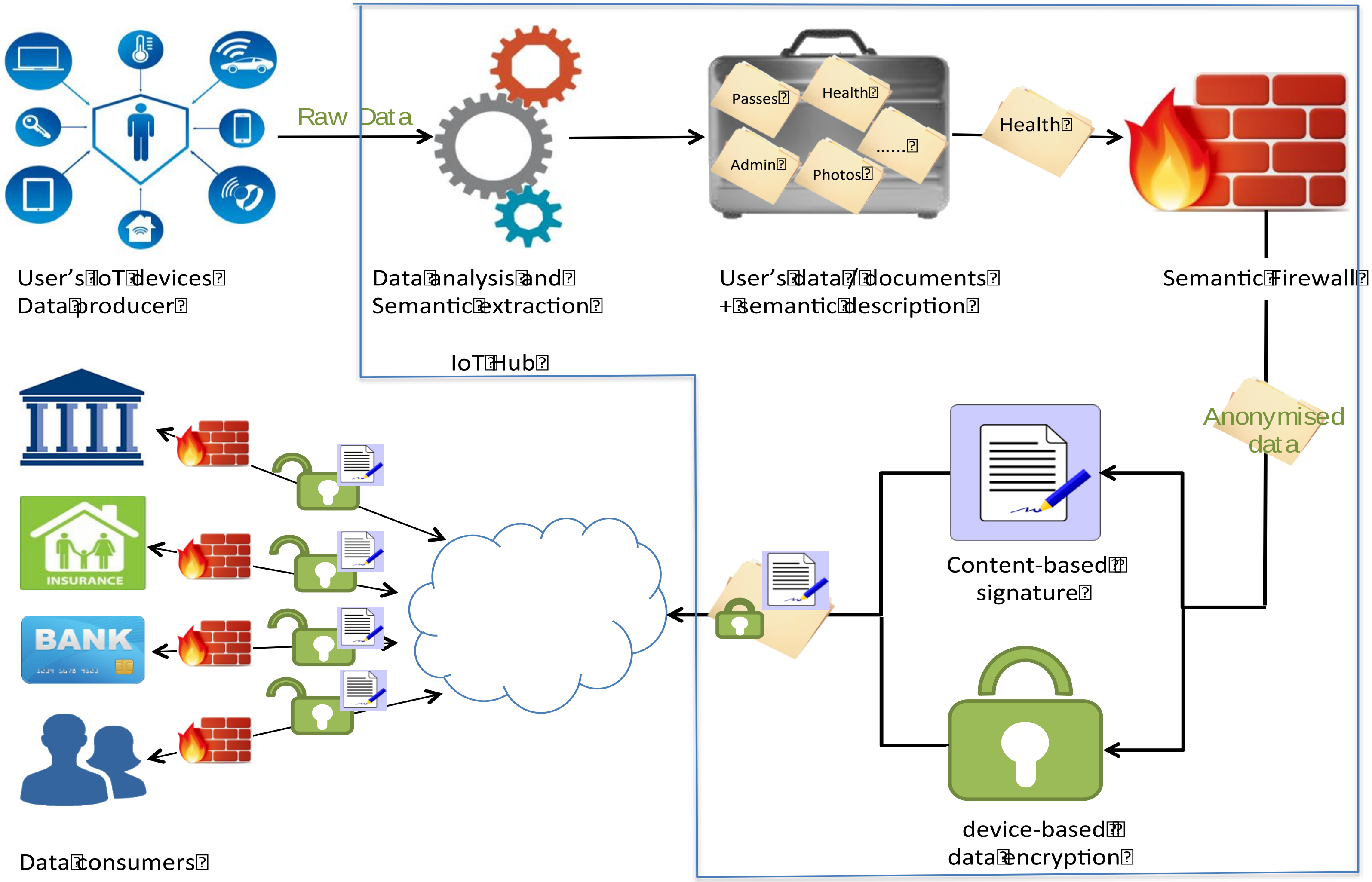
- SPIRiT
- UPRISE-IOT
- ID-IoT
- USE-IT
- SUCCESS
- COCOON

SPIRiT: Security and Privacy foR the Internet of Things

Aim of the project:

- **Enhance trust and integrity of IoT technology**
- **Address lack of user confidence in the technology**
- **Specifically**
  - How to ensure data originates from claimed device?
  - How to ensure it has not been altered?
  - How to ensure users comply with security requirements?
  - How to ensure the solution is easy and cheap to deploy?
  - How to ensure system may evolve to changing requirement?

SPIRiT: Security and Privacy foR the Internet of Things



User’s IoT devices
Data producer

Data analysis and
Semantic extraction

User’s data / documents
+ semantic description

Semantic Firewall

IoT Hub

Content-based
signature

device-based
data encryption

Data consumers

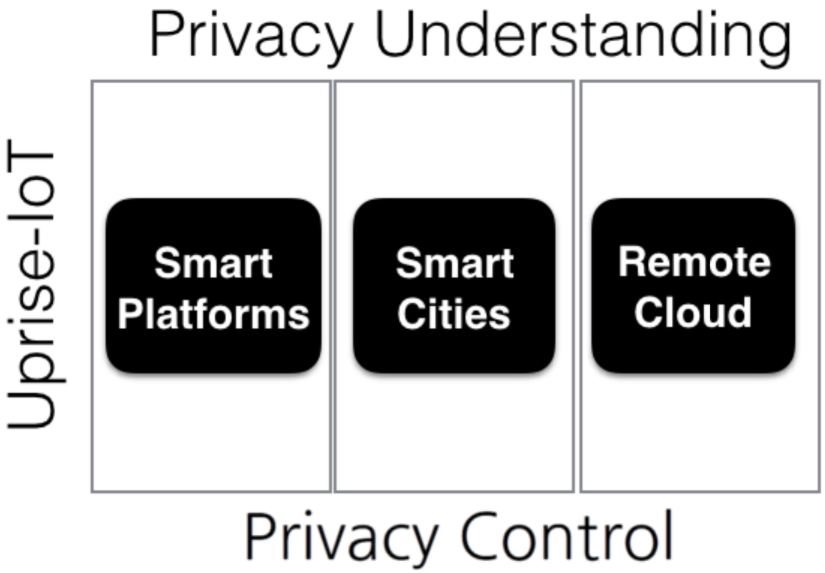
SPIRiT: Security and Privacy foR the Internet of Things

Major Achievements and Outputs

- Comparison of content based on layout done
- Comparison based on text/graphics in progress
- Semantic decomposition of documents
- Global model of the Semantic Firewall done
- Test in real conditions to be conducted soon
- Models for device authentication produced.
- Initial integrator demonstrator developed

UPRISE-IOT: User-Centric PRivacy & Security In The IoT

- Goal: UPRISE-IoT's goal is to let the users gain awareness and control over data generated and collected by the IoT devices surrounding her.
- Create models for describing the current context of the IoT devices
- Create novel strategies to secure IoT.
- Develop tools that will empower users in IoT.
- Increase the user’s awareness.



UPRISE-IOT: User-Centric PRivacy & Security In The IoT

Major Achievements and Outputs

- Strategies to increase privacy awareness & enforce data control
  - Measure the privacy intrusiveness of analytical tools (e.g., ML)
  - Evaluate users' awareness of privacy risks
  - Properly represent & communicate risks to users
  - Communicate intelligible information (related to personal data collection and processing) to data subjects
  - Manage specific and informed consent
- Privacy-Preserving architectural solutions
  - Establishment of trust, service authentication and access control
  - Protection of sensitive and business-critical information
- Design of Privacy Primitives
  - Design primitives to build privacy-by-design IoT systems

http://uprise-iot.supsi.ch/

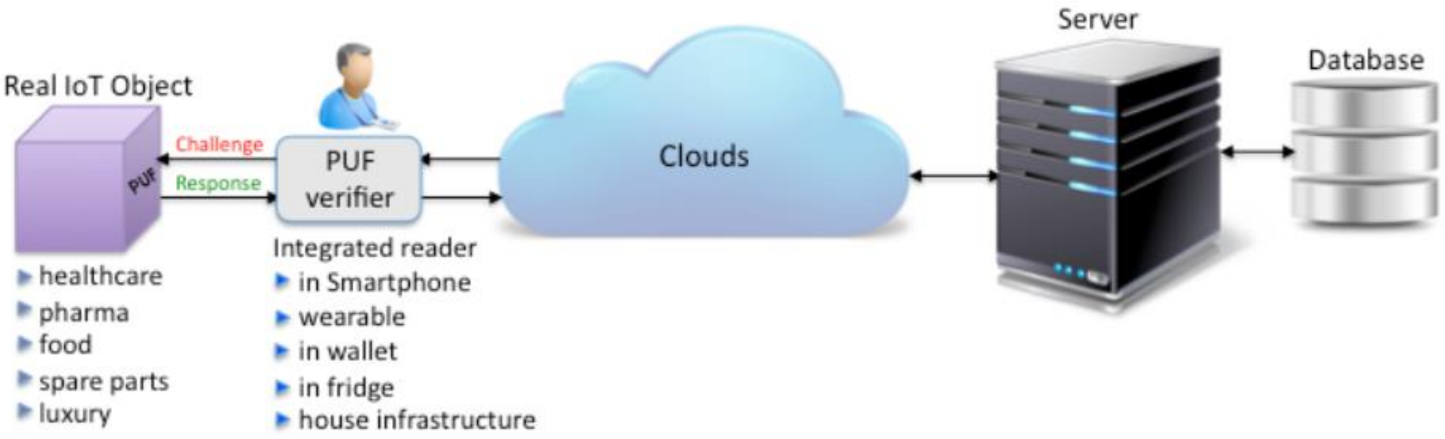
ID-IoT : IDentification for the Internet of Things

IoT problem areas:

- identification/authentication of constrained IoT devices
- scalability problems

Technologies:

- (optical) PUFs, quantum readout
- approximate nearest neighbor search
- scalable signal processing



ID-IoT : IDentification for the Internet of Things

Major Achievements and Outputs

- **Assessing speckle pattern are Physical Unclonable Function (PUF)**
  - Measuring big enough entropy from speckle patterns
- **Privacy-enhancing features extraction from PUF**
  - By quantization, sparsification, and privacy amplification
  - Prevents reconstruction from features
- **Group membership protocols**
  - Provide evidence a device is part of a group without identification
  - Application to biometry and image search (100 M database)
- **Applications of Optical PUF**
  - Quantum Secure Authentification, Key Distribution, and Key Recycling

- **Highlights**
  - “Object identification and authentication”, special session at IEEE WIFS
  - Best C.S. PhD thesis @ University of Rennes 2018
  - Starting collaboration with Airbus on Quantum PUF

USEIT : User Empowerment For Security And PrIvacy In Internet Of Things

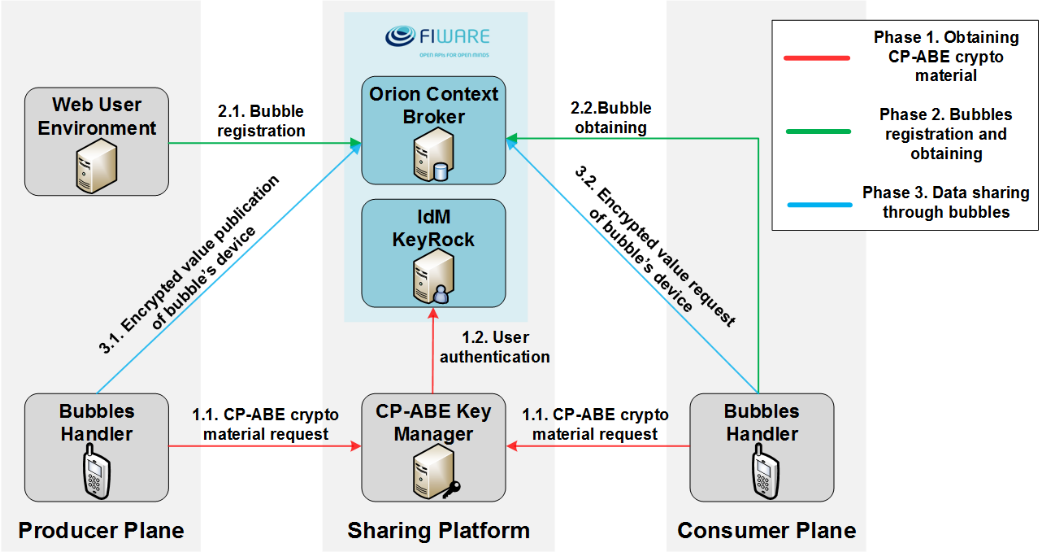
- **USE-IT: U**ser empowerment for **SE**curity and privacy in **I**nternet of **T**hings (http://useit.eu.org)
- **Objective:**
  To let users and devices easily and tightly control who has access to which data in which context, without leaking collateral information such as location or behaviour data.
  - ✓ Design new privacy-preserving authentication and encryption schemes for constrained IoT environments
  - ✓ Create simple policy languages to govern crypto protocols and access control
  - ✓ Develop powerful, flexible, lightweight intrusion detection/ reaction for IoT
- **Partners:**
  - ✓ University of Murcia, ES; IBM Research – Zurich, CH; Commissariat à l'Energie Atomique et aux Energies Alternatives (CEA), FR; Technical University Eindhoven (TUE), NL:

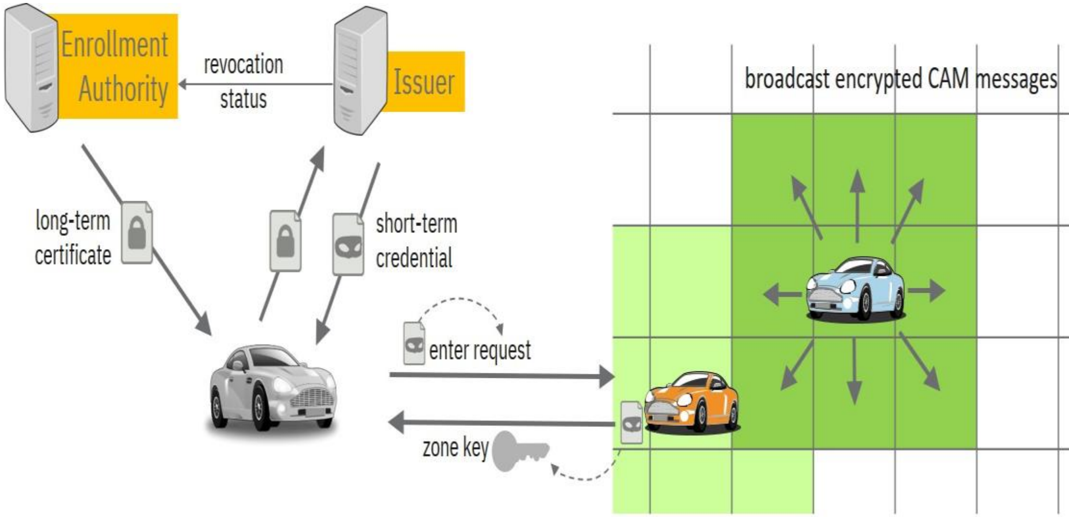
chist-era

USEIT :User Empowerment For Security And PrIvacy In Internet Of Things

Major Achievements and Outputs

- ❖ Users empowerment through the use of encryption-based selective disclosure and policy-based approaches
- ❖ Design of flexible and scalable cryptographic mechanisms to enable a secure IoT-enabled data sharing platform
- ❖ Proxy-based Attribute-based re-Encryption approach
- ❖ Providing advanced and lightweight cryptographic schemes to be used in C-ITS scenarios
- ❖ Privacy-friendly authentication when entering a new zone & receiving zone key


FIWARE
Web User Environment
2.1. Bubble registration
Orion Context Broker
2.2.Bubble obtaining
IdM KeyRock
3.1. Encrypted value publication of bubble's device
3.2. Encrypted value request of bubble's device
1.2. User authentication
Bubbles Handler
1.1. CP-ABE crypto material request
CP-ABE Key Manager
1.1. CP-ABE crypto material request
Bubbles Handler
Producer Plane
Sharing Platform
Consumer Plane
Phase 1. Obtaining CP-ABE crypto material
Phase 2. Bubbles registration and obtaining
Phase 3. Data sharing through bubbles

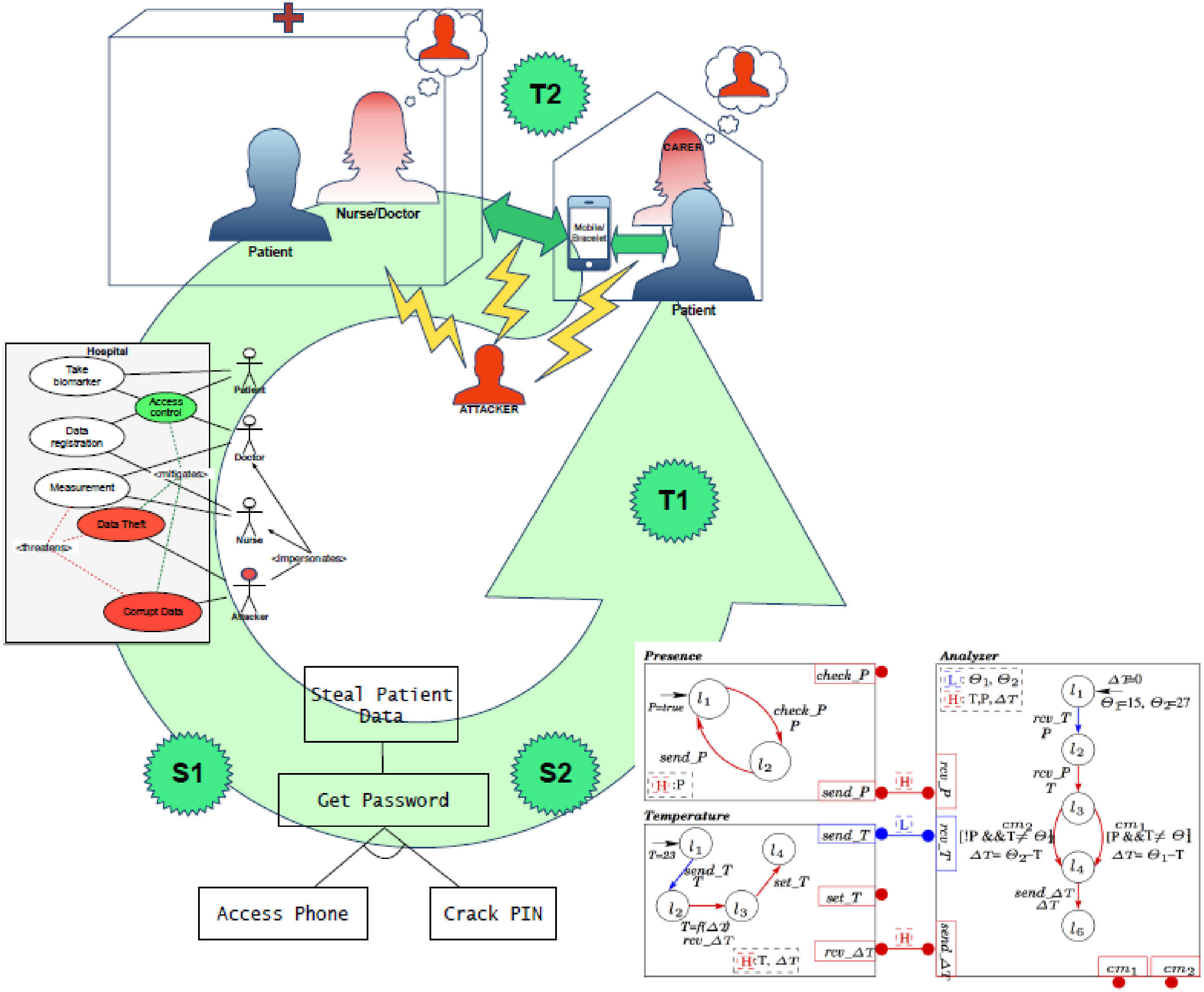


SUCCESS: SecUre ACCESSibility For The Internet Of Things

Overview/Main Goals: SUCCESS, Secure Accessibility for the IoT

- Formal design of privacy-critical IoT scenario
- Risk visualisation by attack tree analysis
- Certified implementation for IoT component architectures
- IoT Pilot scenario: sensor based monitoring for Alzheimer’s patient

SUCCESS: SecUre ACCESSibility For The Internet Of Things



SUCCESS: SecUre ACCESSibility For The Internet Of Things

Major Achievements and Outputs

- Pilot infrastructure fully functional
- Security Engineering process is defined in Isabelle (Refinement-Risk Loop)
- BIP methodology extended and Toolchain implemented: Attack Trees and Probabilistic Modelchecking for IoT systems
- ATTop tool provides translation of Attack Trees between different modeling languages

COCOON: Emotion Psychology Meets Cyber Security In IoT Smart Homes

„In Cocoon, we want to understand and build from the User's experience, as a central part in the definition of intrusion detection systems"

Objectives:

- Examine the User's emotional experience
- Put mainstream IoT to the test & develop a new kind of IDS

Major Achievements and Outputs

- 2000 Participants took part in series of studies to understand experience of victims of cybercrime

Topic Challenges and Needs

- To reach out to the stakeholders to validate our visions
- Certified code generation for IoT devices from component specifications
- Quality and instability of data
- Need to define guidelines for common strategy on data generation and metrics
- Need for new lightweight cryptography for constrained small devices
- Synergy between IDS and reaction system
- Empower users ability to effectively control their data

Possible Roadmap and Role of the CHIST-ERA support

- Stress out the importance of the SPTIoT topic as complementary technologies with respect to blockchain for security and privacy of user data

- Agreement on publishing a book on SPTIoT topic

- Adressing the policy makers on the EU level to include SPTIoT topic in the next Framework programme

Questions

Questions ?