PIVOT: Privacy-Integrated design and Validation in the constrained IoT

https://pivot-project.info/

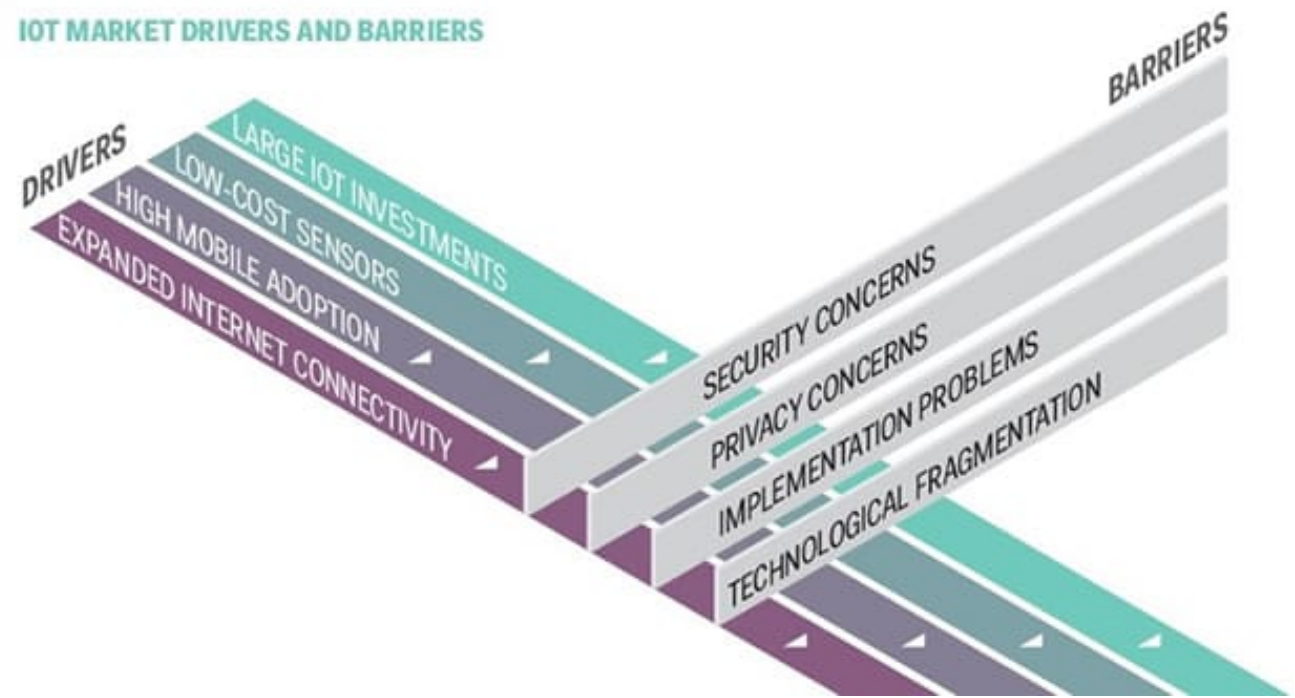
WISG (25-26 January 2022)

SPONSORED BY THE
Federal Ministry of Education and Research
Agence Nationale de la Recherche ANR

Agenda

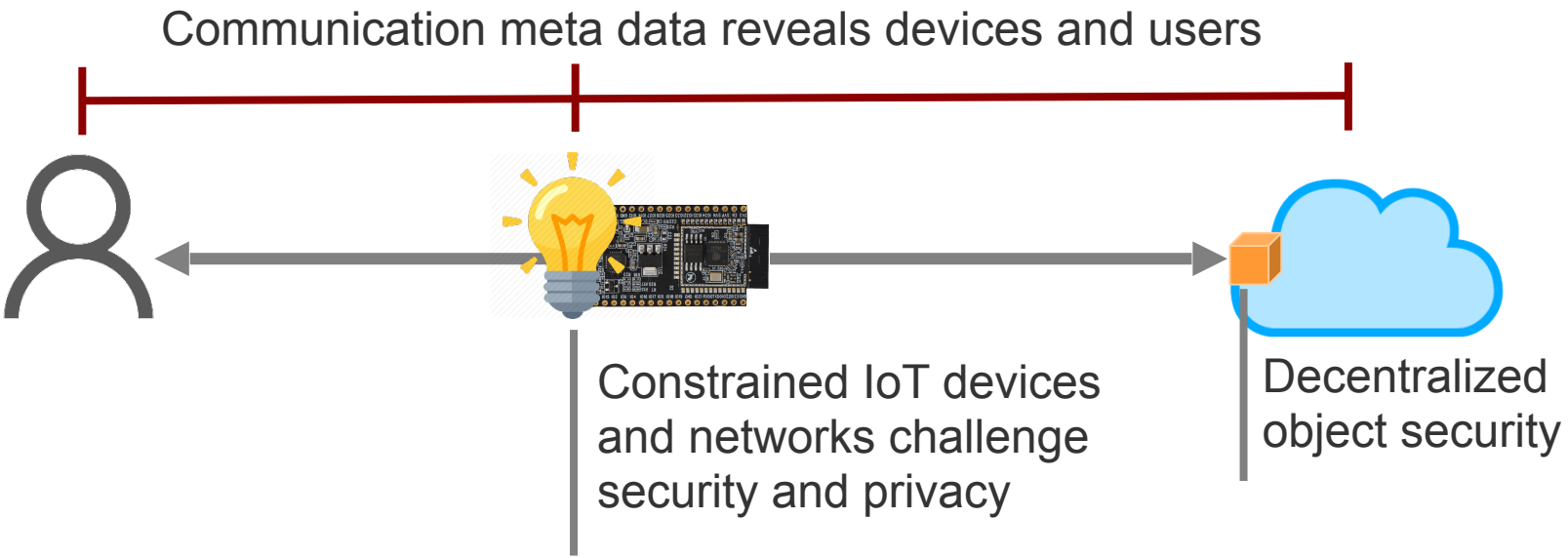
- Technological Challenges
- Objectives
- Consortium Complementarity
- First Results

PIVOT focuses on overcoming the following IoT barriers



Source: IoT market drivers and barriers – source Digitize or Die

Technological challenges



Our objectives in PIVOT

Privacy for constrained IoT devices

Decentralized object security

Minimal trust anchor provisioning

Multi-stake holder namespace management

Proposed building blocks

Privacy for constrained IoT devices	Decentralized object security	Minimal trust anchor provisioning	Multi-stake holder namespace management
Based on an open crypto framework	Designing protocols and architectures	To allow for constrained resources	Global and scalable

Standardization

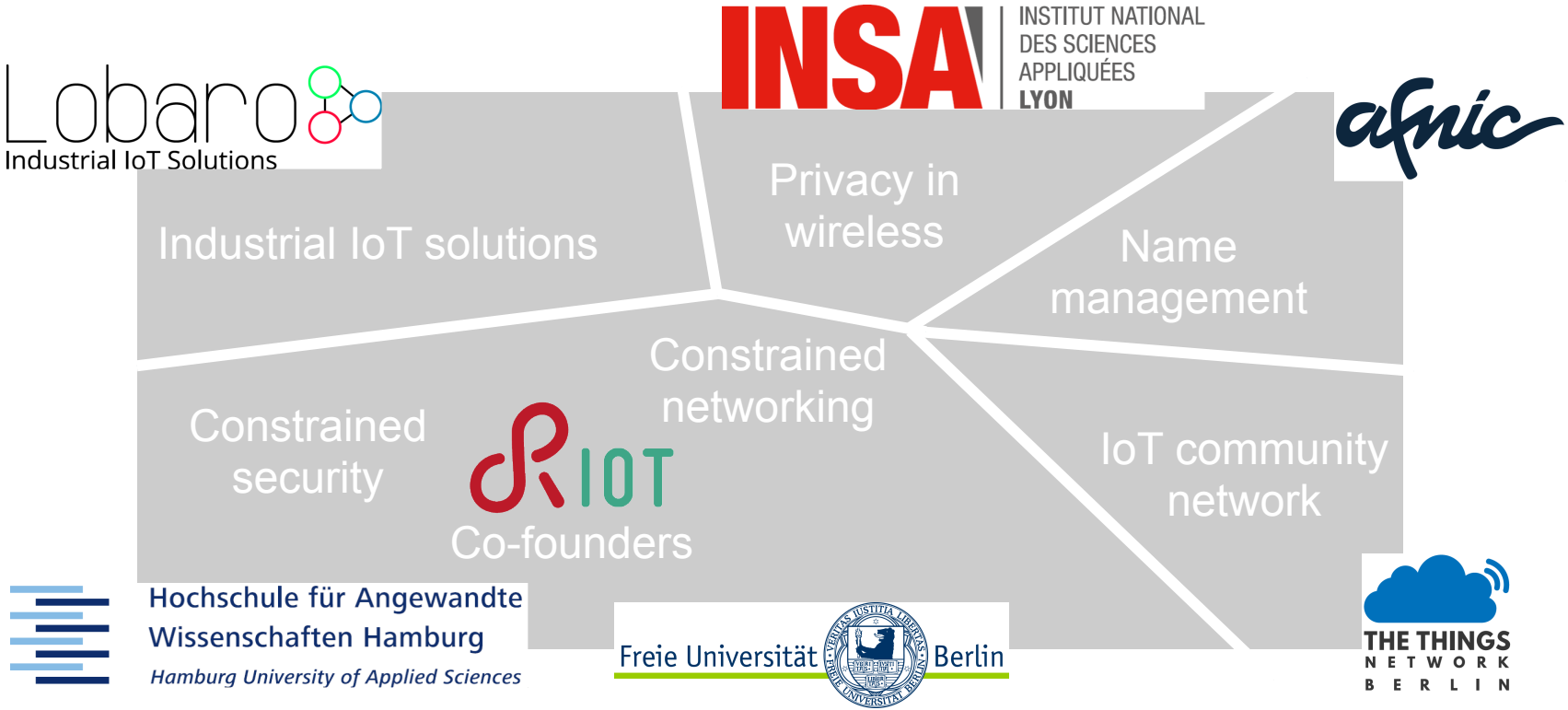
Evaluation



Demonstrator

Field tests

Consortium complementarity



First results

ACM Computing Surveys

2019 Impact Factor: 7.990
CORE2020: A*

112

A Guideline on Pseudorandom Number Generation (PRNG) in the IoT

PETER KIETZMANN and THOMAS C. SCHMIDT, HAW Hamburg, Germany
MATTHIAS WÄHLISCH, Freie Universität Berlin, Germany

published in vol. 54, no. 6, article 112, July 2021.
Online: https://doi.org/10.1145/3453159

IETF®

Internet standardization

CoRE
Internet-Draft
Intended status: Standards Track
Expires: 28 April 2022

M.S. Lenders
FU Berlin
C. Amsüss

C. Gündoğan
T.C. Schmidt
HAW Hamburg
M. Wählisch
FU Berlin
25 October 2021

DNS Queries over CoAP (DoC)
draft-lenders-dns-over-coap-02

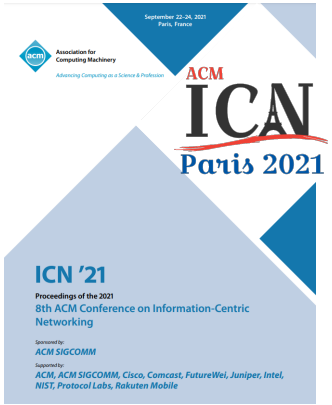
https://datatracker.ietf.org/doc/html/draft-lenders-dns-over-coap

First results

IEEE Access

Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

2019 Impact Factor: 3.367



Acceptance rate: 25%

Fragment Forwarding in Lossy Networks

MARTINE S. LENDERS[1], THOMAS C. SCHMIDT[2], (Member, IEEE), AND MATTHIAS WÄHLISCH[1], (Member, IEEE)
[1]Department of Mathematics and Computer Science, Freie Universität Berlin, 14195 Berlin, Germany
[2]Department Informatik, HAW Hamburg, 20099 Hamburg, Germany
Corresponding author: Martine S. Lenders (m.lenders@fu-berlin.de)

This work was supported in part by the German Federal Ministry of Education and Research within the projects RAPstore and PIVOT, and in part by the Open Access Publication Fund of the Freie Universität Berlin.

published in vol. 9, October 2021.

Online: https://doi.org/10.1109/ACCESS.2021.3121557

Reliable Firmware Updates for the Information-Centric Internet of Things

Cenk Gündoğan
HAW Hamburg
cenk.guendogan@haw-hamburg.de

Christian Amsüss
christian@amsuess.com

Thomas C. Schmidt
HAW Hamburg
t.schmidt@haw-hamburg.de

Matthias Wählisch
Freie Universität Berlin
m.waehlisch@fu-berlin.de

ABSTRACT

Security in the Internet of Things (IoT) requires ways to regularly update firmware in the field. These demands ever increase with new,



Online: https://doi.org/10.1145/3460417.3482974

OLD

Technological Challenges

- Protecting the IoT device identity from divulgating the person behind the identifier
- Divulgating the metadata information as and where needed
- Handling object security in a decentralized manner
- Standardised crypto library framework
- Constrained IoT devices & networks

Our objectives in PIVOT

- Design an open crypto framework to build privacy for constrained IoT devices
- Advance protocols and architectures that integrate decentralized object security
- Minimal trust anchor provisioning on IoT devices to enable object security
- Design a global and scalable multi-stake holder namespace management for IoT data

Proposed building blocks (Work Packages)

- Establishing the design framework
- Crypto tool box
- Multi-stakeholder Name Management
- Content Object Security framework
- Integrated protocol stack
- Demonstrator, field tests and evaluation
- Standardization and implementation in RIOT OS