HELSINKI
INSTITUTE FOR
INFORMATION
TECHNOLOGY

Securing Interactions of Smart Objects in Smart-M3 Spaces

Ilya Nikolaevskiy, Andrei Gurtov, Dmitriy Korzun

Aalto University

UNIVERSITY OF HELSINKI

Table of Contents

- Smart objects in Mobile Health (mHealth) scenarios
- Smart-M3 drawbacks
- Host Identity Protocol
- Implementation
- Conclusion

HELSINKI INSTITUTE FOR INFORMATION TECHNOLOGY

Smart Objects in mHealth

- On-body/implantable sensors
- Mobile gateway
  - Internet connection
- Back-end service
  - Medical personnel, data storage

Smart Objects in mHealth (cont'd)

- Data from sensors is sent to back-end service via gateway
- Gateway possesses limited storage and computational capabilities
  - Able to make conclusions without Internet connection with back-end

Smart-M3

- Existing solution for information sharing between Smart Objects
- Semantic data enables portable devices to process data locally easily

Problems

- Privacy
  - No encryption
  - Sensitive patients data is easy to intercept
- Security
  - No access control
  - Adversary may gain control over patients' devices

Host Identity Protocol

- New Internet Protocol Stack waist
- Security association establishment procedure: HIP Base Exchange (BEX), HIP Diet Exchange (DEX)
- All communications are secured by symmetric cryptography
- DoS resistant (Cryptographic puzzle)

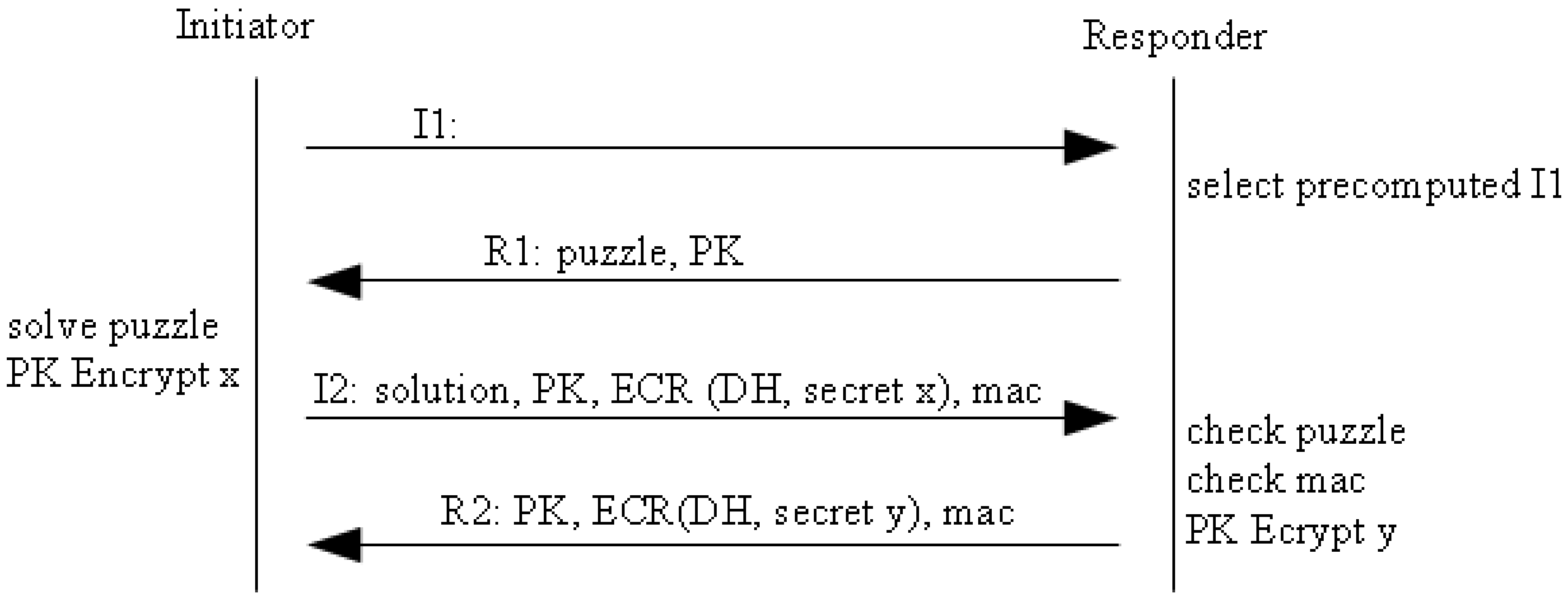
HELSINKI
INSTITUTE FOR
INFORMATION
TECHNOLOGY

BEX vs. DEX

	DEX	BEX
Total packets	4	4
Total bytes	528	~1500
Key exchange	Fixed ECDH	ECDH
MAC	CMAC (AES-CBC)	SHA-1
Hash function	No	SHA-1
Encryption	AES-CBC	AES-CBC, 3DES-CBC, BLOWFISH-CBC

DEX requires less hardware capabilities but provides less flexibility and security level

HIP DEX


Initiator
Responder
I1:
select precomputed I1
R1: puzzle, PK
solve puzzle
PK Encrypt x
I2: solution, PK, ECR (DH, secret x), mac
check puzzle
check mac
PK Ecrypt y
R2: PK, ECR(DH, secret y), mac

HIP in Smart-M3

- Knowledge Processor (KP) is Initiator (Small agent generating and processing data)
- Semantic Information Broker (SIB) is Responder (Stores and manages data in Resource Description Framework representation)

HELSINKI
INSTITUTE FOR
INFORMATION
TECHNOLOGY

Smart-M3 Architecture

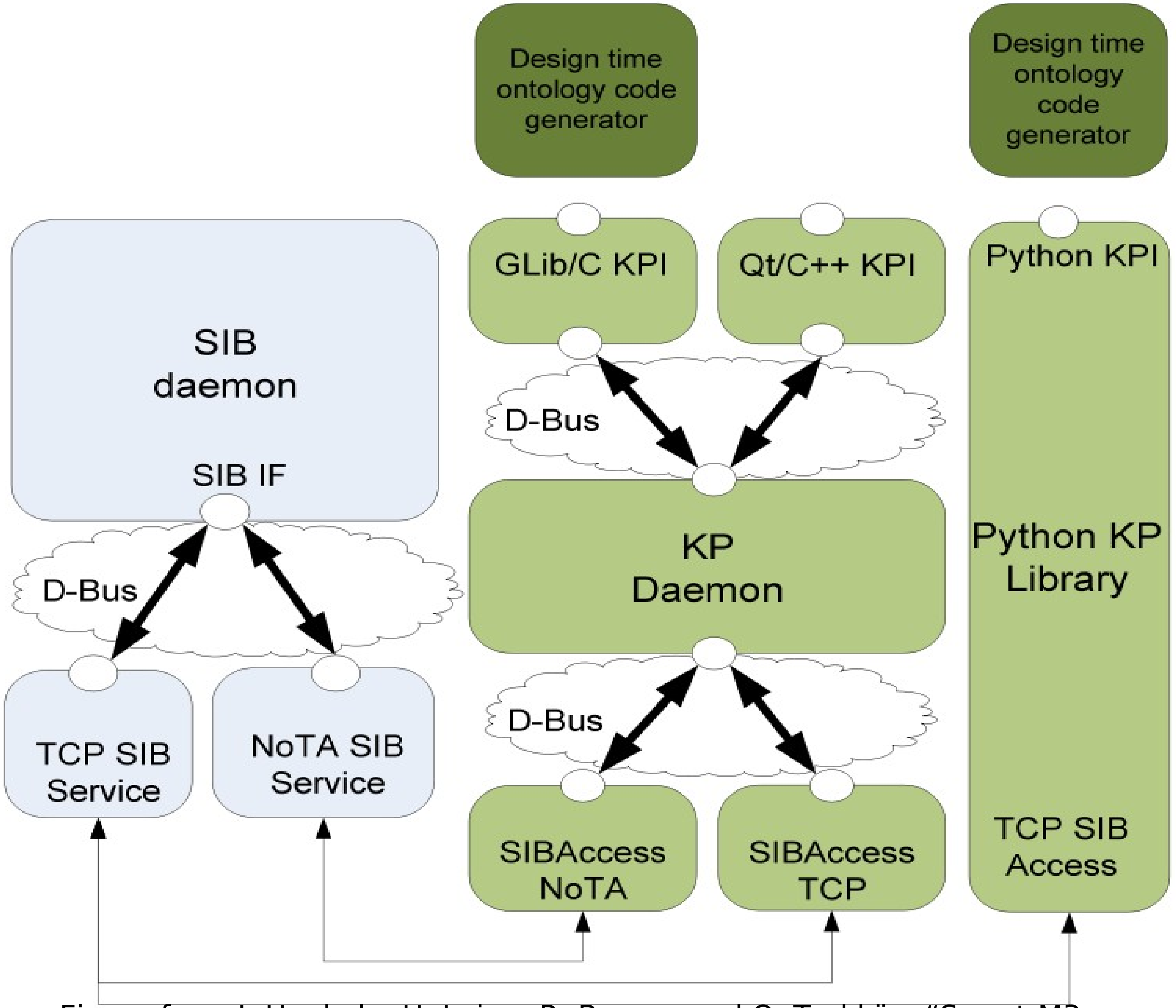


Figure from J. Honkola, H. Laine, R. Brown, and O. Tyrkk¨o, “Smart-M3 information sharing platform,” in Proc. IEEE Symp. Computers and Communications, ser. ISCC ’10.

Smart-M3 Architecture

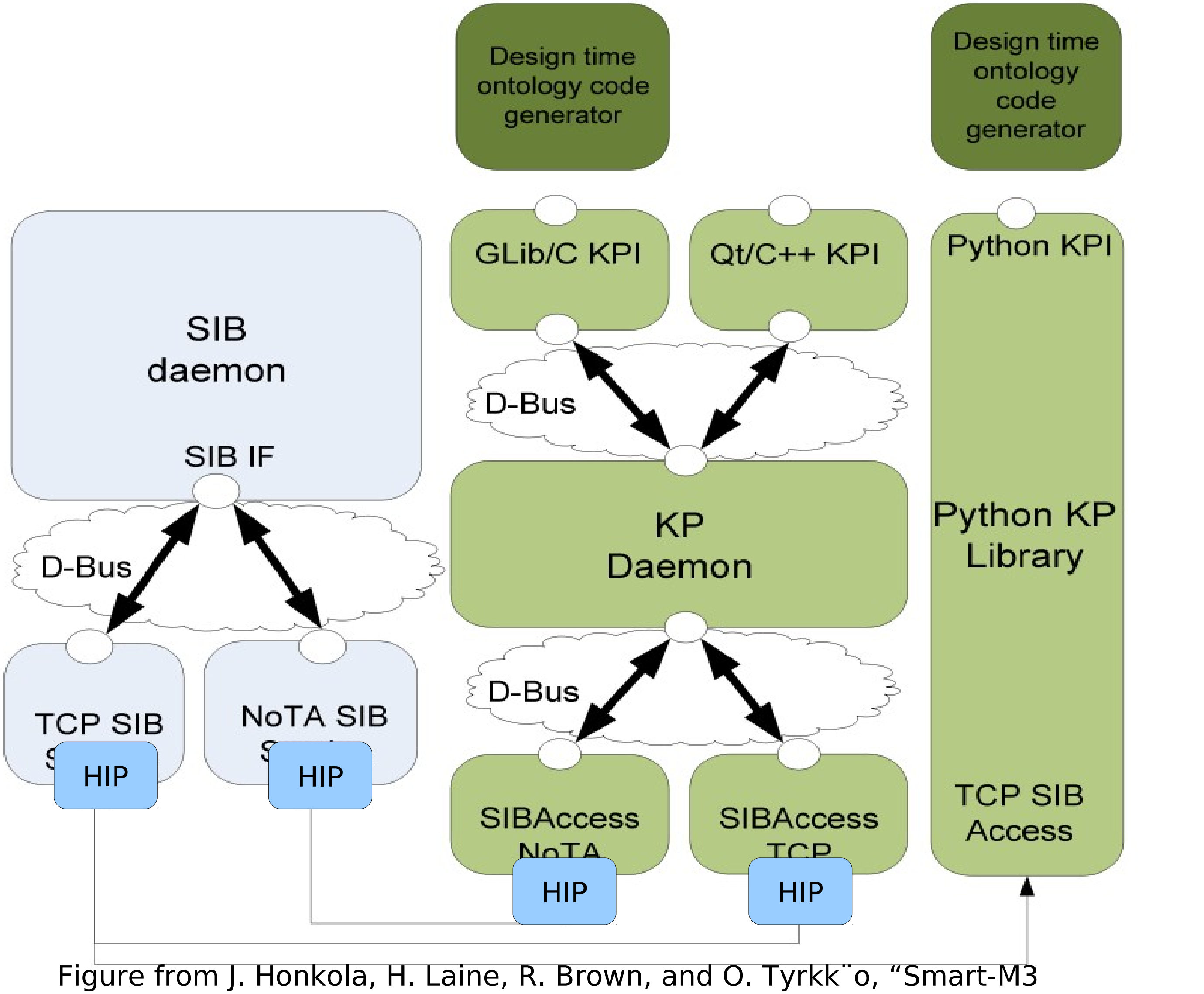


Figure from J. Honkola, H. Laine, R. Brown, and O. Tyrkk¨o, “Smart-M3 information sharing platform,” in Proc. IEEE Symp. Computers and Communications, ser. ISCC ’10.

Implementation

- HIP DEX to establish secure communication
- AES-CBC encryption between KP and SIB
- Based on ANSI C KPI
- Based on sib-tcp module from RedLand SIB
- Implementation is based on HIP-DEX++ library

Conclusion

- Implemented secure TCP KP and SIB communication
- Future plans
  - Implement Secure NoTA access
  - Another encryption options
  - IPSec support for capable devices
  - Utilization of HIP identities for access control

HELSINKI INSTITUTE FOR INFORMATION TECHNOLOGY

Thank you for your attention!

Questions?

HELSINKI
INSTITUTE FOR
INFORMATION
TECHNOLOGY