HELSINKI INSTITUTE FOR INFORMATION TECHNOLOGY

Security and Smartness for Medical Sensor Networks in Personalized Mobile Health Systems

I. Nikolaevskiy, D. Korzun, **Andrei Gurtov**
Aalto University

23.04.2014

FRUCT'15

HELSINKI INSTITUTE FOR INFORMATION TECHNOLOGY

Motivation for Medical ICT

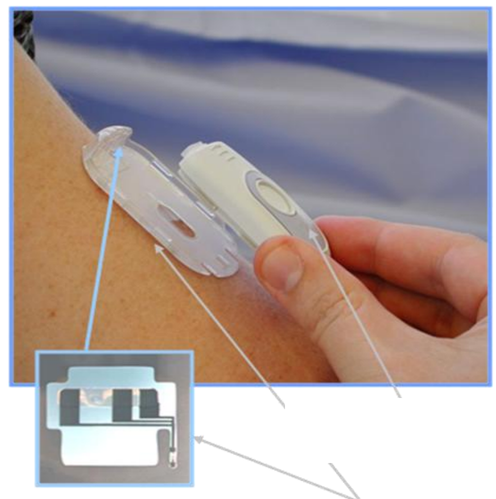
Population gets older, high costs of medical care

Insulin pumps, Implanted Cardio Defibrillators could be monitored remotely

Threatening state of security in current medical devices

- Demonstrated remote triggering of heart shock

How to combine security with limited hardware and battery capabilities?



HELSINKI INSTITUTE FOR INFORMATION TECHNOLOGY

Two Related Devices for Diabetics

Continuous Glucose Monitors (CGM)

- Small wire in tissue to measure electrical elements of fluid
- Graphs sugar values over time
- Transmits data blindly over wireless
- Better than urine tasting ☺

Insulin Pump

- Insulin delivered through tubing attached to body
- Tubing replaced every 3 days
- Special USB dongles used to program Insulin Pumps and download history data
- Devices not designed to be updated. No way of patching. 5+ year lifespan.

Both Devices Hacked by J. Radcliff

- Using patents and FCC specs
- Publicly available equipment
- Acquire ”root” access to devices up to 30 m
- Requires finding out device serial number
- No built in security!

Enabling logging gives out packet structure

Currently some human participation is needed, in future ’Artificial Pancreas’ project will be bring CGM-pump automatic connection

Hacker Shows Off Lethal Attack By Controlling Wireless Medical Device

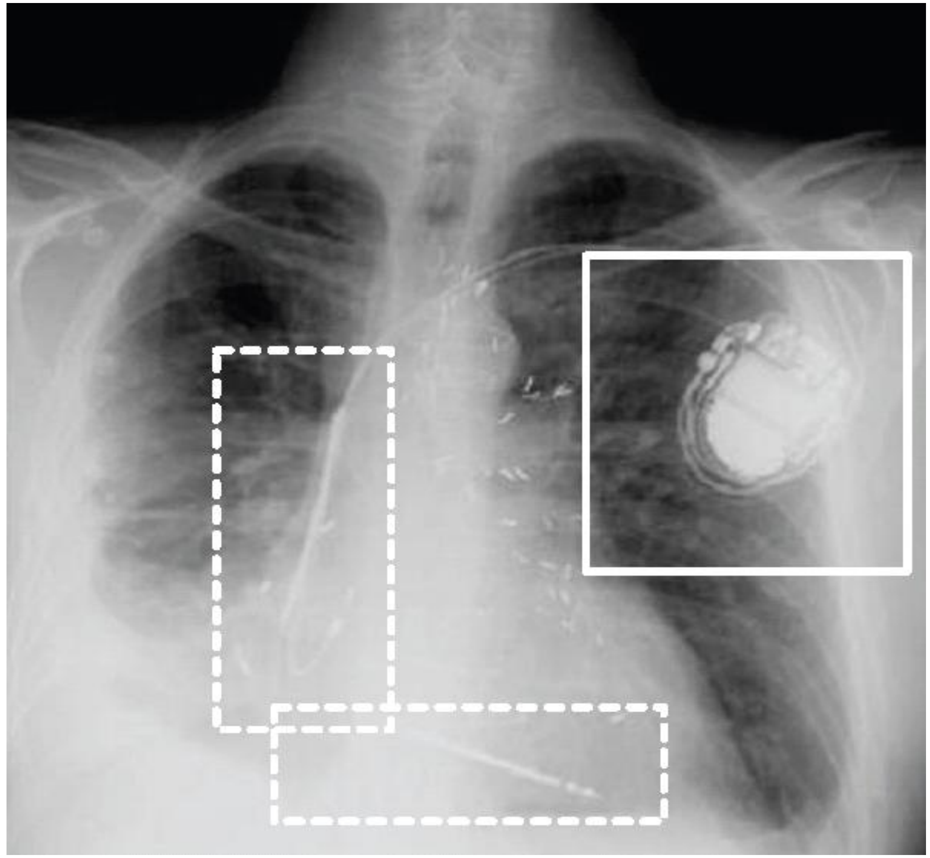
Barnaby Jack has discovered a way to
scan a public space from up to 300 feet away, find vulnerable pumps made by Minneapolis-based Medtronic Inc., and force them to dispense fatal insulin doses. Jack doesn't need to be close to the victim or do any kind of extra surveillance to acquire the serial number, as Jay Radcliffe did.

Demonstrated Attack on IMDs

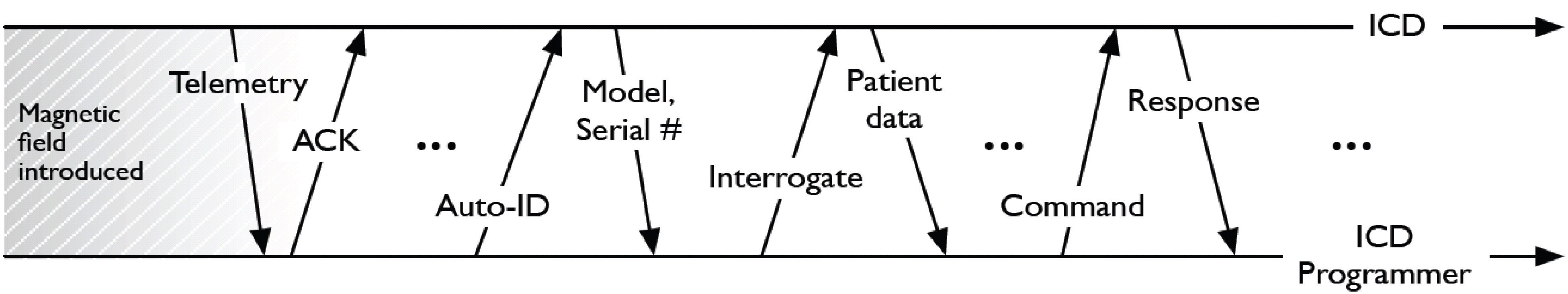
Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses

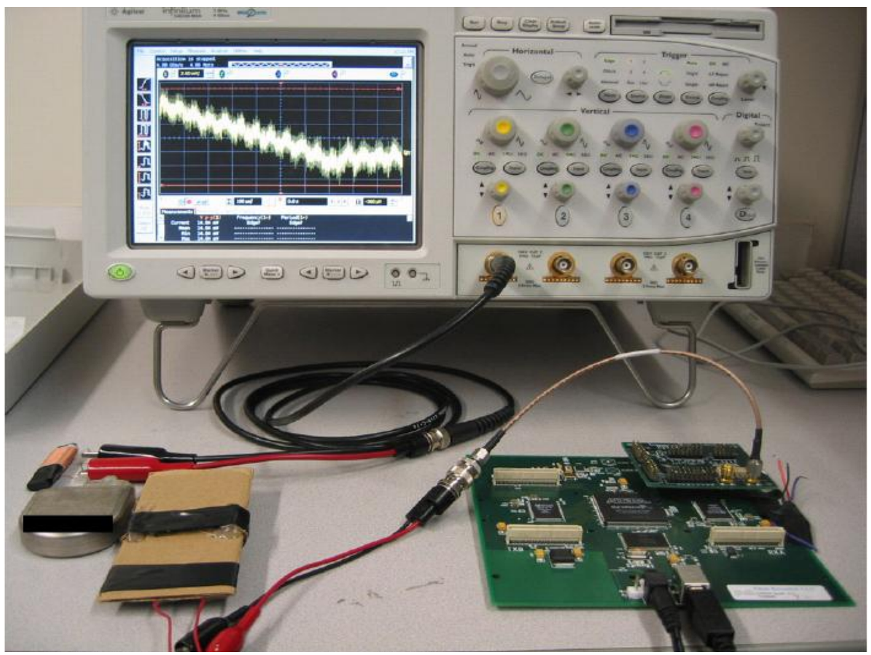
Daniel Halperin, Thomas S. Heydt-Benjamin, Benjamin Ransford, Shane S. Clark, Benessa Defend, Will Morgan, Kevin Fu, Tadayoshi Kohno, and William H. Maisel

IEEE Symposium on Security and Privacy, May 2008



Decoded Plain-text Communication Protocol

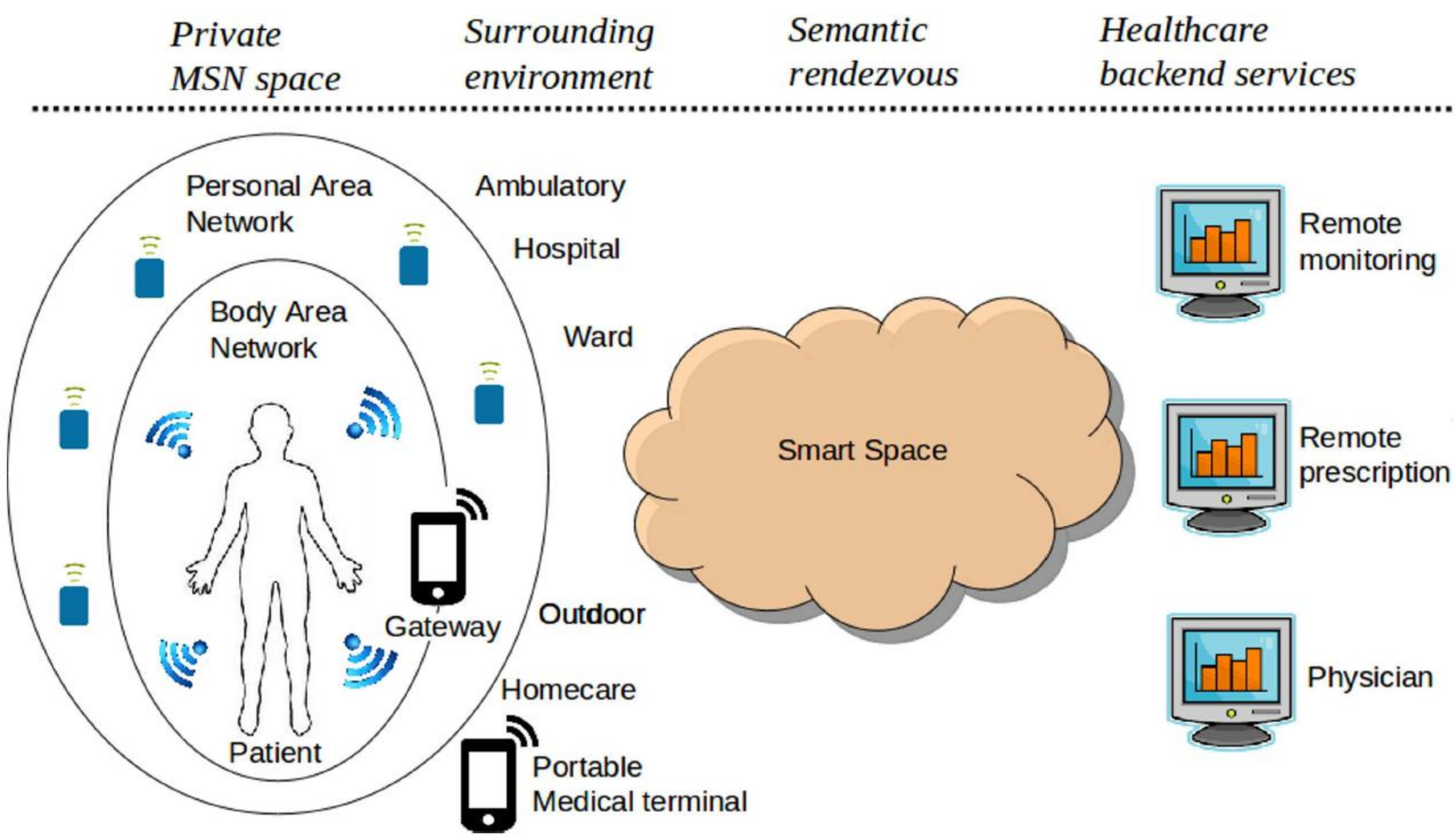




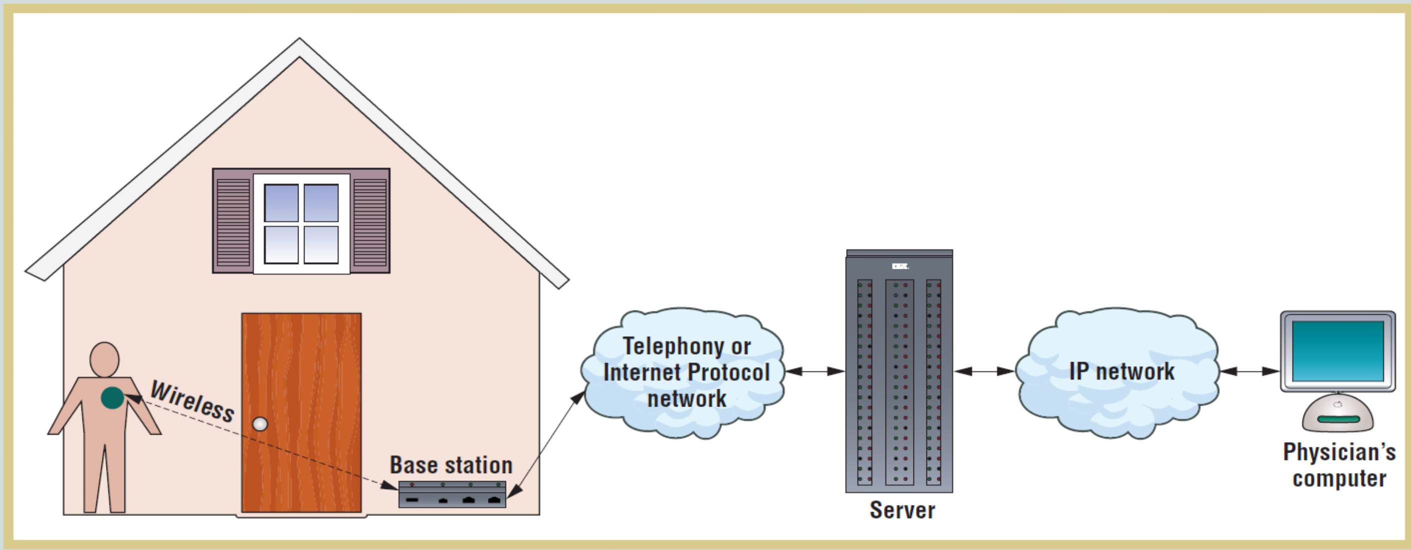
Demonstrated Attacks on Implanted Cardio Defibrillator

	Commercial programmer	Software radio eavesdropper	Software radio programmer	Primary risk
Determine whether patient has an ICD	✔	✔	✔	Privacy
Determine what kind of ICD patient has	✔	✔	✔	Privacy
Determine ID (serial #) of ICD	✔	✔	✔	Privacy
Obtain private telemetry data from ICD	✔	✔	✔	Privacy
Obtain private information about patient history	✔	✔	✔	Privacy
Determine identity (name, etc.) of patient	✔	✔	✔	Privacy
Change device settings	✔		✔	Integrity
Change or disable therapies	✔		✔	Integrity
Deliver command shock	✔		✔	Integrity

Medical Smart Space Architecture



Remote Monitoring Architecture



Hybrid IPless/IP architecture based on Host Identity Protocol (HIP)

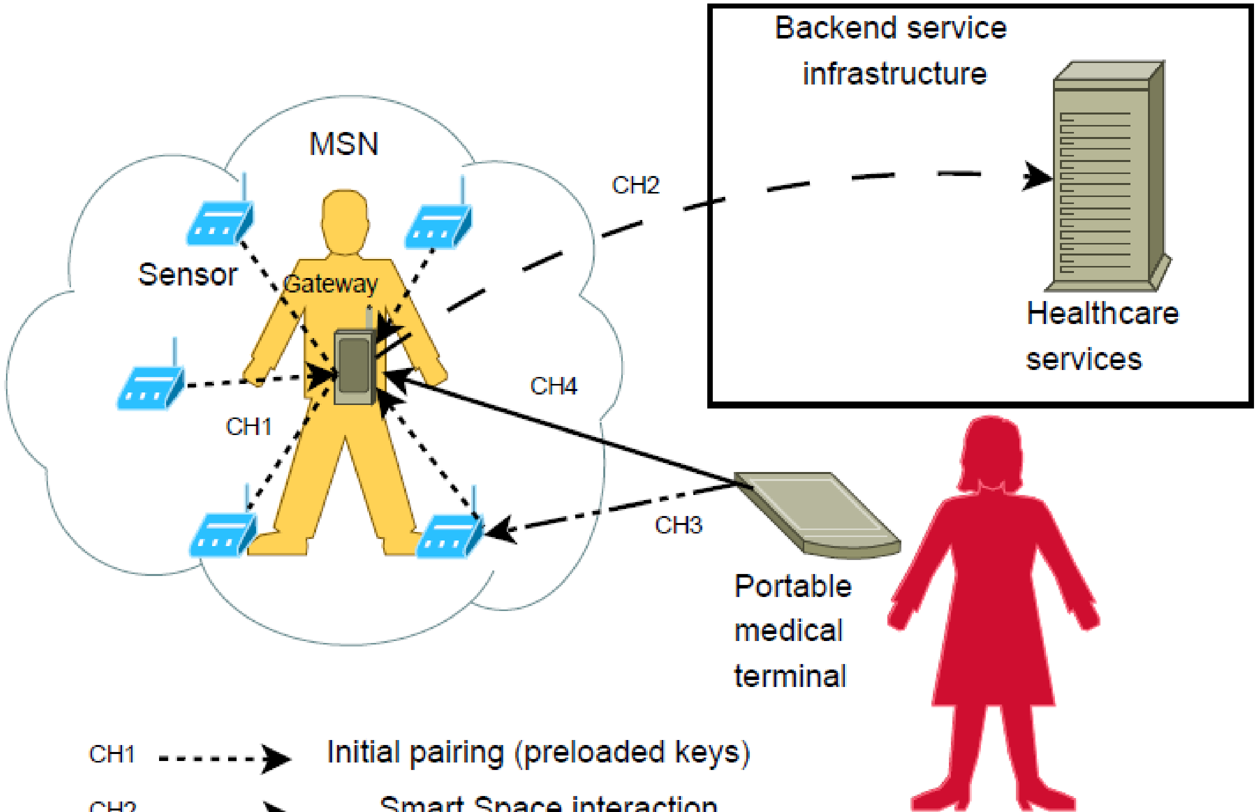
Use of a mobile phone as a secure gateway for connecting personal devices to Internet

Secure key exchange

Trust management and revocation infrastructure

Emergency access; Secure key storage; Preserving battery

Communication Channels



CH1 - - - - → Initial pairing (preloaded keys)

CH2 — → Smart Space interaction

CH3 — - - → Pairing with sensors (fallback mode)

CH4 ——→ Pairing with gateway (normal operational mode)

Properties of the Channels

	Assumptions	Requirements	Solution
CH1: Gateway to sensors	The channel is established in the controlled environment when devices are installed		Preshared keys, installed during devices configuration by medical personnel or by manufacturer
CH2: Gateway to backend	The gateway is a powerful enough device; the gateway has an Internet access	Strong security level	Standard Host Identity Protocol (HIP) [9]
CH3: PMT to sensors	Sensors are constrained devices	Lightweight key exchange scheme; Mutual authentication	Custom lightweight key exchange protocol, as defined in section 3.2
CH4: PMT to Gateway	TH medical terminal has only a short range radio interface	Mutual authentication	The same key exchange scheme as in channel CH3

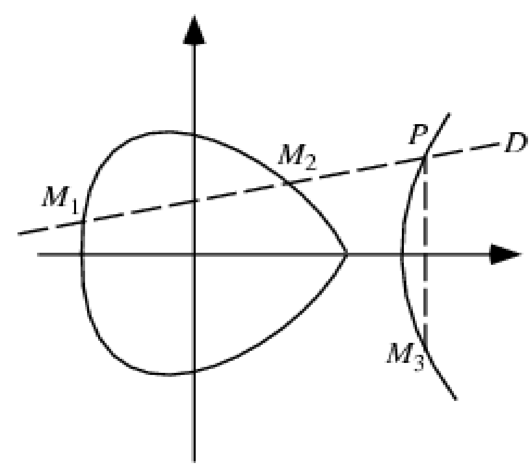
Host Identity Protocol (HIP) in a Nutshell

- HIP Base Exchange (BEX) – end-to-end key exchange protocol
- 4-way handshake (I1, R1, I2, R2 packets):
  - Mutual authentication with DSA/RSA signatures
  - Protection against DoS with puzzles
  - Key exchange with Diffie-Hellman (DH)
- HIP Diet Exchange (DEX) is a lightweight version
  - No signatures – fixed Elliptic curve DH (ECDH) keys are used instead
  - No hash functions

Duration of HIP Base Exchange (BEX)

- Basic HIP uses heavyweight RSA/DSA cryptography
- Association establishment can take up to a second even on regular PC
- Small devices have very restricted capabilities
- The use of Elliptic Curve Cryptography (ECC) is almost mandatory

Authentication	Session Key	BE
RSA1024	DH1536	275 ms
RSA1024	ECDH192	39 ms
ECDSA160	ECDH192	33 ms
RSA2048	DH2048	747 ms
RSA2048	ECDH224	187 ms
ECDSA224	ECDH224	129 ms



Security Properties of ECC and HIP BEX

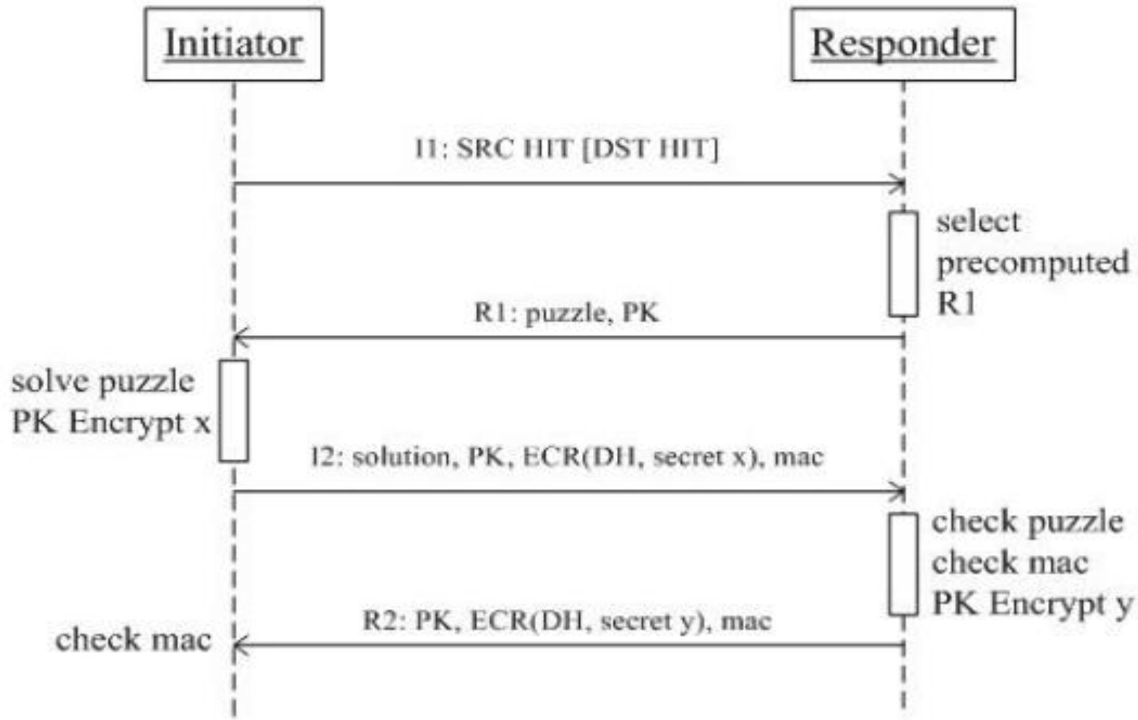
- ECC offers same cryptographic strength with almost order of magnitude less space
- HIP BEX requires signature operations and Diffie-Hellman key exchange

Security level	ECC	DSA/RSA
80	160	1024
112	224	2048
128	256	3072
192	384	7680
256	512	15360

Message	Initiator	Responder
I1	-	-
R1	verify, DH_compute_key	sign
I2	sign	verify, DH_compute_key
R2	verify	sign
CLOSE	sign	verify
CLOSE_ACK	verify	sign
Total	$2 \times T_{sign} + 3 \times T_{verify} + T_{dh}$	$3 \times T_{sign} + 2 \times T_{verify} + T_{dh}$
Only Base Exchange	$T_{sign} + 2 \times T_{verify} + T_{dh}$	$2 \times T_{sign} + T_{verify} + T_{dh}$

HIP Diet Exchange (DEX)

- Four-way handshake protocol proposed by Robert Moskowitz
- Packet size [40, 216)
  - Fragmentation needed
- Security primitives:
  - Puzzle
  - ECDH
  - AES encryption
  - CMAC

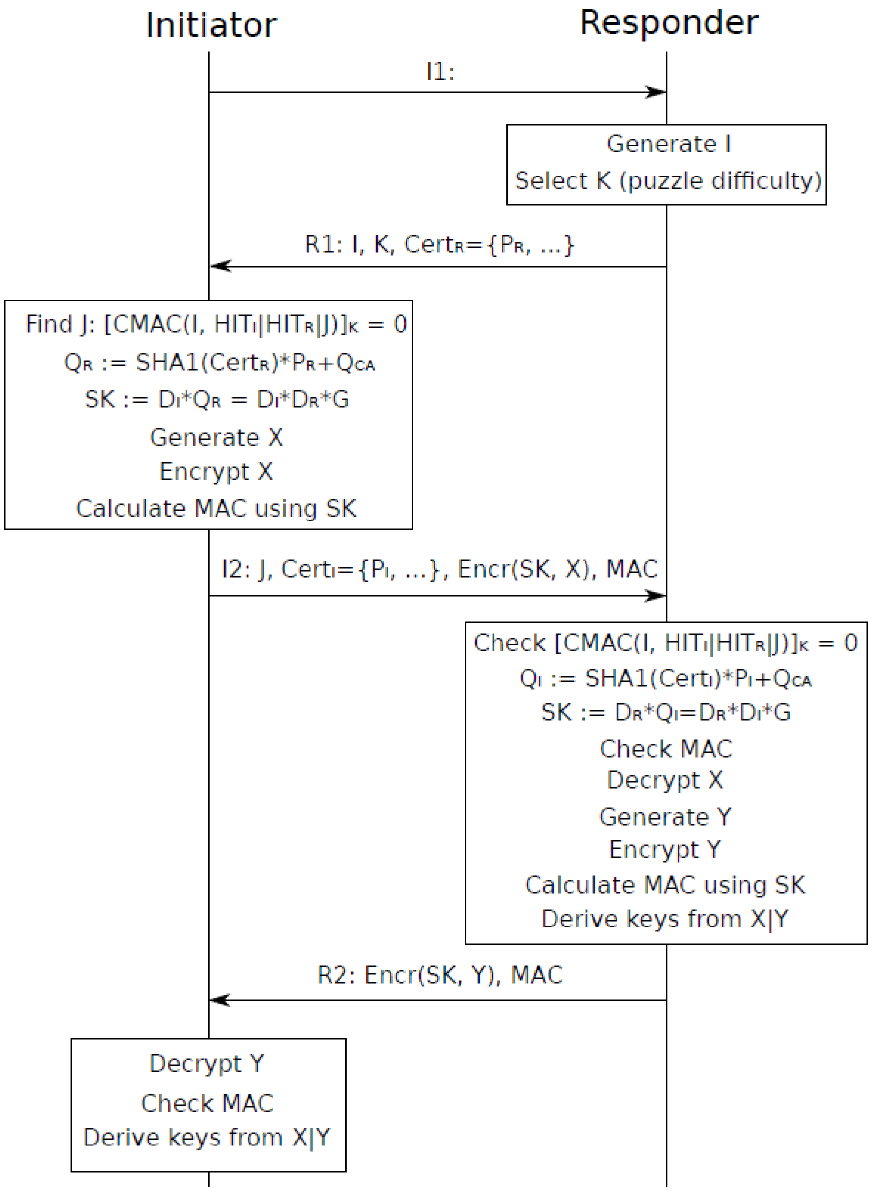


Security analysis of HIP DEX

Protection against six attack models

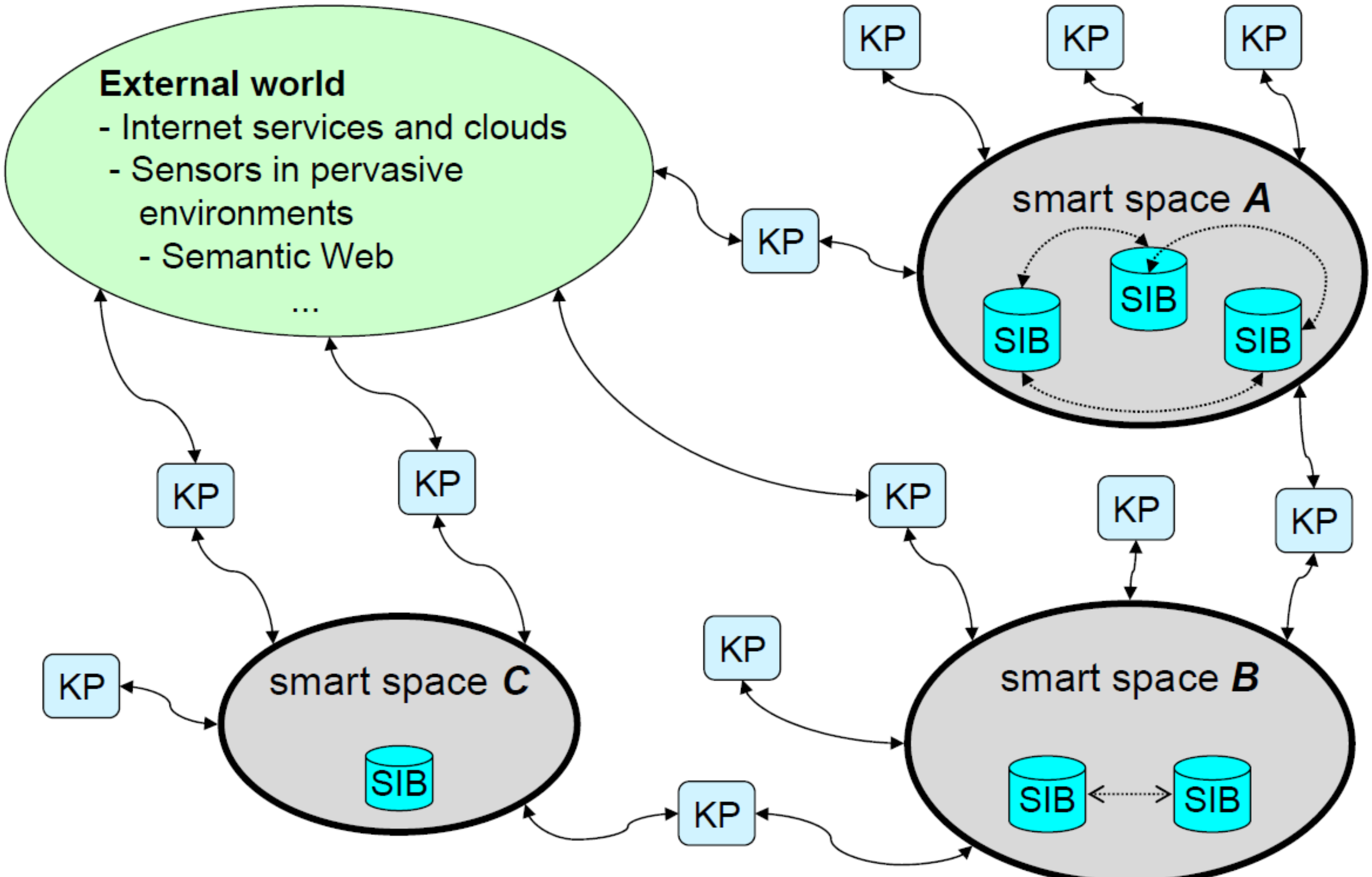
Radio jamming:	None
Packet DoS attack:	Puzzle
Replay attack:	Nonce + CMAC
Spoofing/Sybil attack:	Password authentication
Message eavesdropping:	AES encryption
Man-in-the-middleware/wormhole:	ECDH

Proposed Authentication Protocol HIP DEX + implicit certs



HELSINKI INSTITUTE FOR INFORMATION TECHNOLOGY

Smart M3: Knowledge Processors&Semantic Information Brokers



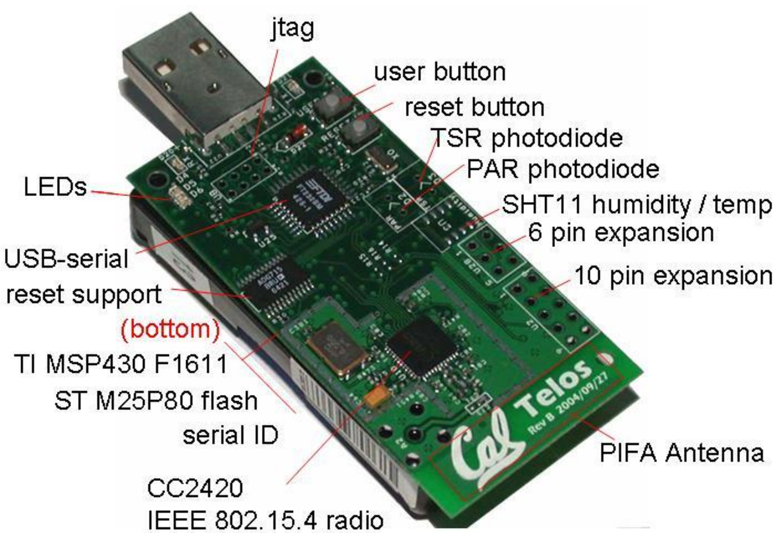
HELSINKI INSTITUTE FOR INFORMATION TECHNOLOGY

Knowledge Processors in Medical Smart Space

KP Type	Device	Role
MSN data collector	Gateway, PMT	KP collects health data from the patient and publishes to its smart space.
Service	Backend server	KP activates appropriate service and mediator KPs to construct the service when there are clients. Its outcome is semantically represented in the smart space for client KPs.
Mediator	Backend server	KP runs appropriate data processing over its database and makes the outcome semantically represented the smart space.
UI agent	Gateway, PMT	KP shows results from the healthcare services to the user based on current situation in the smart space and at the patient side.

Device Characteristics

Resource	TelosB	MAXQ2010	Imote2
RAM	10kB	2kB	256kB
ROM	48kB	64kB	32MB
CPU	16-bit	16-bit	32-bit
Freq	8Mhz	1Mhz	13-416Mhz



Processing Time and Energy Consumption of Protocol Messages

Operation	Duration	Current	Energy
I1 proc. (sensor)	3.91 ms	2.2 mA	0.03 mJ
R1 proc. (PMT)	50.13 ms	—	—
I2 proc. (sensor)	10.89 s	2.2 mA	79.1 mJ
ECDH key gen.	5.41 s	2.2 mA	39.3 mJ
ECQV key proc.	5.35 s	2.2 mA	38.8 mJ
R2 proc. (PMT)	0.23 ms	—	—
Data transmission	13.8 ms	19.4 mA	0.9 mJ
Total handshake	10.95 s	—	80.03 mJ

Typical LR44 battery capacity of 150 mAh
will be enough for more than 20,000 handshakes.

Standardization Status

- New Task Group IEEE 802.15.9
  - Key management protocol for 802.15.4 and .7 links
  - HIP DEX, IKEv2, PANA, etc
  - Best Current Practice specification are expected within a year
- Internet Engineering Task Force (IETF)
  - Standards-track HIP RFCs
  - Developing DEX
  - New WGs: DICE, ACE
- Internet Research Task Force (IRTF)
  - Published HIP experiment report
  - Related work on Internet-of-Things

HELSINKI INSTITUTE FOR INFORMATION TECHNOLOGY

Conclusions

- Designed an integrated system consisting of medical sensors, terminal readers, smart space processors
- Using state-of-the-art security protocols ECC
- Support of implicit certificates in HIP Diet Exchange (HIP DEX)
- Prototyped using Telos B sensors
- Secured interactions within Smart M3 system