On Secure Access to Medical Implants

(and a bit about privacy)

Srdjan Čapkun
Department of Computer Science
ETH Zurich

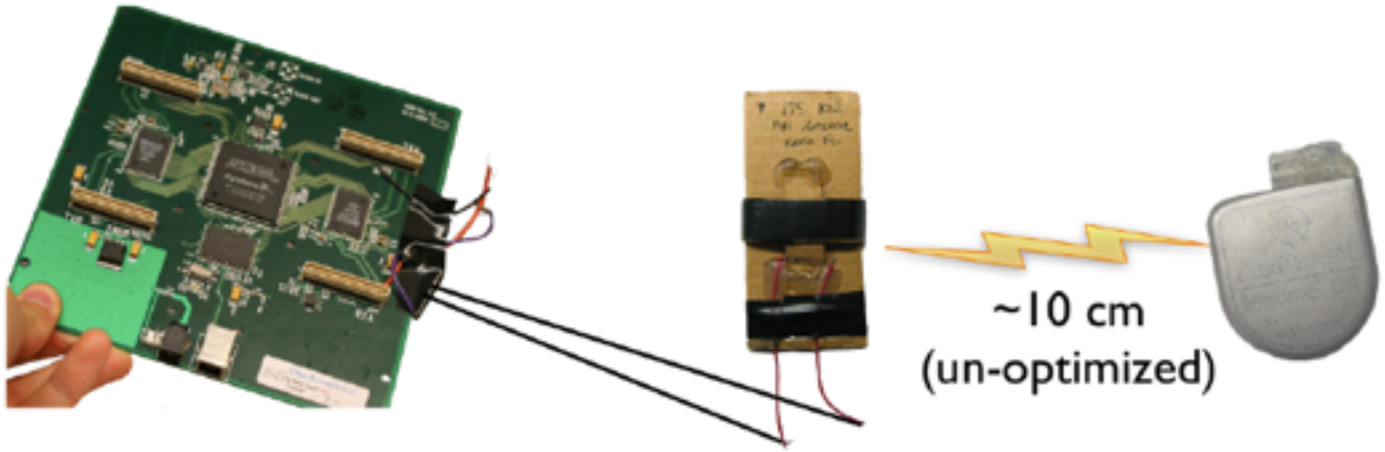
31.03.2011

Who to blame ...

t

The Need for Access Control

- Software radio, GNU Radio software $0, ***USRP*** board, $700
- Daughter boards, antennas: $100
- Communication by inductive coupling (175kHz) and in the MICS band (400MHz)
- *Access control by "Near Field Communication"*

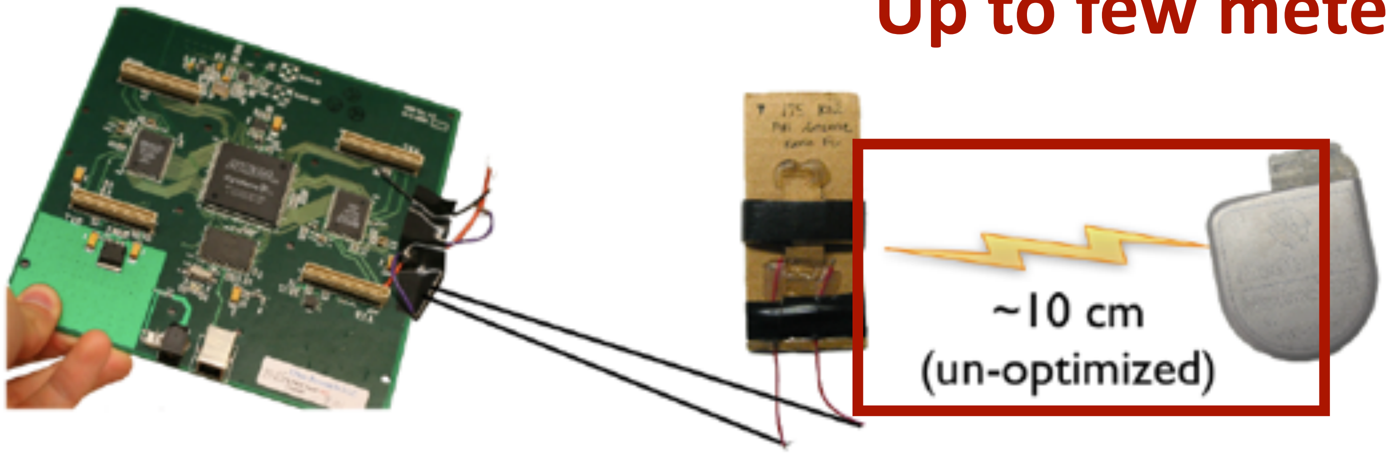


- Pacemakers and Implantable Cardiac Defibrillators ...., D. Halperin, T.S. Heydt-Benjamin, B. Ransford, S.S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W.H. Maisel., Oakland 2008

The Need for Access Control

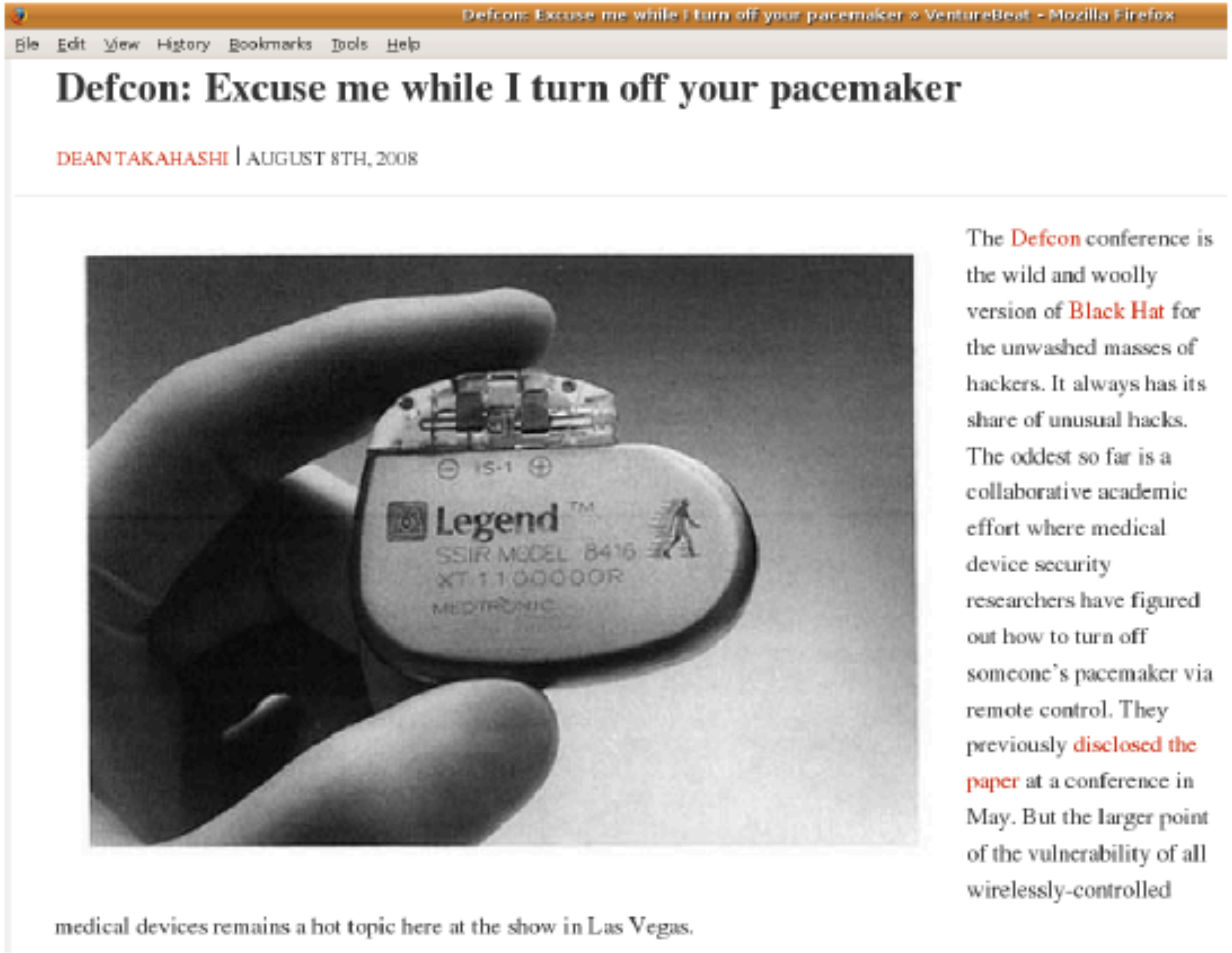
- Software radio, GNU Radio software $0, ***USRP*** board, $700
- Daughter boards, antennas: $100
- Communication by inductive coupling (175kHz) and in the MICS band (400MHz)
- *Access control by "Near Field Communication"*

Up to few meters



- Pacemakers and Implantable Cardiac Defibrillators ...., D. Halperin, T.S. Heydt-Benjamin, B. Ransford, S.S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W.H. Maisel., Oakland 2008

The Need for Access Control


Defcon: Excuse me while I turn off your pacemaker » VentureBeat - Mozilla Firefox
File Edit View History Bookmarks Tools Help
IS-1
Legend™
SSIR MODEL 8416
XT 1100000R
MEDTRONIC

Defcon: Excuse me while I turn off your pacemaker

DEAN TAKAHASHI | AUGUST 8TH, 2008

The Defcon conference is the wild and woolly version of Black Hat for the unwashed masses of hackers. It always has its share of unusual hacks. The oddest so far is a collaborative academic effort where medical device security researchers have figured out how to turn off someone's pacemaker via remote control. They previously disclosed the paper at a conference in May. But the larger point of the vulnerability of all wirelessly-controlled medical devices remains a hot topic here at the show in Las Vegas.

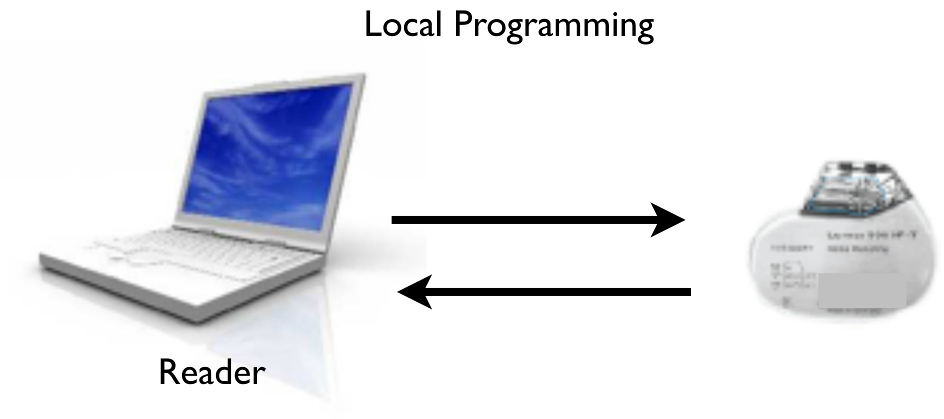
- *Wireless interfaces*
- Trigger information disclosure
- Change patient name
- Change ICD clock
- Change therapies (disable functions)
- *Induce fibrillation*

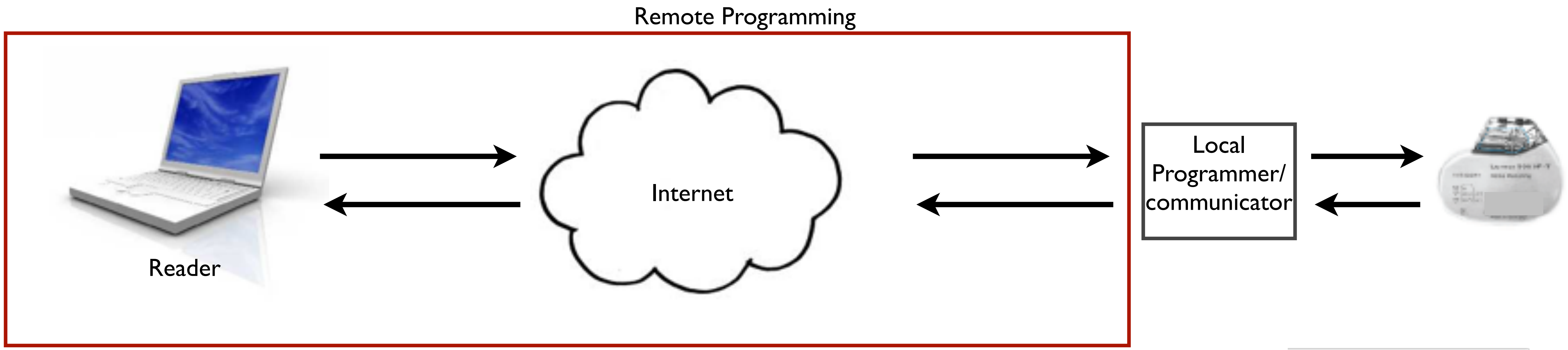
- Replay attacks

http://venturebeat.com/2008/08/08/defcon-excuse-me-while-i-turn-off-your-pacemaker/
http://www.secure-medicine.org/icd-study/icd-study.pdf

(Implantable) Medical Devices and Access

- Today:
  - local programming *(therapy and firmware updates)*
  - remote monitoring
- Future: remote programming





We want to add secure access, but ...

We want to add secure access, but ...

Must *prevent unauthorized access*

- Medical data is private and sensitive.
- Device settings can be critical.

We want to add secure access, but ...

Must *prevent unauthorized access*

- Medical data is private and sensitive.
- Device settings can be critical.

Must *allow local (and remote) access by authorized physicians*

- Change settings, readout data, access history.

We want to add secure access, but ...

Must *prevent unauthorized access*

- Medical data is private and sensitive.
- Device settings can be critical.

Must *allow local (and remote) access by authorized physicians*

- Change settings, readout data, access history.

Must *not get in the way*

- In case of emergency
- new / replacement doctor, new hospital, holidays, ...

We want to add secure access, but ...

Must *prevent unauthorized access*

- Medical data is private and sensitive.
- Device settings can be critical.

Must *allow local (and remote) access by authorized physicians*

- Change settings, readout data, access history.

Must *not get in the way*

- In case of emergency
- new / replacement doctor, new hospital, holidays, ...

Must be *accepted by the users*

We want to add secure access, but ...

Must *prevent unauthorized access*

- Medical data is private and sensitive.
- Device settings can be critical.

Must *allow local (and remote) access by authorized physicians*

- Change settings, readout data, access history.

Must *not get in the way*

- In case of emergency
- new / replacement doctor, new hospital, holidays, ...

Must be *accepted by the users*

We want to add secure access, but ...

Must *prevent unauthorized access*

- Medical data is private and sensitive.
- Device settings can be critical.

Must *allow local (and remote) access by authorized physicians*

- Change settings, readout data, access history.

Must *not get in the way*

- In case of emergency
- new / replacement doctor, new hospital, holidays, ...

Must be *accepted by the users*

In case of remote access

- *Provide access control to the user*
- *Must not introduce a single point of failure*

Proposed Solutions for Access Control to IMDs

Credentials: *single point of failure - but a good basis*

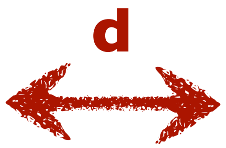
- Pre-shared secret keys / public-key certificates

Token Based Approaches: *usability / acceptance*

- Token based access (USB, Smartcard, ...)
- Communication Cloaker
- Tattoos, Heartbeats, ...

User Alerts: *does not prevent unauthorized access*

- Sound/vibration when IMD is engaging in communication.

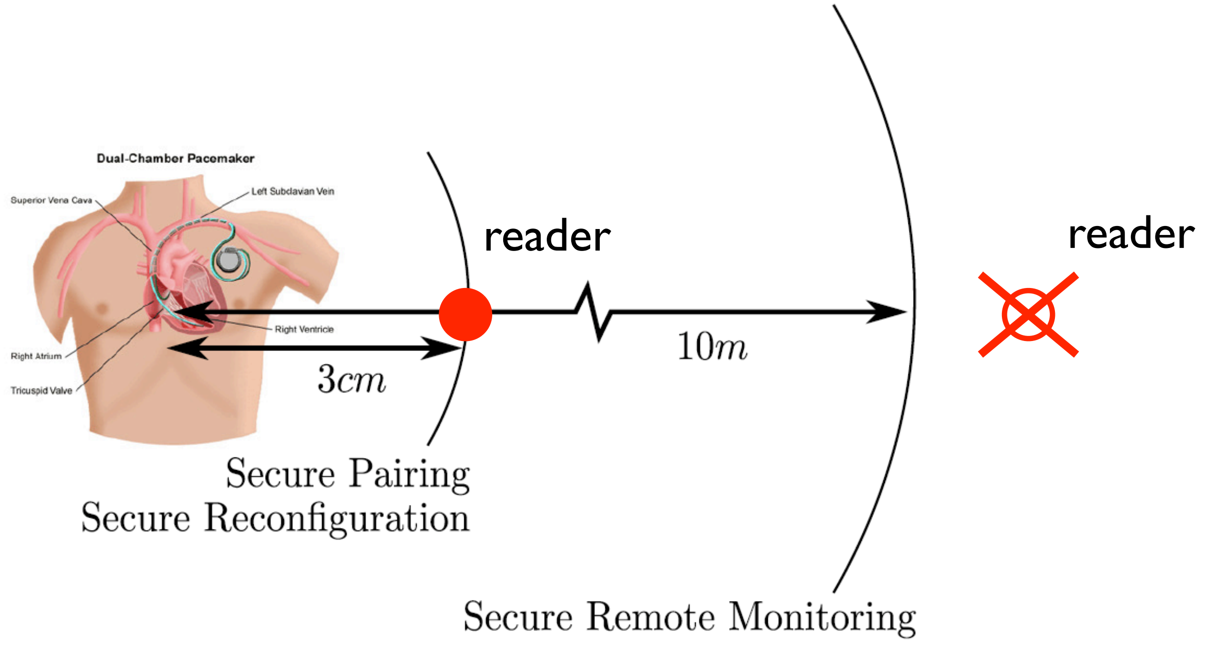


Proximity-Based Approaches

Proximity-Based Access Control

Only If a reader is close to the implant, it gets access.

- An untrusted device - *the prover (reader)* wants to *prove that it is close* to another device - *the verifier* (pacemaker).



reader

reader

$10m$

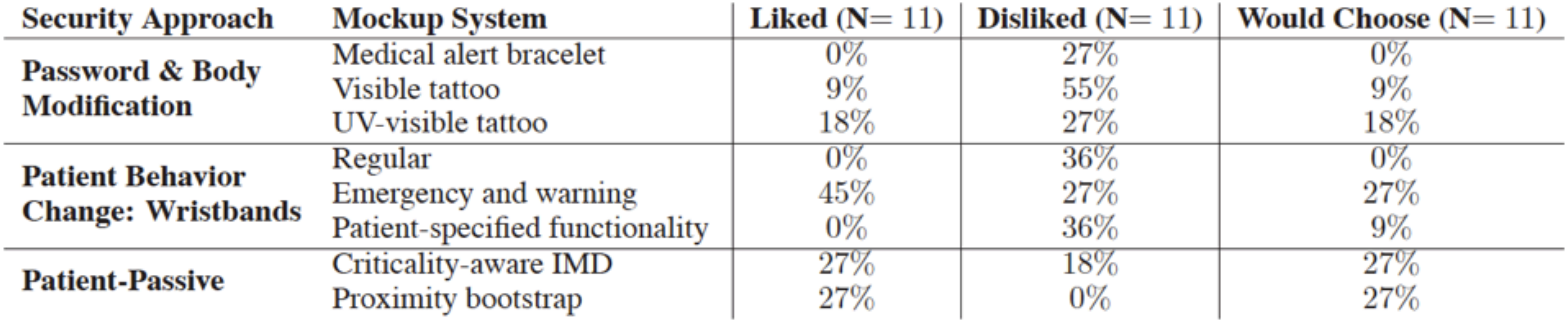
$3cm$

Secure Pairing
Secure Reconfiguration

Secure Remote Monitoring

Proximity-Based Access Control

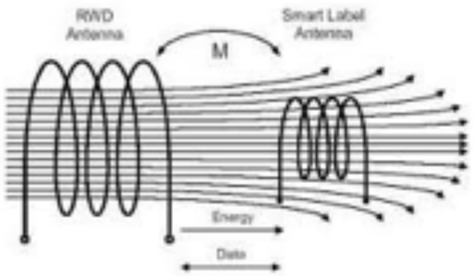
- Liked and the least disliked by the patients



Security Approach	Mockup System	Liked (N= 11)	Disliked (N= 11)	Would Choose (N= 11)
Password & Body Modification	Medical alert bracelet	0%	27%	0%
	Visible tattoo	9%	55%	9%
	UV-visible tattoo	18%	27%	18%
Patient Behavior Change: Wristbands	Regular	0%	36%	0%
	Emergency and warning	45%	27%	27%
	Patient-specified functionality	0%	36%	9%
Patient-Passive	Criticality-aware IMD	27%	18%	27%
	Proximity bootstrap	27%	0%	27%

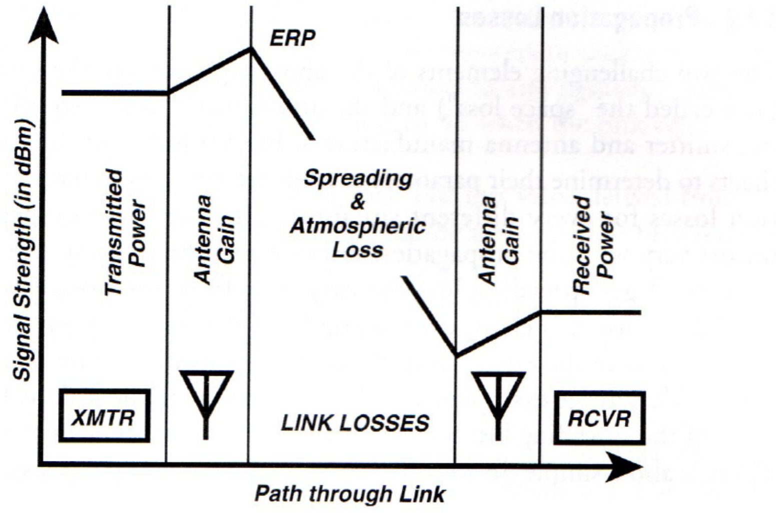
Patients, Pacemakers, and Implantable Defibrillators: Human Values and Security for Wireless Implantable Medical Devices, Tamara Denning†, Alan Borning†, Batya Friedman‡, Brian T. Gill, Tadayoshi Kohno†, andWilliam H. Maisel, CHI 2010

Secure Proximity Verification



Secure Proximity verification

- Magnetic Switch: *no range guarantees, no authentication*
- Short range LF - *no range guarantees*
- MICS band RF
  Communication DOES NOT imply physical proximity (in adversarial environments)



To calculate the received signal level (in dBm), add the transmitting antenna gain (in dB), subtract the link losses (in dB), and add the receiving antenna gain (in dB) to the transmitter power (in dBm).

©D. Adamy, A First Course on Electronic Warfare

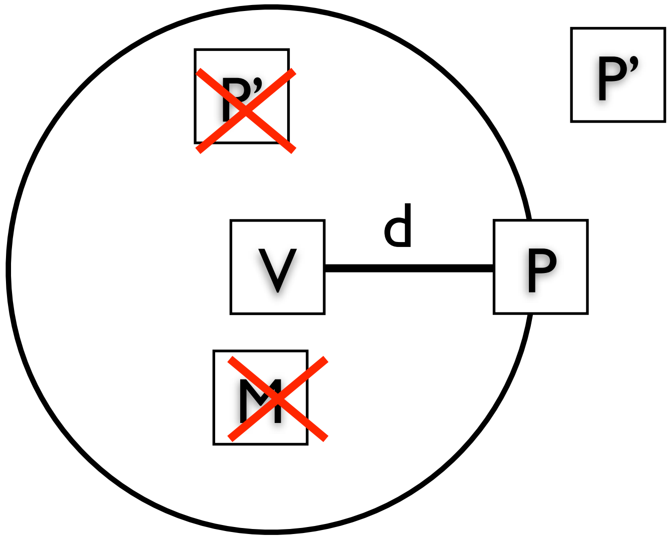
Solution:

- *Secure Proximity Verification using Distance-Bounding.*

Distance Bounding (0)

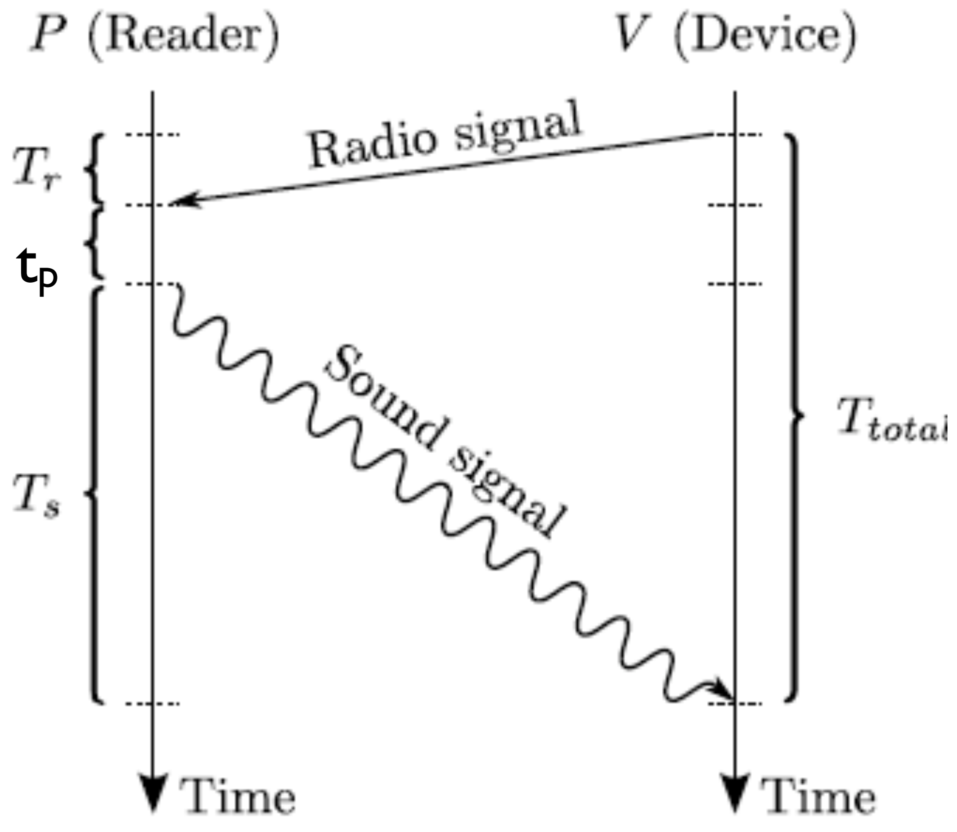
Distance Bounding (DB) Protocols:

- Enable the Verifier to measure an upper-bound on the physical distance to the Prover
- *Prevent distance frauds:* P pretends to be closer to V than it is (i.e., the measured distance is shorter than the actual distance d). P is untrusted.

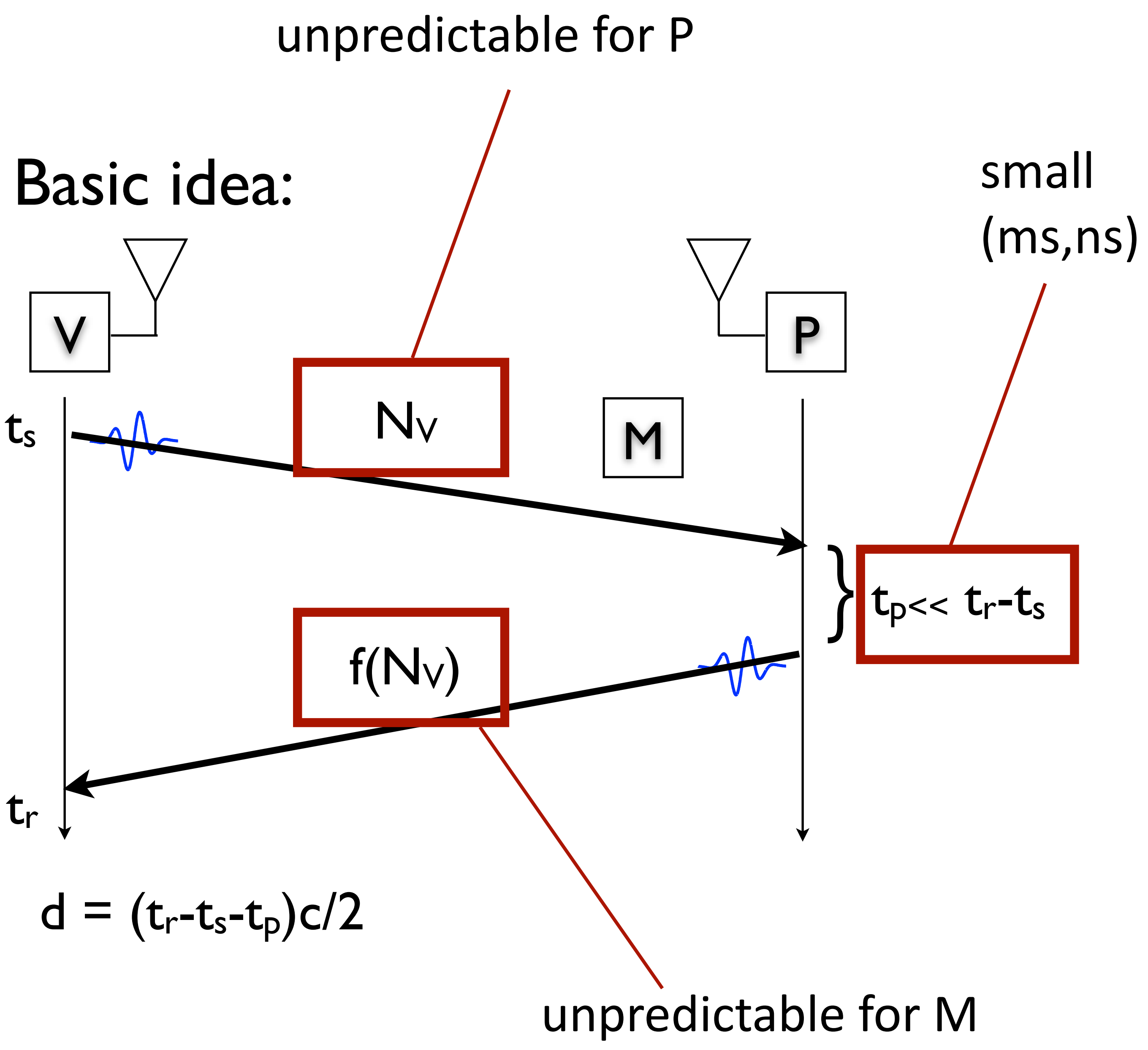


Distance Bounding (I)

Distance Bounding (DB) Protocols: Basic idea



Basic idea:


unpredictable for P

small (ms,ns)

V

P

M

t_s

N_V

$t_p << t_r - t_s$

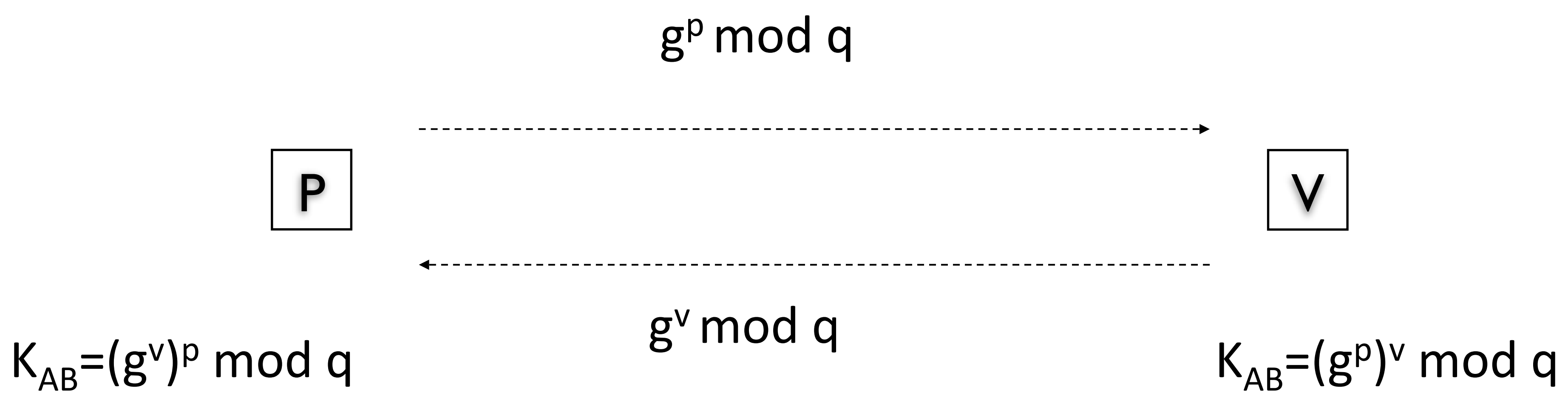
$f(N_V)$

t_r

$d = (t_r - t_s - t_p)c/2$

unpredictable for M

Background: Diffie-Hellman



$g^p \bmod q$

P

V

$g^v \bmod q$

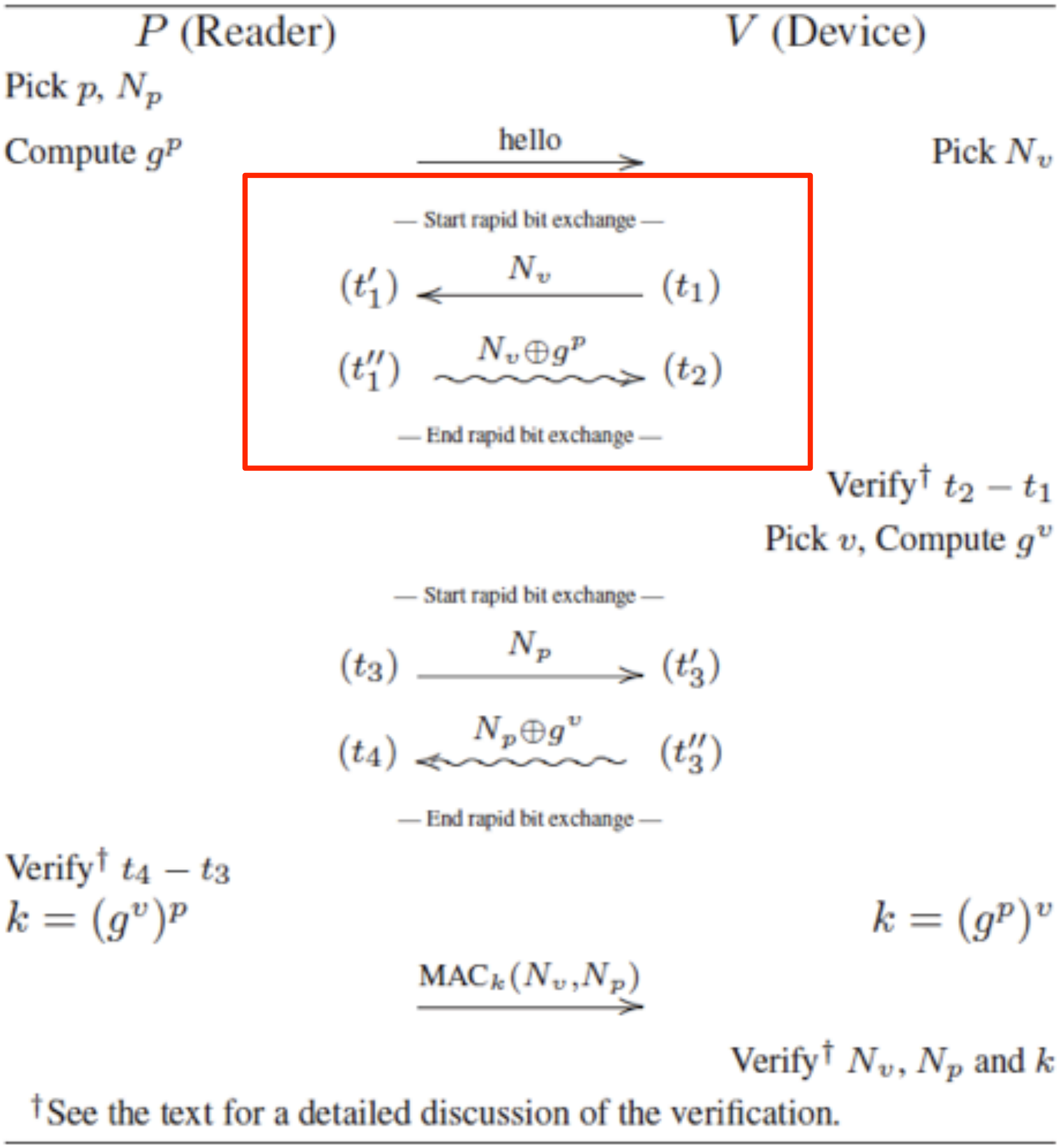
$K_{AB}=(g^v)^p \bmod q$

$K_{AB}=(g^p)^v \bmod q$

Idea:

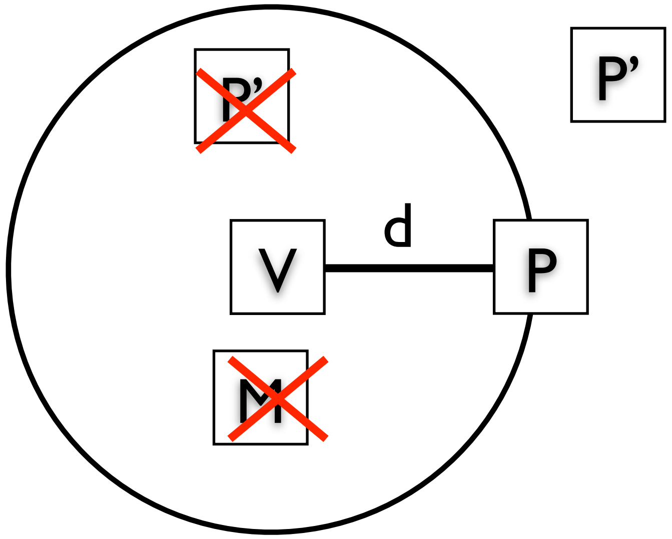
- Authenticate *g^p mod q* by the distance from which it came
- If $d \leq d^*$ => grant access and establish the key
  else reject access

Proximity-Based Access Control



P (Reader)		V (Device)
Pick p, N_p		
Compute g^p	$\xrightarrow{\text{hello}}$	Pick N_v
	— Start rapid bit exchange —	
	$(t'_1) \xleftarrow{N_v} (t_1)$	
	$(t''_1) \overset{N_v \oplus g^p}{\rightsquigarrow} (t_2)$	
	— End rapid bit exchange —	
		Verify† $t_2 - t_1$
		Pick v, Compute g^v
	— Start rapid bit exchange —	
	$(t_3) \xrightarrow{N_p} (t'_3)$	
	$(t_4) \overset{N_p \oplus g^v}{\leftsquigarrow} (t''_3)$	
	— End rapid bit exchange —	
Verify† $t_4 - t_3$		
$k = (g^v)^p$		$k = (g^p)^v$
	$\xrightarrow{\text{MAC}_k(N_v, N_p)}$	
		Verify† N_v, N_p and k

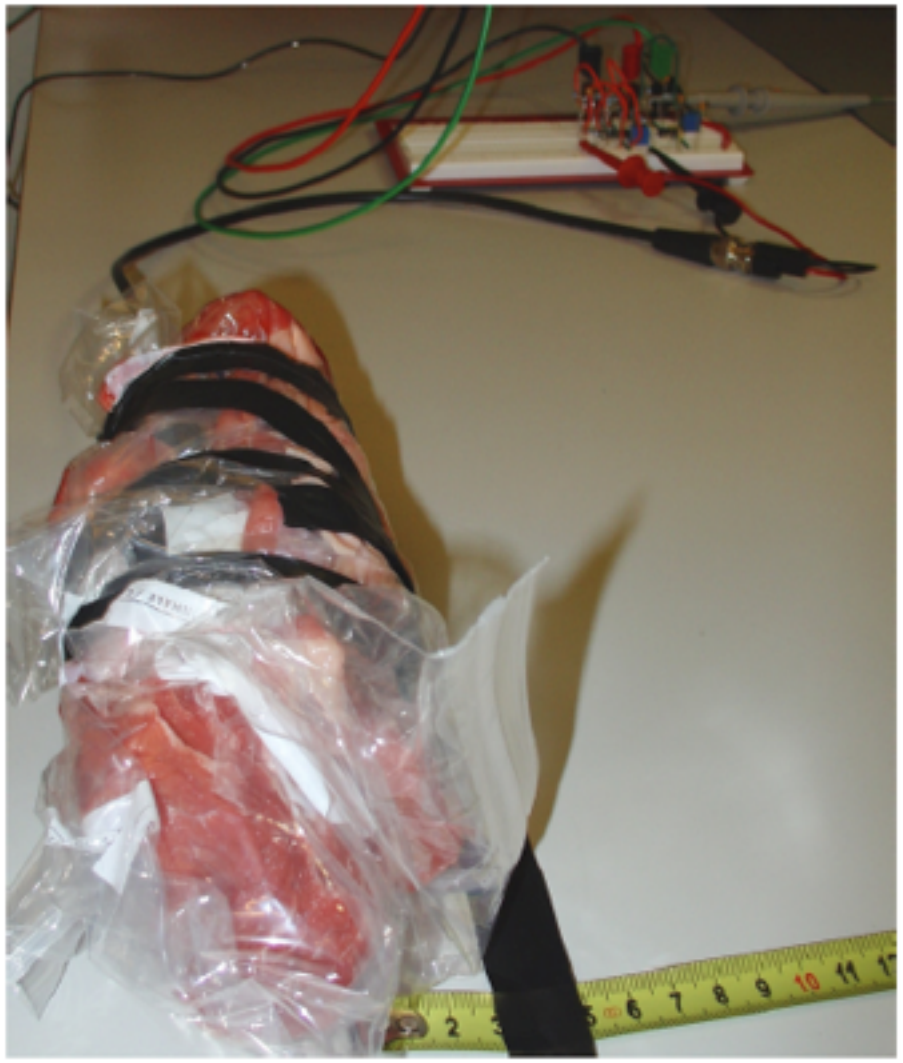
†See the text for a detailed discussion of the verification.

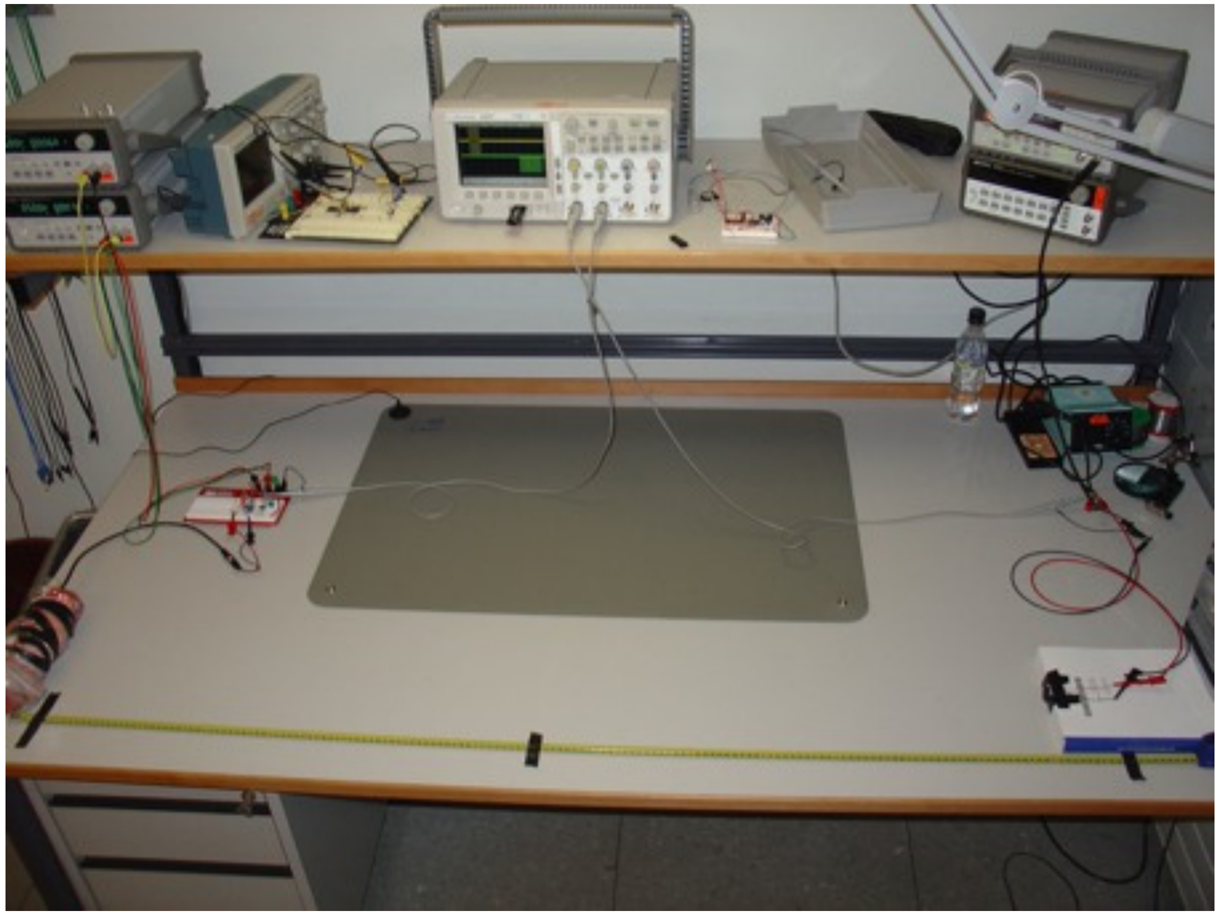


P cannot pretend to have sent g^P from closer distance, only from further away.

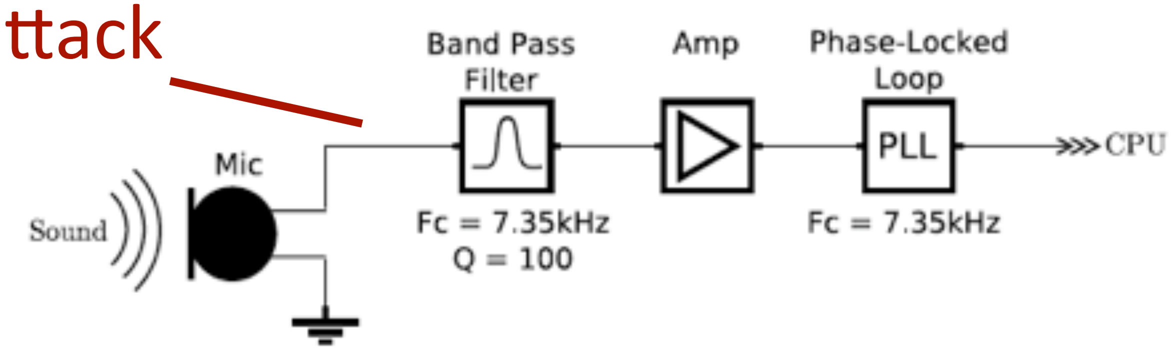
K. Rasmussen, C. Castelluccia, T. S. Heydt-Benjamin, S. Capkun, Proximity-based Access Control for Implantable Medical Devices, CCS 2009

Implementation and Tests





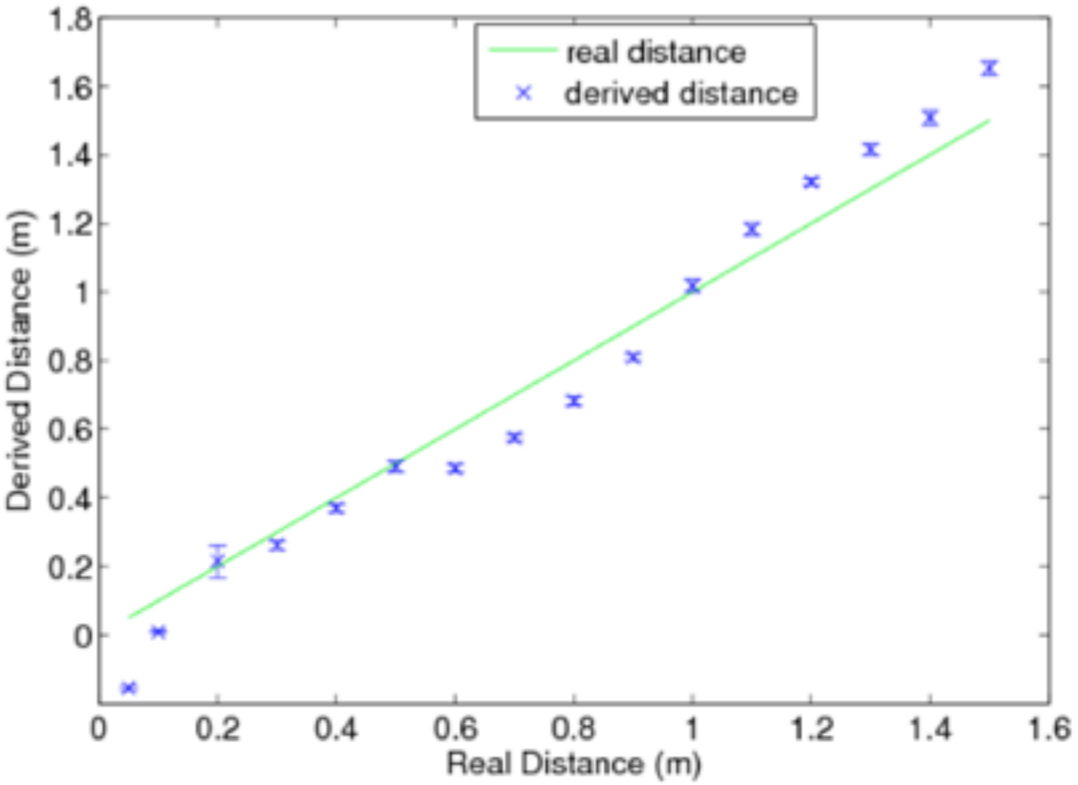
Possible attack



Implementation and Tests

Speed of sound (air) 340m/s, (meat) 1500m/s

t_p = 412ns, *<1mm of security guarantee* (in our prototype)



Distance measurement granularity: < 1cm

Summary (Access)

- Access control is a problem
- Proximity can be used to enforce Access Control
- Intuitive for the users
- Is not subject to single point of failure (remote)

- Easy to define intuitive policies e.g.
  - <5cm => full access
  - < 1/2 m => only monitoring
  - < 1/2 m + key => full access

A bit about privacy ...

A bit about privacy ...

If a patient wears/has a device implanted.

- Is tracking feasible? How accurately can people be tracked?

A bit about privacy ...

If a patient wears/has a device implanted.

- Is tracking feasible? How accurately can people be tracked?

Due to manufacturing imperfections, devices exhibit *observable 'fingerprints'*

- RFID tags, WiFi, sensor nodes, mobile phones, etc ...
- *IMDs? very likely*

A bit about privacy ...

If a patient wears/has a device implanted.

- Is tracking feasible? How accurately can people be tracked?

Due to manufacturing imperfections, devices exhibit *observable 'fingerprints'*

- RFID tags, WiFi, sensor nodes, mobile phones, etc ...
- *IMDs? very likely*

Wireless signal collection + pattern recognition = successful remote identification / classification.

A bit about privacy ...

If a patient wears/has a device implanted.

- Is tracking feasible? How accurately can people be tracked?

Due to manufacturing imperfections, devices exhibit *observable ‘fingerprints’*

- RFID tags, WiFi, sensor nodes, mobile phones, etc ...
- *IMDs? very likely*

Wireless signal collection + pattern recognition = successful remote identification / classification.

A bit about privacy ...

If a patient wears/has a device implanted.

- Is tracking feasible? How accurately can people be tracked?

Due to manufacturing imperfections, devices exhibit *observable 'fingerprints'*

- RFID tags, WiFi, sensor nodes, mobile phones, etc ...
- *IMDs? very likely*

Wireless signal collection + pattern recognition = successful remote identification / classification.

A bit about privacy ...

If a patient wears/has a device implanted.

- Is tracking feasible? How accurately can people be tracked?

Due to manufacturing imperfections, devices exhibit *observable 'fingerprints'*

- RFID tags, WiFi, sensor nodes, mobile phones, etc ...
- *IMDs? very likely*

Wireless signal collection + pattern recognition = successful remote identification / classification.

A bit about privacy ...

If a patient wears/has a device implanted.

- Is tracking feasible? How accurately can people be tracked?

Due to manufacturing imperfections, devices exhibit *observable 'fingerprints'*

- RFID tags, WiFi, sensor nodes, mobile phones, etc ...
- *IMDs? very likely*

Wireless signal collection + pattern recognition = successful remote identification / classification.

A bit about privacy ...

If a patient wears/has a device implanted.

- Is tracking feasible? How accurately can people be tracked?

Due to manufacturing imperfections, devices exhibit *observable 'fingerprints'*

- RFID tags, WiFi, sensor nodes, mobile phones, etc ...
- *IMDs? very likely*

Wireless signal collection + pattern recognition = successful remote identification / classification.

A bit about privacy ...

If a patient wears/has a device implanted.

- Is tracking feasible? How accurately can people be tracked?

Due to manufacturing imperfections, devices exhibit *observable ‘fingerprints’*

- RFID tags, WiFi, sensor nodes, mobile phones, etc ...
- *IMDs? very likely*

Wireless signal collection + pattern recognition = successful remote identification / classification.

A bit about privacy ...

If a patient wears/has a device implanted.

- Is tracking feasible? How accurately can people be tracked?

Due to manufacturing imperfections, devices exhibit *observable ‘fingerprints’*

- RFID tags, WiFi, sensor nodes, mobile phones, etc ...
- *IMDs? very likely*

Wireless signal collection + pattern recognition = successful remote identification / classification.

Usenix Security 09, Mobicom 10, ...

A bit about privacy ...

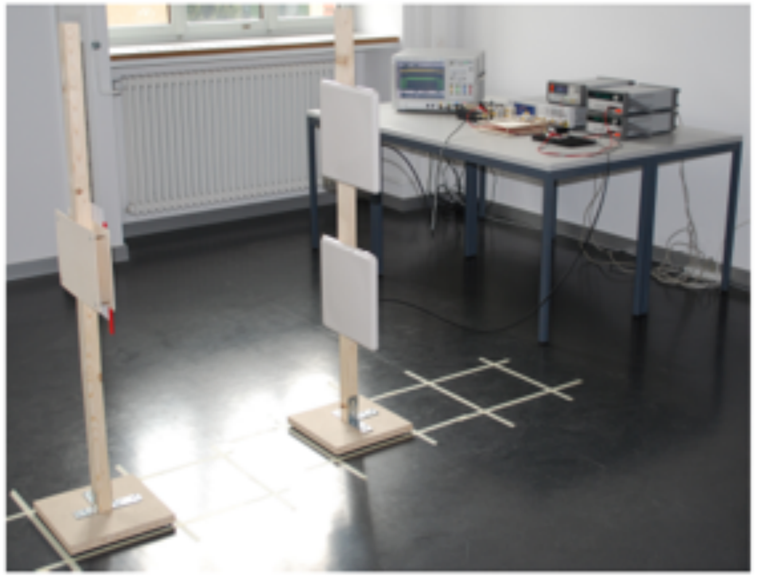
If a patient wears/has a device implanted.

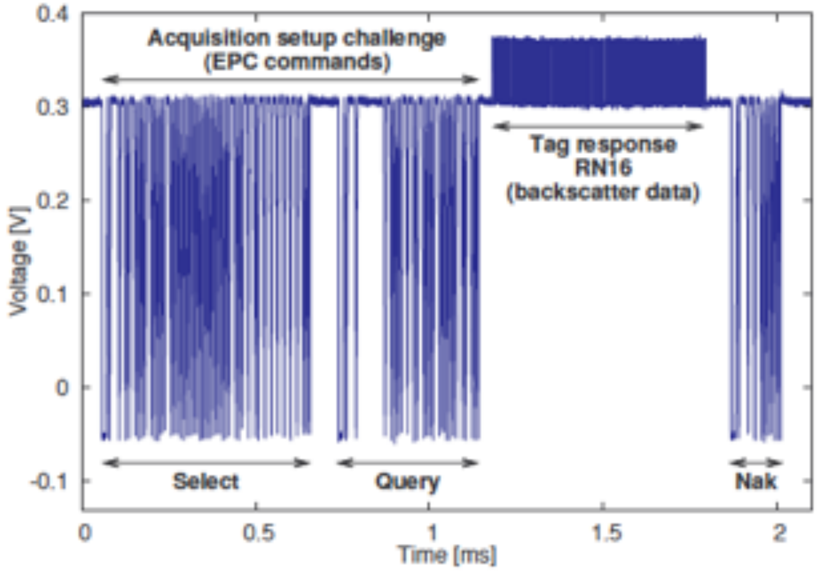
- Is tracking feasible? How accurately can people be tracked?

Due to manufacturing imperfections, devices exhibit *observable ‘fingerprints’*

- RFID tags, WiFi, sensor nodes, mobile phones, etc ...
- *IMDs? very likely*

Wireless signal collection + pattern recognition = successful remote identification / classification.





Usenix Security 09, Mobicom 10, ...

A bit about privacy ...

A bit about privacy ...

Some problems are inherently difficult to solve

- e.g., tracking, location privacy

Contact

- www.syssec.ethz.ch
- capkuns@inf.ethz.ch