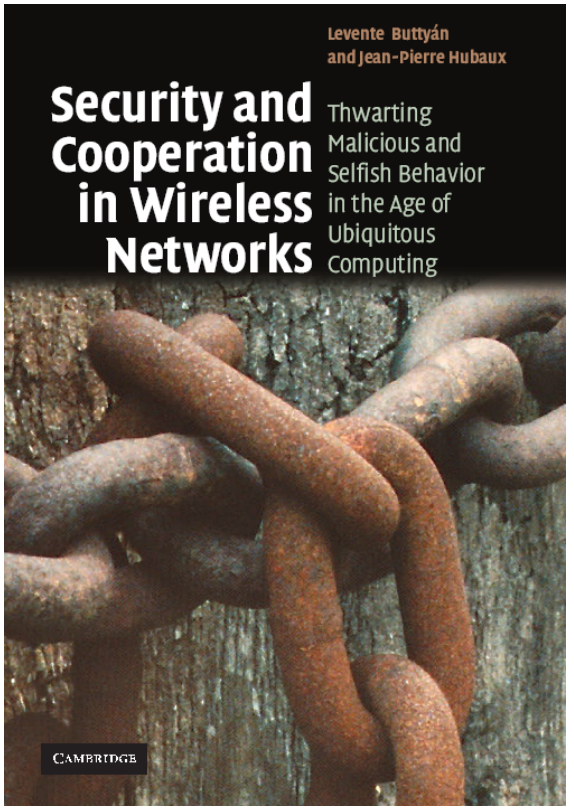
Security and Privacy in Wireless Networks

Mohammad Hossein Manshaei
manshaei@gmail.com



Security and Cooperation in Wireless Networks

TEXTBOOK REVIEW

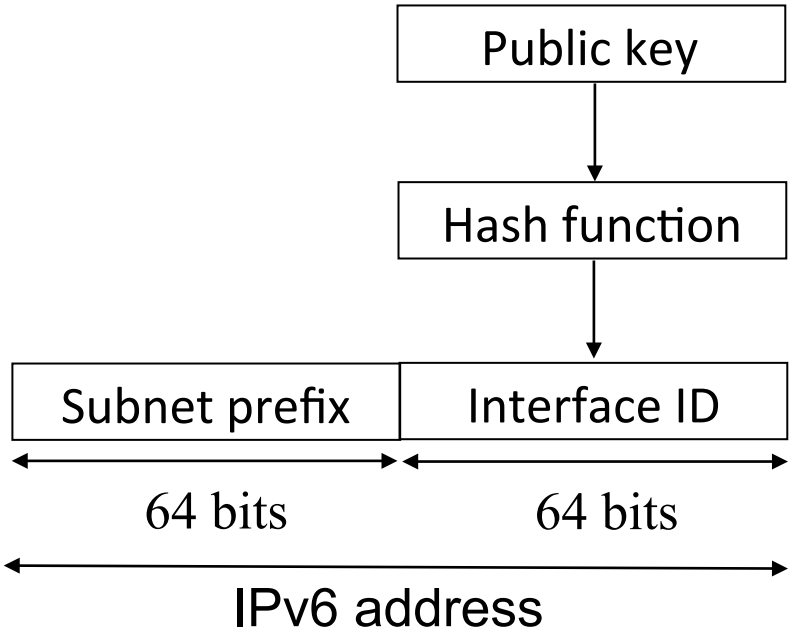
http://secowinet.epfl.ch

Security and Cooperation in Wireless Networks

1. Introduction
2. Thwarting **malice**: security mechanisms
    - 2.1 Naming and addressing
    - 2.2 Establishment of security associations
    - 2.3 Secure neighbor discovery
    - 2.4 Secure routing in multi-hop wireless networks
    - 2.5 Privacy protection
    - 2.6 Secure positioning
3. Thwarting **selfishness**: behavior enforcement
    - 3.0 Brief introduction to game theory
    - 3.1 Enforcing fair bandwidth sharing at the MAC layer
    - 3.2 Enforcing packet forwarding
    - 3.3 Wireless operators in a shared spectrum
    - 3.4 Secure protocols for behavior enforcement

2.1 Naming and addressing

- Typical attacks:
  - Sybil: the same node has multiple identities
  - Replication: the attacker captures a node and replicates it
    ➔ several nodes share the same identity
- Distributed protection technique in IPv6: Cryptographically Generated Addresses (T. Aura, 2003; RFC 3972) → only a partial solution to the problem

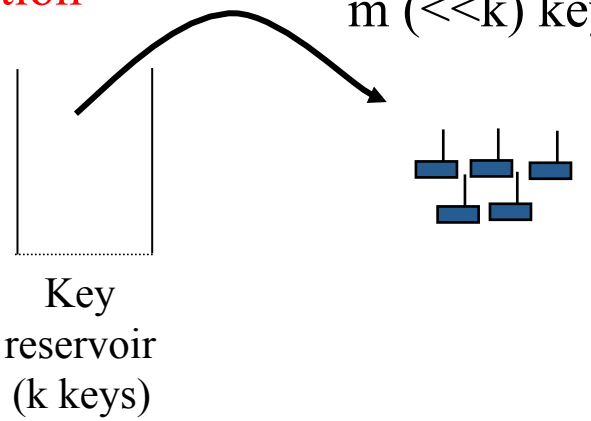


For higher security (hash function output beyond 64 bits), *hash extension* can be used

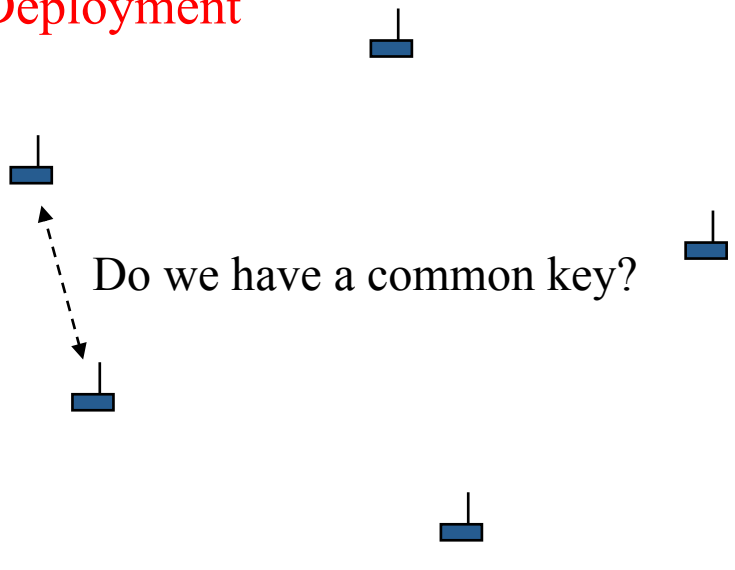
Parno, Perrig, and Gligor. Detection of **node replication** attacks in sensor networks. *IEEE Symposium on Security and Privacy, 2005*

2.2 Pairwise key establishment in sensor networks

1. Initialization



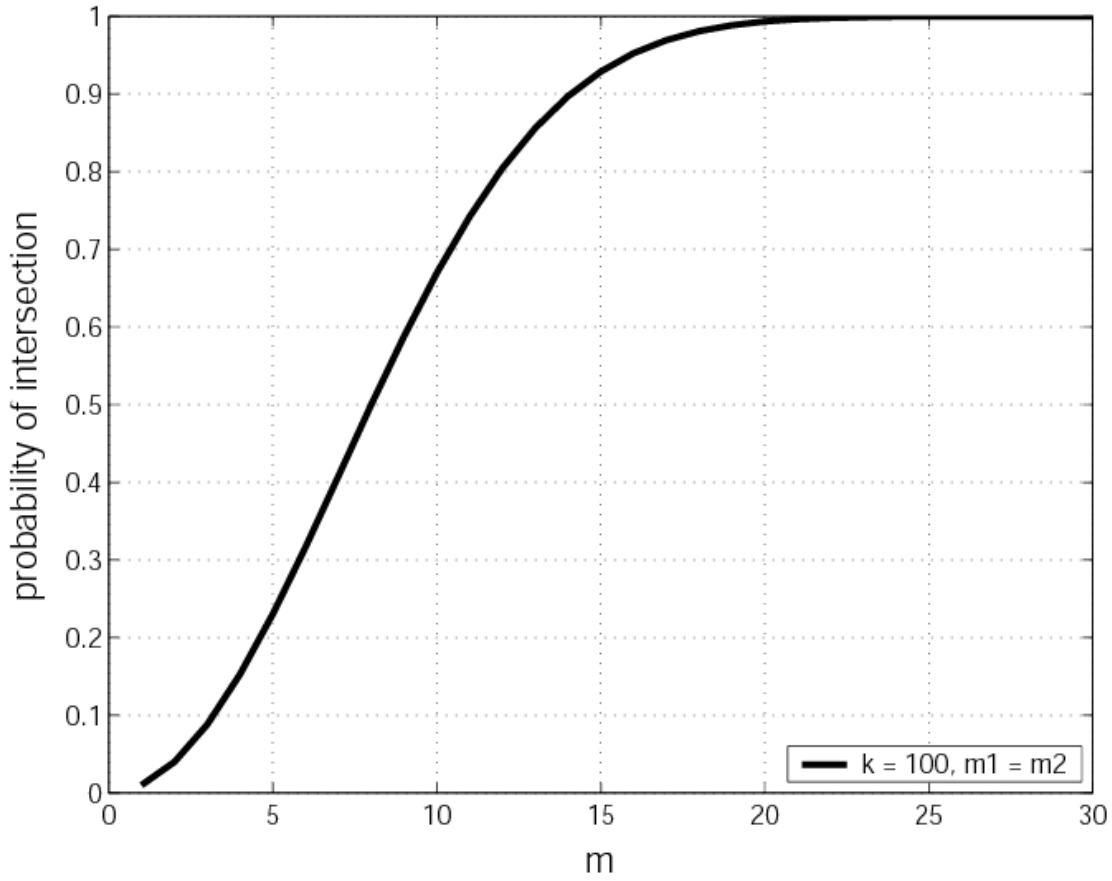
2. Deployment



Probability for any 2 nodes to have a common key:

$$p = 1 - \frac{((k-m)!)^2}{k!(k-2m)!}$$

Probability for two sensors to have a common key

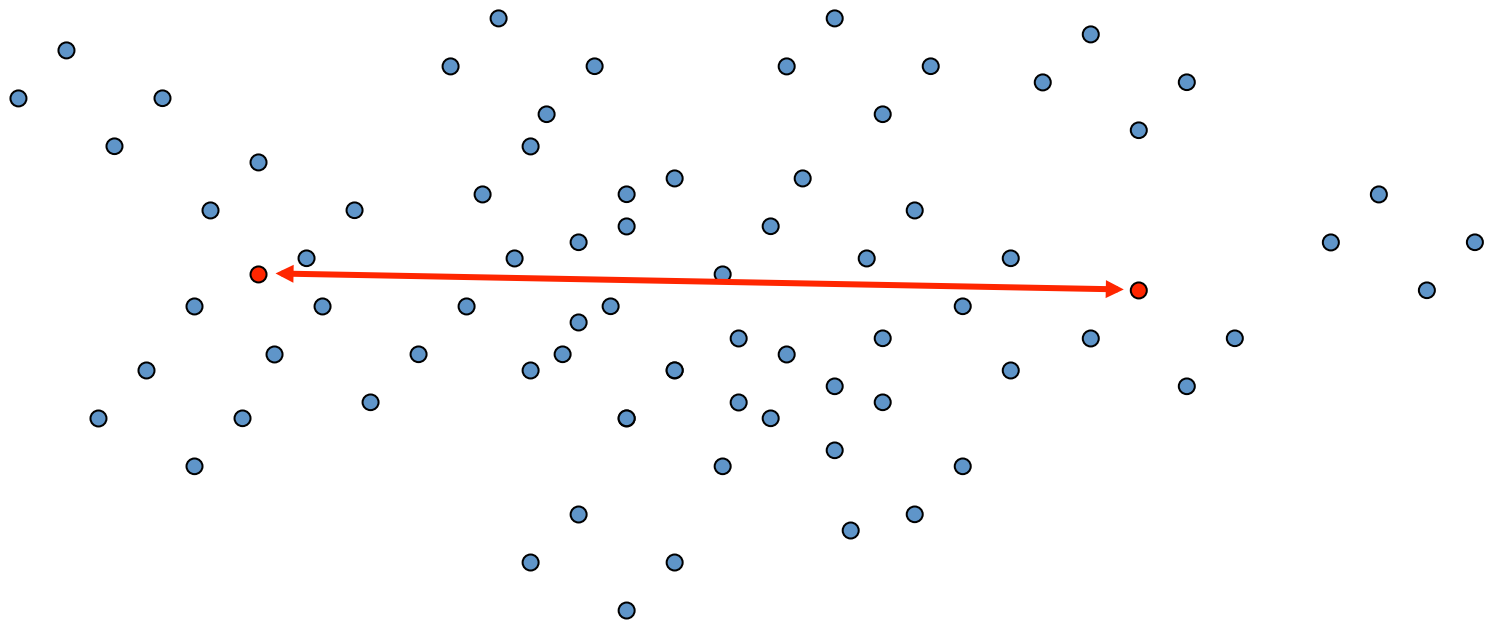


Eschenauer and Gligor, *ACM CCS 2002*

See also:

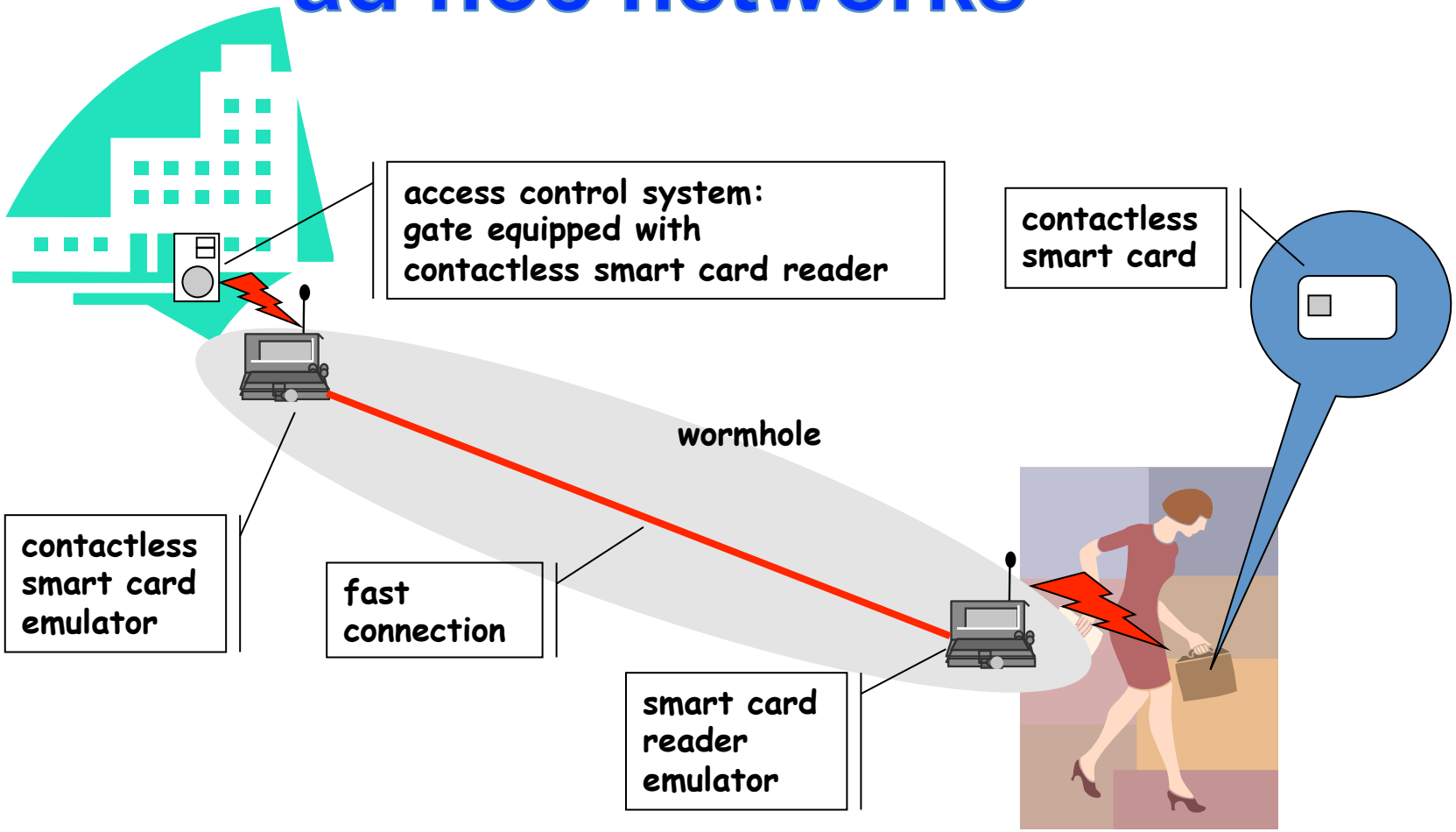
- Karlof, Sastry, Wagner: TinySec, *Sensys 2004*
- Westhoff et al.: On Digital Signatures in Sensor Networks, *ETT 2005*

2.3 Securing Neighbor Discovery: Thwarting Wormholes



- Routing protocols will choose routes that contain wormhole links
  - typically those routes appear to be shorter
  - Many of the routes (e.g., discovered by flooding based routing protocols such as DSR and Ariadne) will go through the wormhole
- The adversary can then monitor traffic or drop packets (DoS)

Wormholes are not specific to ad hoc networks



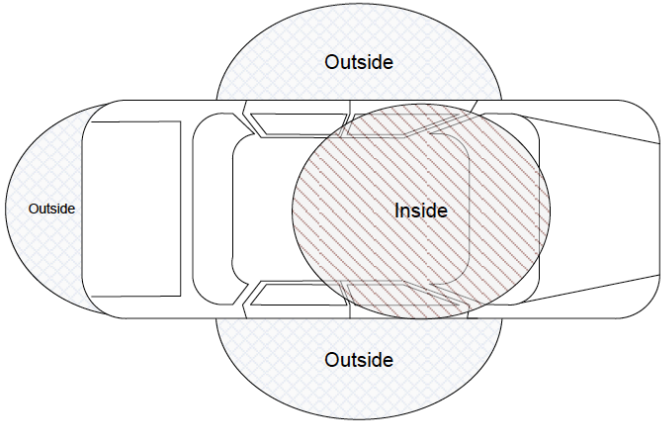
Hu, Perrig, and Johnson
Packet leashes: a defense against wormhole attacks in wireless networks
INFOCOM 2003

Example: Passive Keyless Entry and Start

- Cars, babies and convenience ...
- Passive Keyless Entry and Start Systems (PKES)

("the key is in the pocket and when the user **is near**, the car opens when the key is in the car, the car can be started by pressing a button")

PKES key

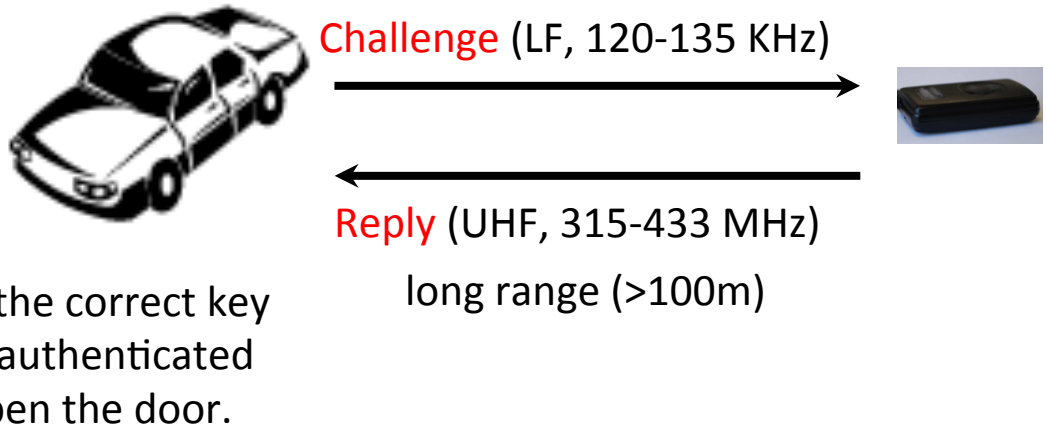


Areas in which the car detects the presence of the PKES key

- Implemented by all major car manufacturers.

Example: Passive Keyless Entry and Start

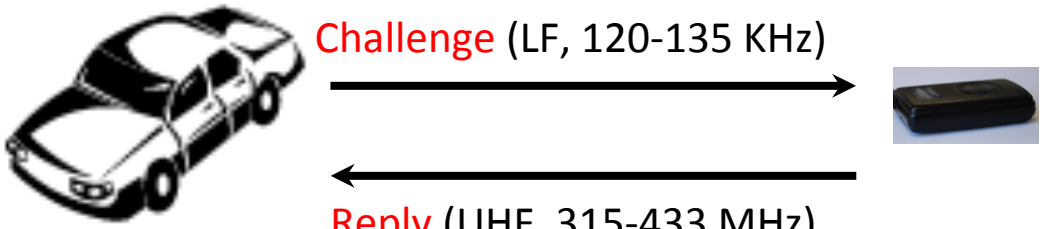
- Sketch of the Protocol:



- If the key battery is dead, only LF communication is used (passive RFID tag)

Example: Passive Keyless Entry and Start

- Sketch of the Protocol:



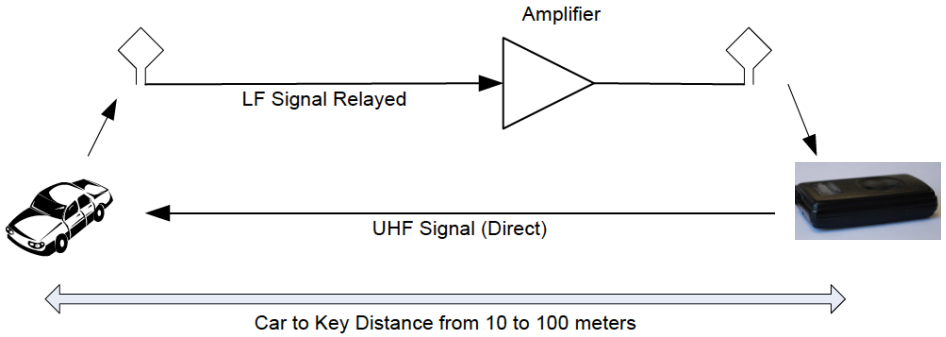
If the correct key is authenticated open the door.

- Main intuition:
- Key authentication by cryptographic means (c-r protocol)
- LF Communication implies physical proximity

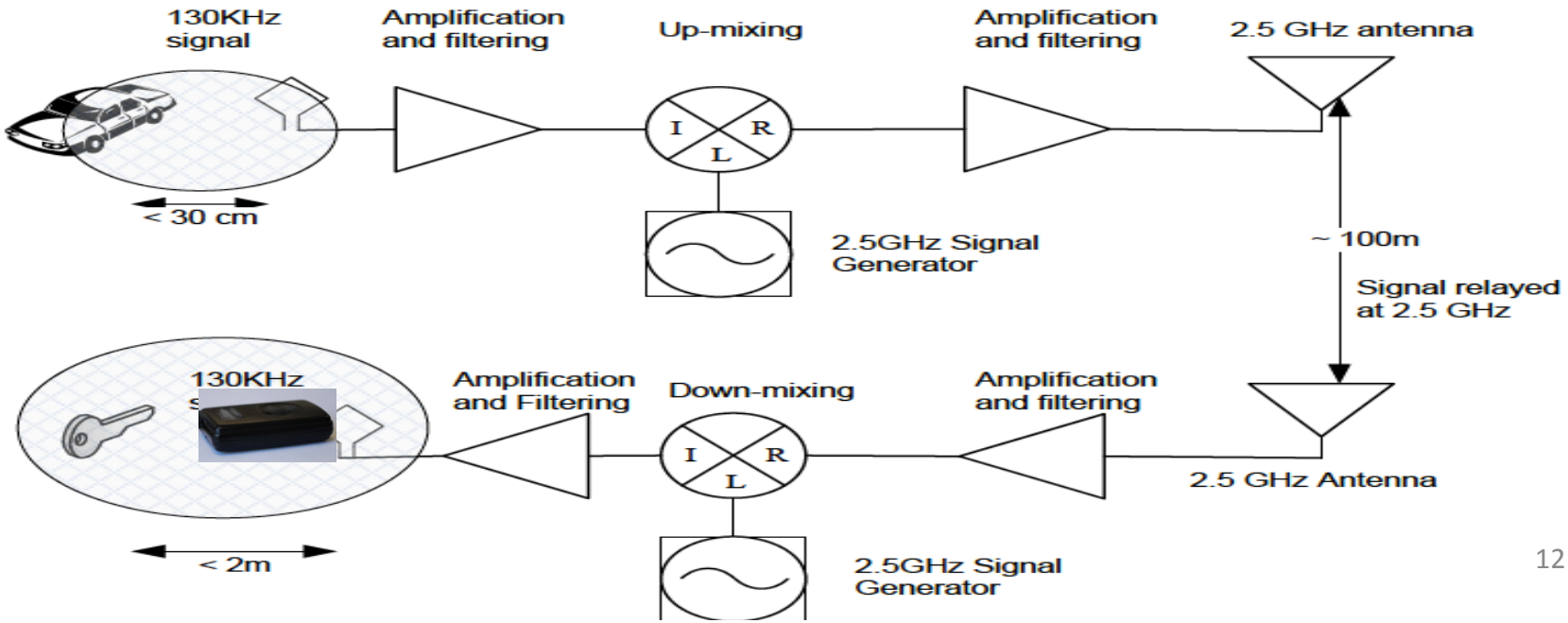
The system is vulnerable to relay attacks!

Relay Attack on PKES (Eprint 2010)

- Wired



- Wireless

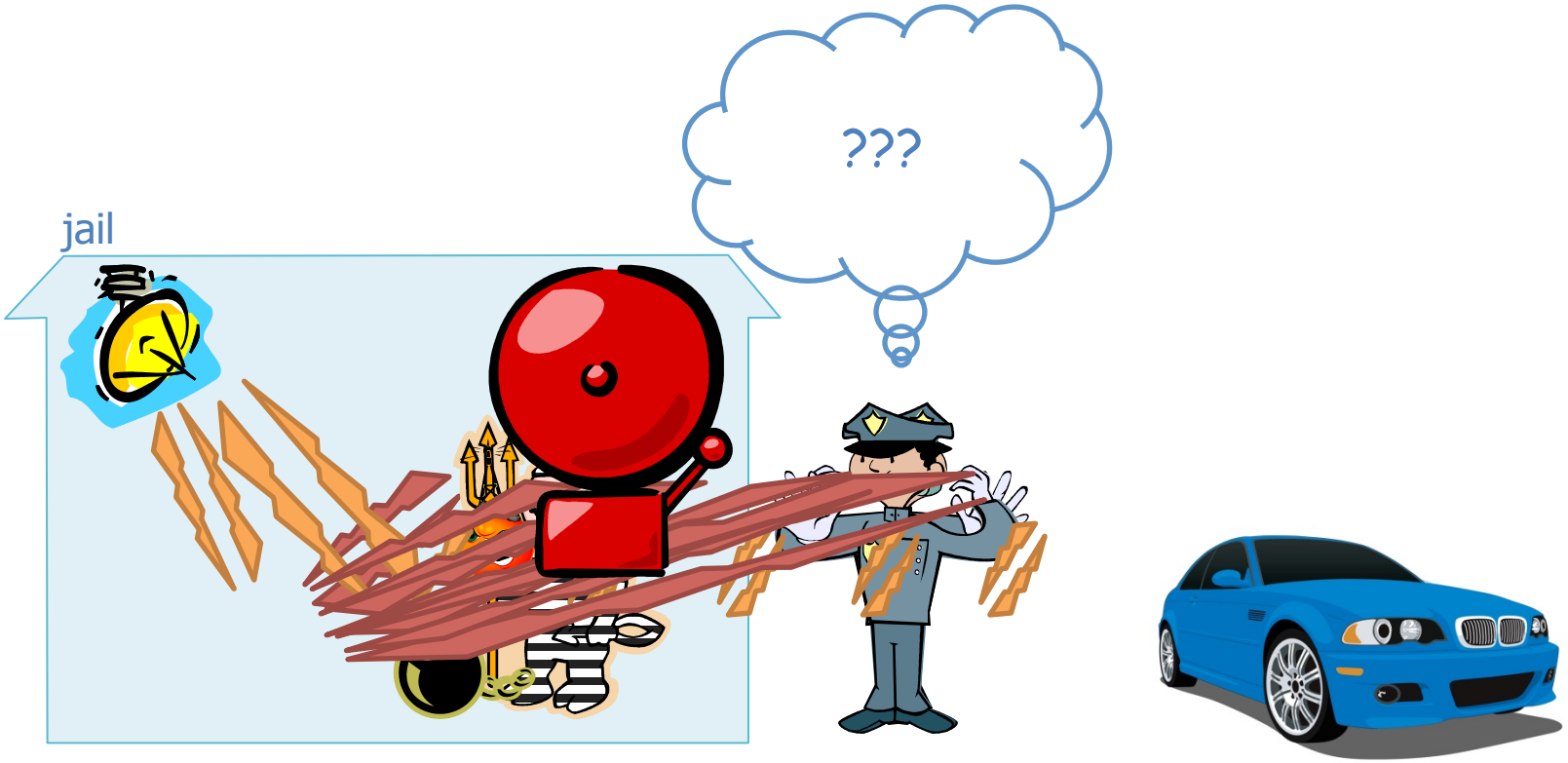


Implications

- Opening and Starting a Car without the possession of a key.
- No traces of entry/start.
- Legal/insurance issues.
- Can be combined with other attacks

- Protection mechanisms:
- Shield the key. (immediate)
- Remove the battery key. (immediate)
- Build a new system (e.g., based on distance bounding)

Application example: Tracking



Proximity-based Access Control for Implantable Medical Devices

K. B. Rasmussen, C. Castelluccia,
T. S. Heydt-Benjamin, and S. Capkun
ETH Zurich, Switzerland
CCS, 2010

Problem

- Access Control to Implantable Medical Devices

Why is this a Problem?

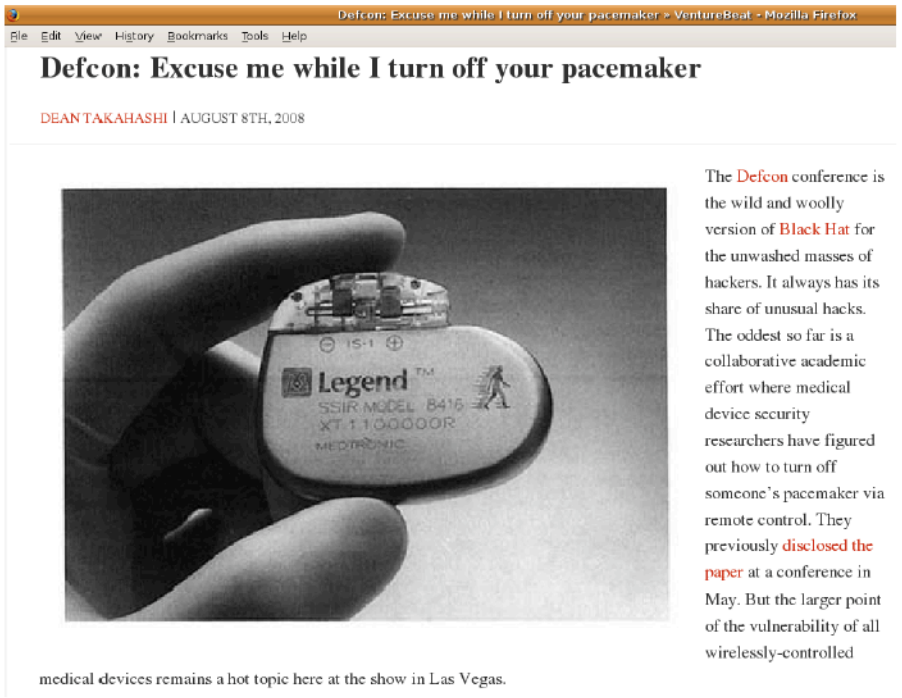
There are demonstrated attacks on IMDs (pacemakers) using SDRs

Current systems:

- Near-Field Communication
- Magnetic Reed switch
- No crypto

Attacks:

- Replay attacks
- Trigger information disclosure
- Change patient name
- Change clock
- Change therapies (disable functions)
- Induce fibrillation



Defcon: Excuse me while I turn off your pacemaker » VentureBeat - Mozilla Firefox

File Edit View History Bookmarks Tools Help

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.

Some Constrains

MUST prevent unauthorized access.

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

MUST allow access to authorized physicians.

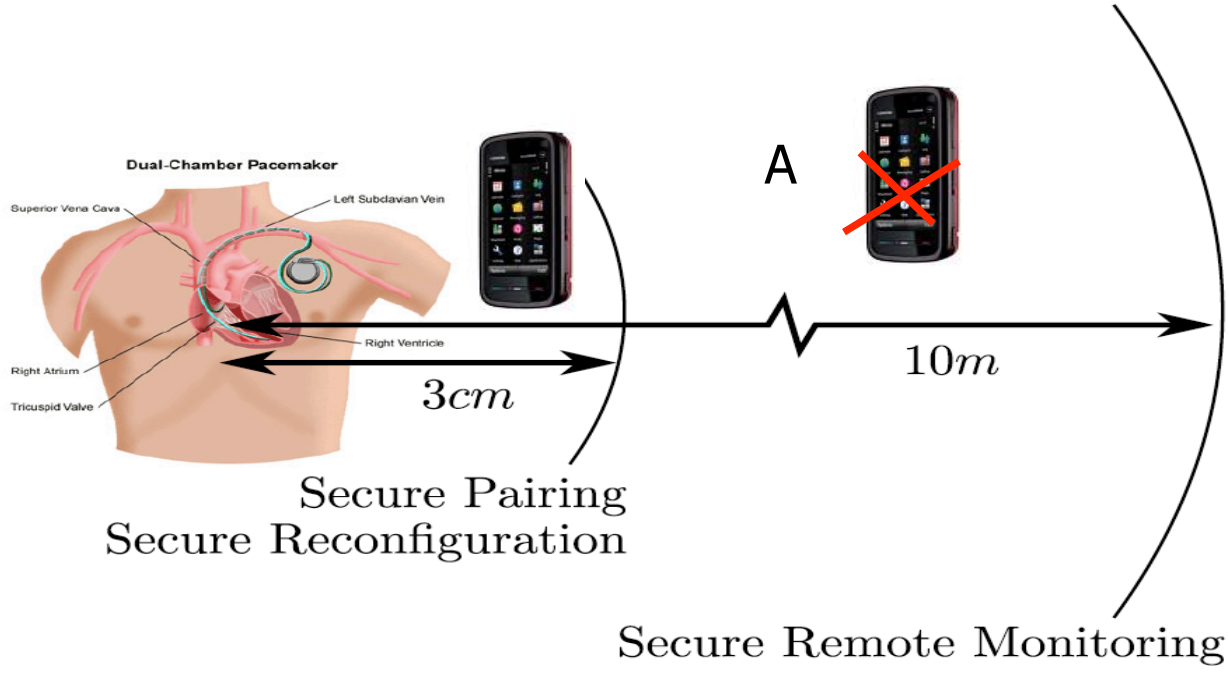
- Change settings.
- Readout data.
- Access history.

MUST NOT

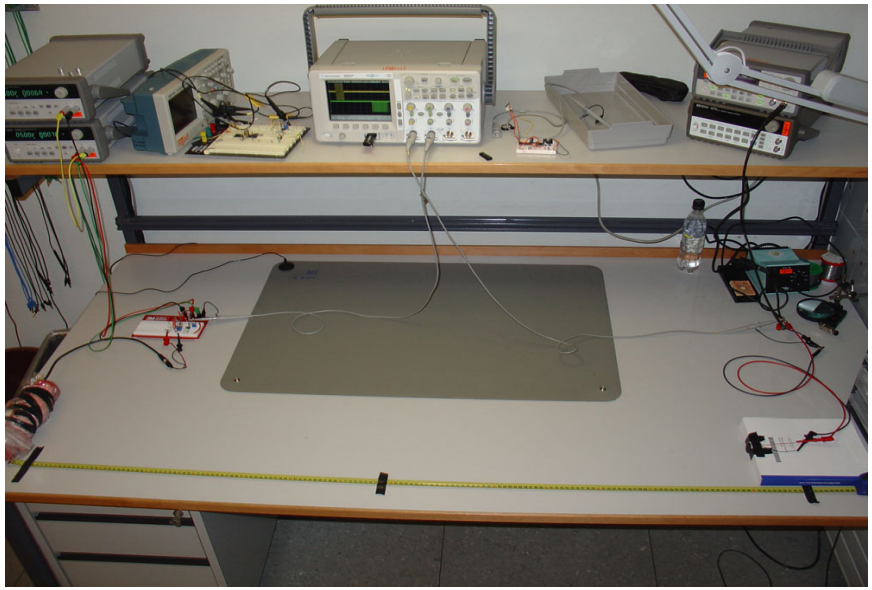
- ’get in the way" in case of an emergency.
- Emergency staff must be able to access the medical device.
- . . . possibly in another country.

Our Solution: Proximity Verification

- Main idea:
  - bind messages to distances &
  - physically proximity => trust
  - physical proximity is verified using ultrasonic distance bounding
  - no reliance on propagation assumptions



Implementation



- Speed of sound (air) 340m/s, (meat) 1500m/s
- Tr = few ns (<1mm)
- δp = 412ns (<1mm) in our prototype
- Ttotal ≈ Ts
- Distance measurement granularity: < 1cm
- Low power (0.28J / 1s protocol), 10J Defibrillation shock.

Summary

- Secure Proximity Verification can be a basis

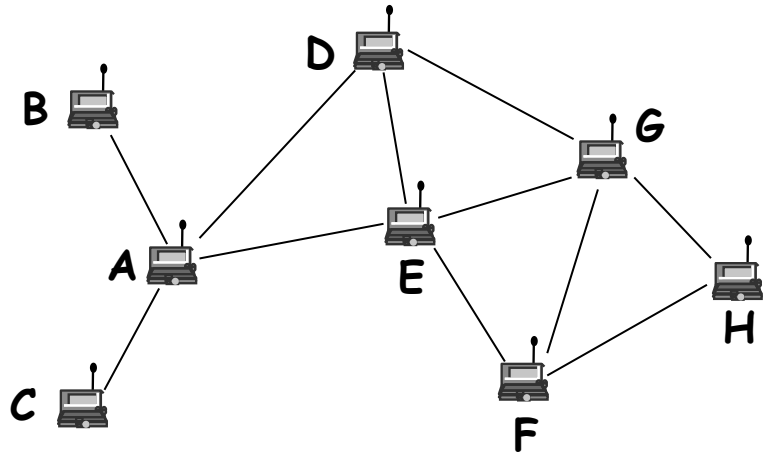
for Access Control to Implantable Medical devices.

- The solution is both secure and (patient) safe
- It can be built on top of either ultrasonic

or radio distance bounding

2.4 Secure routing in wireless ad hoc networks

Exchange of messages in Dynamic Source Routing (DSR):

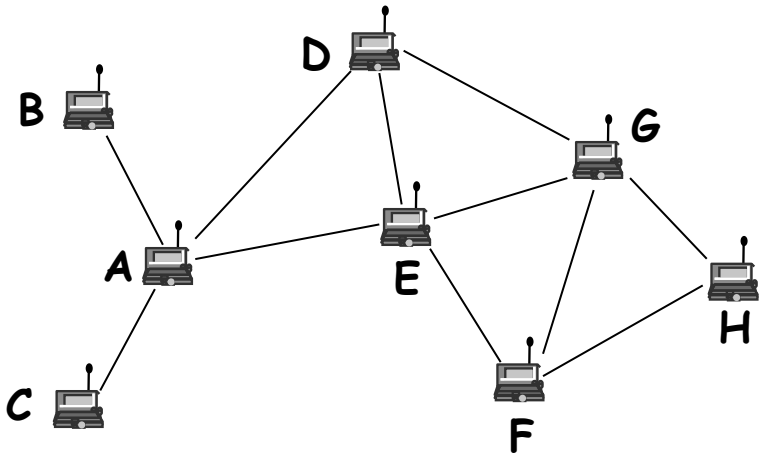


A → *: [req,A,H; -] → B, C, D, E
B → *: [req,A,H; B] → A
C → *: [req,A,H; C] → A
D → *: [req,A,H; D] → A, E, G
E → *: [req,A,H; E] → A, D, G, F
F → *: [req,A,H; E,F] → E, G, H
G → *: [req,A,H; D,G] → D, E, F, H

H → A: [H,F,E,A; rep; E,F]

- Routing disruption attacks
  - routing loop
  - black hole / gray hole
  - partition
  - detour
  - wormhole
- Resource consumption attacks
  - injecting extra data packets in the network
  - injecting extra control packets in the network

Operation of Ariadne illustrated



A → *: [req, A, H, $MAC_{K_{AH}}$, (), ()]

E → *: [req, A, H, h(E|$MAC_{K_{AH}}$), (E), ($MAC_{K_{E,i}}$)]

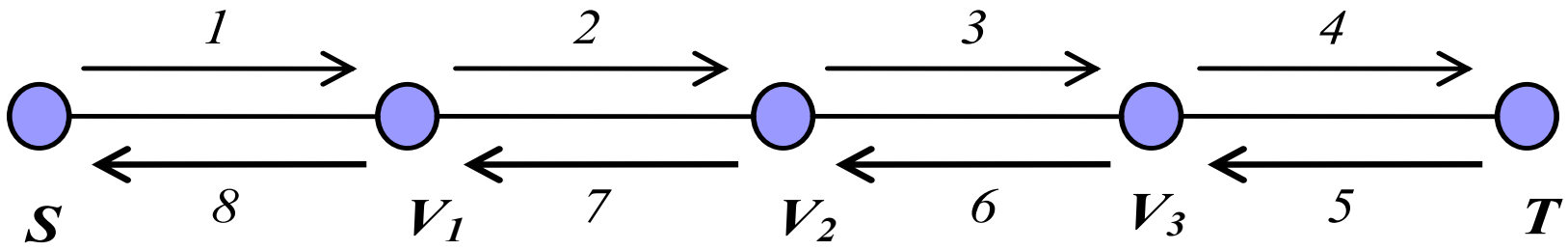
F → *: [req, A, H, h(F|h(E|$MAC_{K_{AH}}$)), (E, F), ($MAC_{K_{E,i}}$, $MAC_{K_{F,i}}$)]

H → F: [rep, H, A, (E, F), ($MAC_{K_{E,i}}$, $MAC_{K_{F,i}}$), $MAC_{K_{HA}}$, ()]

F → E: [rep, H, A, (E, F), ($MAC_{K_{E,i}}$, $MAC_{K_{F,i}}$), $MAC_{K_{HA}}$, ($K_{F,i}$)]

E → A: [rep, H, A, (E, F), ($MAC_{K_{E,i}}$, $MAC_{K_{F,i}}$), $MAC_{K_{HA}}$, ($K_{F,i}$, $K_{E,i}$)]

Secure route discovery with the Secure Routing Protocol (SRP)



Route Request (*RREQ*): S, T, Q_{SEQ}, Q_{ID}, $MAC(K_{S,T}, S, T, Q_{SEQ}, Q_{ID})$

(1) S broadcasts *RREQ*;
(2) V_1 broadcasts *RREQ*, V_1;
(3) V_2 broadcasts *RREQ*, V_1, V_2;
(4) V_3 broadcasts *RREQ*, V_1, V_2, V_3;

Route Reply (*RREP*): Q_{ID}, T, V_3, V_2, V_1, S,
$MAC(K_{S,T}, Q_{ID}, Q_{SEQ}, T, V_3, V_2, V_1, S)$

(5) $T \rightarrow V_3$: *RREP*;
(6) $V_3 \rightarrow V_2$: *RREP*;
(7) $V_2 \rightarrow V_1$: *RREP*;
(8) $V_1 \rightarrow S$: *RREP*;

Q_{SEQ}: Query Sequence Number
Q_{ID} : Query Identifier

More on secure routing

Secure Route Discovery

Hu, Perrig, and Johnson:
Ariadne, Sept. 2002, SEAD, Jun. 2002

Sangrizi, Dahill, Levine, Shields, and Royer: ARAN, Nov. 2002

Papadimitratos and Haas: Secure Routing Protocol (SRP), Jan. 2002

Zapata and Asokan: S-AODV, Sept. 2002

All above proposals are difficult to assess
➔ *G. Ács, L. Buttyán, and I. Vajda*:
Provably Secure On-demand Source Routing
IEEE Transactions on Mobile Computing, Nov. 2006

Secure Data Communication

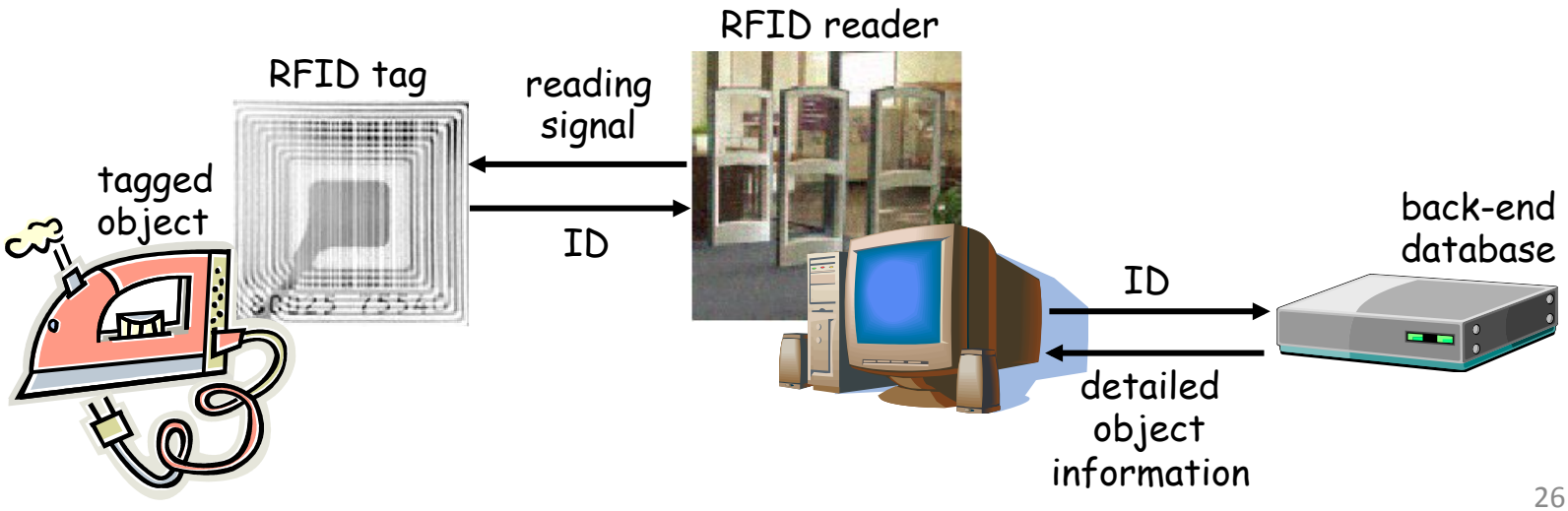
Papadimitratos and Haas: Secure Single Path (SSP) and Secure Multi-path (SMT) protocols, Jul./Sept. 2003, Feb. 2006

Cross-layer attacks

Aad, Hubaux, Knightly:
Jellyfish attacks, 2004

2.5 Privacy: the case of RFID

- RFID = Radio-Frequency Identification
- RFID system elements
  - RFID tag + RFID reader + back-end database
- RFID tag = microchip + RF antenna
  - microchip stores data (few hundred bits)
  - Active tags
    - have their own battery → expensive
  - Passive tags
    - powered up by the reader's signal
    - reflect the RF signal of the reader modulated with stored data

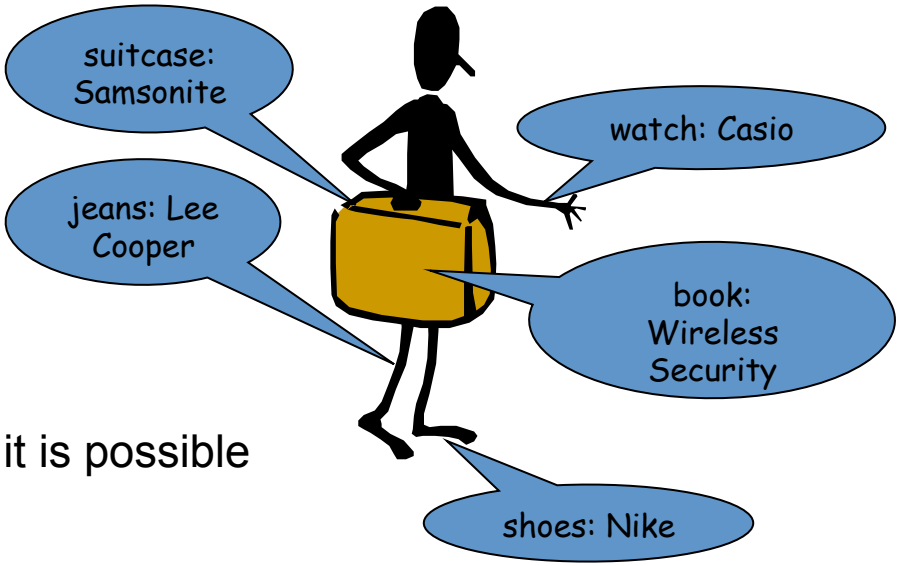


RFID privacy problems

- RFID tags respond to reader's query automatically, without authenticating the reader

→ clandestine scanning of tags is a plausible threat

- Two particular problems:
  1. **Inventorying**: a reader can silently determine what objects a person is carrying
     - books
     - medicaments
     - banknotes
     - underwear
     - …
  2. **Tracking**: set of readers can determine where a given person is located
     - tags emit fixed unique identifiers
     - even if tag response is not unique it is possible to track a set of particular tags



Juels A., RFID Security and Privacy: A Research Survey, *IEEE JSAC, Feb. 2006*

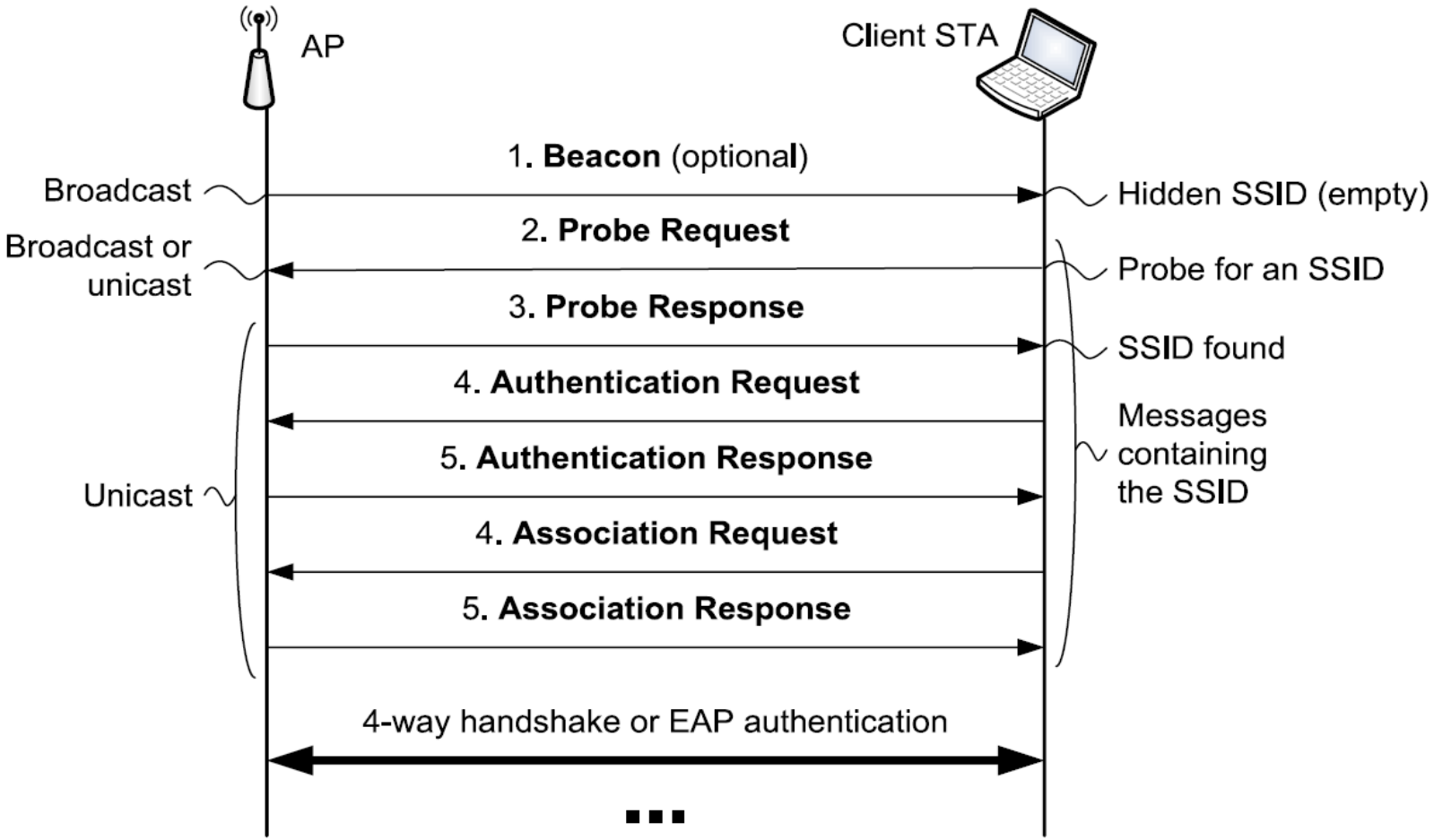
Privacy-Preserving 802.11 Access-Point Discovery

J. Lindqvist, T. Aura, G. Danezis, T. Koponen,
A. Myllyniemi, J. Mäki and M. Roe
Helsinki University of Technology (TKK) and
Helsinki Institute for Information Technology (HIIT), Finland
Microsoft Research, Cambridge, UK
WiSec 2009

WiFi Privacy Problem

- Directed active probes (in hidden networks) reveal preferred networks SSID to anyone listening
- SSIDs:
  - Human-readable
  - Names of Organizations, Companies, and government departments

WiFi Privacy



Extensible Authentication Protocol

Privacy Threat Examples (1):

- John works at a major consultancy company
- He often visits client sites as part of his work
- An eavesdropper observers the probes from John's laptop at a local cafe.
- Eavesdropper learns the client sites that John has visited
- Eavesdropper may infer information about their commercial relationships.

Privacy Threat Examples (2):

- Jenny works at a local hospital.
- An attacker seeks unauthorized access to patient records.
- Attacker eavesdrops a coffee-shop network and identifies Jenny's laptop as having been connected to the hospital WLAN.
- Attacker can then target her for social engineering or steal her laptop in order to extract her credentials for the hospital network.

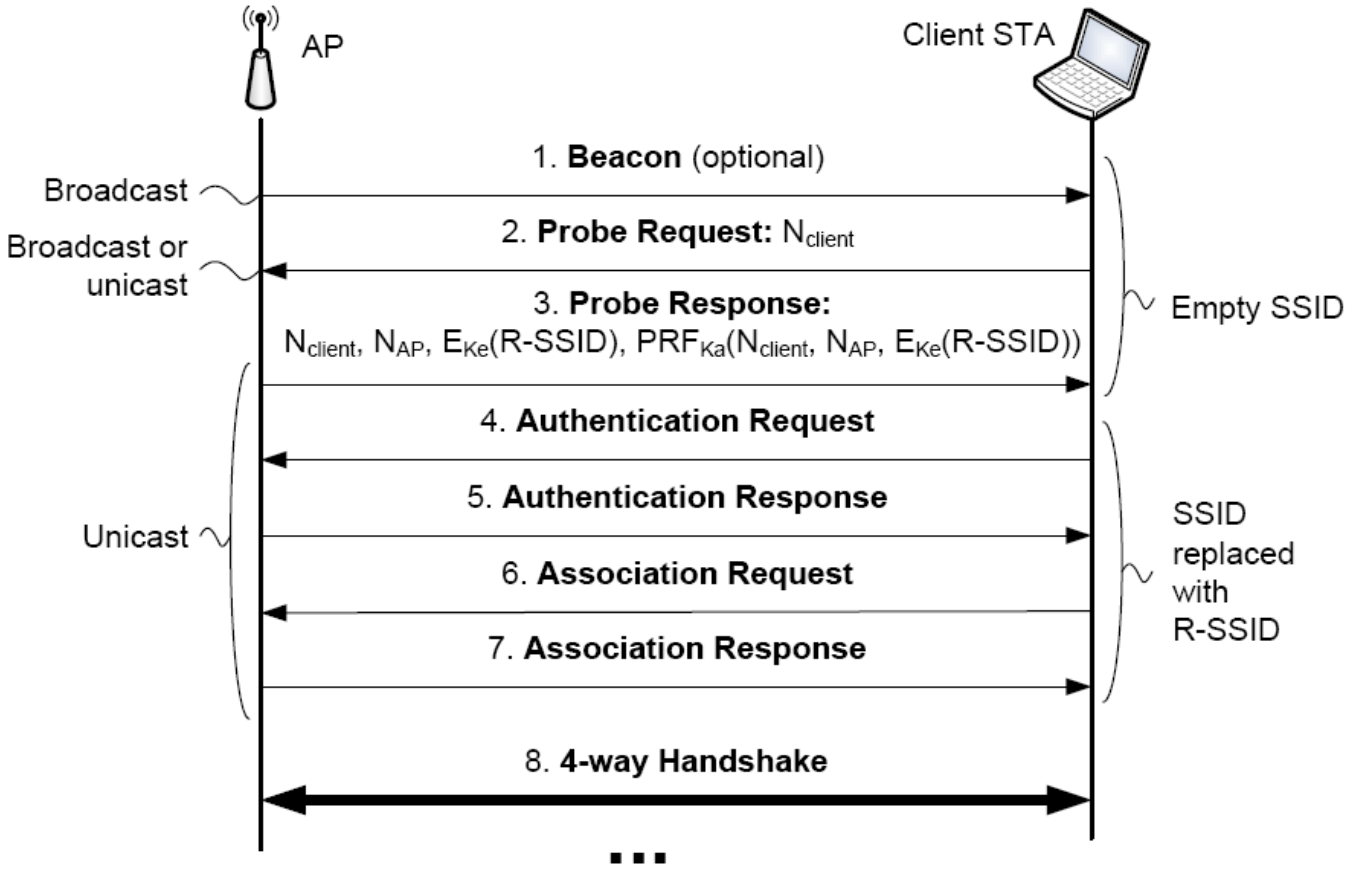
Privacy Threat Examples (3):

- Jack works for the government and participates in a conference abroad.
- A local extremist group detects his association with a foreign government network and targets him for abuse.

Information Leaks in WiFi Networks

physical fingerprint of the radio transmitter
logical MAC-layer fingerprint (capabilities and parameters)
client MAC address, access point BSSID
SSID(s) in Beacon and Probe Response
willingness to associate with an SSID
SSID in authentication and association exchanges
TLS certificates in EAP-TLS
physical location of the clients and AP
association between clients and APs (implicitly associates APs with each other)

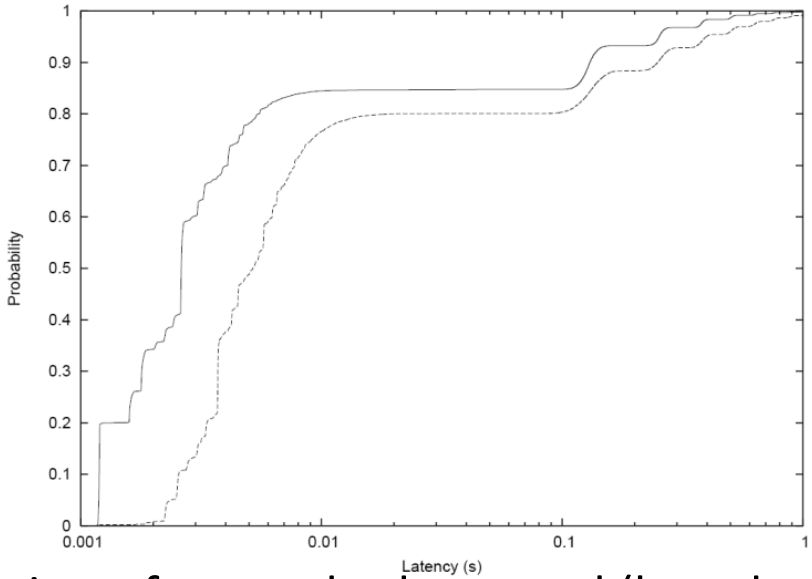
Privacy-preserving access-point discovery protocol



Main Idea:
AP and all STAs share a single pre-shared secret key PSK

Implementation and Conclusion

- This could be easily implemented and is also compatible with the previous version
- There is no significant performance loss when it is implemented on commercial 802.11 devices



Probe processing times for standard protocol (broadcast SSID) (solid line) and for proposed protocol (dotted line)

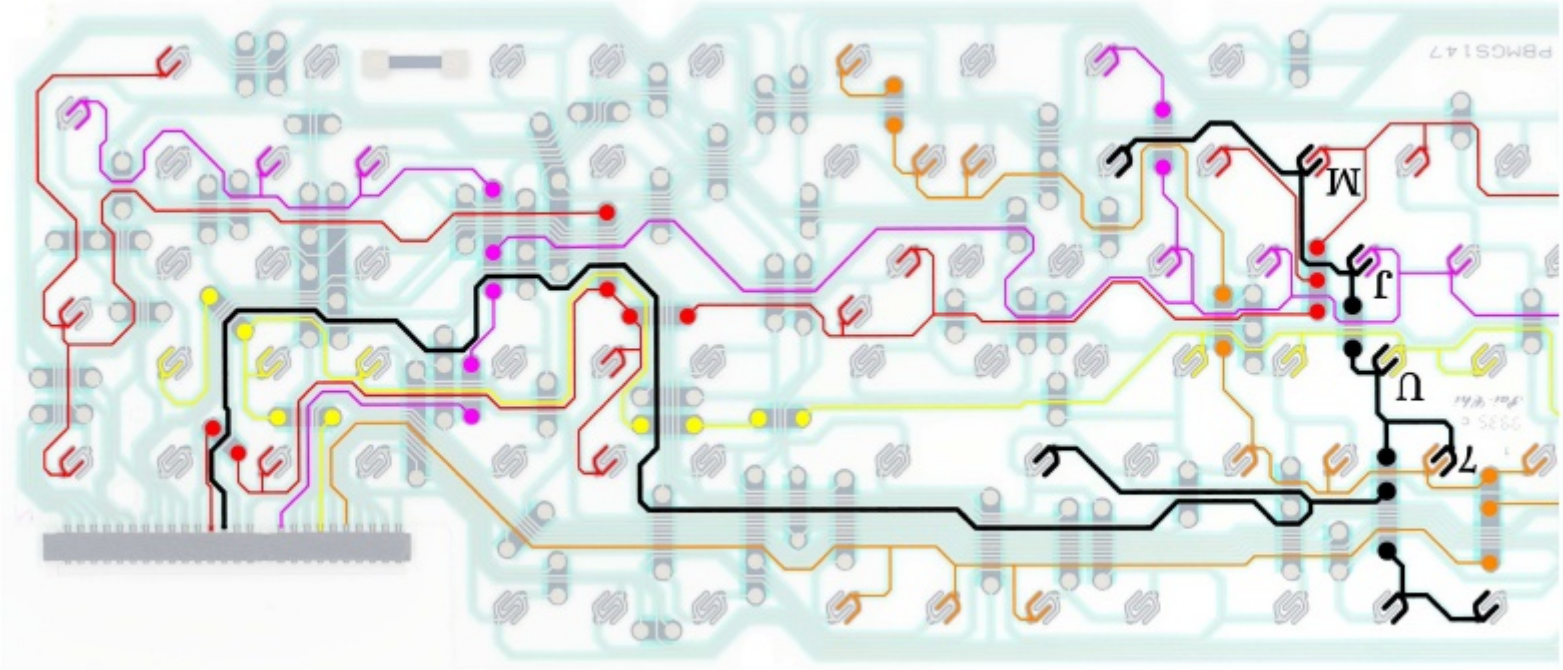
Compromising Electromagnetic Emanations of Wired and Wireless Keyboards

M. Vuagnoux and S. Pasini
EPF Lausanne, Switzerland
USENIX Security Symposium 2009

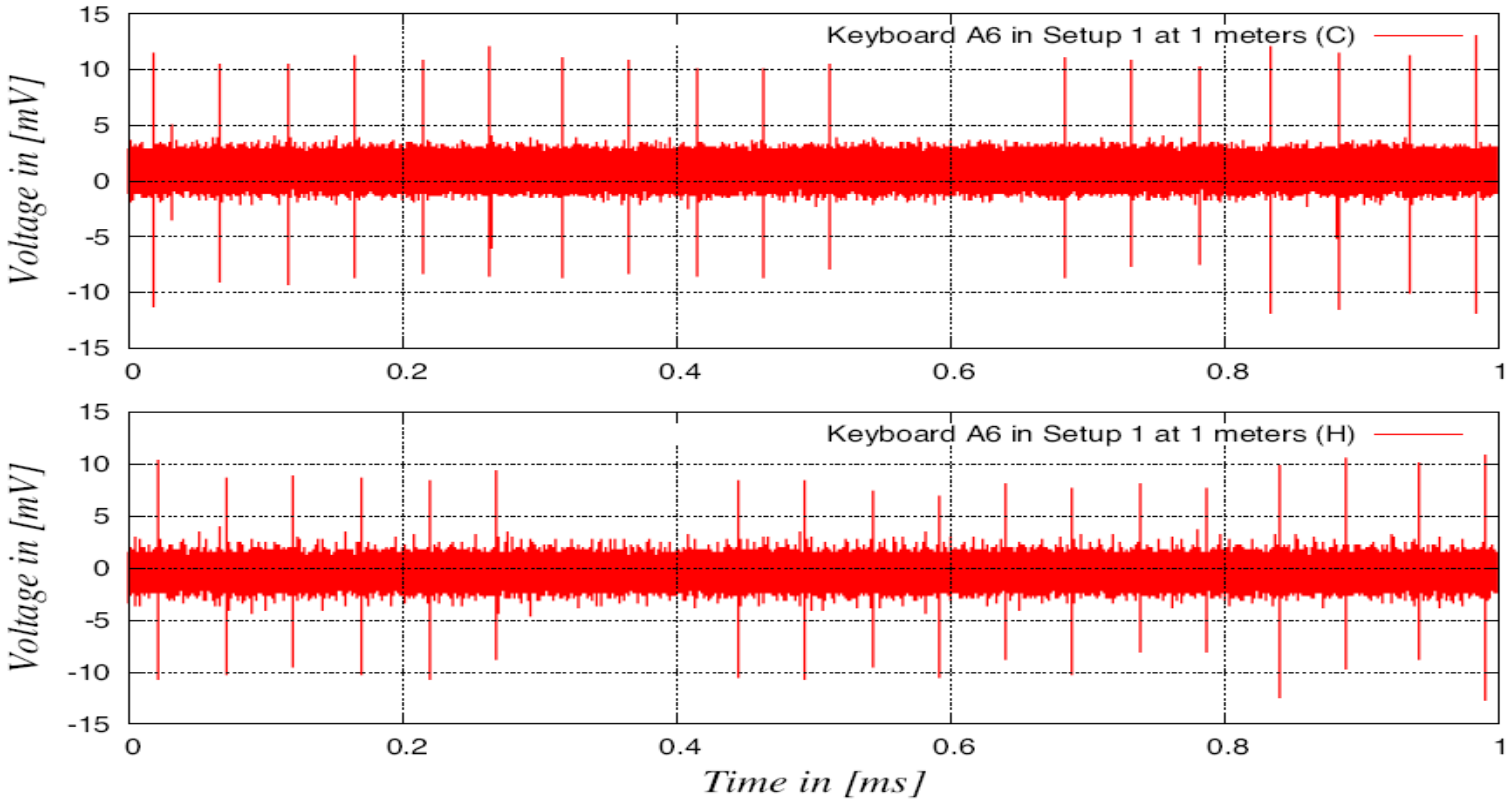
Keyboard Eavesdropping

- We type confidential data with our keyboards
- Keyboards emit electronic waves
- Can we eavesdrop keystrokes?

Matrix Polls Columns One-by-one



Matrix Scan Emanations for Letter C and H



Alpha-numeric key classification according to the key scanning routing

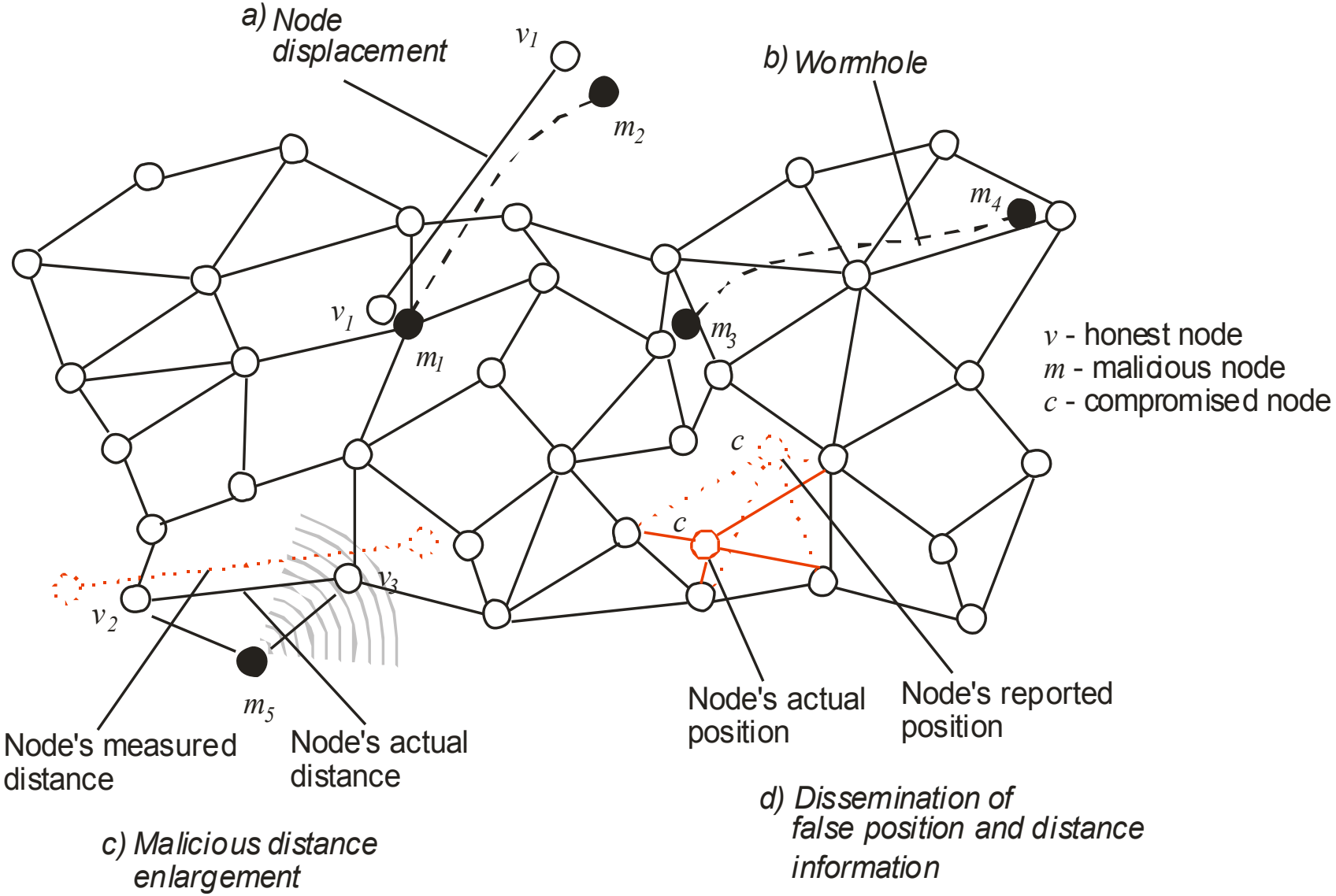
Peak trace	Possible Keys
7	6 7 h J M N U Y
8	4 5 B F G R T V
9	Backspace ENTER
10	9 L O
11	0 P
12	3 8 C D E I K
13	1 2 S W X Z
14	SPACE A Q

Vulnerability of Some Keyboards

Keyboard	Type	FETT	GTT	MT	MST
A1	PS/2	✓	✓	✓	✓
A2	PS/2	✓	✓		✓
A3	PS/2	✓	✓	✓	✓
A4	PS/2	✓	✓	✓	
A5	PS/2	✓	✓	✓	
A6	PS/2	✓	✓		✓
A7	PS/2	✓			✓
B1	USB				✓
B2	USB				✓
C1	LT	✓	✓		✓
C2	LT				✓
D1	Wi				✓

Falling Edge Transition Technique (FETT)
Generalized Transition Technique (GTT)
Modulation Technique (MT)
Matrix Scan Technique (MST)

2.6 Secure positioning

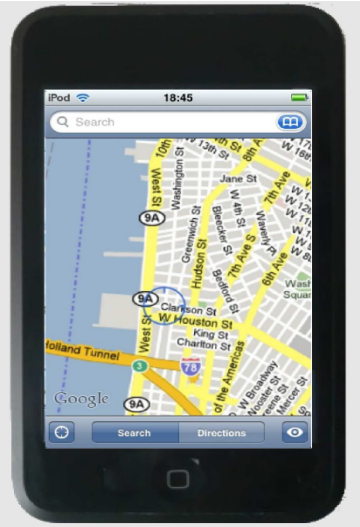


http://www.syssec.ethz.ch/research/spot

Attacks on Public WLAN-based Positioning Systems

Nils Ole Tippenhauer, Kasper Bonne Rasmussen,
Christina Popper, and Srdjan Capkun
ETH Zurich, Switzerland
MobiSys 2009

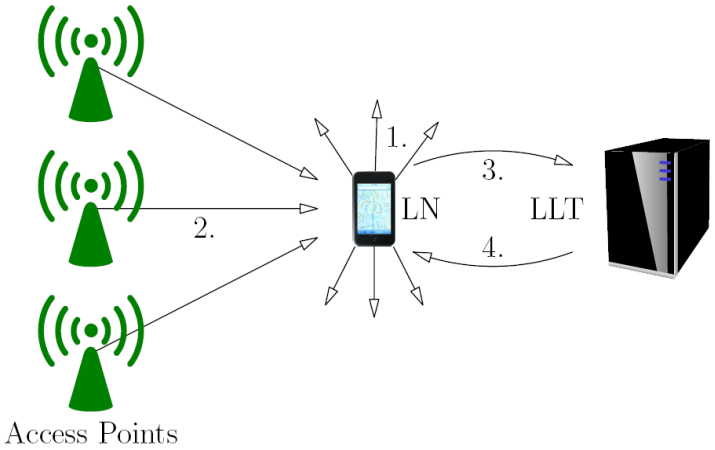
Introduction



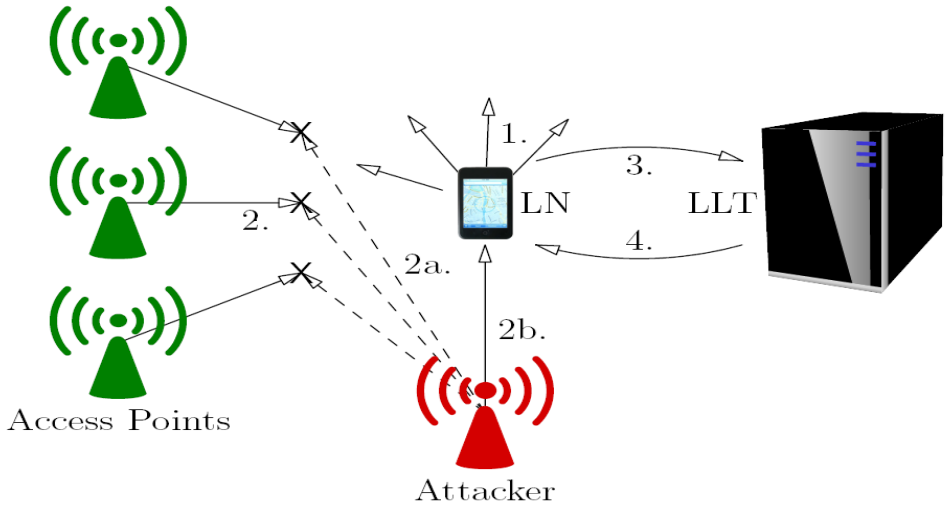
- **Public WLAN-based positioning systems**
  - Allow localization using omnipresent wireless access points
  - Enable devices without GPS to establish their position
  - Allow localization with precision of 10m, even indoors or underground
- **Skyhook's WPS in the iPod and iPhone**
  - In iPhone and iPod touch since late 2007
  - Skyhook also offers additional services such as localization of stolen devices
  - iPhone OS 3.0 allows tracking of iPhone via PC

How does it work?

- The localized node (LN) sends out probe request frames on all channels
- Access points announce their presence
- Observed MAC addresses are sent to the location lookup table (LLT)
- The LLT replies with location information (the traffic between LN and LLT is encrypted)



AP Impersonation Attack



2a. Attacker jams legitimate AP announcements

2b. Attacker inserts own impersonated AP announcements

3. LLT is now queried for location of remote APs

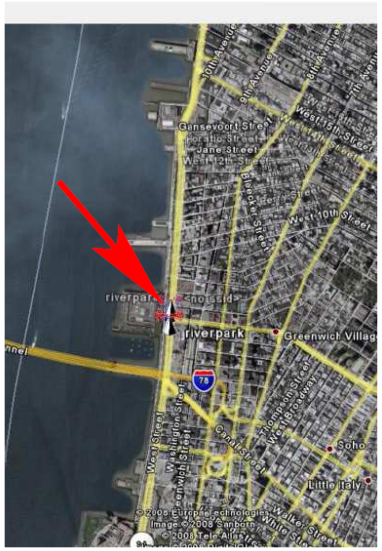
Attack Details

- Impersonating APs
  - MAC addresses of real APs at remote location
  - Obtained through WiGLE - a public wardriving database
  - Impersonation by single laptop constantly changing its MAC address

Attack Details

- Jamming the legitimate APs
  - We sent noise on 3 channels using two GNURadios
  - Many alternative options: physical layer, protocol layer
  - Fourth channel was used to send data of 4 impersonated APs

Results of Attack



- Jamming worked very reliably and was easy to achieve
- When using only the public WLAN localization, the devices localized themselves at the remote location in New York city
- For the iPhone, additional GSM cell localization prevented a change of location outside the local city radius

Countermeasure

Several proposals to mitigate the presented impersonation attack:

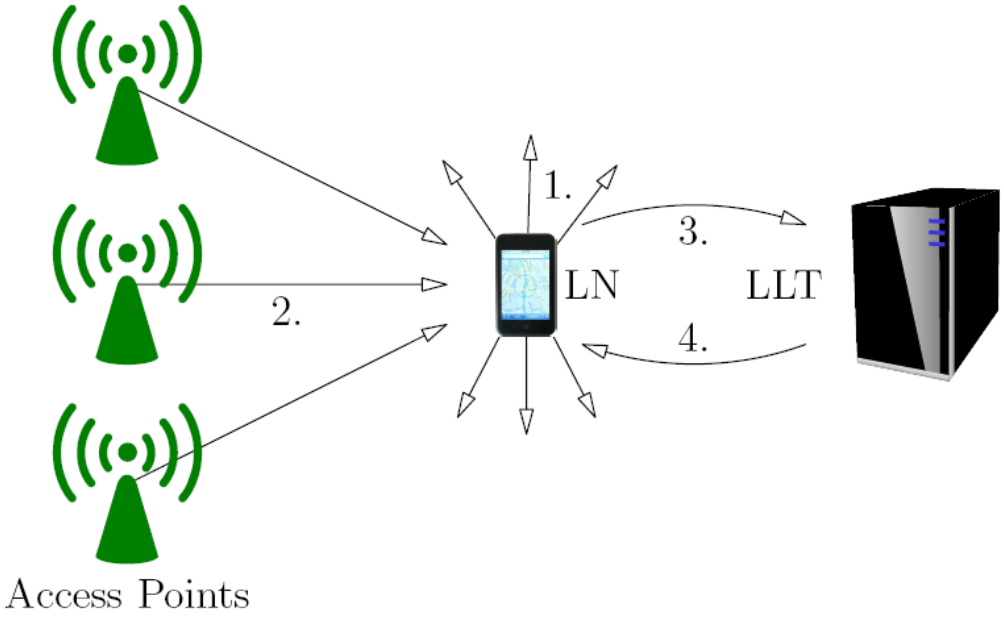
1. AP authentication
2. Aggregation of multiple localization methods
3. LN-based integrity checks
4. AP fingerprinting

LN based integrity checks

- Basic variant:
  - Compare new position with last known position
  - Assume maximum speed to detect large displacements
- Continuous version:
  - Periodically record MAC addresses from present location
  - Integrity check over last n locations
  - Warn user or abort localization

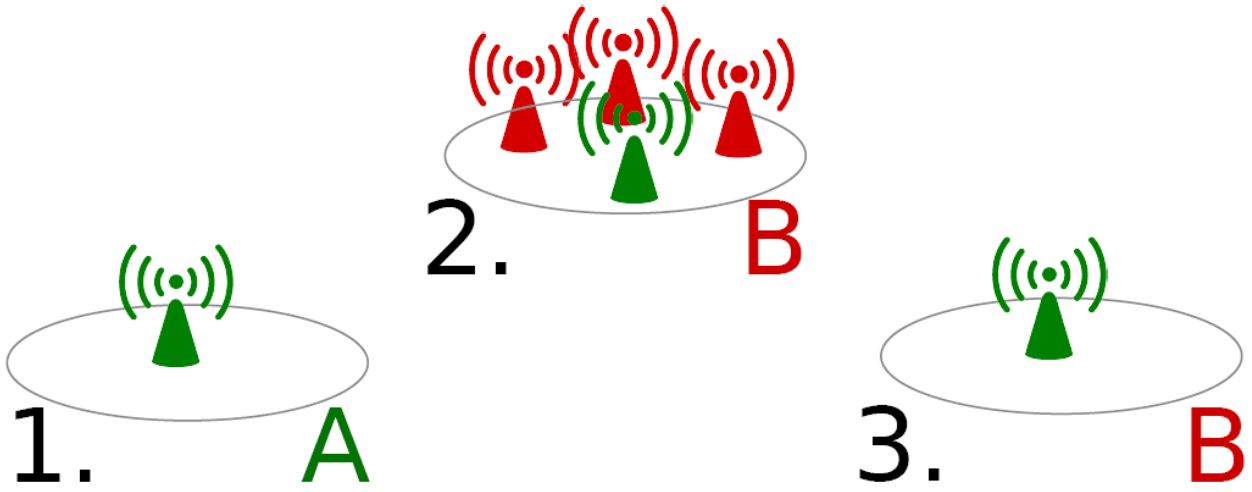
Low cost solution, but low precision and prone to false alarms. Prevents only large displacements.

Database Manipulation Attacks



So far, attacks on the left side were discussed.
Attacks on the LLT are possible as well, and will affect all users of the service.

Database Manipulation Attacks



1. The AP's location in the LLT is A
2. The attacker reports the AP among other APs at location B
3. As a result, the AP's location is changed to location B in the LLT

Database Manipulation Countermeasures

- ❖ Data update rules: allow several possible locations with different confidence values
- ❖ The location with the highest confidence value is active
- ❖ Confidence depends on majority votes or consistency of location reports with current data
- ➢ Temporal update rules: update the LLT quicker for changes with high confidence, and slower for changes with low confidence
- ➢ Tradeoff between database freshness and resistance against attacks

The provider can choose to only rely on self collected data, but this will lead to outdated entries.

Final Remarks

- Similar attacks are possible on GSM and even GPS
- Combine these attacks to defeat devices using all these mechanisms
- Exploration of signal fingerprints of APs