Wireless Security gets Physical

Srdjan Čapkun

Department of Computer Science
ETH Zürich

10.03.2009
Age of wireless communication ...

- Mesh Networks (Inter and Inter-home)
- Vehicular Networks
- Sensor/Actuator Networks
- Networks of Robots
- Underwater Networks
- Personal Area (body) Networks
- Satellite Networks (NASA 2007)
- Cellular, WiFi, ..

- Digitalization of the physical world: every physical object will have a digital representation
- “Internet of things” communication with every object/device
What changed?

- Physical layer
- Physical locations of devices

![Diagram showing change from wired to wireless connections]
The change for worse or for better?

- **Physical layer**
  - “New” risks: insertion, jamming, eavesdropping, ...
  - Opportunities: broadcast, localization, device identification, ...

- **Physical locations of devices**
  - New problems: how do we (securely) localize devices, track them, how do we verify their claimed locations?, location privacy, ..
  - Opportunities: using location information to secure even basic network services (key establishment), access control, data gathering ...
A simple example
Example: Distance bounding (Verification)

B node cannot pretend to be closer than it really is, only further !!!


\[ \epsilon \text{ time (xor)} \]

\[ t_0 \]

\[ t_3 \]

\[ 1 \ldots n \]

\[ \text{sign}_{KU} \{ \text{decommit (} N_B \}) \]

Brands and Chaum, 1993

Many variants and implementations followed.
From Distance to Location Verification

- Verifiable Multilateration
  - prevent distance reduction attacks (distance bounding)
  - multilateration using distance bounding within a verification triangle

Device cannot cheat on its location within the triangle !!!

Can only pretend to be outside of the triangle.

$d = \text{distance bound from BS to B}$
From Distance Verification to Message Auth. (I)

- **Main idea:**
  - bind messages to distances &
  - keep your friends close

- **Authentication through (attacker) absence awareness**
  - No reliance on propagation assumptions
From Distance Verification to Message Auth. (II)

\[ (c,o) = \text{commit}(m=g^b) \]

A: \[ d^* = (t_R - t_S) v_{\text{sound}} \]

verify that there are no devices at any distance \( d^{**} \ll d^* \)

Integrity regions prevent MITM attacks e.g., on DH protocol.
Authentication through presence awareness

- Main idea:
  - Use special message encoding (Integrity coding)
  - Receiver(s) know that they are in range of the sender (presence awareness)
Integrity Coding

- k-bit Beacon1 spread to 2k bits (1->10, 0->01) \( (H(m) = k/2) \)
- transmitted using on-off keying (each “1” is a fresh random signal)

\[ H(m) = \text{the number of bits “1” in } m \text{ (Hamming weight)} \]
Integrity Decoding

- **Beacon detection:**
  - presence of signal ($> P_1$) during T on CH1 interpreted as “1”
  - absence of signal ($< P_0$) during T on CH1 interpreted as “0”

- **Beacon integrity and authenticity verification**
  - IF $H(m) = |m|/2$ THEN “m” was not modified in transmission

---

10 → 1, 01 → 0 (Manchester)
Integrity Coding Analysis

- Message Hamming weight is a public parameter $H(m) = |m|/2 = 2$
- Attacker can change $0 \rightarrow 1$ and $\text{NOT } 1 \rightarrow 0$ (except with $\varepsilon$)
- $A$ can detect all modifications of the message on channel CH1
- $A$ knows that BS is transmitting on CH1

$$m = 110110$$

$$H(m) \neq |m|/2 \Rightarrow m \text{ is invalid}$$
IC: Anti-blocking property of the wireless channel

1) $0 \rightarrow 1\langle \theta$, where $\theta \in [0, 2\pi)$

- phase shift

$$r(t) = \cos(\omega_0 t) - \cos(\omega_0 t - \theta).$$

receiver sender adversary

$$E_r = \int_0^{T_s} r^2(t) \, dt$$

$\approx 2T_s \sin^2 \left( \frac{\theta}{2} \right)$

original signal energy

signal energy of the cumulative sender + attacker signal

error in distance estimation (by the attacker)
IC: Randomization At the Sender

- K-slotted signal (spreading)
- \( \Phi \) random (e.g., chosen uniformly from \([0,2\pi])\)

\[
R(t) = \cos(\omega_0 t + \Phi) - \cos(\omega_0 t - \Theta), \quad \Phi \in U [0, 2\pi)
\]

Diagram:

\[ P[K_{attenuated} \leq K_\varepsilon] \geq 1 - \varepsilon \]
Implementation

10m

Power

Time (ms)

20m

Power

Time (ms)

50m

Power

Time (ms)

70m

Power

Time (ms)

90m

Power

Time (ms)
Integrity Coding: Summary

BS
- sends Integrity-coded messages (e.g., localization beacons or time-synchronization timestamps) on a designated channel

Node/User
- knows the coverage area
- is aware of its presence in the covered area (e.g., ETHZ campus)

Attacks
- Overshadowing results in all 1s being received => incorrect H(m)
- Jamming results in all 1s being received => incorrect H(m)
- Replay results in an incorrect H(m)

Benefit
- Broadcast authentication and message integrity protection through presence awareness
Anti-Jamming Broadcast and Key Establishment
Anti-jamming Techniques

- FHSS: Frequency Hopping Spread Spectrum

![Hopping sequence PRNG](image)

Hopping sequence (PRNG seed) must be known to the sender and receiver but not the jammer

- DSSS: Direct Sequence Spread Spectrum

![Spreading code PRNG](image)

Spreading code (PRNG seed) must be known to the sender and receiver but not the jammer

- Common anti-jamming techniques rely on pre-shared secret codes (keys)
Anti-jamming broadcast and key establishment

**Problem:** BS needs to broadcast a message to a large number of unknown receivers in an anti-jamming manner.

Anti-Jamming techniques rely on shared keys, but broadcasting node cannot share the same key with all recipients => dependency

The receivers might be untrusted and/or unknown!

Jamming in Wireless networks pushes us back to pre-PK era!
Solution: Uncoordinated Frequency Hopping

$$M := A, PK_A, \ldots$$

Problem: A message might be too long (contains a signature as well)
Solution: Fragment message and transmit each fragment in one slot

Problem: Fragments are not individually authenticated (poisoning attack)
Attacker might insert its own fragments => computationally infeasible message reconstruction.
Solution: Link fragments (e.g., using hash-links)

$$h_i := h(m_i) \quad h_i := h(m_{i+1} \| h_{i+1})$$
Solution: Uncoordinated Frequency Hopping

- Fragmentation

- Hash linking
  \[ h_l := h(m_l), h_i := h(m_{i+1} \mid h_i + 1) \]

- Bit coding/interleaving

Other approaches: accumulators, turbo-codes, short signatures, Merkle trees ...
UFH: analysis

Uncoordinated Frequency Hopping: brief analysis
insertion/poisoning

Cross-layer (DoS on communication and on computation)
Performance Evaluation: Illustrative Example

Relative throughput w.r.t. coordinated FH

- 1 MBit/s, 1600 hops/s, $c = 200$
- 128 bit key / 256-bit prime field for EC
- $|M| = 2176$ bits
- $l = 13$

![Graph showing relative throughput](image-url)
Broadcast Anti-jamming Communication: Summary

- Key establishment-anti-jamming dependency cycle
- New solutions break this dependency

- UFH
- Other ideas:
  - Yvo Desmedt (pre-shared sets of hopping sequences)
  - UDSSS (Uncoordinated Direct Sequence Spread Spectrum)
- Implementations using SDR (0.2-300s latency)

UFH and UDSSS achieve broadcast anti-jamming communication but reduce communication throughput.
Example: Attacks on iPhone localization system

- Attack goal: device displays an incorrect location
- Attack: **Jam** signals from legitimate APs
  - insert messages with MACs corresponding to other APs

- More attacks: database poisoning, ...
Summary/Conclusion

- We should not abstract-away the physical layer
  - When reasoning about the security of Wireless Networks we need to consider:
    - Their physical layer
    - Physical node locations and how they are obtained
  - ... and make use of the physical layer and the locations
References

- Brands, Chaum, Distance Bounding Protocols, Eurocrypt '93
- Capkun, Hubaux, Secure Positioning in Wireless Networks, Infocom'05, JSAC'06
- Rasmussen, Capkun, Location Privacy of Distance Bounding, CCS'08
- Tippenhauer, Capkun, UWB-based Secure Ranging and Localization, Tr ETHZ'08
- Capkun, Cagalj, Integrity Regions: Authentication Through Presence in Wireless Networks, WiSe'06
- Capkun, Cagalj et al., Integrity Codes: Message Integrity Protection and Authentication Over Insecure Channels, S&P(Oakland)'06, TDSC'08
- Strasser, Poepper, Capkun, Cagalj, Jamming-resistant Key Establishment using Uncoordinated Frequency Hopping, S&P(Oakland)'08
- Strasser, Poepper, Capkun, Efficient Uncoordinated FHSS Anti-jamming Communication, ACM MobiHoc 2009
- Boris Danev, Srdjan Capkun, Transient Based Identification of Sensor Nodes, ACM/IEEE IPSN 2009

- Other research: http://www.syssec.ethz.ch/research
Srdjan Čapkun, capkuns@inf.ethz.ch

http://www.syssec.ethz.ch/research
ACM Conference on Wireless Network Security (WiSec)

March 16-18, 2009
ETH Zürich, Switzerland

SPONSORED BY: