Device Pairing at the Touch of an Electrode

Marc Roeschlin, Ivan Martinovic, Kasper B. Rasmussen

NDSS, 19 February 2018
Bootstrap secure communication

Two un-associated devices derive a mutual secret

No trusted third party

Problem: Establish the identities of the devices

→ Device pairing protocol
Device Pairing (II)

Most existing schemes either

- require physical assumptions on the communication channel
- use an auxiliary channel → Security relevant decision

Desirable Properties

- Minimal user interaction / Simple interface
- Action of pairing devices should be a natural task
Our Idea

→ Two devices can be paired if they are being held by the same human at the same time

→ Physical access to both devices implies ability to pair
Our Approach

- Devices share two communication channels:
  - Unauthenticated wireless channel
  - **Body channel** via capacitive coupling

- Human touches an electrode on each device to establish data transmission
Intra-Body Communication

### Galvanic Coupling
- Induce alternating current into the body
- Small current propagates through human
  - Short transmission
  - Two electrodes required

### Surface Wave
- Similar to conventional RF transmission
- Uses body as a wave-guide
  - Affected by external electromagnetic waves

### Capacitive Coupling
- Return path through the environment
- Electrostatic coupling to earth ground
  + Hand-to-hand communication
  + One electrode
  + Low electromagnetic interference

---

![Diagrams of Galvanic Coupling, Surface Wave, and Capacitive Coupling](image-url)
**Adversary Model**

**Attacker**
- No physical access to devices
- Access to wireless channel
- Can listen on body channel

**Body Channel**
- Devices extract channel properties
- Read-only to external transmitter
Pairing Protocol

**Device A (Alice)**
- Pick $a, N_A$
- $A, (g^a \mod p), N_A$
- $K = (g^b)^a \mod p$
- $R_N = \text{MAC}_K(A||B||N_A||N_B)$
- Verify MAC
- Verify channel

**Device B (Bob)**
- Pick $b, N_B$
- $B, (g^b \mod p), N_B$
- $K = (g^a)^b \mod p$
- $L_N = \text{MAC}_K(R_N)$
- Verify MAC
- Verify channel

Body channel
Security Guarantees

Remote Pairing

- Attacker can establish key
- Key confirmation fails as body channel is read-only

MITM Attacks

- Not feasible if body channel is inaccessible
- Injection on body channel fails
The Body Channel

- Security of the pairing protocol relies on read-only property
- The receiving device needs to be able to distinguish between
  - A. Messages from another device being held by the person
  - B. Messages from an external source
- We experimentally verify this property
Proof-of-concept for body channel transmitter and receiver

- Frequency bandwidth: 0.5 MHz - 3.5 MHz
- Sending power: 5 milli-Watts
- Sender voltage: 3 Volts (pp)
- Current through body: ∼10 micro-Amperes

→ Miniaturized version can be manufactured as single chip
Encoding and Modulation

- On-off keying of manchester-encoded data
- Frequency sweep during "on"-periods
- Sweep allows to characterize the channel

Throughput and Error rate

- 500 bit/s (on-period is 1ms)
- Transmitting two 56bit MACs takes 224ms
- Measured bit error rate is below $10^{-6}$

User Safety

- Very little current flow through body
- < 12 micro-Amperes
- Much weaker than e.g., body composition scales
Body Channel Characteristics

- Energy transmitted on body channel is lost due to:
  - Capacitive coupling
  - Body is not perfect conductor

→ Sweeps are attenuated depending on frequency

→ Most specific frequencies between 0.5 MHz and 3.5 MHz
Experimental Analysis

We verify the read-only property in two ways:

1. Can messages be classified according to their origin?
2. Can messages be injected into the body channel?

Evaluation

Classify attenuation patterns generated by the frequency sweep

Two classes
- Intended use of body channel
- Injection attempts

Signal injection
- Different emitters
- At varying distances
Classification

Receiver operating characteristic for body channel receiver

Injection attempts and success rates

→ External sources can be detected with high probability

→ External source needs to be close to receiver and carry large capacitance
External Signal Injection

Human Body Model

- Simulate injection from near field
- Approximation with three cylinders
- Dielectric properties of human tissues
  - Receiver and transmitter can be attached anywhere on body

Read-only assumption holds if there is 50cm between body and adversary
Conclusion

1. Novel approach to device pairing using intra-body communication

2. Pairing becomes natural and straightforward

3. Body channel is read-only if there is at least 50 cm between body and signal source

4. Small form factor and low manufacturing cost
Questions and Discussion

Thank you!

marc.roeschlin@cs.ox.ac.uk
External Signal Injection

External Source

- Has to match body channel characteristics
- Attacker can not measure attenuation pattern of external transmitter
- Capacitive coupling only works in near field
- High capacitance and/or highly directional antenna with high output power needed

Pattern changes significantly if sheet is 5 cm further away from body

→ Attenuation pattern is volatile