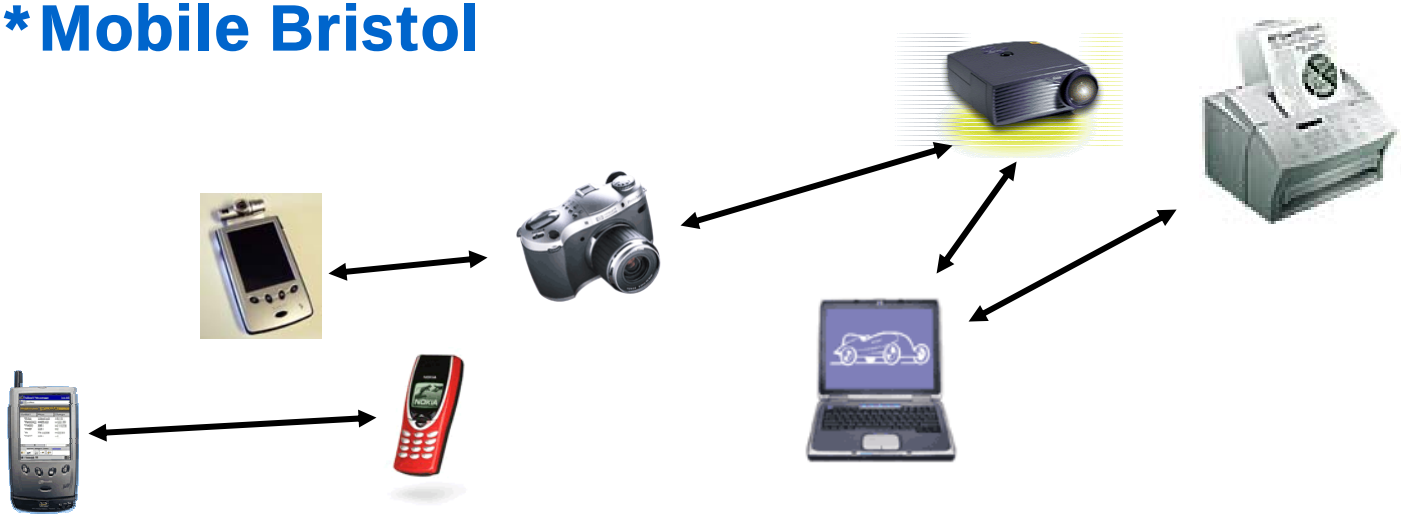
Secure Spontaneous Interactions in Ubiquitous Computing

Tim Kindberg* & Kan Zhang
HP Labs Bristol & Palo Alto
***Mobile Bristol**



hp invent

Overview

- Introduction
- Related work
- Protocols for secure spontaneous association
- Status and discussion

hp invent

Spontaneity

- Mobile users, wireless world
- Serendipitous opportunities for interaction
  - Human-human encounter
  - Device-device data exchange over wireless
- In infrequently visited locations

hp invent

Spontaneous interaction examples

- Conference attendees exchange data between PDAs/laptops
- Visitor sends photo to friend's printer (not neighbour's)
- Group of people in a café play a wireless game just between themselves
- Customer in Luigi's restaurant pays bill wirelessly using her "electronic wallet"

hp invent

Wireless spontaneous associations

‘Hotel Nomad’

Visited locations

Infrastructure devices

Personal devices

= data over 802.11, bluetooth, ..

hp invent

Speed & convenience

- No time to re-boot, or type IP numbers etc. into a configuration dialogue, ...
- At a distance (line of sight)
- Discreet
- Handing a password on a scrap of paper won’t do!

hp invent

Limited trust*

- Trust only one or more nearby users/devices
  - Dynamic “trusted computing base”
  - Others nearby on same network are untrusted
  - No trusted third-party
    - True peer-to-peer interaction

*A large topic in itself. See talk at UK-UbiNet workshop, Cambridge, May 5-7, 2004

hp invent

Level of security

- Spontaneity ⇒ low-to-medium sensitivity
- Need security good enough for “everyday” interactions

hp invent

Stages to secure interaction

1. Discovery/association
   - Virtual (name → address)
   - Physical (name/address → device)
2. Key exchange
3. Validation of key exchange
4. Secure communication channel (privacy, integrity)

hp invent

Virtual wire

- Want effect of wire...
  - Can see endpoint
  - Secrecy, integrity
- ....over wireless
- Physically validated key-exchange
- With *that* trusted device
  - (Might not be trustworthy!)

hp invent

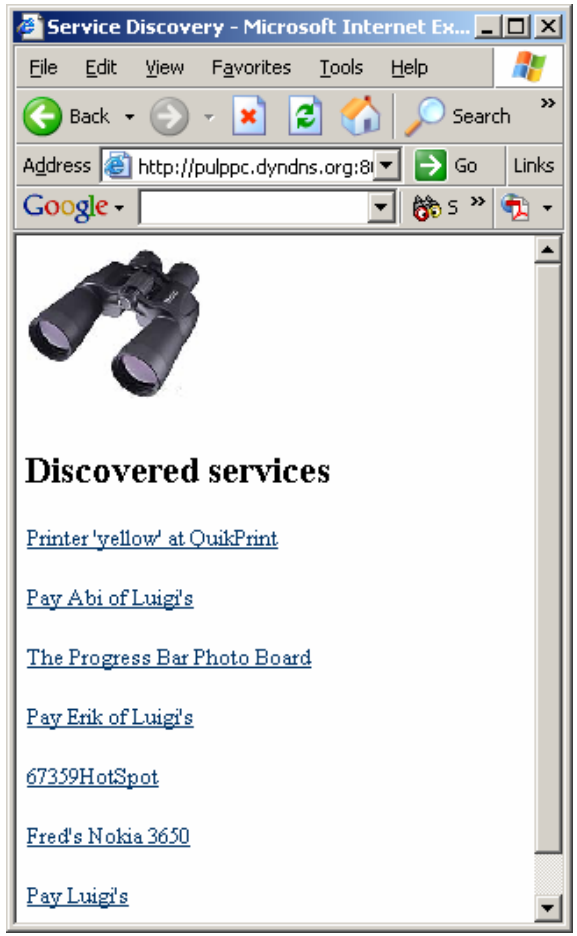
Overview

- Introduction: problem and contribution
- Related work
- Protocols for secure spontaneous association
- Status and discussion

hp invent

Discovery, association

- What's on this subnet?
- Unfamiliar names
- Similar names
- Bogus names



hp invent

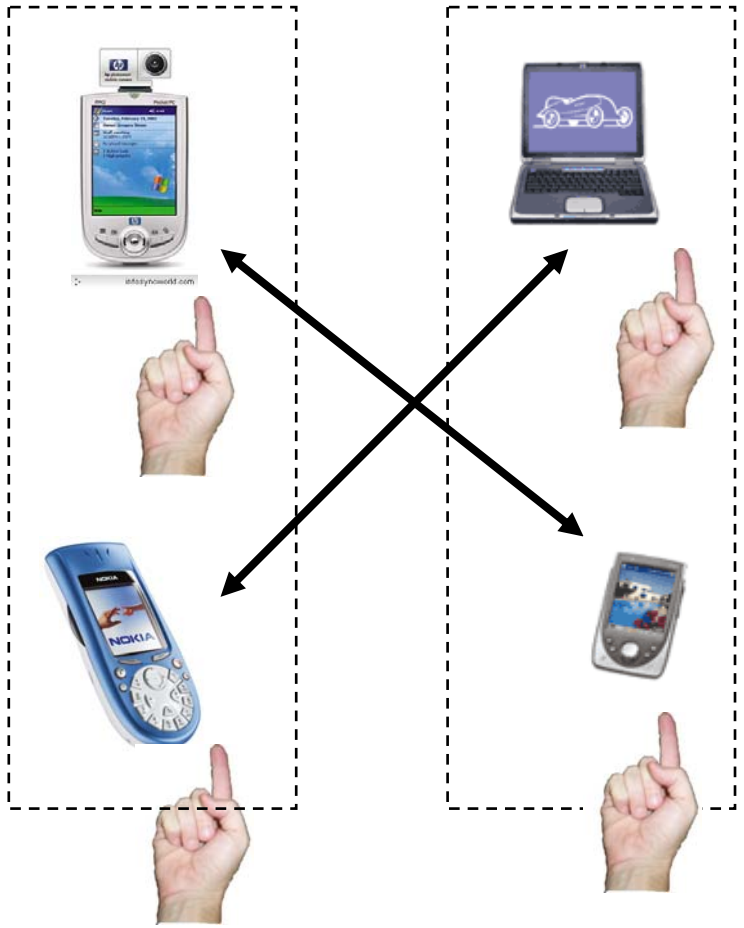
Two-button protocol

- Press buttons at more-or-less same time
- Multicast “associate”
- Listen for “associate” message in $\pm \Delta t$
- (HomeRF Technical Committee, 1998)

hp invent

Two-button protocol

- Fails the “crowd test”: liable to lead to accidental mis-associations



hp invent

Device-shake!

- Shake two devices together
- Record accelerometer readings
- Multicast signature of readings
- (Smart-Its)

hp invent

Direct electrical contact

- Use electrical terminals as a “physically constrained channel”
- (“Resurrecting duckling”, Stajano & Anderson)

hp invent

Human touch

- Use the human body as a physically constrained channel
- (Fukomoto et al, Partridge et al)

hp invent

Near Field Communication

- Short-range RF for communication parameters
  - C.f. RFID
- Nokia, Philips, Sony
- Protocol is “inherently secured”*

*Here we refer to the avoidance of unintended connections rather than protection against malicious intent (sic)

hp invent

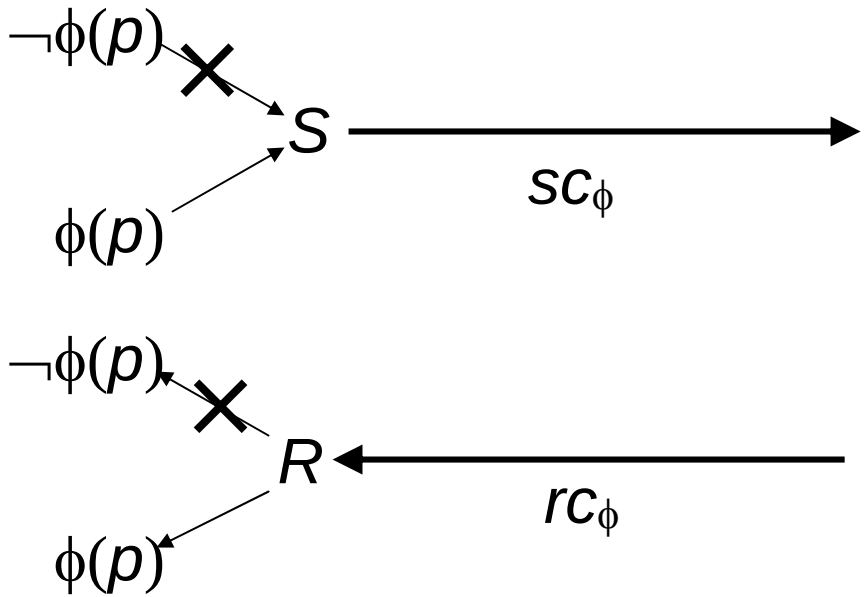
Infrared, audio

- Infrared
  - But 60º spread, reflected
- Audio
  - Leakage from room?
- (Balfanz et al PARC, Madhavapeddy et al, U Cambridge)
- “Constrained but leaky” channels
  - Fail crowd test
- Convenient

hp invent

Constrained channels

- Only sender/receiver with certain physical circumstances (ϕ) can send/receive
- Use:
  - Send authenticating material over channel
  - Send secret material over channel
- (Kindberg et al, Balfanz et al)



hp invent

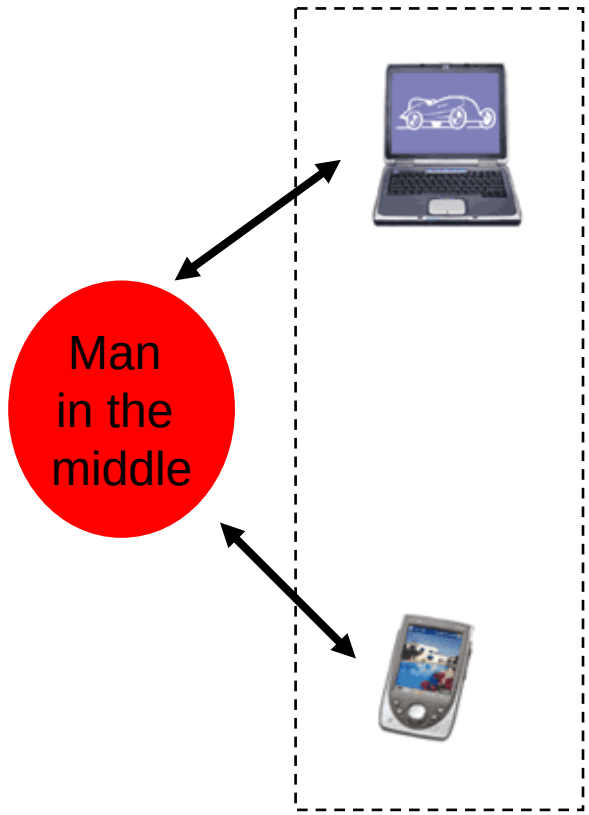
Overview

- Introduction: problem and contribution
- Related work
- Protocols for secure spontaneous association
- Status and discussion

hp invent

Threat model

- Send to wrong device is bad
- Man in the middle is worse



hp invent

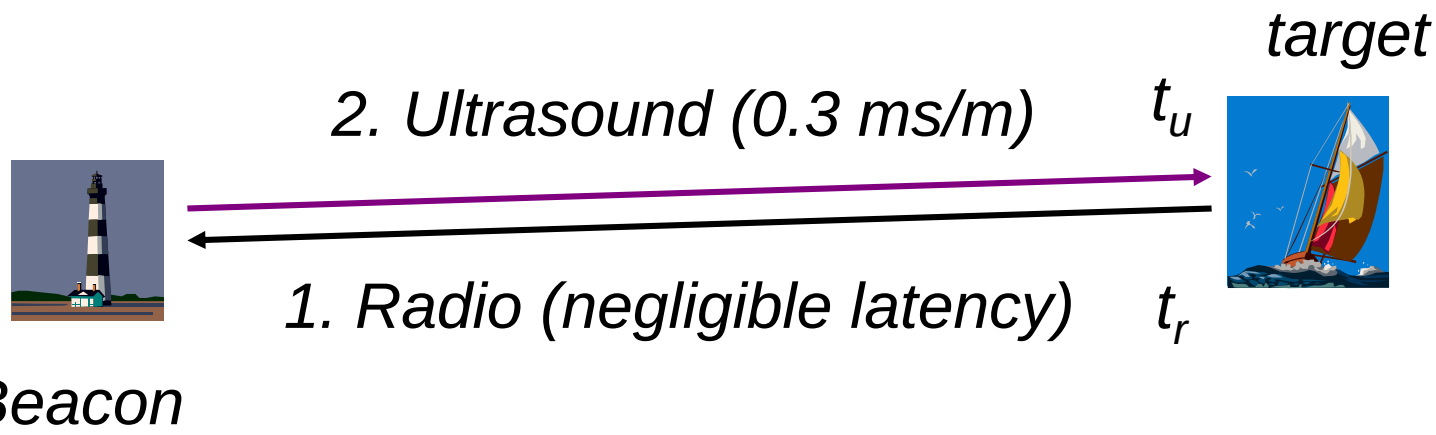
Contributions

- Protocols for two types of physically constrained channel not used for security before:
  - Ultrasound + RF
  - Laser
- Protocols requiring no special hardware
  - Harmony protocol

hp invent

Ultrasound & RF location

- U. Cambridge BATs; MIT crickets; Bristol, ..

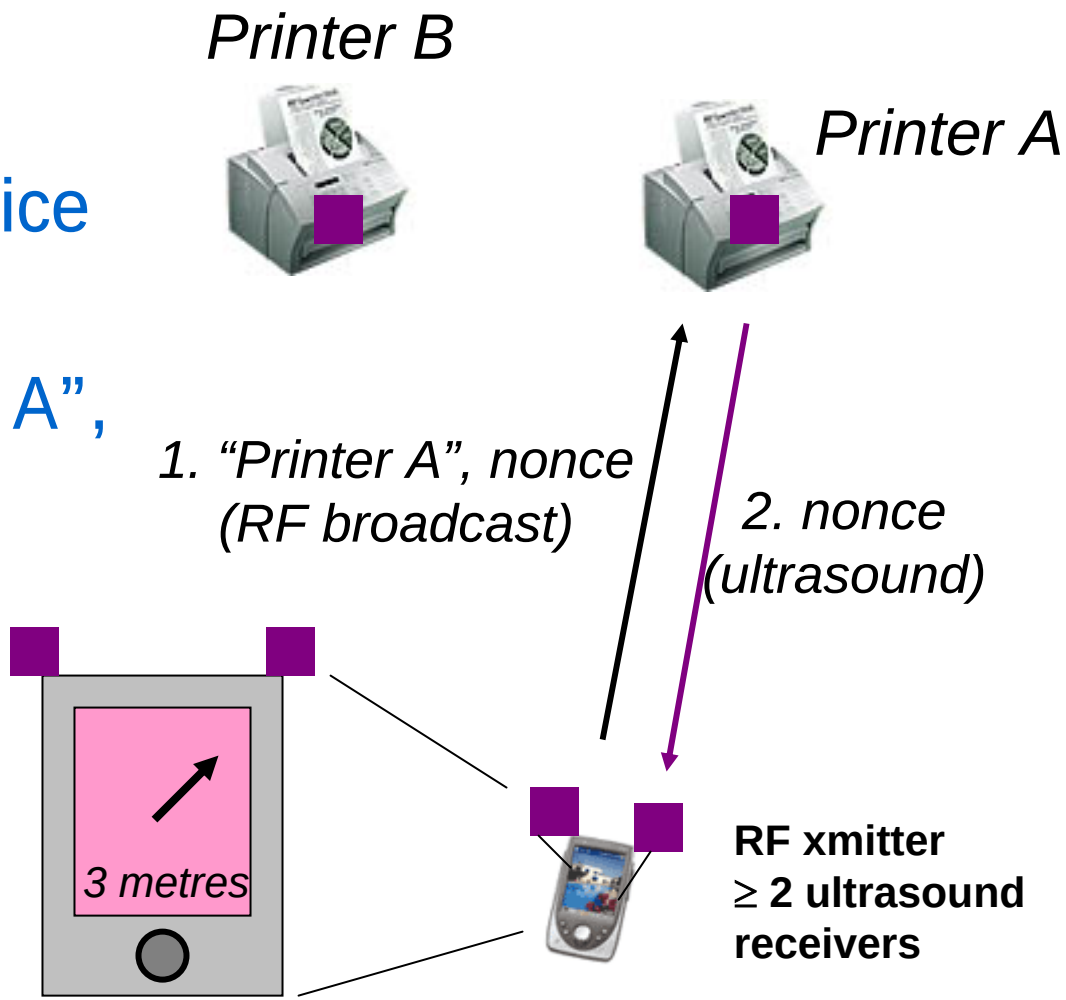


$$Distance = (t_u - t_r) / v_{sound}$$

(For location, now use N beacons and N-lateration)

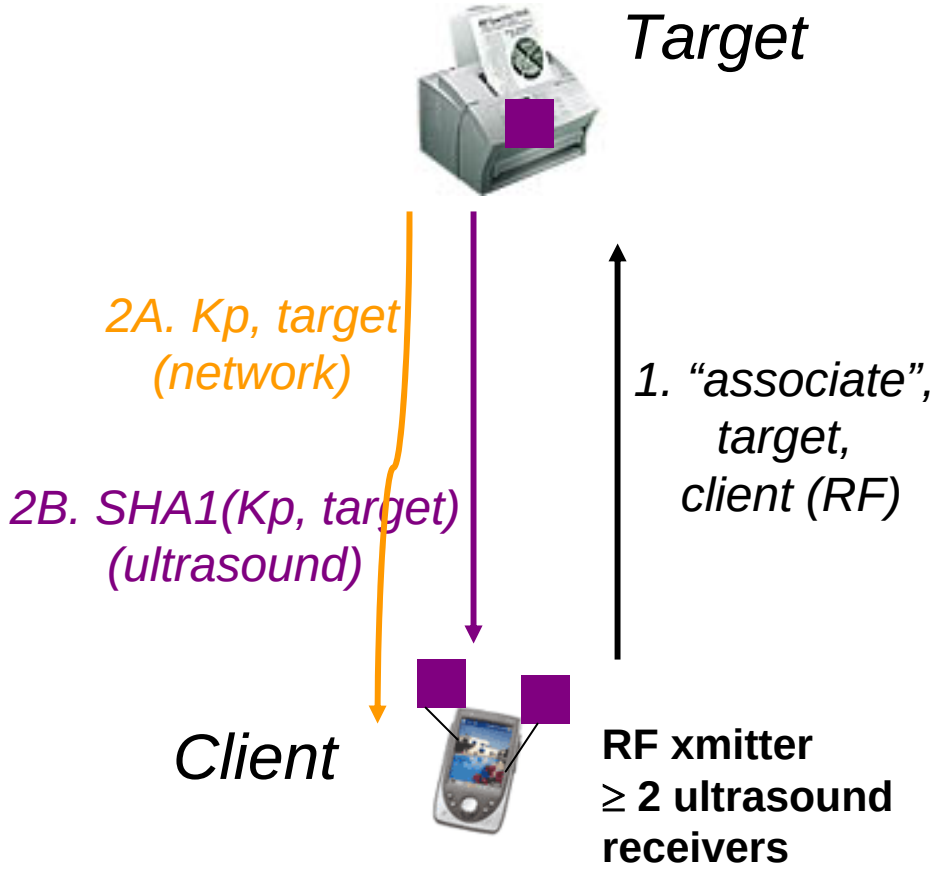
Protocol 1: Physically discover a network-discovered device

- The personal device as “divining rod”
- Where is “Printer A”, ”Bob’s mobile gamer”?
- (No security)



Protocol 2: Physically validated public-key exchange

- One-way validation of binding key ↔ device
- User verifies reported distance & angle



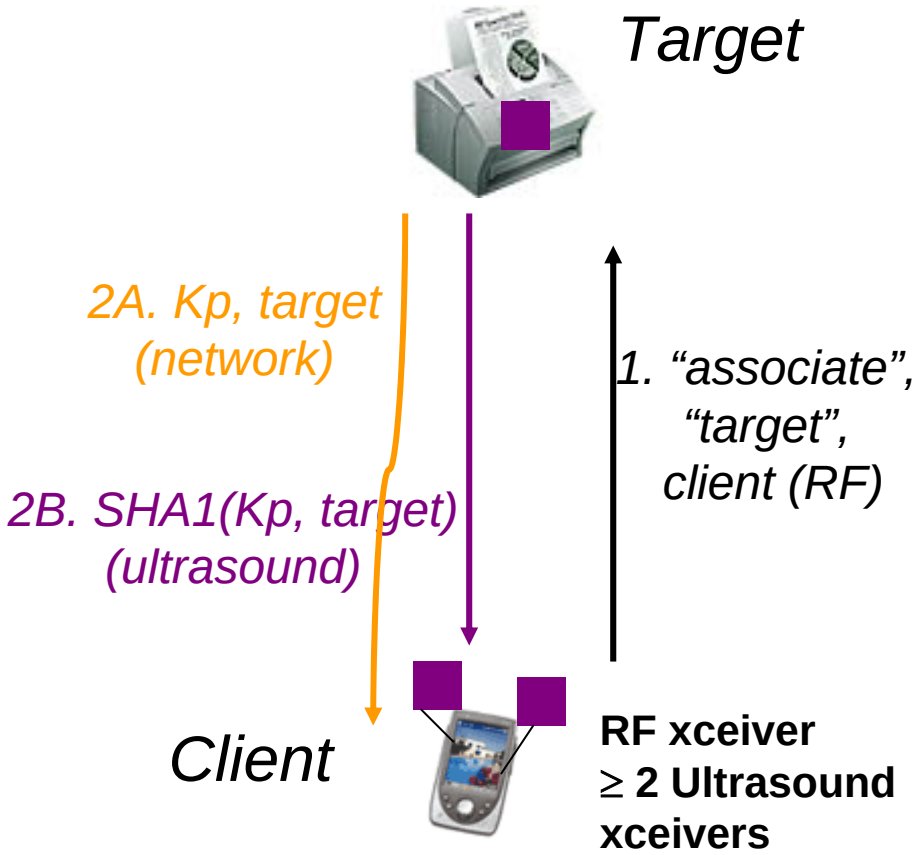
Protocol 3: Mutual validation

- E.g. wireless game-playing
- Run protocol #2 in each direction

RF xceiver
≥ 2 ultrasound xceivers

Difficult to spoof ultrasound message

- Attacker's ultrasound message must travel along same path (5º)
- Send from behind? Reflection?
  - No! Distance wrong
- In front?
  - No! User checks for obstructions
- Run from >1 positions



Implementation issues

- MIT experience suggests do-able
- But ultrasound noise/multipath $\Rightarrow$ few bits can be transmitted in hash (enough?)
- Specialised hardware: could we make it as normal/integrated as IR in a TV remote?

hp invent

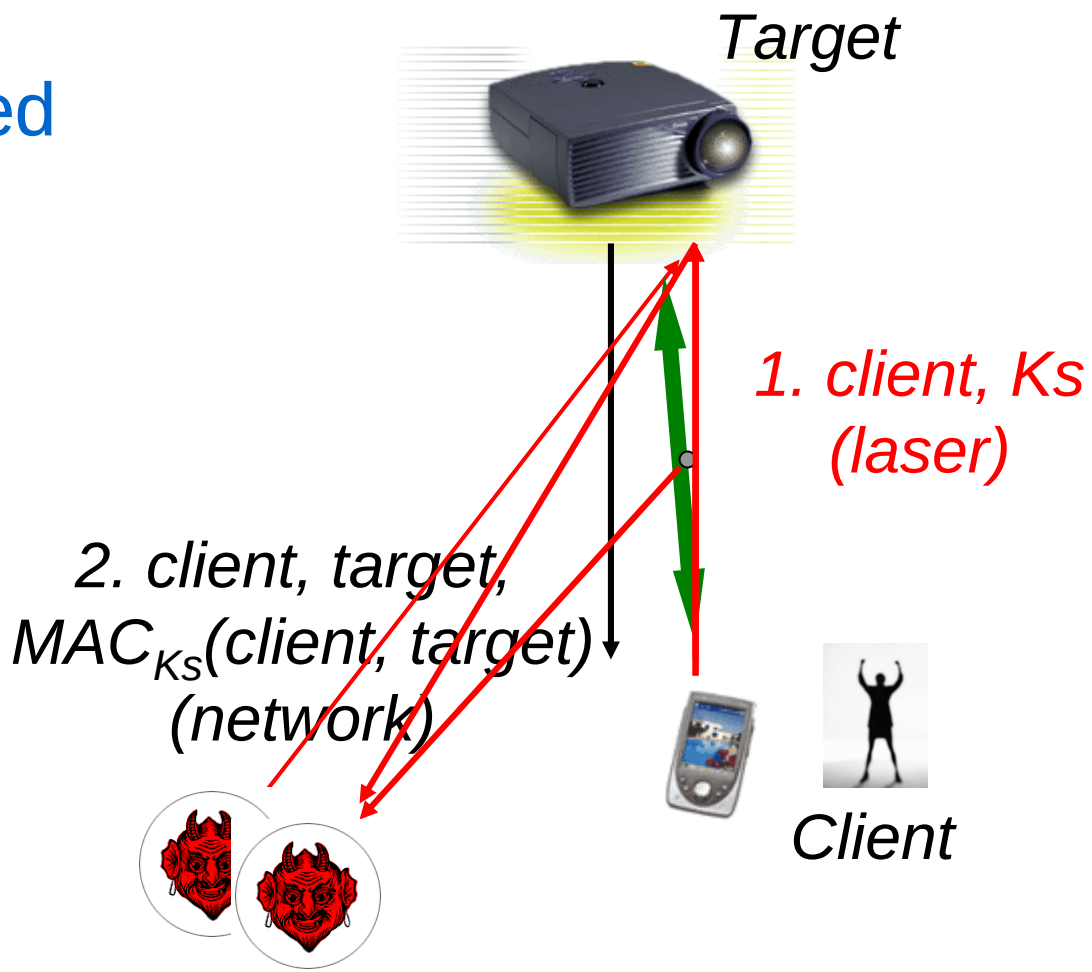
Contributions

- Protocols for two types of physically constrained channel not used for security before:
  - Ultrasound + RF
  - Laser
- Protocols requiring no special hardware
  - Harmony protocol

hp invent

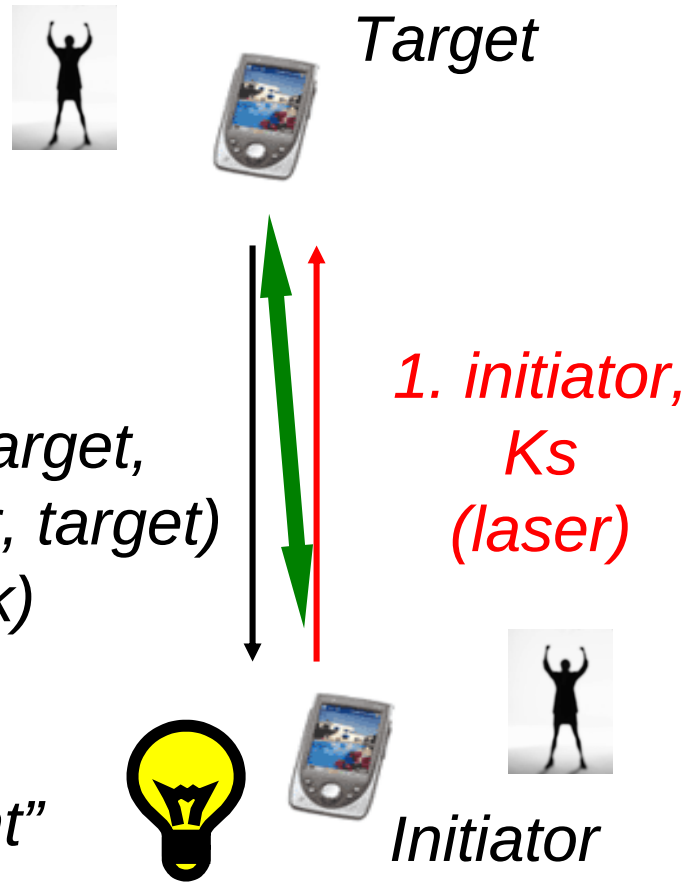
One-way key exchange

- One-way validated binding of key ↔ device
- Attacks
  - Reflection
  - Another laser



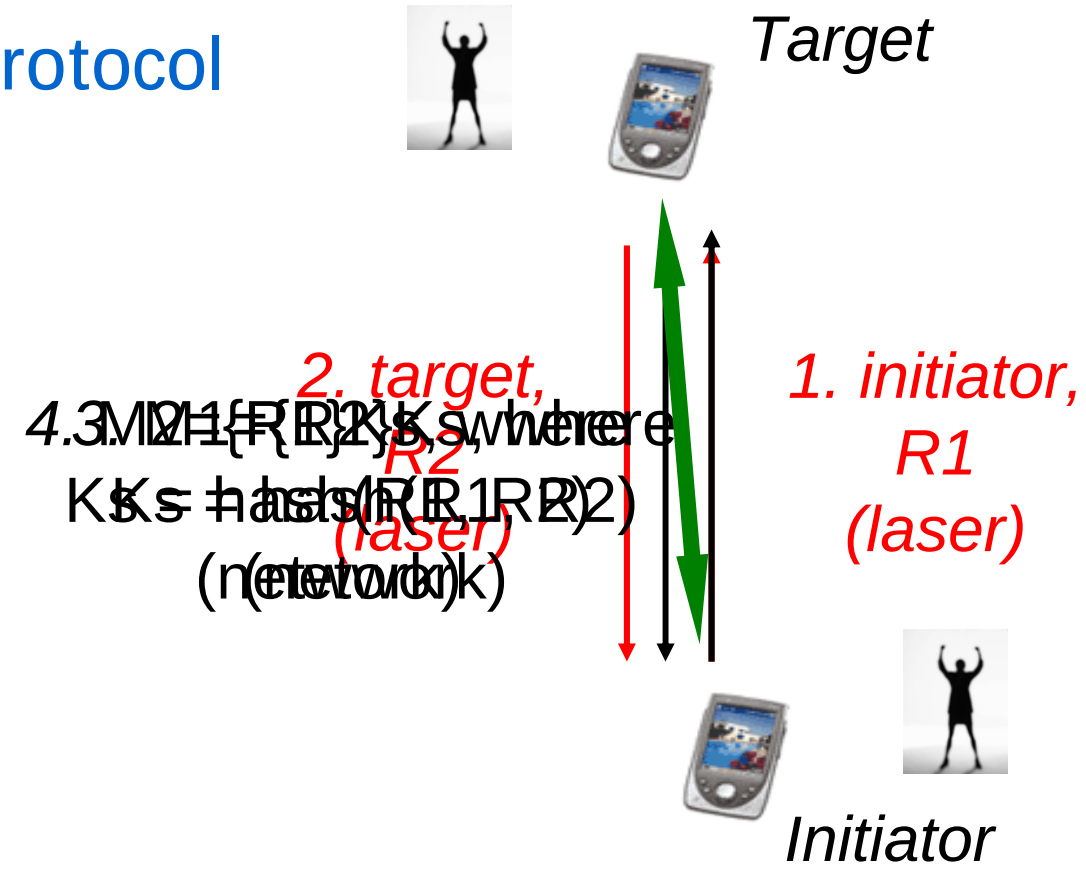
Two-way key-exchange #1

- Two-way validated binding of key ↔ device



Two-way key-exchange #2

- Symmetric protocol



Analysis of laser protocols

- Attacker can intercept, modify or spoof any network message
- But too difficult to intercept laser
  - At worst denial of service
- Human confusion possible
  - Unlikely with symmetric protocol (but more for user to do)

hp invent

Contributions

- Protocols for two types of physically constrained channel not used for security before:
  - Ultrasound + RF
  - Laser
- Protocols requiring no special hardware
  - Harmony protocol

hp invent

The Harmony Protocol

- Devices exchange keys...
  - Using existing protocols, e.g. 2-button + Diffie-Hellman
- ... Then validation by human(s) comparing multimedia streams
- Traffic analysis to look for man in the middle
- Ordinary devices with audio, displays, LEDs, ..

hp invent

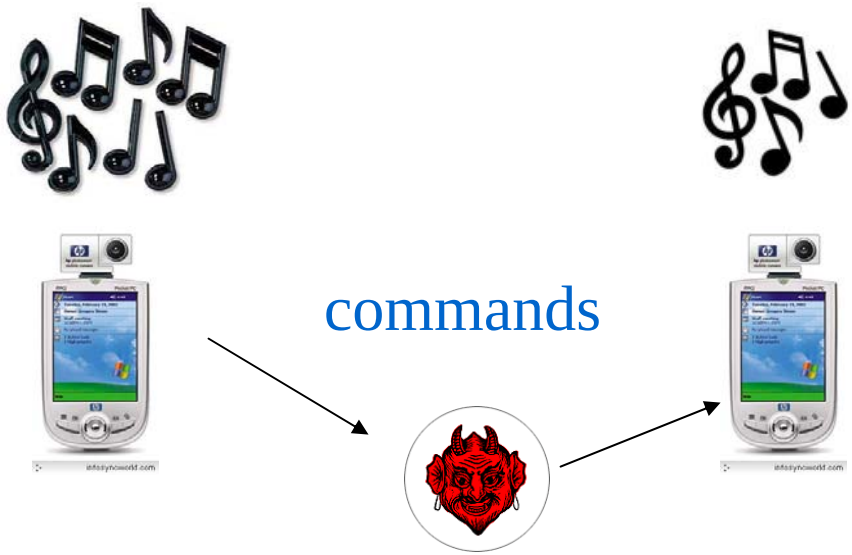
“Harmonised” events at devices

- Piano plus walking bassline
- Tune plus “sound to light”
- Random button-press plus beep/light
- …

hp invent

Traffic analysis to detect M-in-M

- Look for evidence of relaying
- Listen for “just-before” packets
- Works only for broadcast networks
  - Most 802.11, not Bluetooth



hp invent

Overview

- Introduction: problem and contribution
- Related work
- Protocols for secure spontaneous association
- Status and discussion

hp invent

What has been achieved?

- Much engineering needed to make ultrasound+RF, laser solutions convincing
- Human factors of multimedia protocols?
- Taking a step back:
  - Paying at Luigi's restaurant
  - Analysis of users' perceptions of trust/security issues in restaurant
  - Function of connection type, target device
  - Talk at UK UbiNet workshop, Cambridge, May 5-7, 2004

hp invent

Thank you!

Questions?

purl.org/net/TimKindberg
www.mobilebristol.org

tag:timothy@hpl.hp.com,2004:presentations:Newcastle:SecureSpontaneous

hp invent