A Human-Verifiable Authentication Protocol Using Visible Laser Light

WAIS 2007, ARES 2007
12. April 2007 9:30, Vienna, AT

Rene Mayrhofer, Martyn Welch
Lancaster University, UK

The problem

Wireless communication is insecure

- Especially problematic for spontaneous interaction: no a priori information about communication partners available

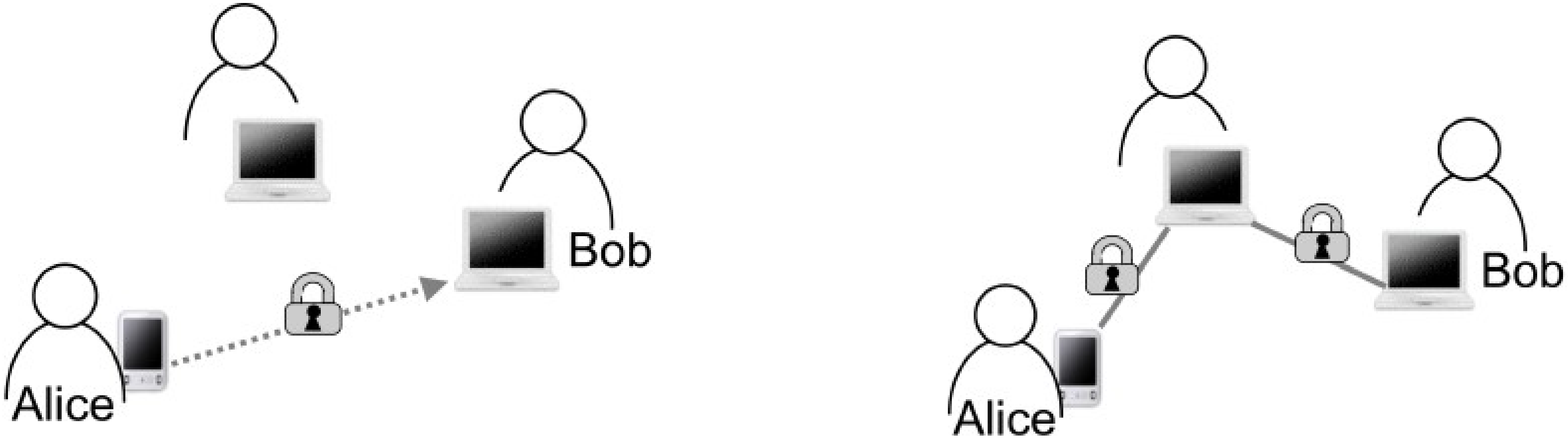
⇒ User needs to establish shared secret between devices

Example: mobile phone + photo printer, display, ...

Why is it a problem?

Secret key exchange over wireless channels

- Can use Diffie-Hellman (DH) for key agreement
- Problem of Man-in-the-Middle (MITM) attacks:



⇒ Secret keys need to be authenticated securely, intuitively and efficiently

Scalability is an issue

User authentication does not scale!

- Vision of ubiquitous computing: using Hundreds of services each day, seamlessly embedded into daily live, spontaneous usage, different realms of control
- Who would like to enter passwords or biometric data into each of them?

Approach: using trusted personal devices

- A personal device for each user (2006: 478.4 million mobile phones in the EU, 108% mobile phones rate in Austria [DerStandard.at, 2007/03/30])
- Important: personal device device may be trusted, but wireless connections are not ⇒ human-verifiable authentication

Overview of assumed setting

- Personal device is used to authenticate to remote services
- Interaction (+connection) initiated by personal device
- Some wireless communication channel with broadcast capabilities
- An out-of-band channel for verification
- Remote devices equipped with appropriate receivers

⇒ Visible laser as out-of-band channel

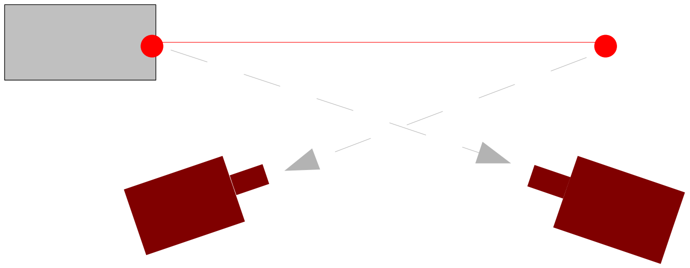
Properties of the laser channel

- Laser diode (sender):
  - cheap
  - small
  - reliable
  - (relatively) power efficient
  - intuitive
- Suggested before [KZ2003] for confidential transmission of secrets
- But: laser channel is not confidential

[KZ2003] T. Kindberg and K. Zhang. Secure spontaneous devices association. In Proc. UbiComp 2003, pages 124–131. Springer-Verlag, October 2003.

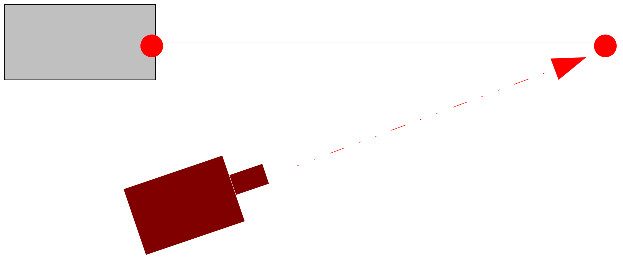
Assumptions and threat model

- Personal and remote devices are trusted (for the particular interaction)
- Wireless communication completely open to attack
- Laser channel is not confidential



attacker can read

- Laser channel is not completely authentic ⇒ "semi-authentic"



attacker can modify
(add but not subtract)

What can we do with it?

Components

- **P**: personal device with laser diode
- **R**: remote device offering some service with appropriate photo receiver
- **RF**: wireless communication channel, used for DH and communication
- **L**: laser channel, used to verify key with commitment scheme

Process

- Interaction combines selection + authentication
- Two steps for interaction: turn on laser and aim, then select

How can we do it?

1. Button 1 pressed $P \overset{L}{\rightarrow} *: ping$ (stream)
2. $P \overset{L}{\rightarrow} R: ping$
   $R \overset{RF}{\rightarrow} *: found$
3. $P \overset{RF}{\rightarrow} R: K := DH(P, R)$
   $R: peer := P$, turn on LED1 (yellow)
4. Button 2 pressed
   loop because of noisy transmission on L

   a) $P: generarate\, N_i$

   b) $P: M_1 := HMAC_K(N_i|1)$
   $P \overset{RF}{\rightarrow} R: M_1$

   c) $R: M_2 := HMAC_K(M_1)$
   $R \overset{RF}{\rightarrow} P: M_2$

   d) $P: verify\, M_2$
   $P \overset{L}{\rightarrow} R: M_3 := N_i$

   e) $R: verify\, HMAC_K(\acute{N}_i|1) = M_1$
   $R: M_4 := HMAC_K(N_i|2)$, turn on LED2 (green)

   f) $R \overset{RF}{\rightarrow} P: M_4$
   $P: verify\, M_4 = HMAC_K(N_i|2)$, turn on LED (green)

Exploiting properties of the laser channel

Integrity of L exploited in 4b to 4e:

- on MITM attack: $K_R \neq K_P$
- 4e: $HMAC_{K_R}(\acute{N}|1) \neq HMAC_{K_P}(N|1)$
- only with $HMAC_{K_R}(\tilde{N}|1) = HMAC_{K_P}(N|1)$

M_1

- relay or change M_1, but N_i not yet seen in plain text

Confidentiality of L exploited in 4d to 4f:

- M_4 generated by R (or MITM)
- contains N_i
- only transmitted via L

Simplicity of the protocol

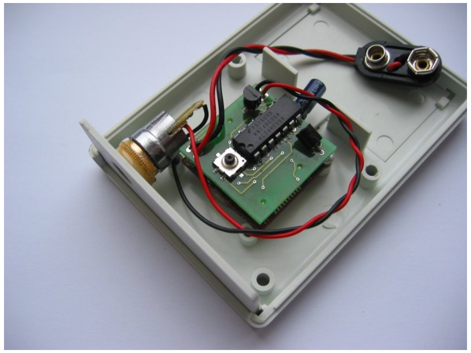
- M_1 necessary as commitment of P to N_i in 4d, bound to K
- M_2 necessary as "blind commitment" of R to N_i and acknowledge of unmodified M_1 (before receiving N on R)
- M_4 necessary against injection of fake N_i to match check in 4e on R
- LEDs guard against asynchronous relaying attacks

Attack possible only if attacker can perfectly overhead N_i over L **and** modify $\acute{N}_i$ to match $\tilde{N}_i$ that it sent in its modified M_1

Not quite there yet ...

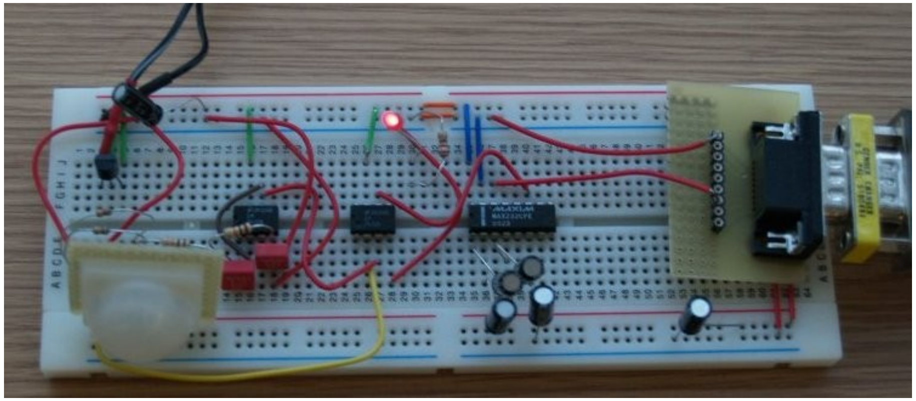
Sender

- Prototype with pulsed laser based on iMote1 (ARM7, 12 MHz) and TinyOS
- Missing: implementation of (EC)DH and opportunistic connection management with Bluetooth



Receiver

- Prototype for connecting to standard serial port based on photo resistor and simple high-pass and thresholding
- Missing: improvements of reception quality and transmission speed



... but work continues

Improving laser transmission

- Modulation instead of on/off pulsing
- Receiver filtering for modulation frequency only to alleviate problems with changing lighting conditions
- Higher transmission rates

Sender

- Reducing battery consumption
- “Nicer” packaging
- Integrating with mobile phones

Summary

- Secure communication set-up is difficult for spontaneous interaction because user authentication requires explicit interfaces and does not scale.
- Personal devices can be used as proxies when interacting with pervasive computing services, but authentication needs to be human-verifiable.
- Visual laser light is intuitive and can be used both for service selection and authentication.
- Our protocol is secure under the assumption that an attacker can not perfectly overhear and arbitrarily modify laser communication at the same time.
- All source code will be part of OpenUAT at http://www.openuat.org, hardware designs will be made available.

“Believe only half of what you see and nothing that you hear.”

Dinah Maria Mulock Craik (1826 – 1887)
English novelist and poet

Thank you for your attention!

Slides: http://www.mayrhofer.eu.org/presentations
Later questions: rene@mayrhofer.eu.org

OpenPGP key: 0xC3C24BDE
7FE4 0DB5 61EC C645 B2F1 C847 ABB4 8F0D C3C2 4BDE