A Human-Verifiable Authentication Protocol Using Visible Laser Light

Rene Mayrhofer and Martyn Welch
Computing Department, Lancaster University
Infolab21, Lancaster LA1 4WA, UK
rene@comp.lancs.ac.uk, martyn@warpedlogic.co.uk

Abstract

Securing wireless channels necessitates authenticating communication partners. For spontaneous interaction, authentication must be efficient and intuitive. One approach to create interaction and authentication methods that scale to using hundreds of services throughout the day is to rely on personal, trusted, mobile devices to interact with the environment. Authenticating the resulting device-to-device interactions requires an out-of-band channel that is verifiable by the user. We present a protocol for creating such an out-of-band channel with visible laser light that is secure against man-in-the-middle attacks even when the laser transmission is not confidential. A prototype implementation shows that an appropriate laser channel can be constructed with simple off-the-shelf components.

1. Introduction

Authentication is one of the key issues for secure wireless communication in ubiquitous computing applications. Realising the vision of ubiquitous computing, i.e. of services being integrated into our daily environment, is inherently dependent on intuitive, efficient, and secure methods for spontaneous interaction. When users start interacting with hundreds of services throughout the day, they can neither afford to pay close attention nor invest noticeable effort into these interactions. Securing wireless communication during the interaction must therefore be unobtrusive and implicit; additional steps required "just for security" will most likely be unacceptable. Nonetheless, intuitive interaction demands that the authenticity of communication partners must be easily verifiable by humans.

One approach to solving this issue is to rely on personal, trusted, mobile devices to interact with the environment. These are only used by one user at a time and act as representatives for interactions with other devices, utilising wireless communication in the process. To protect against man-in-the-middle (MITM) attacks on the wireless channel, an out-of-band channel is required for authentication. Various out-of-band channels have already been suggested, most of which provide "physical evidence" for the communication peers in the sense that humans can verify either or both sides of the wireless channel. Examples for such human-verifiable out-of-band channels are relative location measured via ultrasound [9], visual markers photographed with camera phones [10], audio [4], or common motion [8].

In this paper, we present a protocol for creating an out-of-band channel for authentication with visible laser light. In contrast to an earlier protocol suggested by Kindberg and Zhang [6], we do not assume the laser transmission to be confidential. Instead, we assume an attacker to be able to either violate the confidentiality of data transmitted via laser, i.e. to read it, or to violate its authenticity, i.e. to inject own data into the receiver, but not both at the same time. Our contribution is a protocol to establish a secret, authenticated shared key between the personal trusted device and a remote device under these assumptions. The personal device incorporates a laser diode and thus acts as the transmitter on the out-of-band channel, while the remote device is capable of detecting the light from the laser.

In section 2 we briefly analyse related work before discussing our threat model in more detail in section 3. Our protocol is presented in section 4 and analysed from a security point of view in section 5. Finally, section 6 describes an initial prototype implementation that we are currently working on.

2. Related work

Ringwald was among the first to present a working prototype for device-to-device interaction using lasers [12], followed by Patel and Abowd [11]. Both used relatively simple ways of modulating a laser diode and reconstructing the signal at the receiver end, whilst using the laser as an out-of-band method for initiating wireless communication by transmitting the device network address, although without considering security of the interaction.

Kindberg and Zhang previously suggested the transmission of secret keys via modulated laser light [6], under the assumption that the laser emits no light except onto the receiving sensor. However, as explained in section 3, this assumption may not be valid when considering attackers with free line of sight.

Seeing-is-Believing uses 2D barcodes and camera phones as a visual channel [10]. This approach allows users to directly verify what the sensor, i.e. their camera phone, measures. In comparison to a personal device equipped with a laser diode and the service equipped with a sensor, this approach swaps the roles of sender and receiver on the out-of-band channel. The advantage is that it is easier for users to verify the authenticity of the communication peer because authentication in the protocol sense matches what the user verifies. On the other hand, it forces the user to pay closer attention than for simply pointing a laser at a target device.

3. Threat model

Previous work assumed a modulated laser beam to be confidential from attackers [6]. However, this assumption does not seem valid considering two practical experiences:

- Laser diodes do not produce perfectly focused beams of light. This can be observed for example on laser pointers; parts of the light emitted by the laser diode can be seen from almost any angle within its front hemisphere (even if the majority is emitted along the primary axis).
- The laser light is reflected as scattered light from most surfaces, including photovoltaic elements suitable for use as receivers.

That is, the laser light can be seen both at the sender and at the receiver from almost any other point with direct line of sight. With high-speed cameras, it seems possible to capture the modulated signals with reasonable accuracy. We therefore do not assume a modulated laser channel to be confidential.

It is also questionable whether this channel can be assumed to be authentic, because most photovoltaic elements suitable for receivers can not distinguish angle of arrival and thus not between different senders. It is possible for an attacker to point their laser beam on the receiver and therefore inject their own messages into the out-of-band channel. Detecting such message injection will depend on the relative pulse strengths and the sophistication of the receiver. Users may also be unable to spot a “second dot” on the receiver if for example infrared lasers are used by the attacker. However, any such message injection will modify the original messages sent by the user’s personal device.

Therefore, we can only assume that an attacker can not easily block or completely change the information transmitted via a modulated laser beam without previous knowledge of the message contents. We also need to assume the remote device to be secure and trustworthy. Cases where information sent to it by the user is forwarded after successful authentication are out of the scope of this paper.

All wireless communication is generally assumed to be completely open to attack and possibly controlled by a MITM. The aim of our protocol is to prevent MITM attacks on the wireless channel.

In comparison with related protocols for constructing out-of-band channels like MANA I [3], SAS [13], and proposals by Balfanz et al. [2] and Hoepman [5], our assumptions are slightly less constrained. In contrast to MANA I, we do not assume the channel to be confidential. In contrast to the proposal by Balfanz et al., the direction of the channel is reversed. In contrast to Hoepman’s proposal, we do not assume the channel to be confidential and authentic at the same time. Our protocol is most closely related to SAS [13]. However, a further important difference to these protocols is that, for light sensors capable of detecting laser light, we can not assume the user’s laser beam to be the only input. This necessitates some additional precautions in our protocol, and makes it generally difficult to construct completely secure authentication schemes.

4. Protocol

Our proposed authentication protocol combines a wireless channel ($\mathbf{RF}$) with a modulated laser ($\mathbf{L}$) to create an authenticated secret key, similar to previous work [6]. The difference is that we can not use $\mathbf{L}$ for transmitting secret keys due to our assumption of $\mathbf{L}$ not providing confidentiality. Instead, $\mathbf{L}$ is used to transmit random numbers used only once (*nonces*) as part of a commitment scheme, comparable to e.g. the MANA III protocol [3] and a more recent proposal by Wong and Stajano [14, section 7]. Our protocol is designed so that an attacker would need to violate both the confidentiality and the integrity properties of the laser channel at the same time, i.e. to read what the user’s personal device sends and to inject their own messages into the receiver.

From a user interaction point of view, we combine two steps into one: device selection and implicit authentication. Nonetheless, this combined selection and authentication requires two user actions to prevent accidental selection of a “wrong” device. First the laser needs to be turned on to allow aiming, then the selection and implicit authentication needs to be performed. This can be implemented e.g. with two buttons or with one two-action button.

In the following description, the notation $m|n$ is used to describe string concatenation and $HMAC_K$ refers to an

HMAC [7] with key K. A message M sent over a noisy channel is received as M', to point to possible changes during transmission.

The protocol consists of the following steps between the user's personal device P and the remote device R:

1. The user presses the first button on P to turn on the laser and modulate it with a continuous stream of "ping" messages.
2. When the laser hits the receiver and the "ping" messages are detected, R switches to the "authentication in progress" state and broadcasts a "found" message over $\mathbf{RF}$. In this state, R will only interact with a single personal device (the first to contact it in the next step).
3. By receiving the broadcast, P learns the network address of R. P and R agree to a secret key K via standard Diffie-Hellman key agreement (DH) over $\mathbf{RF}$ and R turns on its first LED (e.g. yellow).
4. When satisfied with the selection of R, the user presses the second button and the devices loop through the following steps until authentication is successful or the user stops the process by releasing the button:
    (a) P generates a fresh nonce N.
    (b) P computes $M_1 := HMAC_K(N|1)$ and sends it to R over $\mathbf{RF}$.
    (c) R acknowledges the receipt by sending $M_2 := HMAC_K(M_1)$ to P over $\mathbf{RF}$.
    (d) P verifies M_2 and transmits $M_3 := N$ over $\mathbf{L}$ by modulating the laser.
    (e) R receives N', computes $HMAC_K(N'|1)$ and verifies that it matches M_1. It then sends $M_4 := HMAC_K(N|2)$ over $\mathbf{RF}$ and turns on its second LED (e.g. green).
    (f) P verifies M_4 and notifies the user of successful verification, e.g. by turning on an LED (green).

The loop is necessary due to the possibility of transmission errors over $\mathbf{L}$; it is important not re-use nonces but to generate fresh nonces in each iteration. Only when both R and P signal success (e.g. with green LEDs) should the user continue with the interaction.

Note that the authentication part of the protocol does not rely on asymmetric primitives and is thus suitable for implementation on resource limited devices such as sensor nodes. However, when not assuming the laser channel to be confidential, asymmetric cryptography like DH or its Elliptic curve variant (ECDH) is necessary for creating a secret shared key (see step 2 in the protocol).

5. Analysis

Our protocol uses both the (weak) confidentiality and integrity properties of the modulated laser channel:

- Integrity of $\mathbf{L}$ is exploited in steps 4b) to 4e): a MITM can only pass the check in 4e) when it can inject its own nonce $\widetilde{N}$ so that the $HMAC_K(\widetilde{N}|1)$ matches. Without such an injection on $\mathbf{L}$, there are only two options: When the MITM simply relays M_1, the HMAC will not match because of the different shared key. On the other hand, the MITM can not generate a valid HMAC message because N has not yet been transmitted and is therefore unknown. Step 4b) thus serves to commit the sender P to the content that will be sent over $\mathbf{L}$ and to bind this commitment to the shared key K.
- Confidentiality of $\mathbf{L}$ is exploited in steps 4d) to 4f): a MITM can only pass the checks in 4e) and 4f) when they can eavesdrop on the laser, because only then will N be revealed.

Each of the steps is necessary under our assumptions:

- M_1 needs to be sent in 4b) and acknowledged in 4c) before transmitting N over $\mathbf{L}$ in 4d), otherwise the attacker could just postpone sending the message from 4b) until N has been sent in plain text (i.e. assuming authenticity but not confidentiality of $\mathbf{L}$) .
- M_4, generated in 4e) and verified in 4f), is necessary otherwise the attacker could inject their own nonce $\widetilde{N}$ in steps 4b) to 4d) and pass the check in 4e) (i.e. assuming confidentiality but not authenticity of $\mathbf{L}$).
- The LEDs on P and R are necessary so that the user can check synchronicity. Without these the attacker could just generate message M_4 in step 4e) without verifying that $HMAC_K(N'|1)$ matches M_1 (i.e. assuming authenticity but not confidentiality of $\mathbf{L}$).

Due to using long (i.e. $\geq$ 128 bits) nonces, this protocol is not susceptible to attacks against short codes on the out-of-band channel [14, section 3]. Only when an attacker can perfectly overhear the original nonce N (sent by P over $\mathbf{L}$) and inject an own nonce $\widetilde{N}$ over $\mathbf{L}$ (as received by R) will a MITM attack on $\mathbf{RF}$ go undetected. As outlined in section 3, a laser channel is neither strictly confidential nor authentic. An attacker close to the target device R can observe the "red dot" at the sender and can shine a (possibly stronger and/or invisible IR) laser beam on the receiver, thus violating both the channel's confidentiality and authenticity. It remains to be shown how practical such attacks on both the confidentiality and the integrity are, taking the mobility of P and short interaction times into account.

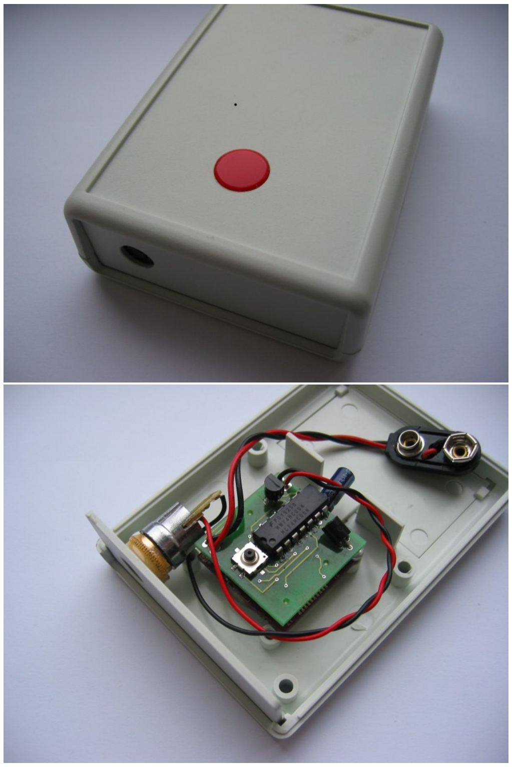

Figure 1. Prototype implementation of a personal trusted device with an Intel Mote and off-the-shelf components

Denial-of-service attacks on the laser receiver can not be avoided, but would be even easier to perform on the wireless channel.

6. Prototype implementation

Figure 1 shows our prototype personal trusted device with a laser diode. It is based on an Intel Mote ISN100-BA (with an ARM7 core at 12 MHz and integrated Bluetooth radio); a laser diode stripped from a £ 1 laser pointer; a two-action button and a few additional off-the-shelf components (NAND gates, transistor, etc.). The Intel Mote runs TinyOS [1] and is used to implement the P side of our protocol using Bluetooth as the $\mathbf{RF}$ channel and the UART for modulating the laser channel $\mathbf{L}$. Our first receiver prototype, shown in Fig. 2, uses a photo resistor (covered with the lens from a PIR) and a simple high-pass and thresholding circuit for reconstructing the signal. The signal is fed (via a RS232 level converter) into a serial port of a PC which also has a Bluetooth dongle. Not considering the Intel Mote, the overall cost of building both the prototype sender and the receiver was below £ 10.

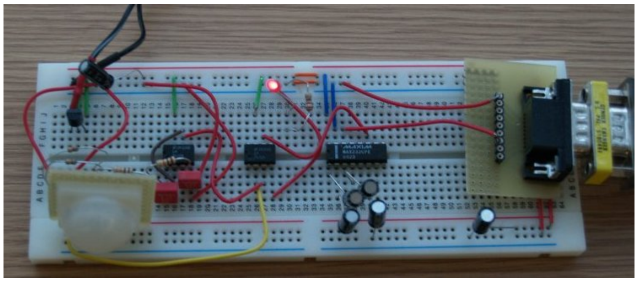

Figure 2. Prototype implementation of the receiver part.

User interaction is designed to be as simple as possible. We use a two-action button, similar to the buttons commonly used in digital cameras, to implement the two levels of action. By pressing the single button half-way, the laser lights up and allows proper aiming. By depressing the button fully, the target is selected and authenticated. Patel and Abowd also suggested to use a two-action button, but did not report a practical implementation of such an interaction [11].

Our prototype is still under development, and first results suggest improvements to the receiver are required. In practise it seems difficult to focus the laser beam on a target area that is about 2 cm in diameter, we thus intend to experiment with solar cells as receivers, as suggested e.g. by Ringwald [12]. The prototype is currently a proof of concept for modulated laser transmission and simple user interaction, but does not currently implement our complete protocol under TinyOS. We have not yet considered higher-level error correction methods for recovering from transmission errors on the laser channel $\mathbf{L}$. Instead, our protocol loops at sending nonces until successful authentication. This is not only robust against actual transmission errors, but also against "wiggle" when aiming the laser.

Another practical issue we have not yet considered is network discovery. In our protocol step 2, we assume some method for R to announce on the $\mathbf{RF}$ channel to P that it has been found by the laser beam. Bluetooth is a promising protocol for supporting wide interoperability, but does not provide broadcasts, and inquiry times are also particularly slow. One possibility to overcome this issue is to opportunistically run a DH key agreement (protocol step 3) with every Bluetooth device in range and to send the "found" message via multiple unicast packets to all previously discovered devices.

7. Conclusions

We have presented a protocol for creating a shared secret key over a wireless channel and authenticating it with a modulated laser channel. Under the assumption that an attacker can not both eavesdrop on the laser transmission and inject their own laser messages at the same time, our protocol is secure against man-in-the-middle attacks, eavesdropping, and message alterations.

Our prototype implementation is work in progress, but first results confirm that it is possible to transmit short modulated messages with laser diodes and simple off-the-shelf components. This low-cost solution makes a laser channel a viable option for wide-spread implementation in consumer devices such as mobile phones. We suggest that a laser channel can be used as an intuitive and secure out-of-band channel for spontaneous device pairing.

8. Acknowledgements

We gratefully acknowledge support by the Commission of the European Union under FP6 Marie Curie Intra-European Fellowship contract MEIF-CT-2006-042194 "CAPER" and thank Matt Oppenheim for support in building the prototype sender.

References

[1] TinyOS web page. `http://www.tinyos.net`, 2006.

[2] D. Balfanz, D. K. Smetters, P. Stewart, and H. C. Wong. Talking to strangers: Authentication in ad-hoc wireless networks. In *Proc. NDSS'02: 2002 Network and Distributed Systems Security Symposium*. The Internet Society, February 2002.

[3] C. Gehrmann, C. J. Mitchell, and K. Nyberg. Manual authentication for wireless devices. *RSA Cryptobytes*, 7(1):29–37, 2004.

[4] M. T. Goodrich, M. Sirivianos, J. Solis, G. Tsudik, and E. Uzun. Loud and clear: Human verifiable authentication based on audio. In *Proc. ICDCS 2006: 26th Conf. on Distributed Computing Systems*, page 10. IEEE, July 2006.

[5] J.-H. Hoepman. The emphemeral pairing problem. In *Proc. 8th Int. Conf. Financial Cryptography*, pages 212–226. Springer, February 2004.

[6] T. Kindberg and K. Zhang. Secure spontaneous devices association. In *Proc. UbiComp 2003: 5th Int. Conf.*, pages 124–131. Springer, October 2003.

[7] H. Krawczyk, M. Bellare, and R. Canetti. RFC2104: HMAC: Keyed-hashing for message authentication, February 1997.

[8] R. Mayrhofer and H. Gellersen. Shake well before use: Authentication based on accelerometer data. In *Proc. Pervasive 2007: 5th International Conference on Pervasive Computing*. Springer, May 2007. *to appear*.

[9] R. Mayrhofer, H. Gellersen, and M. Hazas. An authentication protocol using ultrasonic ranging. Technical Report COMP-002-2006, Lancaster University, October 2006.

[10] J. M. McCune, A. Perrig, and M. K. Reiter. Seeing-is-believing: Using camera phones for human-verifiable authentication. In *Proc. IEEE Symposium on Security and Privacy*, pages 110–124. IEEE, May 2005.

[11] S. N. Patel and G. D. Abowd. A 2-way laser-assisted selection scheme for handhelds in a physical environment. In *Proc. UbiComp 2003: 5th Int. Conf.*, pages 200–207. Springer, October 2003.

[12] M. Ringwald. Spontaneous interaction with everyday devices using a PDA. In *Proc. Workshop on Supporting Spontaneous Interaction in Ubiquitous Computing Settings*, September 2002.

[13] S. Vaudenay. Secure communications over insecure channels based on short authenticated strings. In *Advances in Cryptology - Proc. CRYPTO 2005: 25th Int. Cryptology Conf.* Springer, August 2005.

[14] F.-L. Wong and F. Stajano. Multi-channel protocols. In *Proc. Security Protocols Workshop 2005*. Springer, 2006.