Audio-based Out of Band Channel key exchange

Applied Cryptography

October 28, 2015

Troels Thomsen 152165
Rasmus Haarslev 152175
Vilius Maskovas 107154
Justas Mikalajunas 107083

Contents

1 Abstract

2 Introduction

3 Related work on audio authentication (Justas - 0.5p)

4 State of the art authentication (Vilius - 0.5p)

5 Problem description (Troels 1p)

Secure authentication between previously unknown devices without a connection to the Internet is an open problem. Without pre-shared keys, a trusted third party, trusted certificate providers and the key-signing-chain more commonly used in authentication, it is very difficult to prevent man-in-the-middle attacks and identity spoofing.

Allowing two devices to authenticate each other without a trusted third party or any pre-shared keys opens up for dishonest agents in the communication. Any attacker listening in on the initial communication between the two parties can either eavesdrop on all of their communications, or if the attack is able to modify or intercept the transmissions, fake the identify of either party.

This is especially apparent in situations where the key exchange occurs on a common communication bands where attackers can easily scan packets for authentication requests.

6 Proposed solution

6.1 Solution description (Troels 1p)

We propose a scheme which uses an out of band channel (OOB) in order to prevent attackers from intercepting or modifying the key exchange. An out of band channel is a different channel for transmitting data, besides the one regularly used by the devices or protocol. In our solution we are going to use inaudible (high frequency) noise for exchanging a symmetric key between the two authenticating devices.

We will base-100 encode the symmetric key, transmit it over an audio channel, decode it and start communicating over any standard band of communication since the scheme is agnostic to what band the symmetric key is used on.

This authentication scheme requires both devices to have a microphone and a speaker. The devices must be within close proximity of one another in order to receive the low volume transmission, which is how the protocol guarantees the secrecy of the symmetric key. If the attacker wants to listen in on the exchange and intercept the key exchange, the attacker must get physically very close to both devices.

The low proximity while exchanging the symmetric key is also the downside of the solution, since both parties who wish to be paired need to be right next to each other.

The solution is also limited in the sense that it requires both devices to have both a microphone and a speaker. One can easily imagine a scenario where this is not the case, such as trying to pair a smartphone with home Hi-fi equipment which propably does not have a microphone. In addition the speakers and microphone on each device must respectively be able to distinguish between 100 different transmitted sounds as well as be able to transmit 100 different sounds, in order for the base-100 encoding to work.

The solution is vulnerable to tampering or interference if an attacker transmits a lot of noise in the same frequency, it would be possible to ruin the key exchange if timed correctly. The key exchange could similarly be ruined if the physical location of the two devices happens to have a lot of ambient noise in the same frequency range. One possible solution to this problem is to choose a random communication frequency from a pre-defined set of frequencies. A sophisticated attacker might still be able to transmit in all of these frequencies in order to ruin the transmission, but switching frequencies would propably solve the problem of random ambient noise.

6.2 Strengths (Rasmus 0.5p)

The apparent advantage of using an OOB channel is the fact that it is quite a rare form of communication between mobile devices. This means that a potential intruder will either have to have a wide variety of attacks available, in order to quickly adapt to the sudden use of an obscure OOB channel, or have prior knowledge of the device pairing method being used during device pairing.

Even if the intruder are ready for this specific device pairing method, the fact that the method uses audio during the authentication, makes it extremely difficult for the intruder to temper with the messages being transmitted. This is because sound waves can't be stopped or interrupted, which means the intruder won't be able to change the message, ensuring that correct message will always be sent, thus ensuring authentic communication. Furthermore, we take advantage of the fact, that using low volume audio means that the pairing devices must be close to one another, which means that the intruder must get really close to the pairing, can be difficult.

In addition to the security advantages, utilizing audio for device pairing means that the method will be highly backwards compatible, as almost all, if not all mobile devices (phones) has some kind of microphone and speaker. This further ensures, that the method won't be prone to aging quite as fast as other device pairing methods might.

6.3 Weaknesses (Rasmus 0.5p)

While our proposed solution has strong authentication, it also have disadvantages, that may prove to be difficult to address. While using audio ensures broad device support, it also relies on the device to be able to record and understand the transmitted messages, which might prove difficult for older devices, where the speaker or microphone might be of poor quality. This is very problematic, as our method won't be able to securely authenticate the devices if the audio can't be understood by the device.

The fact that we use low volume audio to ensure better security also comes with the downside of lessened convenience because the low volume decreases the distance within the devices are capable of pairing.

A potential intruder might have difficulties with tempering with the audio messages sent during authentication, but it is extremely easy to interfere with the pairing in such a way, that the authentication process simply can not be completed. This can be done by broadcasting noise in the same frequency as the authentication messages, which will render the pairing devices unable to understand any message being sent to them.

6.4 Threat analysis (Rasmus 1p)

- Man-in-middle attack
- Eavesdropping
- Interference (noise in same frequency)
- Denial of Service

7 (Threat) Comparison with state of the art (Vilius 0.2p)

7.1 Bluetooth 4.0 PIN-code (Vilius 0.5p)

7.2 Bluetooth 4.0 Image scanning (Vilius 0.5p)

8 Conclusion

9 References

[1] Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein. *Introduction to Algorithms*. The MIT Press, 3rd edition, 2009. p. 65-113.

[2] National Institute of Health. GenBank statistics. `www.ncbi.nlm.nih.gov/genbank/statistics/`. Visited May 20th 2015.

[3] Leslie A. Pray. Discovery of DNA Structure and Function: Watson and Crick. *Scitable*, 2008.