Audio-based Out of Band Channel key exchange

Applied Cryptography

October 27, 2015

Troels Thomsen 152165

Rasmus Haarslev 152175

Vilius Maskovas 107154

Justas Mikalajunas 107083

Contents

1 Solution description 1

2 Abstract 3

3 Introduction 4

4 Related work on audio authentication (Justas - 0.5p) 5

5 State of the art authentication (Vilius - 0.5p) 5

6 Problem description (Troels 1p) 6

7 Proposed solution 7

7.1 Solution description (Troels 1p) 7

7.2 Strengths (Rasmus 0.5p) 7

7.3 Weaknesses (Rasmus 0.5p) 7

7.4 Threat analysis (Rasmus 1p) 8

8 (Threat) Comparison with state of the art (Vilius 0.2p) 9

8.1 Bluetooth 4.0 PIN-code (Vilius 0.5p) 9

8.2 Bluetooth 4.0 Image scanning (Vilius 0.5p) 9

9 Conclusion 10

10 References

1 Solution description

1. What is the problem? (a more detailed definition of the project than presented on 24 September)

    - Pairing two devices involves each device authenticating the other, without the use of any pre-shared key and without any trusted authority. This opens up for dishonest agents and man-in-the-middle attacks.

    - If the two devices tries to share keys over Wi-Fi for instance, an attacker might intercept and modify the contents of the transmission.

2. What is the proposed solution? (a brief overview of the proposed architecture)

    - We propose to use a 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 device or protocol. In our solution we are going to use inaudible frequency (high frequency) noise for exchanging a symmetric key between the devices. We will base-100 encode the symmetric key, transmit it over audio, decode it and start communicating over the standard band. This requires both devices to have a microphone and a speaker. The devices must be close together 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, the attacker must get physically very close to both devices.

3. How does 2) address 1)? (an analysis of the solution that will replace the full evaluation that is normally found in a paper)

    - By taking advantage of the low proximity exchange of nonce, we will prevent most attackers from being able to intercept communication. The attacker must physically be standing right next to both devices at the same time. This is also the downside of the solution, since both parties who wish to be paired need to be standing 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. The two microphones must also be able to distinguish 100 different noises, in order for the base-100 encoding to work.

- The solution is vulnerable to tempering if an attacker transmits a lot of noise in the same frequency, it would be possible to ruin the key exchange if timed correctly.

2 Abstract

3 Introduction

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

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

6 Problem description (Troels 1p)

7 Proposed solution

7.1 Solution description (Troels 1p)

7.2 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.

7.3 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.

7.4 Threat analysis (Rasmus 1p)

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

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

8.1 Bluetooth 4.0 PIN-code (Vilius 0.5p)

8.2 Bluetooth 4.0 Image scanning (Vilius 0.5p)

9 Conclusion

10 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.