Audio-based Out of Band Channel key exchange

Applied Cryptography

November 1, 2015

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

Contents

1 Abstract

2 Introduction (Justas)

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

Secure pairing of two devices been a hot topic for the past decade and therefore there are numerous of documents as prior work. One of the early work by Stajano, et al. [9] brought device pairing to the stage and proposed to use physical contact for shared secret sharing. Physical contact such as a cable is not a feasible solution nowadays due to interfaces mismatch on devices and not being user friendly. Nonetheless, this paper was used as an inspiration for new papers in this field. An example of such is Balfanz, et al. [7] where usage of location-limited channels (LLC) was introduced with favor on infrared connection. Though, nowadays infrared is not popular on mobile devices as it used to be making this approach impractical. Yet this paper laid foundation for using Diffie-Hellman key exchange protocol in device pairing. After Balfanz, et al. [7] , the movement of device pairing split into two main parts – improving how Diffie-Hellman key exchange protocol is being implemented into real life systems– Ubisound [1], HADAPEP [8] and handful of variants which LLC to use infrared, sound [7], visible laser light [3], light together accompanied by sound [5]. All of the mentioned documents uses or prefer usage of heavy encryption algorithms, making the pairing slower than it is needed for common usage where data is not critical.

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

Bluetooth version 4.0 includes Secure Simple Pairing (SSP). It defines how two Bluetooth devices are paired. The main idea of SSP is to improve security against eavesdropping and MITM attacks. It is hard to achieve, Bluetooth devices have different input and output capabilities and can be attacked in different ways. Therefore, SSP can be used in four different ways:

1. Numeric Comparison (NC) Both devices generates and displays 6-digit key. User compares generated numbers and if they match, he/she confirms successful pairing. Used when both devices has a display and at least one of them has a capability of entering yes/no command.

2. Just Works (JW) No user interaction and has no MITM protection. Used in devices without user interfaces.

3. Passkey Entry (PE) I: One device has a screen and another device has a numeric keypad. The device with the screen shows 6-digit key and then device with keypad

enters the key. II: Two devices has only numeric keypads. Both devices enter the same 6-digit key.

4. Out of Band (OoB) Generates 6-digit key and transfers it via OoB channel. This method is as secure as the OoB channel it uses.

All four ways are based on passing a short authenticated string, which is used to create a session between devices. SSP decides which method to use based on devices capabilities. The preferred method is OoB, then NC, PE and the least preferred is JW.

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.

6.1.1 Goals (Troels)

The goals of our solution can be summarized as follows:

- Authenticate device A with device B.
- After authentication a secret symmetric key exists between A and B.

6.1.2 Requirements (Troels)

The requirements of our solution can be summarized as either of the following setups:

- Device A has a microphone and device B has a speaker.
- Device A has a speaker and device B has a microphone.
- Device A has a both a microphone and speaker and device B has a microphone.
- Device A has a both a microphone and speaker and device B has a speaker.
- Device A has a both a microphone and speaker and device B has both a microphone and a speaker.

All microphones must be able to transmit 100 different sounds. All speakers must be able to distinguish between 100 different sounds. Device A and B must both have a screen for displaying information to the user, and a way to accept user input.

6.1.3 Use case (Troels)

The primary use case of our solution is secure pairing between two smartphone devices who are strangers to each other, and who both possess a microphone and a speaker. The two smartphone users wish to have their devices paired with each other, in order to share files.

6.1.4 Sequence diagram (Troels)

Diagram of how the protocol works

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 Comparison with state of the art (Vilius 0.2p)

7.1 Image scanning (Vilius 0.5p)

Bluetooth SSP using barcode or any other image as Out of Band (OoB) channel is a common practice. The method is as secure as the OoB channel it uses and image scanning as an OoB is very secure. MIDM attacks are practically impossible. The attacker would have to be in very close proximity, few centimeter from the device that generated the image, for a fast interception of the key. Theoretically, if the attacker would have very high quality camera and could get a good angle, it would be possible to capture the image from a greater distance. However, the timeframe to do that is very small as well. The user will scan the code himself/herself quite fast, few second. To do that, he/she will place second device in from of the displayed image, that way shielding it from the attacker. Eavesdropping attacks faces the same problem as MIDM attacks. Image capture is very secure as an Out of Band channel. However, for this method to work both devices have to have comparably expensive hardware, a camera and a display screen, which is not common in many Bluetooth capable devices. Compared to our solution, we offer a method, which is as secure as image capture method if not even more secure and which could be used by many more Bluetooth devices without having to upgrade the hardware.

7.2 NFC (Vilius 0.5p)

Using NFC OoB channel for Bluetooth communication is not a common practice, though it is a secure method, secure enough for bank to use it. The NFC works in very close proximity, which gives additional security against MITM and eavesdropping attacks on top of the implemented communication protocols. The reason that it is not used widely for Bluetooth devices pairing is that it is quite new method. Therefore, older devices or the ones which go for a lower price don't have required hardware.

7.3 Bluetooth 4.0 JW (Vilius 0.5p)

JW method is the most commonly used Bluetooth pairing method. It is simple and has low hardware requirements. However, it has no protection against MITM attacks, where our solution provides protection against MITM and does not have high hardware requirements.

8 Conclusion

9 References

[1] William R. Claycomb and Dongwan Shin. Secure device pairing using audio. *Proceedings - International Carnahan Conference on Security Technology*, 2009.

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

[3] R. Mayrhofer. A human-verifiable authentication protocol using visible laser light. *Availability, Reliability and Security, 2007.*, 2007.

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

[5] Ramnath Prasad and Nitesh Saxena. *Efficient device pairing using "human-comparable" synchronized audiovisual patterns*. Springer Verlag, 2008. p. 328-345.

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

[7] Dirk Balfanz Smetters, Dirk Balfanz, D. K. Smetters, Paul Stewart, and H. Chi Wong. *Talking To Strangers: Authentication in Ad-Hoc Wireless Networks*. Ninth Annual Symposium on Network and Distributed System Security. 2002.

[8] Claudio Soriente, Gene Tsudik, and Ersin Uzun. *HAPADEP: Human-assisted pure audio device pairing*. Springer Verlag, 2008. p. 385-400.

[9] Frank Stajano and Ross Anderson. *The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks*. Lecture Notes in Computer Science. Springer-Verlag Berlin, 3rd edition, 1999. p. 172-182.