Audio-generated symmetric keys

Applied Cryptography

October 8, 2015

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

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 Litterature reviews

2.1 Formal analysis of secure device pairing protocols

2.1.1 Justas

I think it is a great source for restriction / substitution of traditional attacker model introduced by Dolev and Yao (Dolev-Yao attacker model). The principle is that in Dolev-Yao attacker model, attacker is controlling all communication medium. In our case it would still be restricted whether by human interaction or something else? We could use this paper if we want to go a bit deeper into attack and the protocol itself. Maybe we could even model a protocol in AnB and try to verify with ofmc, however it would require a bit more detailed knowledge of OFMC capabilities in this field (if we would go for Ubisound idea - 2 channels for 1 protocol)

2.1.2 Troels

I agree it is a good example of extending Dolev-Yao, but I am not sure if this is really relevant if we are going to try and design our own theoretical audio pairing protocol / adding audio pairing to an existing protocol's key generation.

2.2 Sondi master thesis

2.2.1 Justas

Well, I admit, it is a crappy and long paper. It goes too much into details not where we need. I would offer to skip this paper for sake of everyone. Otherwise a good paper to get an overview how sound waves work in environment (maybe a picture or two could be used to explain background of sound waves). Another quite okay point, to understand the job of encoding of message using audio channel (numbers are always fancy). We can bring another nice point, that audio channels are not reserved / licensed like radio or wifi channels.

2.2.2 Troels

I think this might be a good article to include for describing state of the art audio pairing. Even though they achieved limited success - especially due to background noise in public

space, their system uses very little power. I think the idea is interesting and we should keep it in mind for our own idea development.

2.3 UbiSOUND

2.3.1 Justas

I like the way of presenting the idea in this paper. The protocol also looks okay, however we can look into opportunities trying to improve it. Overall - interesting point to use 2 different mediums for exchanging data for DH.

2.3.2 Troels

I like the idea behind this protocol. The possibility for visually impaired users are interesting, and for a very simple authentication scenario the protocol might work out well. I am not convinced that there is not a man in the middle attack on this protocol though. If the devices have some distance between them, and an attack intercepts the audio transmitted, disrupts it with noise and subsequently transmits his own audio key, he might be able to imitate the original sender.

2.4 Efficient Device Pairing using 'Human-comparable' Synchronized Audiovisual Patterns

2.4.1 Justas

Another interesting way of pairing devices using audio (beep beep) and visual (blink blink). However, I am not sure if we could use much from this paper and the way it is written is not very good. And the protocol used (SAS), if my memory is not water yet is a serial protocol which in audio (the way we want to use) would be hard to use.

2.4.2 Troels

Good explanation of OOB. Sondi uses SAS, so it might not be a bad idea for audio-based pairing. I don't really like the idea of combining visual and audio channels to do the pairing. It seems like a very elaborate scheme which does not really add anything and could be simplified. What I read from this is basically that using only audio is much more stable and probably more reliable than using visual authentication.

2.5 HAPADEP Human-Assisted Pure Audio Device Pairing

2.5.1 Justas

Ideas from implementation part are good. I would like to look more into codecs with which we could encode whatever noise/sound we are going to use, it should decrease amount of errors. Main point - the importance of codecs and we will need to look into that.

2.6 Analysis of Bluetooth Threats and v4.0 Security

2.6.1 Justas

I did not understand the paper. It says analysis, but for me it is super general overview. Not sure if we can use it.

2.7 Bluetooth Security in Wearable Computing Applications

2.7.1 Justas

Also more of an overview than a research paper, however it contains proper details about security levels in bluetooth which we should compare to audio, maybe?

2.8 Man-In-The-Middle Attacks on Bluetooth

2.8.1 Justas

Variations on man in the middle attacks. Please see suggestion below.

Suggestion: All of these paper do not propose much new information, what I suggest is that we leave these papers for now aside. It will not help much to create new system, however this documents will do great job in comparing our system with pure bluetooth solution if we come to that.