# Audio-generated symmetric keys

Applied Cryptography

*October 22, 2015*

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

# Contents

# 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

## 3.1 Related work

# 4 Problem discription

# 5 Proposed solution

## 5.1 Threat analysis

# 6 Comparison with state of the art

## 6.1 Threat comparison

# 7 Conclusion

# 8 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.