WYDZIAŁ PODSTAWOWYCH PROBLEMÓW TECHNIKI
POLITECHNIKI WROCŁAWSKIEJ

CHANNELS ALTERNATIVE TO WIFI IN AUTHENTICATED KEY ESTABLISHMENT PROTOCOLS FOR MOBILE DEVICES

PAWEŁ KĘDZIA

Praca inżynierska napisana
pod kierunkiem
dr inż Łukasza Krzywieckiego

WROCŁAW 2010

Spis treści

Introduction

The goal of the dissertation is to analyze the usability of channels alternative to WiFi in Authenticated Key Establishment (AKE) protocols for mobile devices. Authentication and communication protocol in audio channel for mobile devices.

Mobile devices to transfer data mainly use internet. Disadvantage of this method is that network not always is available. In that case one can still transmit data using some another embedded devices like IrDA, Bluetooth or NFC. Unfortunately not every device has these kind of accessories implemented. However, basis of handhelds is to have embedded speaker and microphone. That is why, in this dissertation, to communication between devices were choosen audio channel. Availability audio appliance and a lot of uses of this solution are main advantages. Moreover, the sound waves with appriopriate, not to high sound intensity, does not penetrate through the walls. It causing that waves cannot be receive e.g. on the street when some protected data are sending in the house. Furthermore receiver as like sender do not need to known each other (unlike Bluetooth) before starting the communication. Sender just start to transmit data and receiver in the same time listening broudcast.

To authentication and key agreement between mobile devices was choosen Anonymous Mutual Authentication (AMA) protocol, created by L. Hanzlik, K. Klucznik, Ł. Krzywiecki and M. Kutyłowski. AMA is simmetric, which means participants execute the same code. One of the advantage is simple to implemented, even on the devices with low power computing. Every key and encryption are sending by audio channel.

Application created on Android system will serve as proof of concept. Application is called AKEBySound. Managed to determine that exist this kind of applications but none of theme are use to authentication and key exchange protocol. To use this app is enough to have mobile phone/smartform with software Android (version 4.1.2 or higher) and working speaker and micrphone, of course.

Dissertation is divided on X parts. The first section focus on analyse the problem. Explain principal issues used to create the application. The first one obviously is a sound. The next one is one of the method to exchange keys on which AMA protocol base. Tutaj cos o bezpieczenstwie bedzie itp. Dowod poprawnosci protokolu i takie tam.

1 Analysis of the problem

1.1 Sound

1.2 Diffie-Hellman Key exchange

1.3 Random Oracle Model

2 System design

2.1 Assumptions

2.2 Used cases

2.3 Diagram classes

2.4 Activity diagram

2.5 Anonymous Mutual Authentication protocol - Description

2.5.1 Security model assumption

3 System implementation

3.1 Description of technology

3.1.1 C++

3.1.2 Android/Java

3.1.3 Crypto++

4 Tests

5 Installing and implementation