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

1 Analysis of the problem **3**

1.1 Sound 3

1.1.1 Frequency 3

1.1.2 Sound intensity 4

1.2 Diffie-Hellman Key exchange 4

1.3 Random Oracle Model 4

2 System design **4**

2.1 Assumptions 4

2.2 Activity diagram 4

2.3 Anonymous Mutual Authentication protocol - Description 4

2.3.1 Security model assumption 6

3 System implementation **6**

3.1 Description of technology 6

3.1.1 Android/Java 6

3.1.2 C++ 6

3.1.3 JNI 6

3.1.4 Crypto++ 6

4 Tests **6**

5 Installing and implementation **6**

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 chosen audio channel. Availability audio appliance and a lot of uses of this solution are main advantages. Moreover, the sound waves with appropriate, 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 broadcast.

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 microphone, of course.

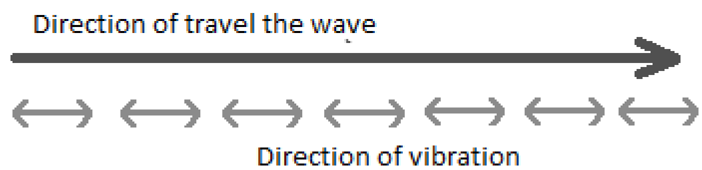
Dissertation is divided on X parts. The first section focus on analysis of the problem. Explain principal issues used to create the application. Due to the fact protocol is executed by audio channel the first subsection is about sound. The next one is one of the method to exchange keys on which AMA protocol base - Diffie-Hellman Key exchange. Tutaj cos o bezpieczenstwie bedzie itp. Dowod poprawnosci protokolu i takie tam.

Next chapter is about System design. In subsections are described assumptions of project and used cases. Then is shown diagram classes

1 Analysis of the problem

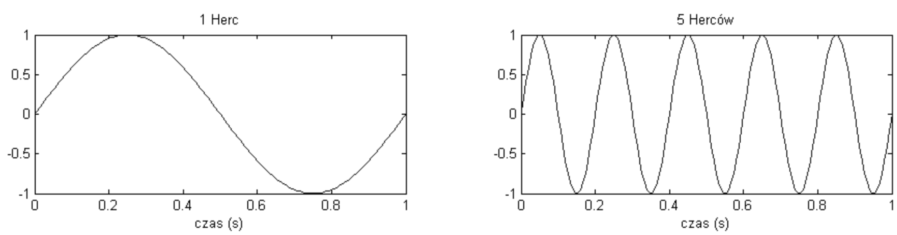
1.1 Sound

Sound is acoustic wave propagating in different substances such as water, air (so called vibrating wire). These waves are causing auditory sensation and these which in appropriate amplitude and frequency are not detected by human organ of hearing. Sound to spread has to have some medium, that is why not propagate in vacuum. Furthermore sound is longitudinal waves, which means that particles of the medium is in the same direction as the direction of travel of the wave.



1.1.1 Frequency

Audio frequency is measured in hertz (Hz), where 1 Hz means one cycle per second. Below figures show graphs of audio frequency 1 Hz and 5 Hz.



Exist three division of sound as to frequency:

- Infrasound - frequency is lower than 16 Hz.
- Hearable sound - frequency is greater than 16 Hz and lower than 20 kHz.
- Ultrasound - frequency is greater than 20 kHz.
- Hipersound - frequency is greater than 10 GHz.

Frequency specify also pitch of sound. A high frequency sound wave corresponds to a high pitch sound and low frequency sound wave corresponds to a low pitch sound.

1.1.2 Sound intensity

Loudness of the sound is dependent to his intensity.

1.2 Diffie-Hellman Key exchange

1.3 Random Oracle Model

2 System design

2.1 Assumptions

System should:

- Works on every middle class mobile devices with system Android.
- Generate keys and encryption during authorization process.
- Use sound wave to sending encoded keys and encryptions to another party to establish authorization.
- Receiving sound wave and decode received data to keys and encryption from another party to establish authorization.

2.2 Activity diagram

2.3 Anonymous Mutual Authentication protocol - Description

Scheme of protocol is shown at the Fig. 1. In scheme are use the fallowing notation:

- *Enc* is a symmetric encryption function. $Enc_K(M)$ means encryption of M using key K.
- H is a cryptographic hash function.
- For confirming public keys are using digital certificates and public key infrastructure (PKI).

Protocol is very simple to implement. In the first state, parties (Alice and Bob) generate their private key - x_A (respectively, x_B) and public key $y_A = g^{x_A}$ (respectively, y_A). Then starts main procedure. Parties generate ephemeral keys. Private is

Alice		Bob
x_A - private key $y_A = g^{x_A}$ - public key $cert_A$ - certificate for y_A		x_B - private key $y_B = g^{x_B}$ - public key $cert_B$ - certificate for y_B
	MAIN PROCEDURE	
choose a at random $h_A := H(a)$ $c_A := g^{h_A}$	$\xrightarrow{c_A}$ $\xleftarrow{c_B}$	choose b at random $h_B := H(b)$ $c_B := g^{h_B}$
$K := {c_B}^{h_A}$ $K_A := H(K, 1)$, $K_B := H(K, 2)$ $K'_A := H(K, 3)$, $K'_B := H(K, 4)$ $r_A := H(c_B^{x_A}, K'_A)$		$K := {c_A}^{h_B}$ $K_A := H(K, 1)$, $K_B := H(K, 2)$ $K'_A := H(K, 3)$, $K'_B := H(K, 4)$
	$\xrightarrow{Enc_{K_A}(cert_A, r_A)}$	check $cert_A$, proceed with random values if $r_A \neq H(y_A^{h_B}, K'_A)$
	$\xleftarrow{Enc_{K_B}(cert_B, r_B)}$	$r_B := H(c_A^{x_B}, K'_B)$
check $cert_B$, proceed with random values if $r_B \neq H(y_B^{h_A}, K'_B)$ $K_{session} := H(K, 5)$		$K_{session} := H(K, 5)$

Rysunek 1: Protocol description - Anonymous Mutual Authentication. Figure from source [**?**].

$h_A := H(a)$ (where a is a random number) (respectively h_B, b) and public ephemeral key $c_A := g^{h_A}$ (respectively c_B). After this parties exchange between themselves public ephemeral key. This is standard Diffie-Hellman key agreement.

When parties obtain ephemeral public key of another party, start compute master key K. Four different one-time keys are establish by hashing K and number parameter - different for each one-time key.

Authenticated party is raising ephemeral public key c_B (respectively, c_A) to power of private key x_B (respectively, x_A). On this base authentication. Verifier compute the same value without private key but with the discrete logarithm of c_A (respectively, c_B) $((y_A)^(h_B))$

2.3.1 Security model assumption

3 System implementation

3.1 Description of technology

3.1.1 Android/Java

3.1.2 C++

3.1.3 JNI

3.1.4 Crypto++

4 Tests

5 Installing and implementation

Literatura