Cryptographic Data Security in Wireless Networks Based on Biometrical Passport

Denis V. Vishnyakov[1], Anton G. Serdyukov[2]

Katanov State University of Khakassia, Abakan, Khakassia, Russia,
e-mail: denis_tmk@rambler.ru[1], antonserdyukov@yandex.ru[2]

***Abstract* — The use of a biometric passport for encoding data which are transmitted across open wireless 802.11g standard channels. The generation of encryption key is based on biometrical data.**

***Index Terms* — biometrics, shorthand, packet encryption, network, biometrical passport**

INTRODUCTION

The security status of wireless networks is unsatisfactory; that increases the possibility of breaking in, scanning and accessing a wireless 802.g network.

In the standard such cryptographic algorithms as WEP, TKIP, AES can be used; it makes no difficulty for a malicious user to break them in. That's why it is necessary to create a new security model.

A biometrical passport is suggested as one of the key moments of the new model. Its use is determined by the uniqueness of biometrical data of each human and by great selection difficulties in breaking this data. This allows generating encryption keys stable to cryptography.

The project objective is to create software designed for encoding data that are transmitted through open radio channels, where a biometrical user passport is used for key generation.

OVERALL SCHEME OF APPLICATION COMPLEX FUNCTIONING

The program complex functions including the following stages:

1) Fingerprint scanning

Fingerprint scanning is made with the help of the hardware Bio-

0-7803-9219-1/05/$20.00 © 2005 IEEE

Link U-Match scanner.

2) User authentication by fingerprinting.
3) Key generation by fingerprinting and a key word.

Generation is performed according to the mathematical fingerprint pattern and a key word entered by the user.

4) Data encryption with the help of generated keys.
5) Data transmission.
6) Data decoding on the base of the already given key.

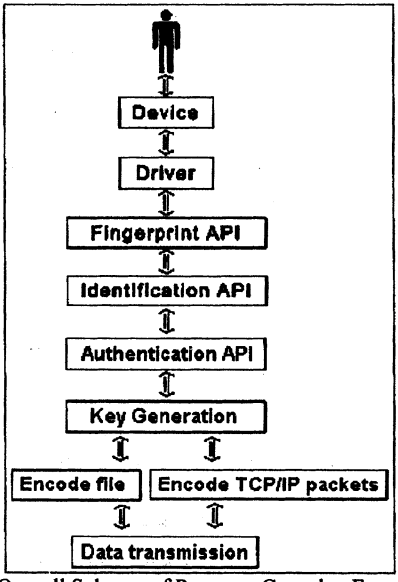

Fig.1. Overall Scheme of Program Complex Functioning

Note: The key transmission mechanism is not considered in the given paper, it means that key distribution has already occurred between clients.

PRACTICAL IMPLEMENTATION

There are two approaches:

1) a single file decryption.

It is performed by the application which uses a biometrical key. The file is transmitted across the network with the help of standard transmission protocols: FTP, HTTP, and SMTP.

2) TCP/IP packets encryption.

On interconnecting computers an extra service is set up, which works at the network TCP/IP level. Its task is transparent TCP/IP packets encryption. The work at TCP/IP network level is performed by means of NDIS (Network Device Interface Specification) driver.

3) Shorthand (data hiding) in the network traffic.

That is building data into transmitted TCP/IP packets without any damage to the integrity of information being transmitted.

At fingerprint scanning a 1.23 kb-sized pattern is created and stored for the following user authentication. It is impossible to get the image of the original fingerprint in order to provide security. After user identification is made it is necessary to enter a key word and then encryption key is generated on the base of fingerprint pattern and the entered word.

At the current stage of the development the following is made: fingerprint is taken, fingerprint pattern is stored in the database for further user identification, encryption key is generated according to fingerprint pattern a key word, a single file is encoded with the help of the given key. TCP/IP packets encryption is to be completed at the following stage.

Further practical usage of the development is for project security organizations dealing with wireless and heterogeneous networks.

References

[1] BioLink Fingerprint Software Development Kit. Developer's Guide.
[2] MSDN April 2004 – NDIS driver.
[3] C.H. Rowland. "Covert Channels in the TCP/IP Protocol Suite", Psionic Technologies Inc., 2002.

Denis V. Vishnyakov has participated in the international student programming contest (team championship) in the quarter-final and semi-final – ACM Programming Contest 2002, 2003.

Anton G. Serdyukov has participated in the 5th Student Paper Contest and Conference on the Information Security (SIBINFO-2005).