Protocol Design for Courier-Dependent Indirect Communication

Name: Chen Sun Supervisor: Dr. Kasper Bonne Rasmussen

Introduction

This is a brief description of an MSc project for final dissertation. It starts in March 2014 and will end before 5th September 2014. This project is related to Computer Security and it is mainly about creating and implementing a communication protocol. The rest of proposal will firstly describe the problem and its related background. Then it will give a rough framework of the protocol, together with some potential challenges. Finally the achievements of the project will be listed.

Motivation and Background

Most existing application-level protocols are all under the circumstances that two entities are connected by network (like XMPP, FTP, etc.), but what if two entities are not directly connected? How is it able to build a secure connection between them? This project proposes a question of creating a communication protocol between off-line entities using a portable device as a message courier to connect them. Although this will be a new communication protocol, the concept is somehow similar to Mobile Agent (an alternative way for doing distributed computing, allowing whole program environment moving between hosts and clients), whose security concerns have been evaluated in publication Mobile Agent Security (Jansen & Karygiannis, 1999), like confidentiality, integrity, authenticity, accountability, availability, etc. Because this protocol will be an application-level protocol, some existing lower level protocol in TCP/IP suite or Bluetooth protocol will be used.

Project Briefing

A simple scenario of this protocol contains 3 entities, Alice, Bob and a Courier. Alice needs to send secret information to Bob, but they are not directly connected. The only way they can do is Alice sends message to Courier – a portable device, and Courier is transported to Bob, then Bob receives message from the Courier. The protocol mainly concerns two parts, the communication between Alice and Courier, and communication between Courier and Bob. It is required that (a) The authenticity and integrity of the message are preserved during communication (b) The confidentiality of message is preserved even when the Courier is hijacked. (c) Malicious operations of Alice, Bob or Courier will be detected and rejected.

Following the basic scenario, there also exists some variants to be considered:

1. Efficiency concerns. If use cryptography, it is expected to achieve relatively low overhead for encrypting/decrypting.
2. Key revocation. If use cryptography, once one of the entities' key is disclosed, it must come up with a method for new keys to be securely revoked/exchanged.
3. Deniable authentication. It means, the participants themselves can be confident in the authenticity of the messages, but it cannot be proved to a third party after the event.

Aim and Objectives

This project will firstly discuss and explore some potential solutions to building this protocol. After protocol defined, an Alice, Bob and a Courier (may be on mobile phone) will be implemented to simulate the protocol. Then some tests will be designed and applied. Finally evaluate and analyse the tests results to expose the features (like efficiency, vulnerability, practicality).