System Requirements

Skullduggery

Greg Baker - Robert Koeninger
Advisor: Prof. Wilsey

Revised: May 13, 2010

Scope

We will be implementing a TLS-like encryption system for a Google Android Phone.
Greg Baker, Robert Koeninger, Dr. Philip Wilsey
This project will allow for more secure phone conversations for the user of the encryption system. The goal is to design an encryption system that can be used without interfering with normal functions of a cellular phone.
This project will be implemented with a 'app' for the Google android smart phone. It will not modify any data sent between the cellular provider and the cellular phone, and will not interfere with any conversations that a user has with the encryption system installs. It needs to be able to encrypt data quickly enough to send it as it's being generated, and be light enough on processing power and memory to be used on a cellular phone.

Project Perspective

There are currently two major third generation (3G) phone communication standards: GSM EDGE and CDMA2000. GSM EDGE has been “cracked”; it is possible to listen to cellular phone conversations in real time with a few hundred dollars in equipment, a desktop computer and free software. This is a problem because the GSM standard is used in 80% of the cellular communication market, with 3 billion users world-wide. CDMA2000 has much better security, but it uses insecure methods to generate the key used for encrypting data. A more secure encryption method will alleviate the problems in the underlying communication protocols and allow for much more secure phone conversations between enabled phones.

Project Functions

The Skullduggery project will implement a TLS-like encryption method over the data communication otherwise used by the phone. The project will perform a “handshake” that determines if the user on the other end of a voice communication is using the Skullduggery encryption system. If so, the encryption system will encrypt voice information and send it to the other phone. If not, the communication between the two users will be ended.

User Characteristics

The encryption system from the user's standpoint should be unobtrusive. It should automatically encrypt cellular communication. When it cannot, it should end the communication between the two users, as no communication enhancement can take place.

Requirements

Functional Requirements

The system will encrypt voice packets using the AES-128 specification. This standard provides secure encryption and validation methods so we will not need to create our own (probably insecure) method.

The system shall encrypt voice packets when able without intervention from the user. When able (when both ends of the call have the encryption system installed), the encryption system will encrypt voice packets automatically for a secure call.

The system shall not encrypt data packets when the receiver cannot decrypt them. Since the deployment of this project is limited, calls should be completed when one end of the call does not have the Skullduggery encryption system running.

The user will be alerted when the conversation cannot be encrypted. The user should be made aware if

the encryption system fails to establish a secure method of communication, and when either the encryption method encounters an error or one user is unable to use the system.

Performance Requirements
Encryption using AES shall be performed in less than 100ms. Any delay less than 1/10 of a second will probably interfere with communication between users of the phone.

Implementation Requirements
Encryption will be implemented using the AES-128 specification. The AES standard includes methods for key generation and specifies methods for secure communication without compromising security.

AES shared keys will be exchanged using the RSA specification. The RSA standard includes methods for key pair generation, and specifies methods for secure one-way exchange of information without compromising the information sent.

The encryption system will be written in Java, using the 1.6 standard. This is dictated by the language that the Android uses for applications.

The development platform for the phone will be Android v2.1. Android v2.1 is the platform which runs on the phones that we can modify to complete this project.

The encryption system should be independent of communication system that the phone does. If the encryption system is independent of the communication system that the phone implements, then we can be sure that we do not interfere with the cell phone provider's systems and we can be more sure that we will not break normal cellular communication.

Definitions, Acronyms and Abbreviations
CDMA – Code Division Multiple Access
GSM – Global System for Mobile communications
AES – Advanced Encryption Standard. Used for shared key (bidirectional) cryptography.
RSA – Rivest, Shamir and Adleman encryption standard. Used for public key (one-way) cryptography.
TLS – Transport layer security

References
GSM on Wikipedia - http://en.wikipedia.org/wiki/GSM
TLS on Wikipedia - http://en.wikipedia.org/wiki/Transport_Layer_Security
RSA on Wikipedia - http://en.wikipedia.org/wiki/RSA
AES on Wikipedia - http://en.wikipedia.org/wiki/Advanced_Encryption_Standard
The CDMA standard - http://en.wikipedia.org/wiki/CDMA2000