Encrypted Cell Phone Communication

Background:

Sensitive information is frequently transmitted over cellular communication networks as voice data. As voice recognition software improves, it will become more important for information such as social security numbers and credit card information to stay private between the parties. Encrypting voice communication more securely will provide more protection against eavesdroppers looking for information.

Problem Statement:

The current standard of secure communication, GSM, has been proven to be insecure. Current cellular phone systems do not provide sufficient privacy for sensitive information to be confidently transmitted over cellular networks. Our cellular encryption system will provide additional security for sensitive information to be transmitted during a call, while preventing an eavesdropper from deciphering the communication.

Team Members:

Greg Baker **bakergo@mail.uc.edu**

Robert Koeninger **koeninrc@mail.uc.edu**
email all team members

Faculty Advisor:

Dr. Philip A. Wilsey

Goal:

Our goal is to modify a smart phone to encrypt voice packets before being sent, and decrypt them on the other end of the voice communication. If the receiving phone is incapable of decryption, the paranoid party will be alerted that the communication is insecure.

Subgoals:

1. Explore encryption techniques that are feasible for use in cellular communication.

2. Develop software on the cellular phone to encrypt and decrypt voice communication during a call.

3. Analyze the power and speed of various techniques to this goal.

Helpful Skills:

- Knowledge of encryption methods

- Some familiarity with host system (Google Android)

- Java and embedded programming skills