EEL 4914 Senior Design
08/01/2006
Project Abstract

BlackChat
Incognito Messaging System

Alpaca Security Solutions

Presented by:

Patrick Lloyd
patrick.lloyd@ufl.edu
(386) 795-7534

Russell Crowe
rcrowe93@ufl.edu
(352) 419-2641

Abstract:
The BlackChat Incognito Messaging System consists of a small USB device with a built in wireless transceiver that can transfer encrypted text messages between computers. The user will interface with the device through an installed applet on their computer where they can enter their note and select various options that control the functionality of the device. On the hardware side, a USB UART will be used to translate messages between the user's computer and the internal microcontroller. The microcontroller will be responsible for encryption and decryption of the messages. In addition, a custom wireless transceiver will read and demodulate incoming messages from other clients or modulate and transmit the user's message.

Introduction:
In many situations it is necessary to send text communication and transfer files discretely between two computers. With the recent exposure of warrantless government wiretapping, protecting one's privacy is now more difficult than ever. The purpose of BlackChat is to create a secure, discrete, and plausibly deniable point-to-point communication system for text between two or more computers.

BlackChat practices to an extent “security through obscurity”. When sending data through the Internet, even on secure channels like SLL and TLS, transaction logs and data monitoring is almost guaranteed. In addition, the development of devices such as the Ubertooth One Bluetooth test tool and relatively cheap software radios like the USRP, monitoring and processing wireless data in standardized channels is trivial. Software solutions like Wickr and Whispr offer very secure point-to-point messaging services but still rely on traditional standardized infrastructure.

Technical Objectives:

- In order to interact with the hardware, the user will utilize a software client run on their computer. This will send configuration settings and messages to the microcontroller through a USB UART bridge.
- The microcontroller will act as an intermediary between the wireless transceiver and the UART bridge. An AES-128 encryption block in the firmware will handle encryption and decryption of messages and a packet handler block will manage encapsulation of data and transmission to the radio.
- The wireless transceiver will be developed on the device using phase-locked loops for modulation and demodulation. They will either be discretely designed or an IC that integrates the two will be used. This is done in lieu of using a pre-built wireless solution such as the Digi Xbee or Xtend product lines. Since the transmitter is only sending text, a data rate of several hundred kBaud would be sufficient.
- Power system design is fairly minimal since the entire device is expected to run off of the user's USB port. This does constrain the design to 500 mA at 5V. Regulation and logic level shifting would be required for 3.3V components if necessary.