SKULLDUGGERY

ENCRYPTED CELL PHONE COMMUNICATION

Team Members:
Greg Baker
Robert Koeninger

Advisor:
Dr. Philip Wilsey

Problem Description

- Most popular cell phone communication standard is GSM
- GSM encryption is very weak
- Calls can be decrypted with free software and cheap equipment

"I remember seeing somewhere that the encryption was based on three shift registers, which immediately says oh, goodness. And now I know exactly how bad it is, and we're going to talk about it today. Basically I'm glad I'm over on Verizon with - and not using GSM. **It's completely cracked. It's completely broken.**"
– Steve Gibson, "Security Now!"

Preliminary Solution

- TLS/SSL is encryption standard used for online transactions
- Still considered secure
- Voice data to be encrypted using TLS and sent through GSM/CDMA channel

Approach

- To encrypt we will need to modify modem control code
- User application will be used to edit encrypt configuration
- Phones will attempt to "handshake" at beginning of call, default to normal call if fail

Approach (cont.)

- Developed using Android, because its open-source
- Modem control is accessible from with OS; platform portable
- Google makes phone that accepts custom builds ($425)