PRIUS
PRIvacy against Unlawful Surveillance

Srujan Kotikela, Mahdevan Gomathisankaran
Trusted and Secure Systems Lab
University of North Texas
The Introduction

- Internet – Synapse of the World
- Connects
  - People
  - Information
  - Businesses
  - Services
- Pervasive and ubiquitous
- Modern day life is ‘wired’
The Problems

- Internet had benign beginning
- Trusted tool for collaboration and sharing
- Afterthought security and privacy
- Privacy and confidentiality challenges
- Weaker wire tapping laws (for packaged data)
The Problem

- Unlawful Surveillance
- Privacy of
  - Business secrets
  - Financial data
  - Personal (health) information
- Identity theft
- Abuse of critical, private data (Quis custodiet ipsos custodes?)
The EFF

- Electronic Frontier Foundation
- Face to Face – most private form of communication
- Voice call – next most private (most protected by the law)
- OTR – Off The Record Protocol
The Solution

- Transfer digitally encoded messages over voice line
- Vocally confirm the recipient
- Exchange cryptographic Diffie-Hellman challenges over DTMF
- Use DH challenges to generate shared key
- Use shared key to encrypt communication
The Protocol

1: Place Voice Call

2: Send DH challenge in DTMF Tones

3: Send DH challenge in DTMF Tones

4: Exchange Public keys

5: Communicate over secure channel

Alice

Bob

Verify Bob (Voice)

Decode Tones

Generate Shared Key

Encrypt public key using the shared key

Decode Tones

Generate Shared Key

Encrypt public key using the shared key

Communicate over secure channel
The Prototype

- An Android App
- The mobile app calls the user
- Sends the DTMF codes
- App on the other end receives the DTMF codes
- Decodes the DH challenge
- Generates shared key
- Exchanges the public keys
- Encrypts communication (communication channel agnostic)
The Challenges

- Discouraged call recording
- No easy access to voice line for recording
- Non standard DTMF tone length
- Non standard tone length with variable string size
The Future Work

- Fine tuning the decoding algorithm
- Enhance live decoding capabilities
- Better encoding scheme
- Alternative uses with encoded data exchange
The Discussion

Questions & Comments