NovaTooth (Men-in-the-middle)

Henry, Rob, Trevor, Kevin, Albert
Introduction & Our Team

Kevin Chan: 4th Year Computer Engineering (Team Lead)

Trevor Morris: 4th Year Computer Engineering (Team Scribe)

Henry Yu: 3rd Year Computer Science

Robert Stosick: 4th Year Computer Engineering

Albert Chen: 4th Year Computer Engineering
Company & Mentor

IT services and solutions company located in downtown Santa Barbara

Renato Untalan
UCSB Computer Science ‘09
Development practices

GitHub

Google Drive

Visual Paradigm

Slack

Trello
A Man-In-The-Middle is a form of eavesdropping where communication between two users is monitored and modified by an unauthorized party.

- Share data, voice, music, video, files
- Uses low power radio frequency, takes up very little energy
- Vulnerabilities
  - Eavesdropping
  - DoS
- Bluetooth range is bigger than you think - 100m
What’s that got to do with us? Problem statement
Technology Overview

Main technologies

- Bluetooth profiles
- Bluetooth scanner
- Connecting to bluetooth media: 3 way handshake
- Connecting to bluetooth phone calls: oFono
- Manipulating and recording the audio
- Automating the entire process
- Web backend and text to speech
Bluetooth Profiles

A Bluetooth profile is a specification regarding an aspect of Bluetooth-based wireless communication between devices. It resides on top of the Bluetooth Core Specification and additional protocols.

A2DP: Advanced Audio Distribution Profile
(Media)

HFP: Hands Free Profile
(Phone calls)

HSP: Headset Profile
Bluetooth Scan

Bluetoothctl scan on: List of available devices to connect to

[CHG] Device 58:51:00:00:1F:8F RSSI: -59
[CHG] Device 50:56:A8:00:0E:EB RSSI: -61
[CHG] Device 58:51:00:00:1F:8F RSSI: -69
[CHG] Device 50:56:A8:00:0E:EB RSSI: -90
[DEL] Device C0:EE:FB:26:95:C5 OnePlus One-spaceteam
[DEL] Device 50:56:A8:00:0E:EB Jon's Jolla
[DEL] Device 58:51:00:00:1F:8F H163
[NEW] Device 58:51:00:00:1F:8F H163
[NEW] Device 50:56:A8:00:0E:EB Jon's Jolla
[CHG] Device 58:51:00:00:1F:8F RSSI: -71
[CHG] Device 58:51:00:00:1F:8F RSSI: -60
Bluetooth media connection: 3-way Handshake

Using Bluetoothctl

First, scan for devices first, then…

Pair: allows device to communicate
Trust: allows device to establish connection
Connect: fully connected, able to send data
Bluetooth Phone calls: Ofono

- Ofono is a “mobile telephony API” that uses the D-Bus interprocess communication system
- It provides the APIs we need to allow Kali to support the Hands-Free Profile (HFP) and emulate a Bluetooth headset
**Recording the Audio**

Pulseaudio: sound server running in a background process that accept multiple sound sources and redirects them to sound systems

1. Turn on pulseaudio
2. Listen to media/phone sound source
3. Redirect source to microphone output
4. Select which output to record
5. Use pulseaudio recording system (pavucontrol) to record output as mp3
Web Backend - Technologies

django

Python

Amazon Web Services

Google Cloud Platform

TASTYPIE

SQLite
### Transcriptions

Upload a file to transcribe or send a POST request to this URL. Currently only configured for single channel, 16-bit FLAC.

<table>
<thead>
<tr>
<th>Description</th>
<th>Transcribed Text</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Choose File</strong></td>
<td><strong>Hello this is a test it is working goodbye</strong></td>
</tr>
<tr>
<td><strong>Upload</strong></td>
<td></td>
</tr>
</tbody>
</table>

### Recent Uploads

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
<th>Transcribed Text</th>
<th>Audio File</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nov. 23, 2016, 11:31 p.m.</td>
<td>python test with auth</td>
<td>hello this is a test it is working goodbye</td>
<td>Download</td>
</tr>
<tr>
<td>Nov. 23, 2016, 11:30 p.m.</td>
<td>curittest no auth</td>
<td>hello this is a test it is working goodbye</td>
<td>Download</td>
</tr>
<tr>
<td>Nov. 23, 2016, 9:54 p.m.</td>
<td>python test4</td>
<td>hello this is a test it is working goodbye</td>
<td>Download</td>
</tr>
<tr>
<td>Nov. 23, 2016, 3:35 p.m.</td>
<td>curittest</td>
<td>hello this is a test it is working goodbye</td>
<td>Download</td>
</tr>
<tr>
<td>Nov. 23, 2016, 3:27 p.m.</td>
<td>python test4</td>
<td>hello this is a test it is working goodbye</td>
<td>Download</td>
</tr>
</tbody>
</table>

---

Novacoast, UCSB CS Capstone
Automating the entire process

Python scripting
1. Start bluetooth, pulseaudio, ofono services
2. Establish bluetooth connection for media and phone calls
3. Set up sound input and output streams

Bash scripting:
1. Start the recording
2. Output to mp3
3. Upload the mp3 to backend
Tests

Bluetooth scan started?
- test by detecting nearby bluetooth devices

Bluetooth media connected?
- test by playing music media

Bluetooth phone connected?
- test by making a phone call

Record audio stream?
- verifying recorded mp3 is not empty
Future Goals and Vision

- Full functionality
- Self-containment
- Statistical Analysis
- Correctness Testing
Demo.

Phone
"Alice"

NovaTooth
"Eve"

Web Backend

Google Cloud Speech

Bluetooth Headset
"Bob"

https://drive.google.com/drive/folders/0B89ugIl8FwyMZ1h1M lhFWHpkZzA