Albert Chen
Henry Yu
Kevin Chan (lead)
Robert Stosick
Trevor Morris (scribe)

NovaTooth Vision Statement

Bluetooth is a widely-used wireless standard that operates on the unlicensed 2.4 GHz band. Bluetooth is ubiquitous in both the corporate environment as well as in consumer products, and it can be found in everything from automobiles to phones, medical devices, keyboards, and hundreds of other applications. Over 25,000 companies are a member of the Bluetooth Special Interest Group, the organization responsible for the maintenance of the Bluetooth standard.

Bluetooth's universal deployment is both an asset and a liability. Although Bluetooth devices make our lives safer and more convenient, most corporations do not consider the extensive security implementations of their Bluetooth usage. Furthermore, available devices, tools, and technologies for Bluetooth security analysis and penetration testing are extremely limited, and are often very expensive, difficult to use, or not available to the general public.

Our group seeks to identify security vulnerabilities in Bluetooth usage, and to exploit these weaknesses by building a device to perform Bluetooth Man-in-the-Middle(MITM) attacks for penetration testing purposes. The innovation we are hoping to create is an active attack on Bluetooth signals. We plan to wait for unsuspecting users to connect to our Bluetooth MITM device, at which time will either reroute the connection or eavesdrop on data transmitted between devices. Furthermore, we will use machine learning techniques by integrating with Google Speech or another third party API that utilizes neural networks in order to transcribe intercepted audio and to facilitate efficient mass data analysis.

The sheer variety of companies and devices using Bluetooth means that implementations are frequently not secured using best-practice design. We believe that by developing a prototype MITM device, and demonstrating its effectiveness in MITM attacks, companies will become more security-conscious in their use of Bluetooth, and vendors will be forced to improve the security of their products.

Specifically, our device will either passively eavesdrop on Bluetooth packets, or perform an active MITM relay attack. Using the captured data, it will encode the recovered audio stream into the MP3 format, where the sound can later be transcribed into text and delivered to a remote source. The device will be built using the Raspberry Pi, which is an ideal platform for a Bluetooth MITM device because of its small size (allowing discreet use), low power usage (allowing it to be powered from a battery), and integrated Bluetooth radio (reducing complexity and time-to-development of the prototype). As the prototype matures and is refined, we will make decisions regarding the user interface. Options the team considered include accessing the Pi using SSH, storing the data on a SD card for later retrieval, and constructing an iPhone/Android app.

The project will be completed in phases. The first milestone will be to decide broad project specifications, such as whether the attack should be a passive eavesdropping attack, an active MITM relay attack, or some other attack, and what kind of user interface should be initially developed. The next milestone will be design; in which we decide how to implement this attack using the Raspberry Pi. In this phase, we will also select test targets, i.e. devices which we will attempt to use the MITM device on. The last milestone will be prototyping, in which we will begin implementation and testing of our design.

To achieve these milestones, we will use industry-standard best practices, such as agile development and scrums. Furthermore, we will take advantage of open-source technologies and information, such as Gstreamer, HFP for Linux (nohands.sourceforge.net), the Bluetooth Protocol, and of course, the Linux operating system itself which will run on the Raspberry Pi. By the end of the project, we will have an effective Bluetooth MITM penetration testing device.

We want to request as much guidance as possible from our mentors at Novacoast. With your guidance and expertise, we believe we can make this idea a reality.