BT-IDS: An anomaly-based Intrusion Detection System for Bluetooth Devices

Shalaka Satam, Pratik Satam and Salim Hariri
Project Team Members

- UA Faculty
  - Salim Hariri

- UA Graduate Students
  - Shalaka Satam
  - Pratik Satam
Background

- IoT devices depend heavily on wireless networks for communications.

- Bluetooth networks have become the wireless network choice for small range communications.

- Bluetooth networks need to be secure against cyberattacks like battery draining attack, DoS, etc.
Project Overview
Project Tasks: Overview

- **Task 1**: Develop innovative data structures (Bluetooth Flow (BTF)) that can accurately model the Bluetooth normal operations.

- **Task 2**: Design an architecture for the Bluetooth Intrusion Detection System (BT-IDS).

- **Task 3**: Build machine learning models that characterize the normal behavior that can be used to detect any attack against Bluetooth network.
Task 1: Develop BT Flow data structures that model the Bluetooth normal operations

- **N-gram** - A data structure that is used to represent an N state transitions sequence of the BT protocol state diagram into one single unit (N-gram).
- **BT Flow (BTF)** - A collection of Ngrams that follow one specific flow of Bluetooth traffic.
Task 2: Design a BT-IDS Architecture

- **Sniffer Module**
  Its main function is to collect data frames that are transmitted over the Bluetooth network

- **BT Behavior Analysis Unit (BT-BAU)**
  It performs data-driven analytics to detect any abnormal behavior in BT network operations that can be triggered by BT attacks
Task 3: Develop machine learning models that characterize the BT normal operations

Preliminary analysis
Activities and outcomes

- The primary goal of this project is to develop an intrusion detection system (IDS) for Bluetooth network that uses anomaly based detection approach.

- The Bluetooth IDS (BT-IDS) can detect and classify accurately new and modified attacks with little or no false positives and false negatives.
Deliverables and benefits

**Deliverables**

- Midterm and final reports documenting research methods, and evaluation results
- One or two scholarly conference and/or journal publications

**Benefits**

- Capability to detect and classify attacks against Bluetooth networks.
Please take a moment to fill out your L.I.F.E. forms.  
http://www.iucrc.com

Select “Cloud and Autonomic Computing Center”  
then select “IAB” role.

What do you like about this project?  
What would you change?  
(Please include all relevant feedback.)