ISOT BrakTooth Attack Dataset - Readme

Overview

The ISOT BrakTooth Attack dataset contains Bluetooth classic traffic from both normal Bluetooth communications and BrakTooth-based attacks. BrakTooth attacks specifically target the LMP and baseband layers of the BT classic stack. Due to the lack of non-commercial BT classic sniffers that can capture LMP traffic reliably, we developed an active sniffer utilizing the InternalBlue framework and Nexus 5 device. The experimental procedure for capturing this traffic is illustrated in Figure 1.

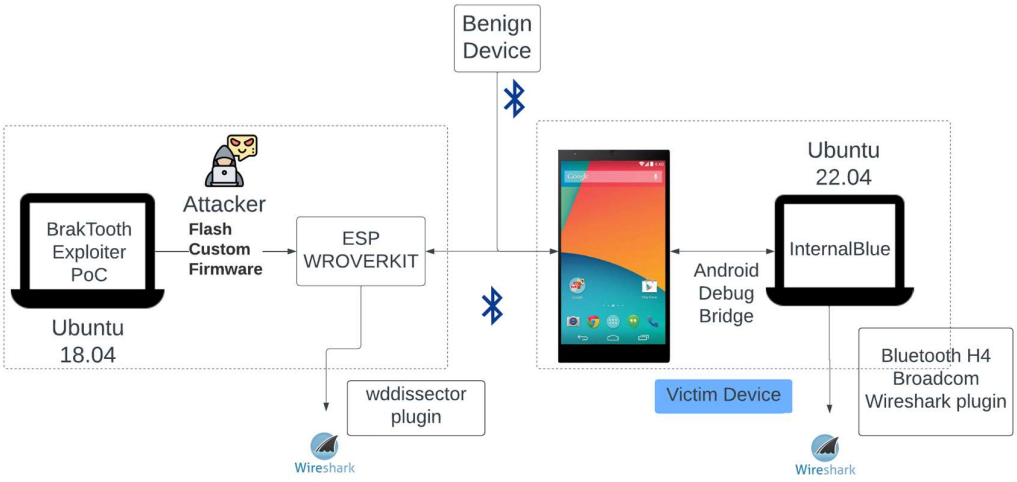

Figure 1: Experimental setup to capture LMP traffic.

Both normal and attack data were extracted from the Wireshark capture files generated by the InternalBlue framework integrated to the Nexus 5 device. To generate normal data, three mobile devices and a Windows 11 laptop were paired with the Nexus 5 device, exchanging sample documents, video, and audio files over the BT Classic protocol. For generating attack data, a PoC tool was used to execute various BrakTooth attacks. A few samples from the dataset are shown in Table 1.

Protocol	Info	Length	Delta	Type
LMP	LMP_timing_accuracy_req	13	0.00049	invalid_timing_accuracy

LMP	LMP_timing_accuracy_res	15	0.050191	invalid_timing_accuracy
LMP	LMP_detach	14	0.000379	invalid_timing_accuracy
Baseband	FHS	28	0.071917	invalid_timing_accuracy
HCI_CMD	Sent Write Scan Enable	5	0	normal
HCI_EVT	Rcvd Command Complete (Write Scan Enable)	7	0.003713	normal
HCI_CMD	Sent Write Scan Enable	5	0.048534	normal

Table 1: Samples from the dataset

The following table gives the distribution between normal and attack data

Type of Vulnerability	**Packets**
Normal	6269
Attack: AU Rand Flooding	655
Attack: Truncated SCO Link Request	340
Attack: Duplicated IOCAP	299
Attack: Truncated LMP Accepted	274
Attack: Invalid Feature Page Execution	250
Attack: Feature Response Flooding	216
Attack: Invalid Timing Accuracy	211
Attack: LMP Overflow DM1	159
Attack: LMP Auto Rate Overflow	151
Attack: Duplicated Encapsulated Payload	111
Attack: Invalid Setup Complete	67

Table 2: Distribution of samples

Dataset Structure

Descriptions for each feature of the dataset are listed in Table 3. The dependent variable, "Type," is manually labelled after the execution of each attack type in isolation. Similarly, the packets of the "normal" type are labelled after allowing the victim device (i.e., the active

sniffer) to exchange multimedia files (video, audio, and text) with three other mobile devices and a Windows 10 laptop.

Feature	Description
Protocol	Refers to the protocol used in the Bluetooth packet such as L2CAP, OBEX, Service Discovery Protocol (SDP), RFCOMM, and others.
Info	Provides additional information about each packet depending on the type of protocol used.
Length	Indicates the length of the packet in bytes.
Delta	Indicates the time difference between the current packet and the previous packet in the pcap file.
Type	Represents normal vs attack conditions and is labelled manually.

Table 3: Features

Reference

To cite this dataset use:

Nandikotkur, Achyuth; Traore, Issa; Mamun, Mohammad. Detecting BrakTooth Attacks. In: Secrypt 2023, 20th International Conference on Security and Cryptography, 10-12 July 2023, Rome, Italy.