HACKING WITH HAYES

**Background Information**

The Hayes command set was originally developed in 1982 by Dennis Hayes for connecting to baud modems (ie., Dial-up modems). In addition to the original commands, manufacturers have added their own vendor-specific instruction sets. This lack of standardization has led to problems with compatibility, especially in newer devices. The Hayes command set is a subset of serial port programming. Operating at a very low level, it allows direct manipulation of the hardware.

I leverage this technology to issue commands to a phone, which allowed me full access to all of the device’s data. In addition, I could also initiate calls, send texts, answer incoming calls, make the phone ring incessantly, and even register my own commands through a Bluetooth connection between myself and the device.

**Common Prefixes and Suffixes**

**AT** [Attention]

**D** [Dial]

**T** [Touch-Tone]

**A** [Answer]

**A/** [Repeat Last Command]

**H** [Hang Up]

**H0** [Hook Status: On] || **H1** [Hook Status: Off]

**I0** through **I9** [Device Information]

**Example**

Command: ATDT15551234

|  |  |  |
| --- | --- | --- |
| **Modem A** | **Modem B** | **Explanation** |
| ATDT15551234 | --- | User at Modem A sends command to Modem B |
| --- | RING | Modem B starts to ring |
| --- | ATA | Modem B issues answer command |
| CONNECT | CONNECT | The modems connect |

The Global System for Mobile Communications (GSM) created their own set of commands for managing the Short Message Service (SMS). These can vary significantly between manufacturers.

**Hayes Commands for Motorola**

|  |  |
| --- | --- |
| **Command** | **Description** |
| AT+CMGS=”5551112345”\n > Type message here | Send a single SMS message |
| AT+MMGL=”ALL” | List all text messages on device |
| AT+MRTONE | Set ringtone |
| AT+MPBR = firstIndex, lastIndex | View entries in phonebook |
| AT+CLAC | List all supported AT commands |

**Important Terminology**

Bluetooth: a wireless technology that allows multiple users to exchange data easily, over distances up to 100 meters (approximately 328 ft)

Piconet: a network of connected Bluetooth devices, with one master device that initiated the connection and up to seven slave devices

Scatternet: two or more interconnected piconets with a piconet master that relays commands between each piconet

Bluetooth Worm: a type of virus that spreads primarily to mobile devices that are connected to a Bluetooth network

**Common Exploitation Techniques**

Bluesnarfing: An information-gathering technique that is able to copy the entire hard-drive of a vulnerable device. It also has the ability to render all phones in the immediate area useless by broadcasting a corrupted message.

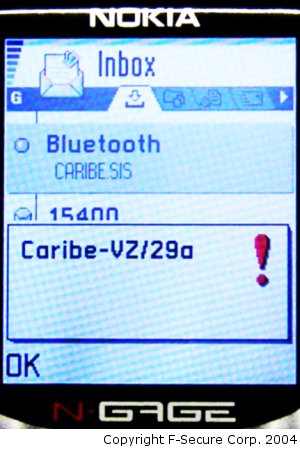
Bluebugging: An attack that manipulates a phone into compromising its own security. Used to create a backdoor in infected devices that allows the hacker to listen in on calls, send messages from the phone, read private messages, etc.,

Bluejacking: A way of sending unsolicited messages to Bluetooth-enabled devices

**The Cabir Worm**

Believed to be the first worm that could infect Bluetooth-enabled mobile devices, it infected phones running the Symbian operating system. The Cabir Worm was created by a group of international hackers as a “proof-of-concept” worm to bring attention to the glaring lack of security in Bluetooth protocols.

An infected device would show the message “Caribe” on its screen. It was considered harmless because the Carib Worm’s main purpose was to spread to as many devices as possible, rather than to destroy or steal information.



**Bluetooth Profiles**

There are approximately 40 different Bluetooth profiles defined in the protocol. I’ve included a small sampling of them.

|  |  |
| --- | --- |
| **Profile Name** | **Profile Description** |
| File Transfer Profile (FTP) | Used for browsing and sending files/folders to a connected device |
| Hands Free Profile (HFP) | Used in newer cars to connect a phone to the radio, allowing for hands-free calls |
| Object Push Profile (OPP) | Used to *push* pictures, virtual business cards, etc., Always instigated by the client. |
| Serial Port Profile (SPP) | Emulates a serial cable using the RFCOMM protocol. Used in my research. |

**Blucat: Netcat for Bluetooth**

Created by Joseph Paul Cohen in 2012.

This program emulates Unix-based tools such as Netcat and Nmap, using the RFCOMM protocol in place of the TCP/IP protocol.

**Examples of Blucat Usage**

|  |  |
| --- | --- |
| **Command** | **Description** |
| ./blucat scan | Scans for all open channels on nearby devices |
| ./blucat devices | Returns the MAC address of nearby devices |
| ./blucat services | Returns every Bluetooth profile used by a nearby device |
| ./blucat -url btspp://00000000CAFE:20 | Connects to the device with the MAC address 00000000CAFE using the serial port 20 |