Satellite hacking: hacking the iridium satellite system

Vasileiadis A. (CyberKid)
Vasileiadis A. (CyberKid)
7 min read

Aug 26, 2024

The Iridium satellite communications system provides global coverage through a network of 66 satellites in low Earth orbit. These satellites are used for voice and data communication in remote areas where there is no cellular coverage or other communication networks.

Illegal access to satellite systems, such as the Iridium system, is a complex and highly specialized activity that requires knowledge in many areas of technology and security. The Iridium system is a

network of communications satellites that provides global coverage for voice and data communications. It is particularly important because of the coverage it offers even in remote areas, such as at sea or in deserts.

Attack on the Iridium System

The Iridium system is known for its strong encryption and security measures. However, there is interest in its hackability, mainly due to its widespread use by government agencies, military forces and professionals in remote places.

What is the Iridium System?

The Iridium system consists of 66 satellites orbiting the Earth in low orbit, providing global coverage. The satellites are connected to each other and to ground

stations through a frequency network that allows continuous communication. This infrastructure is necessary for users who need reliable communication in areas without other telecommunications networks.

How Is Illegal Access Done?
1. System Analysis

Network Architecture: The Iridium network combines satellites in low orbit with ground stations and user units. The satellites communicate with each other and with ground stations to ensure global coverage.

Encryption and Security: Communications are encrypted with strong algorithms to protect against eavesdropping and interference.

2.Popular Tools and Techniques

Signal Recognition: Specialized tools and software are used to analyze and record the signals emitted by the Iridium system.

Vulnerability Exploitation: Although the system has strict security measures, security researchers are constantly analyzing for new vulnerabilities that may allow protection mechanisms to be bypassed.

3. Attack Strategies

Material Attack: The target of the attacks are the user devices and terminals communicating with the network.

Software Attack: The possibility of hacking

the software that manages satellite communications is being looked into.

4. Security and Counterattack

Preventive Measures: The Iridium system is constantly upgrading its security measures and adapting its encryption protocols to cope with new threats.

Attack Detection: Advanced detection systems are implemented to identify and prevent suspicious activity.

Illegal access to the Iridium system usually requires:

Understanding Infrastructure and Communication: Attackers need to understand the network architecture and the communication protocols used.

Collection of information: Analysis of data transmitted over the network and detection of vulnerabilities. This may include monitoring the signals and codes used to communicate between satellites and ground stations.
Use of Specialized Equipment: Equipment capable of communicating with satellite networks is needed. This may include software and hardware that can decrypt data or intercept signals.
Vulnerability Exploitation: If there are weaknesses in encryption or communication processes, attackers can exploit them to gain access to sensitive data or interfere with communication.
Hide Attack: Monitoring and recording of communications can be done without being detected by network security systems.
Important Notes

Legal Significance: Illegal access to satellite networks is illegal and carries serious legal consequences. Interception or falsification of data can lead to serious penalties and prosecution.
Ethical and Insurance Implications: The security of communications critical to defense, rescue and other sensitive applications may be compromised. Understanding and managing the risks associated with such activities is critical to protecting communication systems and avoiding the impact of malicious actions.

In the modern digital age, satellites are used for many essential services, including:

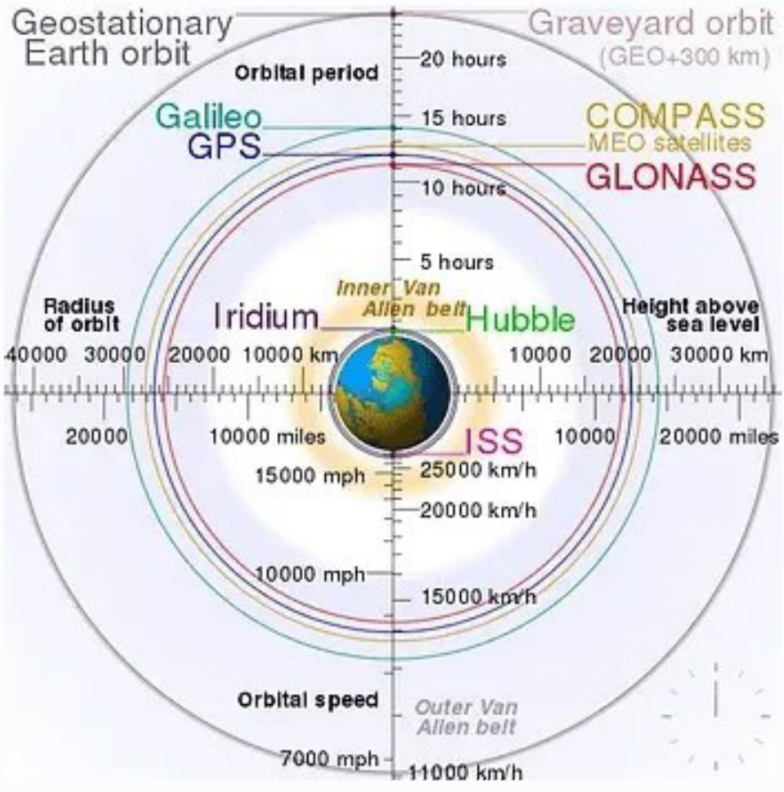
GPS
Connect to the Internet via a broadband connection
Satellite phone

Emergency impacts and disaster relief
Television and radio broadcasting
Weather data
Collection of scientific data
Remote sensing and imaging, and more.
In this series, we will examine and develop ways to jam and hack satellite signals.

In this first tutorial, we will break down how to hack communications on the Iridium satellite network.

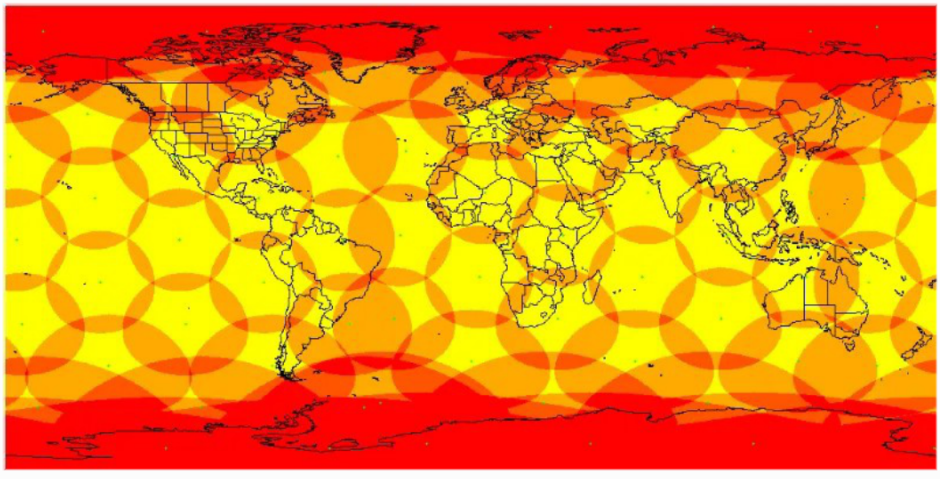
This network was developed by Motorola in the 1990s and became operational in 1998. It provides paying customers with the ability to use a phone with which they can make calls from anywhere on our planet, including the poles, remote areas and summits mountains where there is no mobile phone available. This service has proven invaluable to various militaries,

tourists, environmental groups in remote parts of the world and many others.



Unlike legacy geostationary satellites that are in high orbit, at an altitude of 200.000 miles or more, these 66 satellites move around the planet in north-south orbits in a lower orbit of about 22.000 miles. The advantage of these low orbits is the low delay in communication, while the disadvantage is the small coverage area of each satellite, requiring more satellites to

cover the entire planet.



Iridium service includes voice communication, pager and SMS-like messaging. All these communications can be intercepted using inexpensive SDR software and hardware.

Step #1: Setup
The first step is, of course, to have the basic equipment. As described in the tutorial, you will need the following:

One computer
The DragonOS operating system

An SDR receiver (RTL-SDR or HackRF)
One satellite antenna (flat antenna from the www.rtlsdr.com, about $60)

Step #2: Extract Data from the Log
To extract Iridium data from satellite signals, the first step is to set up the configuration file for the Iridium exporter.

First, go to the folder gr-iridium on DragonOS.

dragon > cd /usr/src/gr-iridium

Then navigate to the folder examples. There you will find configuration files for various SDR devices. Since we will be using the most economical equipment for this hack, mark the file rtl-sdr.config.

Open the configuration file for the RTL-SDR with your favorite text editor (I used featherpad).

Go to the line it says device_args='rtl=0, bias=1' and remove it # from the beginning of the line. Your file should look like the following. This enables the tool to use rtl-sdr and provide power to the antenna (bias=1).

Now, save the file.

Step #3: Recording the Iridium Signal

In this step, we will record the raw signals from the satellite.

Here, we will use the Iridium extractor to capture the Iridium signals.

dragon > iridium-extractor -D rtl-sdr.conf > iridium_output.txt

To make sure you capture enough data to extract voicemails and messages, let this command run for several hours or overnight.

Step #4: Decode the Recorded Data
Now that we have captured the raw data with our RTL-SDR and antenna and saved it to a file named iridium_output.txt, we need to decode this data to understand the messages. To do this, we will use the iridium-parser.py (disaggregation simply

means to break into parts and break down into essential elements). The parsed information will then be saved to a named file iridium_parsed.

dragon > python3 iridium-parser.py -p iridium_output.txt > iridium_parsed

Now we need to add the whole iridium-toolkit in the PATH variable for ease of use.

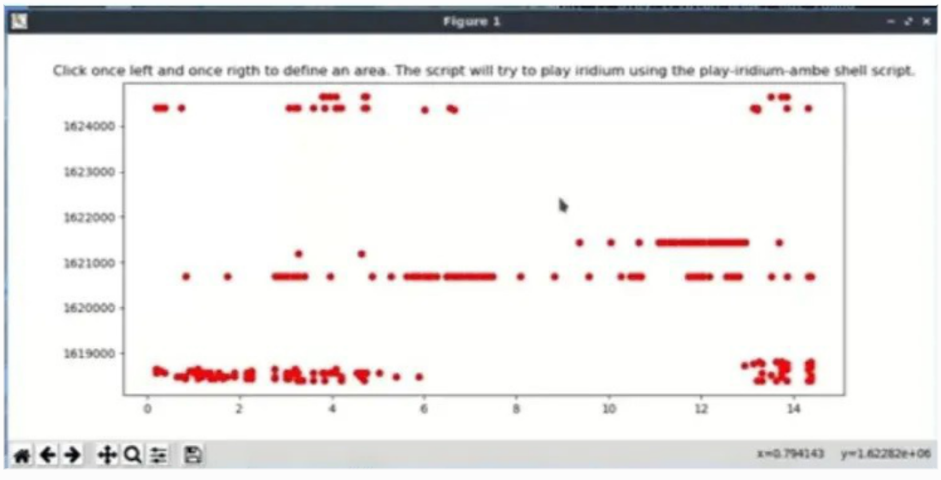
dragon > PATH=$PATH:/usr/src/iridium-toolkit

Note: For more on changing the PATH variable, see Linux Basics for Hackers.

Now we can decode the voice data from this parsed output using the stats-voc.py, part of the iridium toolkit.

dragon > ./stats-voc.py iridium_parsed

This will open a window like the one below. Red dots represent potential audio recordings (the more data you capture, the higher the number of red dots).



Step #5: Reassemble Other Data

Iridium data includes voicemails, pages and texts. Let's see if we can find any of them among our records.

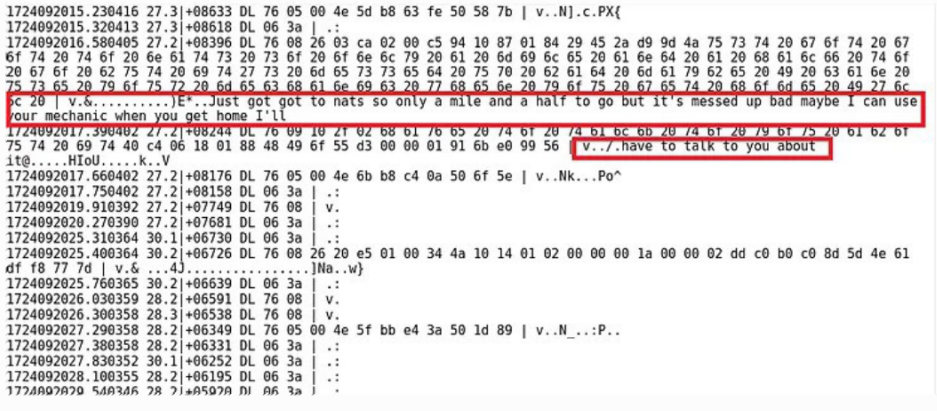
The first step is to reassemble this data. In iridium-toolkit we have a tool called reassembler.py. We can use this to

reassemble the other data. The reassembler has 3 options:

ida – Um Layer 3 messages generally in hex format, some are ASCII
lap – GSM Layer 3 messages in pcap format
msg – Page messages
Let's try the option ida.

golden dragon > sudo ./reassembler.py -i iridium_parsed -m ida

You can see the output below.



Note

Note that almost all messages are in hex format, but some are in human-readable ASCII. Messages in hex format can be converted to ASCII using a hex to ASCII converter.

Summary

Satellites have become a necessary intermediary in our global communication system. These systems are used for radio, internet, television and mobile communication. In most cases, these systems are not properly secured, so that anyone with cheap equipment and some skill can intercept and listen or read these messages.