Satellite Hacking Notes

For use with the CPX SimpleSat ICD

Overview:

GROUND STATION EXPLOITATION

RADIO FREQUENCY EXPLOITATION

REMOTE PHYSICAL EXPLOITATION

Similar to aircraft hacking, there are three main families of satellite hacking techniques: ground station based exploitation, Radio Frequency (RF) based exploitation, and remote physical exploitation.

GROUND STATION EXPLOITATION

This is perhaps the easiest method of satellite hacking to understand and the most straightforward to carry out. The attackers goal is to gain unauthorized access and control of a ground station already paired with a working satellite. Because most modern ground stations are basically a traditional desktop with a fancy antenna attached, this ends up looking and feeling like more conventional enterprise style network attacks.

The downside of this style attack is that it also carries the most risk for the attacker of being discovered. Because this is a more traditional network that they are gaining access to, they have to worry about system logs catching their log in or network monitoring systems catching on to their game. That's one of the reasons why this is the most well documented form of satellite hacking, it's the only one that leaves a paper trail. It's also the lowest cost attack to carry out.

If they succeed though, they get a very low cost win. Because all of their attacks on the satellite will go through a valid ground station, the attacker doesn't have to worry about encryption, encoding schemes, or even message structure. As long as there is an option in the ground station to do X, they just have to press the button and the ground station will handle the rest. This does expose the one big limit in this attack: an attacker can only do things that the ground station will allow it to do. This generally ends up limiting the actual malicious options you can do and takes most of the crazy hollywood stuff off the table.

For CPX Simple Sat, one of the real world examples we used when designing the challenge was the Terra Satellite hacking incident. In this case, an unknown user was able to gain valid login credentials and log into an internet connected ground station remotely. In the real world the attacker never seemed to do more than that, but in our game we let the player go quite a bit farther.

TLDR

- For an attacker this is the lowest cost and lowest effort way to attack a satellite
  - It is also the most limiting in that you can only do what the ground station lets you
    - Real world example: Terra Satellite

- For a defender this is the easiest attack to recognize and monitor
  - Traditional enterprise security tools will let you know who logged in from where
  - Most ground stations will also log and time stamp each time they send a command.

- This attack style is represented by CPX SimpleSat

RADIO FREQUENCY EXPLOITATION

Radio Frequency (RF) is the middle child of the exploitation family. It's harder to do than ground station attacks, but also more powerful and with little risk of traceback. However it is still more practical and lower cost than remote physical exploitation.

In an RF based exploit, the attacker takes advantage of the satellite trusting and acting on any command that it receives correctly. Because of the complexity in updating them and the risk of losing access to them, very few satellite links are actually encrypted. Instead these communications rely on security through obscurity and hope that no one will be able to decode their custom control messages. As such the attacker simply has to patiently collect and analyze the RF communications between the satellite and ground station to begin reversing their message format.

The downside is this is a very time intensive and difficult process when the attacker is starting from a zero knowledge environment. As such, it is common if not required for the attacker to do as much as they can to figure out the format, frequency, and encoding of the control messages from outside sources, things like leaked ICDs, FCC reports, ect to help speed up this process. Once done however, the attacker will be able to send commands to the satellite without fear of retribution. Because the attacker is bypassing the victims ground station network and communicating straight to the satellite, there's no easy trail to follow that could identify them. At the same time, because it is easier to attack the ground station the victim will likely assume that is how the attack is happening and waste time looking for clues that do not exist on their network.

Once the attacker is able to communicate with the satellite, they are only limited by the Interface Control Document (ICD) that the satellites command link was built to. Where the ground station attacker is limited by any additional limits that programs wrote into the ground station software, the RF attacker can send and do anything as long as it can be represented in a valid way within the ICD.

TLDR

- **An attack requires an absurd amount of time if going from a zero knowledge state**
  - **Attackers will often leverage secondary sources of information to help reduce the time taken to reverse engineer the commands**
  - **Attacker needs to be able to see both sides of the communication channel in order to reverse the commands and responses**
- **An attacker doesn't have to be as worried about being tracked**
  - **A defender would need a 3rd party way to track and detect signals to identify and locate the attacker**
- **An attacker is only limited by what is allowed in the ICD**
  - **Anything that talks to the radio they can target**
- **This attack style is represented in DDSat**

REMOTE PHYSICAL EXPLOITATION

Perhaps the most well known instance of this is the concept of a parasitic satellite that attempts to connect to a victim satellite in orbit. However it also includes any hardware implants done via supply chain injection. This is by far the most expensive and long term exploit to use, which has left it almost exclusively in the hands of nation states. That unfortunately means most examples of this are kept classified, despite the fact that this family of exploits are extremely impractical and useless when used in the real world.

In theory the goal of remote physical exploitation is to gain the most freedom possible for the attacker by having a back door into the satellite.

TLDR

- **This is an attack style that only nation states worry about, and only nation states can do**
  - **It looks scary on paper, but is almost impossible to do well in real life**
- **This one also has the most hollywood mystery surrounding it**
- **Don't talk about it unless you have to, but just know its there.**