Hacking a Bird in the Sky
Hijacking Very Small Aperture Terminal (VSAT) Connections

Jim Geovedi and Raditya Iryandi
BELLA ASIA PACIFIC
Disclaimer

This presentation is intended to demonstrate the inherent security, design and configuration flaws in publicly accessible satellite communication networks and promote the use of safer satellite communication systems. Viewers and readers are responsible for their own actions and strongly encourage to behave themselves.
Satellite

• A satellite is **any object that orbits another object** (which known as its primary).

Artificial Satellites

• It was the English sci-fi writer **Arthur C. Clarke** who conceived the possibility of artificial communication satellites in 1945. Clarke examined the logistics of satellite launch, possible orbits and other aspects.

• The first artificial satellite was **Sputnik 1** launched by Soviet Union on 4 October 1957
Types of Artificial Satellites

- Astronomical satellites
- Reconnaissance satellites
- Navigation satellites
- Killer satellites/anti-satellite weapons
- Solar power satellites
- Space stations
- Weather satellites
- Miniaturised satellites
- Biosatellites
How is a Satellite Launched into an Orbit?
Satellite Internet Services

• Used in locations where terrestrial Internet access is not available and in locations which move frequently, e.g. vessels at sea and war zone.

• Can be used where the most basic utilities are lacking, require a generator or battery power supply that can produce enough electricity.
Three Types of Satellite Internet Services

- **One-way multicast**: used for IP multicast-based data, audio and video distribution. Most Internet protocols will not work correctly over one-way access, since they require a return channel.

- **One-way with terrestrial return**: used with traditional dial-up access to the Internet, with outbound data travelling through a telephone modem, but downloads are sent via satellite at a speed near that of broadband Internet access.

- **Two-way satellite access**: allows upload and download data communications.
Very Small Aperture Terminal (VSAT)

- Two-way satellite ground station with a dish antenna that is smaller than 3 metres.
- Nearly all VSAT systems are now based on IP, with a very broad spectrum of applications.
- Most commonly used interactive and transactional application (online communication between head office and branches, flight ticket and hotel reservation, ATM (Automated Teller Machine) and small data traffic) and terminal application with centralised database (data entry, inventory control and payment point)
Satellite Anatomy

- **Internal Computer (TT&C)**
- **Body**
- **Power source**
- **Attitude control**
- **Grapple Fixture**
- **Communications**
Tracking, Telemetry and Command Station
Topologies of VSAT

- A **star topology**, using a central uplink site, such as a network operations centre (NOC), to transport data back and forth to each VSAT terminal via satellite,

- A **mesh topology**, where each VSAT terminal relays data via satellite to another terminal by acting as a hub, minimising the need for a centralised uplink site,

- and a **combination of both** star and mesh topologies.
Satellite Footprint

- The footprint of a satellite is the ground area that its transponders cover, and determines the satellite dish diameter required to receive each transponder's signal.

- There is usually a different map for each transponder (or group of transponders) as each may be aimed to cover different areas of the ground.

- Footprint maps usually show either the estimated minimal satellite dish diameter required, or the signal strength in each area measured in dBW.
100° E - 145.9° E  
(SE Asia, Australia, China, Japan, Korea)

<table>
<thead>
<tr>
<th>Satellite Name</th>
<th>Position</th>
<th>HD TV</th>
<th>TV Digital</th>
<th>TV Analog</th>
<th>Radio Digital</th>
<th>Radio Analog</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASIASAT 2</td>
<td>100.5° East</td>
<td>0</td>
<td>97</td>
<td>0</td>
<td>51</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>EXPRESS A2</td>
<td>103.0° East</td>
<td>0</td>
<td>13</td>
<td>0</td>
<td>12</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>ASIASAT 3S</td>
<td>105.5° East</td>
<td>0</td>
<td>258</td>
<td>0</td>
<td>56</td>
<td>0</td>
<td>22</td>
</tr>
<tr>
<td>CAKRAWARTA 1</td>
<td>107.7° East</td>
<td>0</td>
<td>70</td>
<td>0</td>
<td>19</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>TELKOM 1</td>
<td>108.0° East</td>
<td>0</td>
<td>57</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>AAP 1</td>
<td>108.2° East</td>
<td>0</td>
<td>57</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>17</td>
</tr>
<tr>
<td>BSAT 1A, 2A</td>
<td>110.0° East</td>
<td>10</td>
<td>3</td>
<td>4</td>
<td>14</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>JCSAT 110</td>
<td>110.0° East</td>
<td>0</td>
<td>63</td>
<td>0</td>
<td>20</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>SINOSAT 1</td>
<td>110.5° East</td>
<td>0</td>
<td>59</td>
<td>0</td>
<td>36</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>PALAPA C2</td>
<td>113.0° East</td>
<td>0</td>
<td>31</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>8</td>
</tr>
<tr>
<td>KOREASAT 2</td>
<td>113.0° East</td>
<td>0</td>
<td>48</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>KOREASAT 3</td>
<td>116.0° East</td>
<td>0</td>
<td>125</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>12</td>
</tr>
<tr>
<td>TELKOM 2</td>
<td>118.0° East</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>THAICOM 1A</td>
<td>120.0° East</td>
<td>0</td>
<td>6</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ASIASAT 4</td>
<td>122.0° East</td>
<td>0</td>
<td>79</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>17</td>
</tr>
<tr>
<td>JCSAT 4A</td>
<td>124.0° East</td>
<td>0</td>
<td>93</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>JCSAT 3</td>
<td>128.0° East</td>
<td>0</td>
<td>142</td>
<td>0</td>
<td>103</td>
<td>0</td>
<td>21</td>
</tr>
<tr>
<td>JCSAT 5A</td>
<td>132.0° East</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>APSTAR 6</td>
<td>134.0° East</td>
<td>0</td>
<td>46</td>
<td>2</td>
<td>55</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>APSTAR V / TELSTAR 18</td>
<td>138.0° East</td>
<td>0</td>
<td>151</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>EXPRESS AM3</td>
<td>140.0° East</td>
<td>0</td>
<td>14</td>
<td>0</td>
<td>8</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>SUPERBIRD C</td>
<td>144.0° East</td>
<td>0</td>
<td>57</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

## Hacking a Bird in The Sky

**Warning:** You are allowed to steal any contents of this material with or without notifying the authors.

### Table: Satellite Channels

<table>
<thead>
<tr>
<th>Channel ID</th>
<th>Frequency</th>
<th>Service Type</th>
<th>Carrier</th>
<th>Modulation</th>
<th>Channel</th>
<th>Bitrate</th>
<th>Provider</th>
</tr>
</thead>
<tbody>
<tr>
<td>PAL0C2CE</td>
<td>1K 10.970V</td>
<td>TV-DIG-CRYPT</td>
<td>ABC Asia Pacific</td>
<td>MPEG-2</td>
<td>769</td>
<td>3/4</td>
<td>DEU</td>
</tr>
<tr>
<td>PAL0C2KN</td>
<td>3K 11.472H</td>
<td>TV-DIG-CRYPT</td>
<td>NASA TV</td>
<td>MPEG-2</td>
<td>1281</td>
<td>3/4</td>
<td>ENG</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DATA</td>
<td>Data Service</td>
<td></td>
<td>1</td>
<td>3/4</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>DATA</td>
<td>Data Service</td>
<td></td>
<td>1</td>
<td>3/4</td>
<td></td>
</tr>
</tbody>
</table>

*Note: The table continues with more channels and details.*
MEASAT-1 @ 91.5º East
Hacking a Bird in The Sky

Warning: You are allowed to steal any contents of this material with or without notifying the authors.
Attacks against Satellite Systems

*It’s politically sensitive, but it’s going to happen. Some people don’t want to hear this, and it sure isn’t in vogue … but—absolutely—we’re going to fight in space. We’re going to fight from space and we’re going to fight into space…*

General Joseph W. Ashy
Former Commander in Chief U.S. Space Command


Warning: You are allowed to steal any contents of this material with or without notifying the authors.
Hypothetical Attacks against Satellite Systems
Denial of Service Attacks

- Jam uplink and downlink
  - White noise at frequency.
  - Requires directed antenna.
  - Requires very low power.
  - Difficult to detect, especially if occurring at irregular intervals.

Denial of Service Attacks

- Overpower uplink
  - Can be done with transportable satellite ground terminals
    - In tri-band (C-band, X-band, and Ku-band).
  - Power limited.
  - Uplink equipment now contains ID coding.

Orbital Positioning Attacks

- **Ranging transponder spoofing**
  - Multiple ground stations triangulate satellite position using a series of tones sent to a transponder.
  - Ground stations observe phase differentials.
  - Ground or airborne spoofer could transmit false response, resulting in incorrect orbit determination.

Orbital Positioning Attacks

• Direct commanding
  • Preparation and delivery of telecommand queue.

• Command replay
  • Record outbound telecommand queue from TT&C facility. Replay later to initiate duplicate action.

Orbital Positioning Attacks

- **Insertion after confirmation but prior to execution**

  - SCC formulates telecommand queue and sends to TT&C.

  - TT&C uplinks and receives readback, which it returns to SCC.

  - If readback is correct, SCC waits for proper time to execute.

  - Channel is vulnerable to update during this period — new telecommand queue may be uploaded prior to authenticated execute.

Practical Attacks against Satellite Systems
Warning: You are **allowed to steal** any contents of this material with or without notifying the authors.
Warning: You are allowed to steal any contents of this material with or without notifying the authors.
Warning: You are allowed to steal any contents of this material with or without notifying the authors.
Warning: You are **allowed to steal** any contents of this material with or without notifying the authors.
### Present Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LNB Selected</td>
<td>Single</td>
</tr>
<tr>
<td>LNB Frequency</td>
<td>5.1500 GHz</td>
</tr>
<tr>
<td>Data Lock</td>
<td>Locked</td>
</tr>
<tr>
<td>L-Band Frequency</td>
<td>1.1800 GHz</td>
</tr>
<tr>
<td>Satellite Frequency</td>
<td>3.9700 GHz</td>
</tr>
<tr>
<td>Polarization</td>
<td>VERTICAL</td>
</tr>
<tr>
<td>22 Khz Switch</td>
<td>OFF - Low LNB</td>
</tr>
<tr>
<td>Symbol Rate</td>
<td>12401 (KSym/s)</td>
</tr>
<tr>
<td>Signal Level</td>
<td>70%</td>
</tr>
<tr>
<td>Viterbi Decoded Bit Error Rate</td>
<td>0.0000</td>
</tr>
<tr>
<td>LNB Offset</td>
<td>1.4419 (MHz)</td>
</tr>
<tr>
<td>Signal/Noise Ratio</td>
<td>4.3300</td>
</tr>
<tr>
<td>RSC Error</td>
<td>58085</td>
</tr>
<tr>
<td>Channel Bit Error Rate</td>
<td>0.0150</td>
</tr>
<tr>
<td>Active PIDs</td>
<td>[1]</td>
</tr>
</tbody>
</table>

(RSUE Error : 14751)

(Press (CTRL-C) to Exit)
Warning: You are allowed to steal any contents of this material with or without notifying the authors.
Warning: You are allowed to steal any contents of this material with or without notifying the authors.
Discussion

• Other attacks against satellite?

• Law issues?