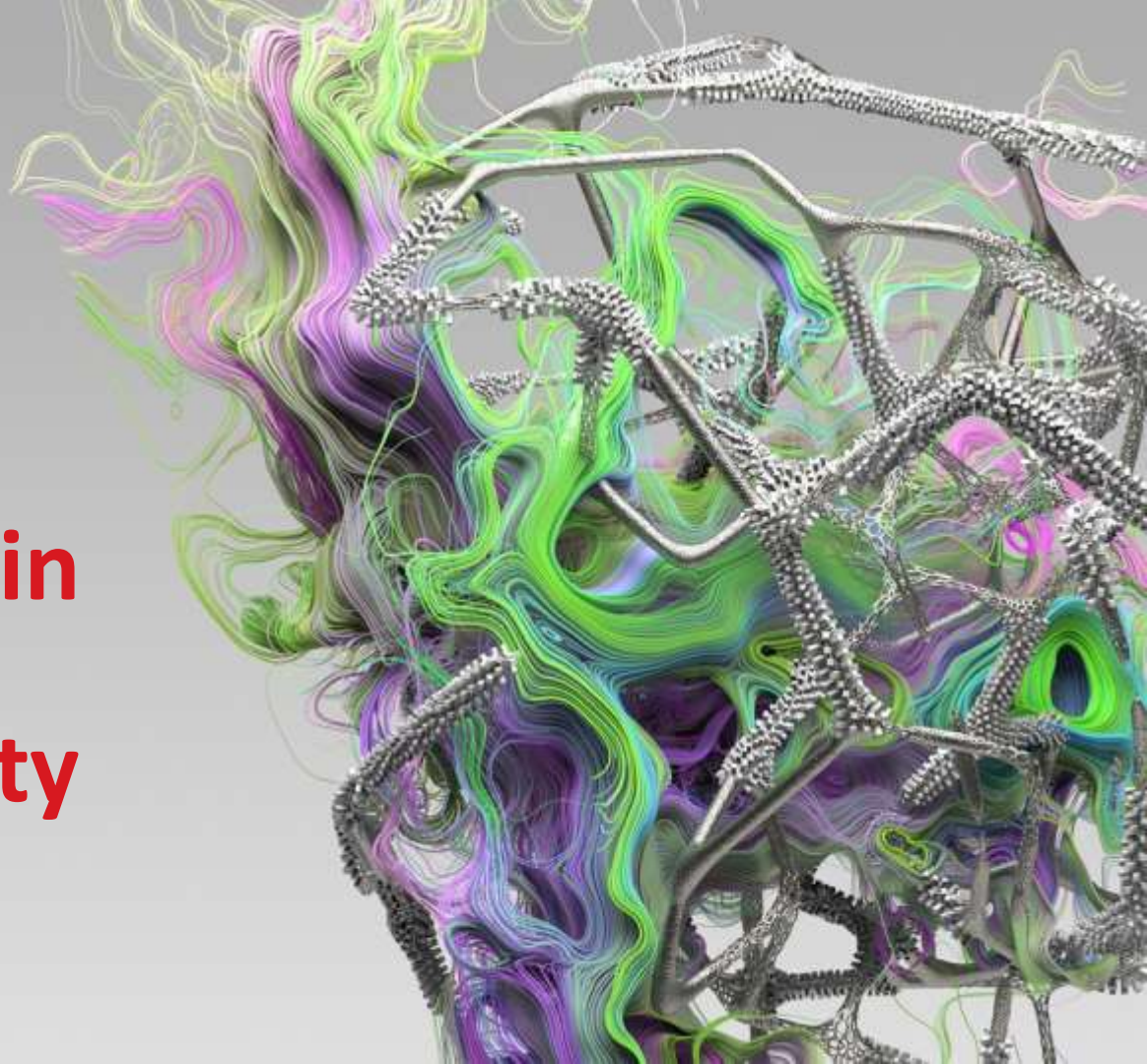
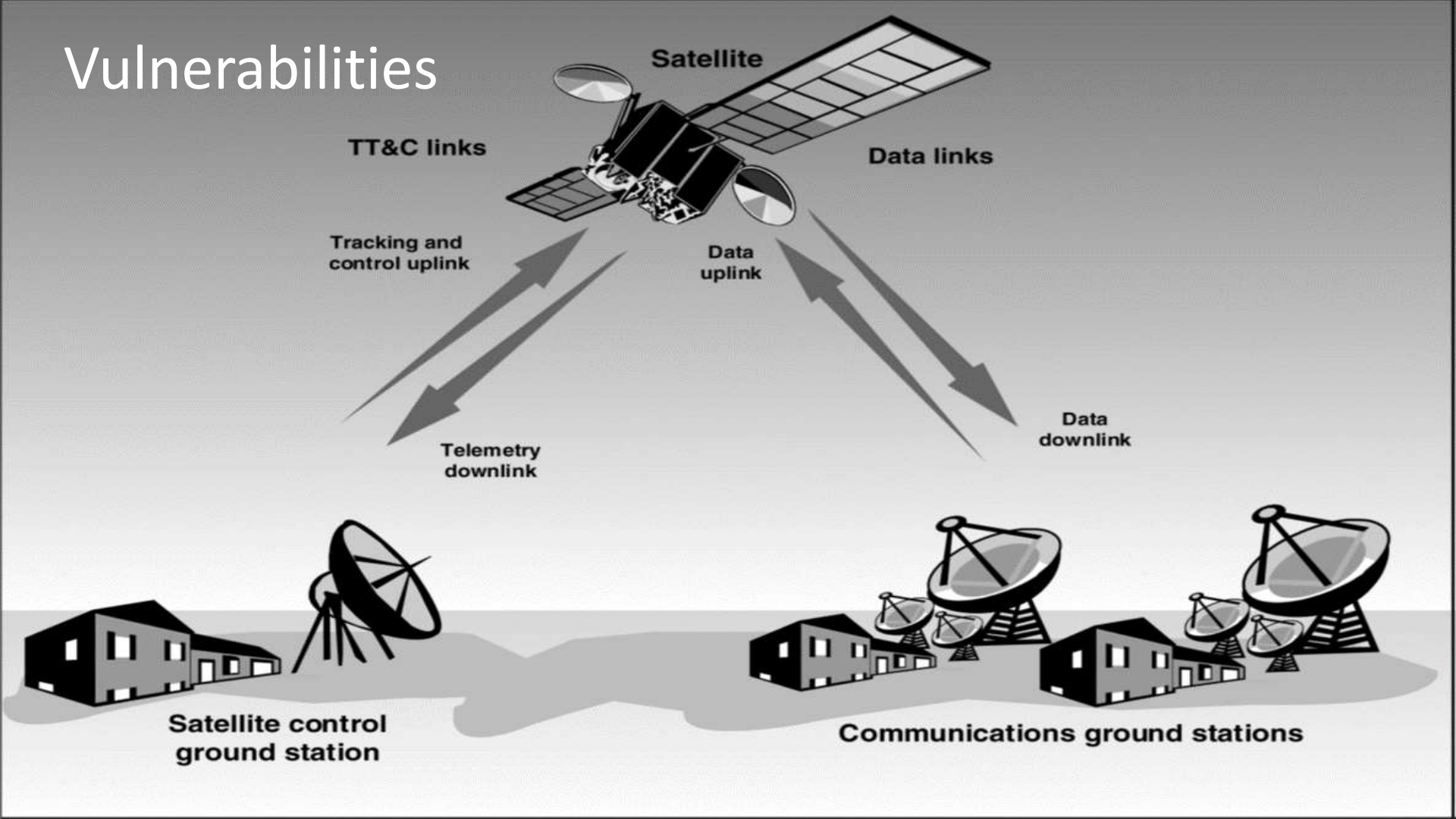


Attack Vectors in Orbit: Satellite Security

William J. Malik, CISA
VP Infrastructure Strategies

Vulnerabilities



Vulnerabilities - Notes

The essential elements of a satellite communications system are shown, with the vulnerabilities highlighted in grey, and black. This simplified chart omits any additional satellites, such as ones used as intermediate relays, for instance.

Satellites are vulnerable to physical attacks or mishaps, as are ground stations. The signal a satellite is broadcasting can be hijacked (replaced with another signal, like the Max Headroom prank in Chicago). The control system can be subverted, allowing a malicious actor to move the satellite or disable it, and the signal can be jammed. Specific measures can defeat some of these attacks.

In 2002 following a series of satellite failures the GAO reported on satellite vulnerabilities. They produced two charts: one showing unintentional threats, the other showing intentional threats.

Unintentional Threats to Satellites

Type of threat	Vulnerable satellite system components
Ground-based:	
Natural occurrences (including earthquakes and floods; adverse temperature environments)	Ground stations; TT&C and data links
Power outages	
Space-based:	
Space environment (solar, cosmic radiation; temperature variations)	Satellites; TT&C and data links
Space objects (including debris)	
Interference-oriented:	
Solar activity; atmospheric and solar disturbances	Satellites; TT&C and data links
Unintentional human interference (caused by terrestrial and space-based wireless systems)	

Unintentional Threats - Notes

Unintentional threats to satellites are accidents that can damage the satellite or its ground station. These include meteorites, solar wind, accidental collisions, and all the things that can go wrong when a complex system is in a hostile environment. None of these is planned, or caused by a human actor.

Intentional Threats to Satellites

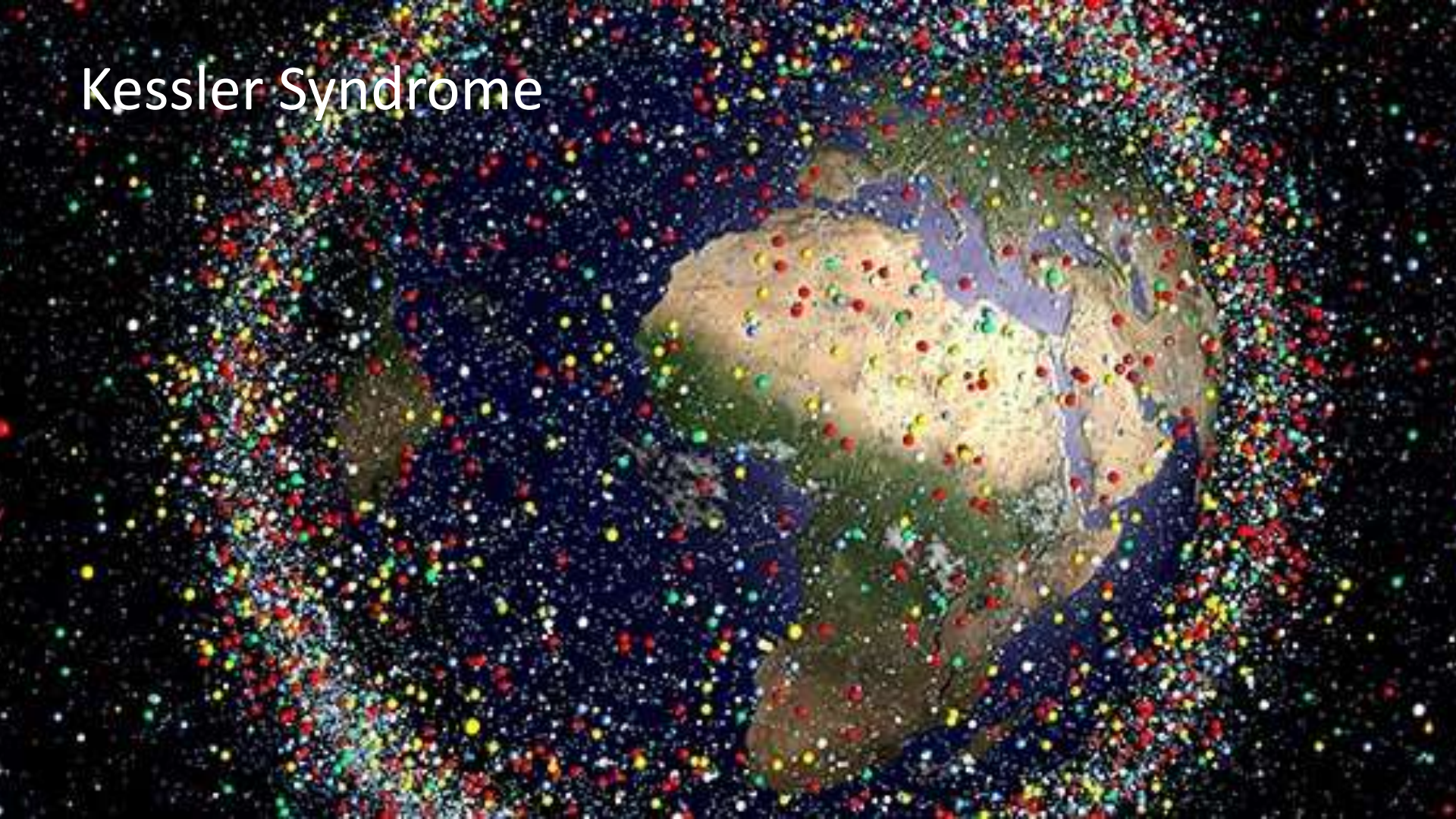
Type of threat	Vulnerable satellite system components
Ground-based:	
Physical destruction	Ground stations; communications networks
Sabotage	All systems
Space-based (anti-satellite):	
Interceptors (space mines and space-to-space missiles)	Satellites
Directed-energy weapons (laser energy, electromagnetic pulse)	Satellites; TT&C and data links
Interference and content-oriented:	
Cyber attacks (malicious software, denial of service, spoofing, data interception, and so forth)	All systems and communications networks
Jamming	All systems

Intentional Threats - Notes

Intentional threats are hostile, planned attacks on the satellite, its payload, or its ground station. All of these require some measure of planning and resources to succeed.

The GAO report goes into detail examining the best measures to thwart these attacks. But there is an additional classes of problems that are neither unintentional nor intentional: unwise architectural decisions and code defects. Let's look at both.

Kessler Syndrome



Kessler Syndrome Notes

Kessler Syndrome was first described in the 1970s by Donald Kessler, Senior Scientist for Orbital Debris Research at NASA. He speculated that when a satellite disintegrated the shrapnel could cause additional satellite failures, generating more debris. This “collisional cascading” would continue until the satellites in the orbit were all disabled and that orbit had to be abandoned.

In 2009 the Socrates system predicted that two satellites would pass within 564 meters. One was a defunct Soviet-era communications satellite, the other was number 33 of the Iridium communications constellation. In reality they collided. The problem here was either a code bug: the location data was accurate but the calculation was performed incorrectly; or a user interfaced bug: the position and trajectory data was not precise but the programmer performed the calculation anyway, inventing precision. If the data was imprecise, the answer should have been, These two satellites will pass within 1/2 km, head’s up.

https://www.nasa.gov/centers/wstf/site_tour/remote_hypervelocity_test_laboratory/micrometeoroid_and_orbital_debris.html

GPS Rollover

Multiple Boeing 787s in China experienced GPS 20 years rollover issue.
Some aircrafts have to be grounded waiting for an update. – China Aviation Review

NYCWiN crashed 7:59 PM Apr 6 – NY Times

GPS Counter Rollover - Notes

Satellites launched before 2010 used a 10-bit field to count the weeks since Jan 1, 1980. This count contributes to the satellite determining its position. Since there are 52 weeks in a year, that counter rolls over in less than 20 years. This unwise architectural decision was not an unintentional act nor a deliberate attack. But the impact was felt by Boeing's 787 jets in China Air, which were not certified as airworthy when they reported today's date as Aug 22, 1999; and by New York City's NYCWiN WiFi network, which crashed at 7:59 PM EST April 5, 2019. That system was down for ten days. The outage meant the 12,000 automatic traffic signals could not count traffic, so defaulted to a regular 90-second green, 15 second yellow, 90 second red pattern. This slowed traffic. Also, the 300 kiosks offering free public Internet access were unavailable. New York spent $330 million setting up the system and pays $50 million a year for ongoing support and maintenance.

This unwise architectural choice ignored the operational longevity of satellites. Telstra, launched July 10 1962, is still in orbit today.

IoT devices, such as satellites, are subject to accidents, malicious attacks, and bad design and implementation choices.