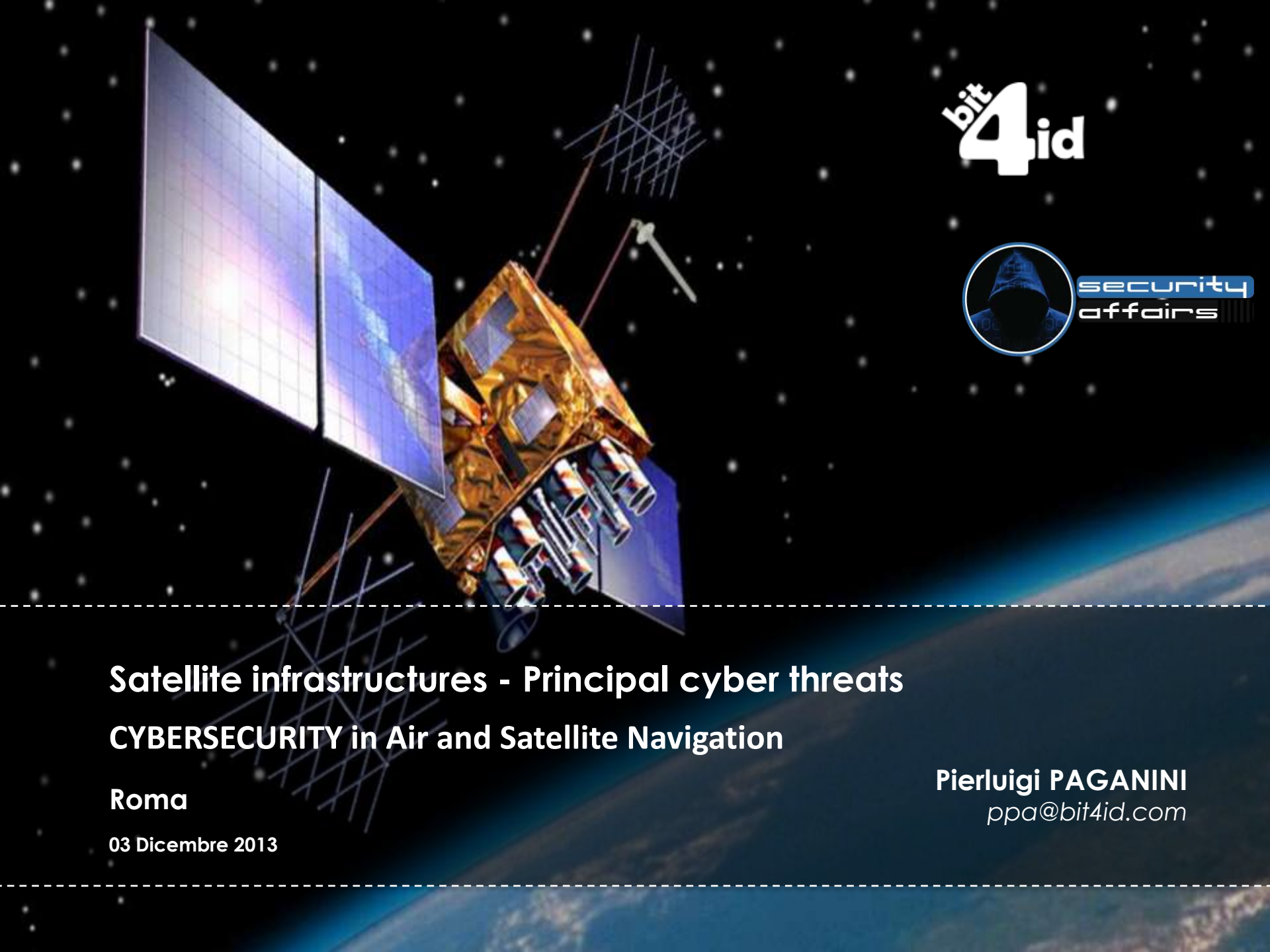


Satellite infrastructures - Principal cyber threats

CYBERSECURITY in Air and Satellite Navigation

Roma

03 Dicembre 2013

Pierluigi PAGANINI
ppa@bit4id.com

AGENDA

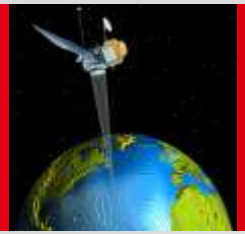
- Intro 
- Jamming 
- Eavesdropping 
- Hijacking/Control 

- Scanning/Attacking 
- Signal encryption and hardening 
- Conclusions 

AGENDA

- Intro

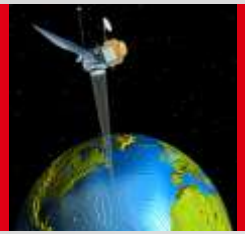
- Jamming
- Eavesdropping
- Hijacking/Control
- Scanning/Attacking
- Signal encryption and hardening
- Conclusions



Intro

Role for satellite in today society

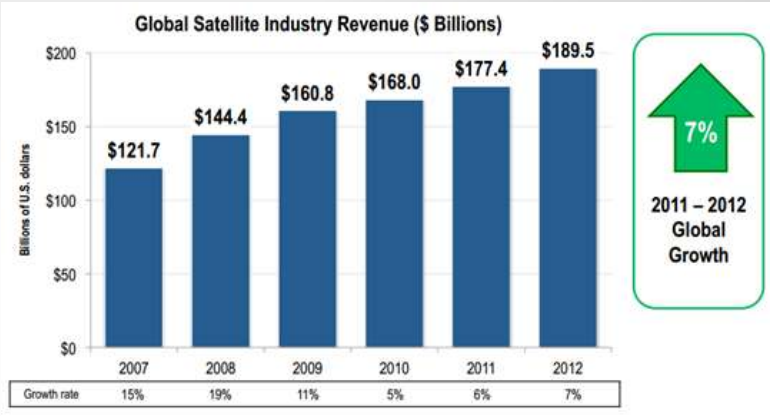
- Satellites have assumed a crucial role in both private and public sectors (e.g. Defense, early warning systems, global broadcasting, meteorology, navigation, reconnaissance, remote sensing and surveillance).
- Any accidental interference or cyber attack could have a serious effect.
- Satellite security is today a pillar of the cyber security strategy of any government, they are considered as "critical infrastructure," therefore are privileged targets for a possible cyber attack.
- Increased interest of state-sponsored hackers, hacktivists, cyber criminals … different actors, similar threats.
- Complex architectures, wide surface of attack.
- Long life cycle compared to the rapid evolution of hacking techniques and technologies.



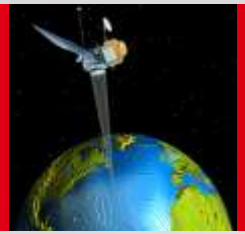
Intro

State of satellite industry

- The global satellite industry revenues in 2012 are $189.5 billion, 62% for space sector and 4% of telecommunications.
- The global satellite industry grew 7% in 2012 (Satellite Industry Association - June 2013)
- More than 50 countries operate at least one satellite.
- It has been estimated that there are over 1,000 operating satellites as of year-end 2012, more than half of which are communications satellites.



Function %	Percentage
Commercial Communications	38 %
Government Communications	16 %
Remote 8% Sensing	10%
Space Science	9 %
R&D	9%
Military Surveillance	10%
Navigation	7%
Meteorology	3%



Intro

Top 10 Cyber Threats (Jim Geovedi)

1. Tracking – tracking over web data and software
2. Listening – listening with the right equipment, frequencies, and locations
3. Interacting – protocols and authentication used, radio transmissions need official license!
4. Using – take over a bird or a TT&C [use payloads, make pictures, transmit something (DVB or radio)]
5. Scanning/attacking – anonymous proof of concept in 2010 by Leonardo Nve Egea, scanning, DoS, and spoofing possible
6. Breaking – old technologies used (X.25, GRE)
7. Jamming – jamming well-known frequencies for satellites
8. Mispositioning/Control – transponder spoofing, direct commanding, command reply, insertion after confirmation but prior to execution
9. Grilling – activating all solar panels when exposed to sun, overcharging energy system
10. Collisioning

AGENDA

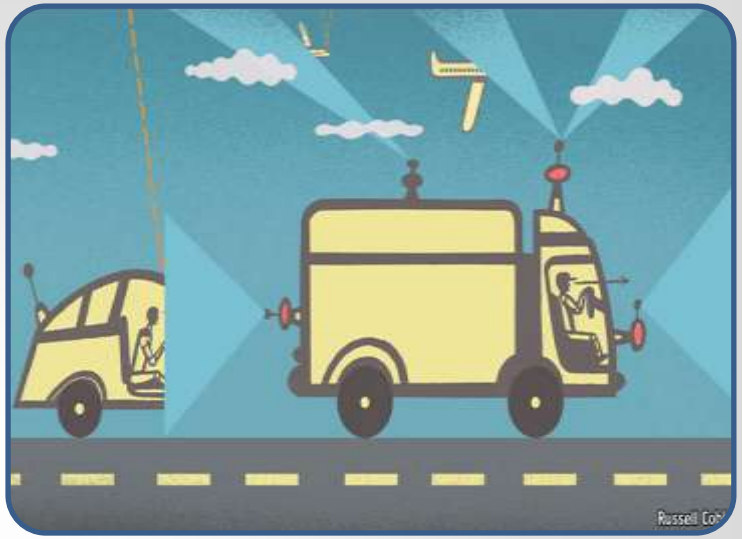
- Intro
- Jamming

- Eavesdropping
- Hijacking/Control
- Scanning/Attacking
- Signal encryption and hardening
- Conclusions

Jamming

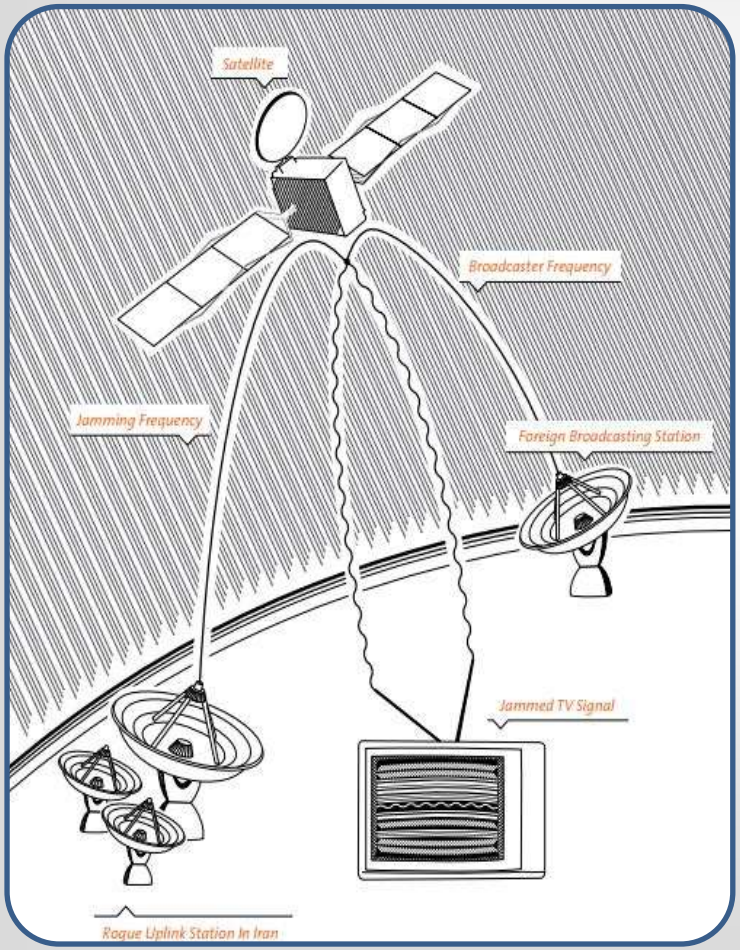
Cyber threats

- Attacker floods or overpowers a signal, a transmitter, or a receiver, interfering with legitimate transmission.
- Interference has become the primary cause of the impairment and degradation of satellite services.
- Hackers use a directed antenna to produce the interference, usually a specifically crafted signal having enough power to override the original transmitted signal.
- Satellite jamming is a hacking method often used to interfere with communication for distribution of media for censorship purpose.
- The two forms of satellite jamming are “orbital” and “terrestrial”.



Jamming

Orbital Jamming



- In orbital jamming, the attacker sends a beam of contradictory signals directly to a satellite via a rogue uplink station.
- The jamming signals are mixed with the legitimate signals, thus interfering with them.
- The jamming signals are able to override the legitimate transmission, blocking its transmission to the recipient.
- An uplink jammer must have at least the same power of the signal it is attempting to block and, during the attack, it must be located within the footprint of the satellite antenna it is targeting.

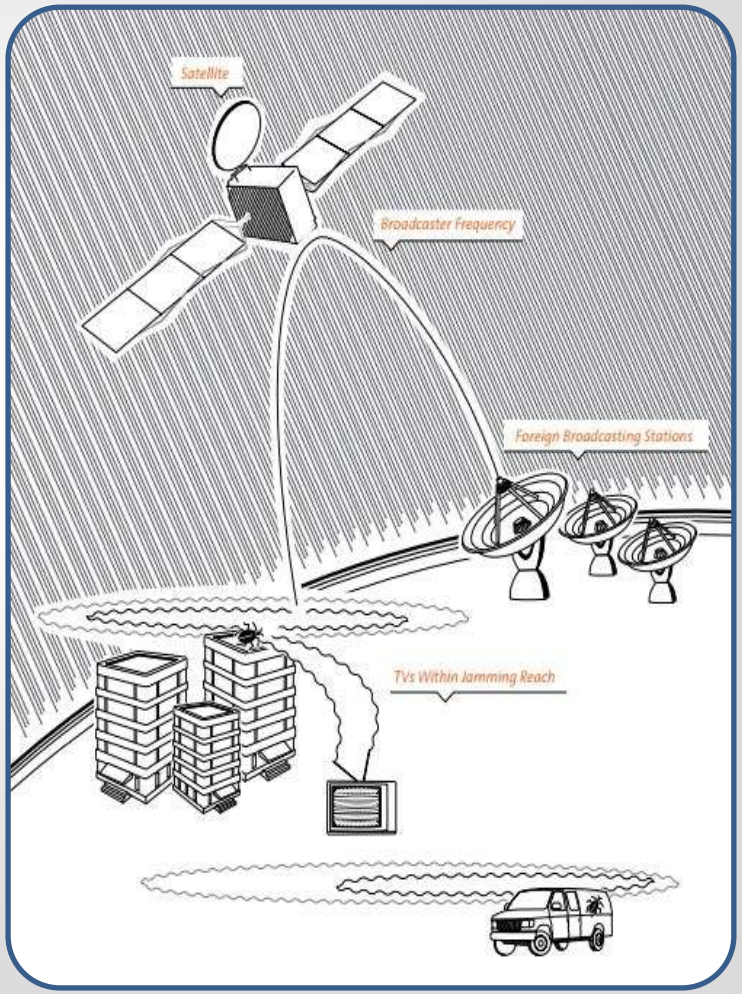
Attack scenario – TV broadcasts :

Attacker transmits a signal up to the satellite on the frequency used by the authorized user. That signal interferes with the authorized service and prevents it from being decoded by viewers' satellite receivers.

Jamming

Terrestrial Jamming

- The attacker transmits rogue frequencies in the direction of terrestrial targets (ground satellite dishes).
- The jamming frequencies are limited to a specific area and are able to interfere only with the frequency emanating from the satellite in a specific location.
- Small, portable terrestrial jammers are easy to purchase and use; they typically have a range of 3-5 kilometers in urban areas, while in rural areas their range can increase to up to 20 kilometers.



Jamming

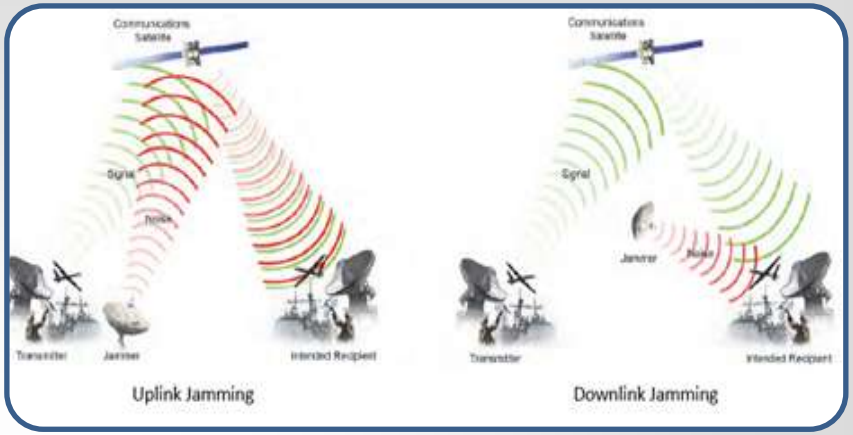
- Uplink jamming has relatively less impact because it can interfere with the transmission of a satellite over a broad area but only for a temporary period and it does not permanently harm the target system.

- The uplink jamming of the control link can prevent a satellite from receiving commands from the ground; it can also target user-transmitted data, thus disturbing the recipients.

- The most concerning aspect of jamming attacks is that they can be undertaken using off-the-shelf technology and the detection and attribution of intermittent jamming can be difficult.

Jamming

Jamming



- U.S. military has already experienced jamming on commercial systems originated in the Southwest Asia region, and involved a transmitter using a continuous wave carrier signal.

- In 2013, Iraq acquired GPS jamming equipment during Operation Iraqi Freedom, allegedly from the Russian company Aviaconversiya Ltd. At least six different jamming stations were discovered and destroyed.

- French commercial satellite fleet operator Eutelsat Communications has recently announced the future deployment of an experimental cutting-edge TV channel interference mitigation function for the first time on its upcoming EUTELSAT 8 West B satellite.

AGENDA

- Intro
- Jamming
- Eavesdropping

- Hijacking/Control
- Scanning/Attacking
- Signal encryption and hardening
- Conclusions

Eavesdropping

Malware based attacks

- Differently from jamming, eavesdropping on a transmission allows an attacker to access transmitted data.
- Availability of off-the-shelf products to intercept satellite transmissions despite communications are encrypted,
- In 2012 German security researchers demonstrated that satellite phones can be easily intercepted and deciphered using equipment readily available on the market (PC, Antenna), hacking the encryption standard algorithms GMR-1 and GMR-2.

Eavesdropping

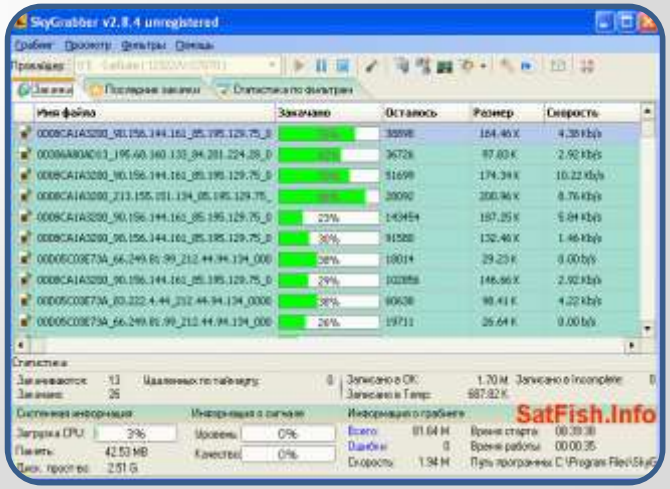
Why not improve encryption for satellite transmissions?

- The encryption of data on satellite transmissions has a series of drawbacks:
  - increasing in the costs of operation. Implementation or upgrade systems to allow encryption and training staff.
  - impact on the overall performance, Geovedi, Iryandi, and Zboralski highlighted the fact that encrypting satellite signals can cause an 80% drop in performance.
- Limited use of encryption for commercial satellites.
- Commercial satellites represent an attraction for hackers.

Eavesdropping

Case study - SkyGrabber

- The off-shelf software SkyGrabber is produced by the Russian firm Sky Software and sold for $26.
- The software was used by hackers in Iraq and Afghanistan to capture unencrypted video feeds of the Predator unmanned aerial vehicles (UAVs).
- The software was used to access data broadcast by satellites.
- The insurgents in those areas weren't able to control or disrupt the UAVs but, using SkyGrabber, eavesdropped on the signals sent.



AGENDA

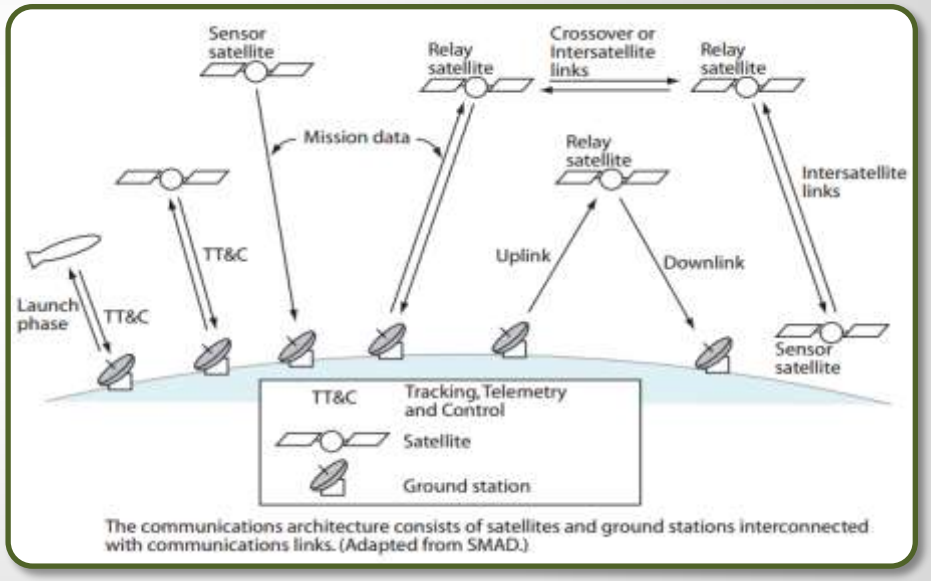
- Intro
- Jamming
- Eavesdropping
- Hijacking/Control

- Scanning/Attacking
- Signal encryption and hardening
- Conclusions

Hijacking/Control

Satellite Hijacking

- Hijacking is the unauthorized use of a satellite for transmission, or seizing control of a signal such as a broadcast and replacing it with another.
- It is very common against Internet data connections and media broadcasts.
- The data transmitted could be acquired (eavesdropping) by attackers that could also modify it in transit (spoofing).



Hijacking/Control

Satellite Control

- With the term "Control" is referred the capability of a hacker to gain the control of part or all the satellite architecture (e.g. ground station, Tracking, Telemetry and Control, bus, payload).
- Wrong commands are sent to the satellite system causing device rotation or movement that could direct solar panels and antenna in the wrong directions.
- Satellite control is considered very difficult to implement because security measures to protect satellite are very effective against these intentional attacks.

Hijacking/Control

Incidents

Following most recent cases for satellite hijacking:

- 2007 - The Tamil Tigers (LTTE) in Sri Lanka broadcast propaganda transmission on Intelsat satellites
- 2009 - Brazilian authorities arrested 39 university professors, electricians, truckers, and farmers who had been using homemade equipment to highjack UHF frequencies dedicated to satellites in the US Navy's Fleet Satellite Communication system for their personal use.
- 2013 - Emergency Alert System systems of TV stations in Montana and Michigan were hacked, the attackers broadcasted a warn of a Zombie invasion. Despite it is unclear if the illegal transmission were possible due an attack against satellites or Internet-connected. The lack of detail provided in reports led many security experts to believe that first hypothesis was most probable.

Hijacking/Control

Incidents

- An attacker could exploit a flaw in the command and control of commercial satellites, such as VSAT hubs, to compromise also military satellite systems.

- Most popular of alleged takeovers of Satellite Control occurred in 2007 and 2008:
  - hackers obtained the control of the NASA Terra EOS earth observation system satellite for 2 minutes in June and for another 9 minutes in October.
  - The second hack affected the Landsat-7 satellite on two occasions, one in October of '07, the other in July of '08. Unlike the Terra OS incident, this hack did not see control taken away, but access was anyway gained.

AGENDA

- Intro
- Jamming
- Eavesdropping
- Hijacking/Control
- Scanning/Attacking

- Signal encryption and hardening
- Conclusions

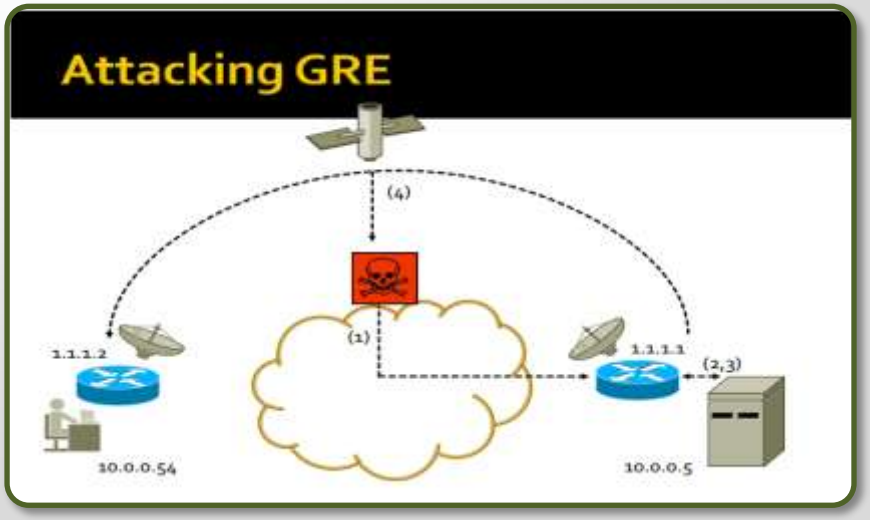
Scanning/Attacking

Distributed-denial-of-service (DDoS)

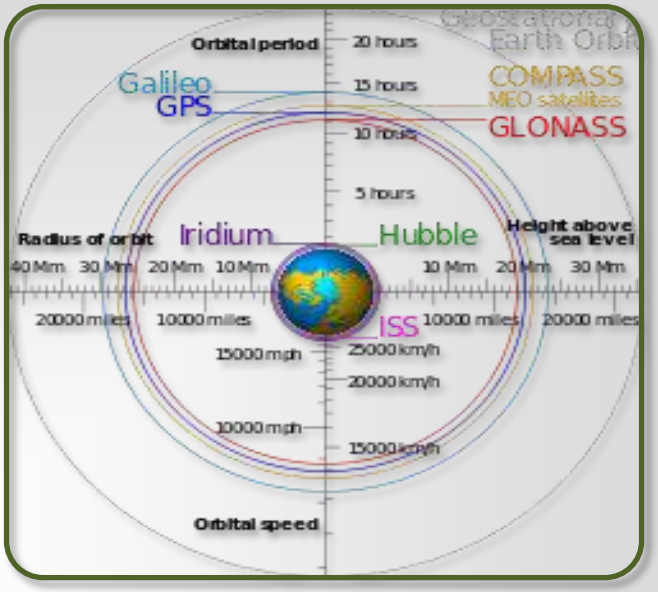
What's interesting about this is that it's very, very easy," "Anyone can do it: phishers or Chinese hackers it's like a very big Wi-Fi network that's easy to access." - Leonardo Nve, Black Hat security conference in Arlington (2010)

- Nve demonstrated how to use satellite signals to anonymize Internet connection, intercept satellite Internet users' requests for Web content and replace it and gain access to private networks. Nve exploited the satellite signal being able spoofing any user identity on the Internet via satellite.

- Resuming the researcher was able to:
  - DNS Spoofing
  - TCP hijacking
  - Attacking GRE



Scanning/Attacking



Attacking GPS systems

- GPS technology is widely used today in commercial and military sectors.
- The most insidious threat for GPS systems is "GPS spoofing" whereby an interference in GPS receiver is fooled into tracking counterfeit GPS signals.
- GPS "spoofers" are devices that create false GPS signals to fool receivers into thinking that they are at a different location or different times.

- These attacks are difficult to detect and can be conducted in numerous sectors, from transportation to financial environments.
- Principal countermeasures implemented in software on GPS receivers are Amplitude discrimination, Time-of-arrival discrimination and Cryptographic authentication.
- Adoption of signal encryption implies that receiver and transmitter use mutual authentication processes avoiding interferences of external sources.
- Signal encryption requires more powerful hardware and systems able to manage the overhead introduced by authentication procedures, due this reasons encryption is limited to the military sector

Scanning/Attacking

Attacking GPS systems

- The GPS technology is also used in other areas, from environmental control to the financial sector.
- Misalignment of a few milliseconds between the various trading systems could be exploited by criminals to have advance knowledge of the value of any trade. (2010 - Flash Crash of 2.45)
- The GPS expert Todd Humphreys demonstrated that just using a cheap apparatus he is able take total control of sophisticated navigation system aboard a vessel.
- Spoofing a GPS receiver on a UAV is possible to manipulate navigation computers providing fake information.

AGENDA

- Intro
- Jamming
- Eavesdropping
- Hijacking/Control
- Scanning/Attacking
- Signal encryption and hardening

- Conclusions

Signal encryption and hardening

How to protect satellites

- The principal countermeasures to protect satellite infrastructures is the hardening of single components such as the ground stations.
- Physical protection of terrestrial environment includes common defense devices and supplementary structures (e.g. access control systems, cameras, fences and guards).
- In a high security environment ground stations are located within military compounds having in place strict security measures.
- Encryption is crucial to protect signals from spoofing attacks and is also used to mutually authenticate communication interlocutors.
- Redundant hardware.

Logical

Physical

Terrestrial components

Orbital Components

Signal encryption

Signal encryption and hardening

How to protect satellites

- Protection against physical or electronic intrusion (e.g. Radio signal interception and jamming).
- Other techniques could be used for terrestrial equipment protection such as directional antennas that reduce interception, shielding and radio emission control measures could be used to mitigate surveillance or jamming activities with third parties.
- Satellite itself may be hardened against radiation, meteoroids and orbital debris, to minimize disruption in case of kinetic or natural disaster it is suggested the deployment of satellite networks with redundant components having multiple satellites and ground stations.
- Hardening of the satellites themselves involves the use of "designs and components that are built to be robust enough to withstand harsh space environments and deliberate attacks" (GAO 2002), the main impact of the implementation of this type of countermeasures is the increase in costs in building, deployment and maintenance.

AGENDA

- Intro
- Jamming
- Eavesdropping
- Hijacking/Control
- Scanning/Attacking
- Signal encryption and hardening
- Conclusions

Conclusions

What's happening while we are talking?

- Security of satellite systems and cyber strategies.
- Malicious cyber activities can be carried out to destroy the satellite systems.
- *"China is one of the top space powers in the world today. The prestige of space exploration and the national security benefits of space systems serve as primary motivators for Chinese decision-makers,"* ("U.S.-China Economic and Security Review Commission".
- Governments need to better define international agreements on the definition of harmful interference to prevent aggressive conduct in outer space.
- It is fundamental to define the attribution of responsibility processes within an international law framework shared on a global scale.
- On the technological side, it is necessary to develop new helpful technologies to improve the security of satellite infrastructures, focusing on the increase of threat mitigation.

Conclusions

Pierluigi Paganini

Pierluigi Paganini has a Bachelor in Computer Science Engineering IT, specialized in Computer Security and Hacking techniques. He is security expert with over 20 years of experience in the field, including a Certified Ethical Hacker certification from the EC Council in London. Within various experiences he has worked as security manager for STMicroelectronics and H3G Italy.
Pierluigi is Chief Security Information Officer at Bit4Id, researcher, security evangelist, security analyst and freelance writer. This passion for writing and a strong belief that security is founded on sharing and awareness has led Pierluigi to found the security blog "Security Affairs." He is author of the books "The Deep Dark Web" and "Digital Virtual Currency and Bitcoin", he is also Editor-in-Chief at CyberDefense magazine (http://www.cyberdefensemagazine.com)

Ing. Pierluigi Paganini

Chief Information Security Officer Bit4id

ppa@bit4id.com

www.bit4id.com

Founder Security Affairs

http://securityaffairs.co/wordpress

pierluigi.paganini@securityaffairs.co

Ing. Pierluigi Paganini

Chief Information Security Officer Bit4id

ppa@bit4id.com

www.bit4id.com

Founder Security Affairs

http://securityaffairs.co/wordpress

pierluigi.paganini@securityaffairs.co