The cyber attack surface of the aerospace industry

Andy Davis, Transport Assurance Practice Director

Global experts in cyber security & risk mitigation

1500+

Employees worldwide

15,000

Helping 15,000 organisations worldwide to manage risk & limit threat of cybercrime

35+

Offices across Europe, North America, Asia-Pacific & Middle East

1999

NCC Group was formed in June 1999

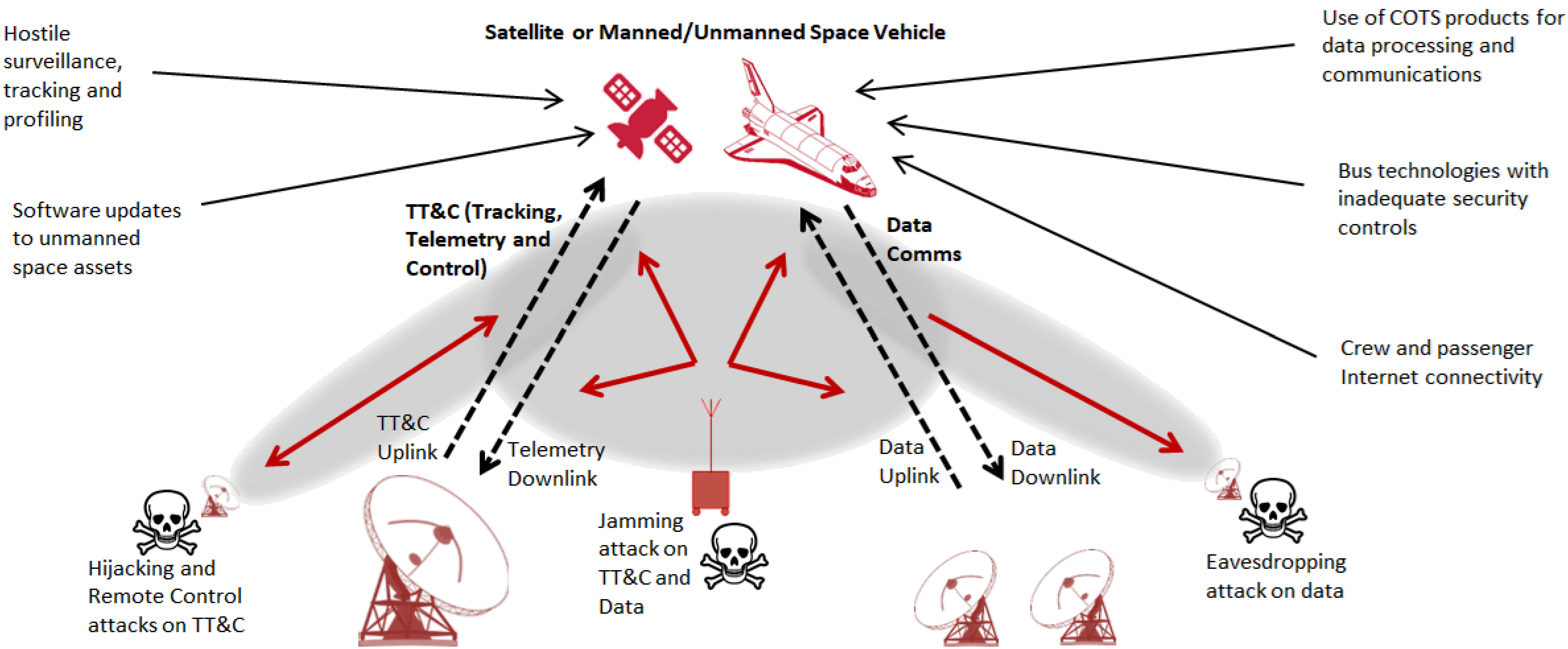
£233.2m

Group Revenue for year end May 2018

Agenda

- Space attack surface overview
- Attacks against terrestrial assets
- RF attacks
- Using COTS products
- Supply Chain attacks
- Reducing the risks
- Q&A

Space Attack Surface Overview


Satellite or Manned/Unmanned Space Vehicle
Hostile surveillance, tracking and profiling
Software updates to unmanned space assets
Use of COTS products for data processing and communications
Bus technologies with inadequate security controls
Crew and passenger Internet connectivity
TT&C (Tracking, Telemetry and Control)
Data Comms
TT&C Uplink
Telemetry Downlink
Data Uplink
Data Downlink
Hijacking and Remote Control attacks on TT&C
Jamming attack on TT&C and Data
Eavesdropping attack on data

nccgroup

Attacks – Terrestrial Assets

Ground Stations

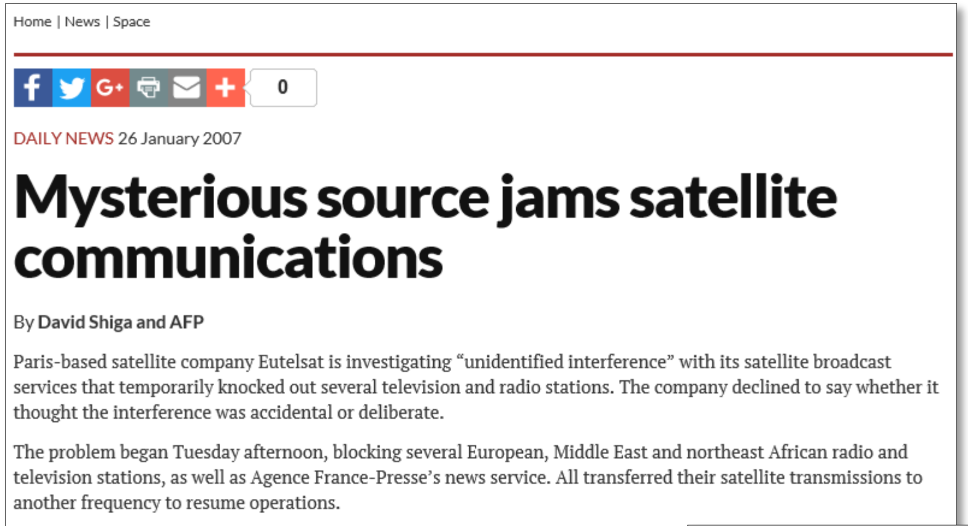
- Phishing attacks against employees
  - Access to workstations controlling satellites
- Physical and network attacks:
  - March 2011: The theft of an unencrypted NASA notebook computer resulted in the loss of the algorithms used to command and control the International Space Station
- By far the easiest way to attack space-based assets

Attacks – DoS, Eavesdrop, Hijack, Spoof & Remote Control

Denial of Service (jamming)

- Preventing or degrading satellite services
- Requirements:
  - Directed antenna
  - Target frequency knowledge
  - Appropriate transmit power level
- Potential targets:
  - Satellite receiving an uplink
  - Ground station
  - User terminal receiving a downlink
- Jamming the uplink requires more skill and power but the disruption can be significantly greater
- “Smart” jamming could involve attacks against software-based radio technologies

Real-world jamming attacks



Home | News | Space

0

DAILY NEWS 26 January 2007

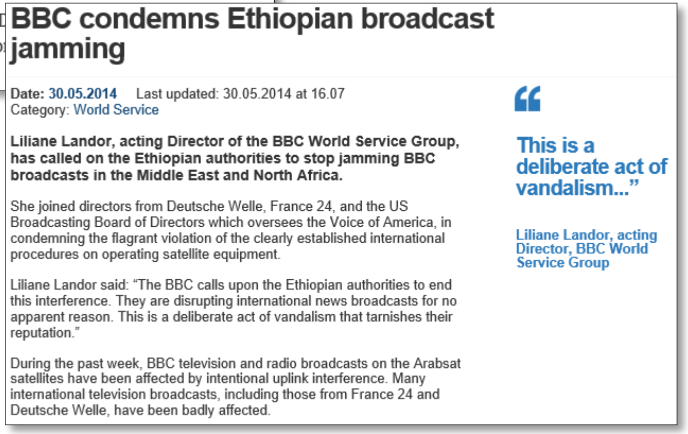
Mysterious source jams satellite communications

By David Shiga and AFP

Paris-based satellite company Eutelsat is investigating “unidentified interference” with its satellite broadcast services that temporarily knocked out several television and radio stations. The company declined to say whether it thought the interference was accidental or deliberate.

The problem began Tuesday afternoon, blocking several European, Middle East and northeast African radio and television stations, as well as Agence France-Presse’s news service. All transferred their satellite transmissions to another frequency to resume operations.

Theresa Hitchens of the Center for Defense Information think-tank in Washington I cases of deliberate satellite jamming in the past, but it is hard to see what motivatio instance.



BBC condemns Ethiopian broadcast jamming

Date: 30.05.2014 Last updated: 30.05.2014 at 16.07
Category: World Service

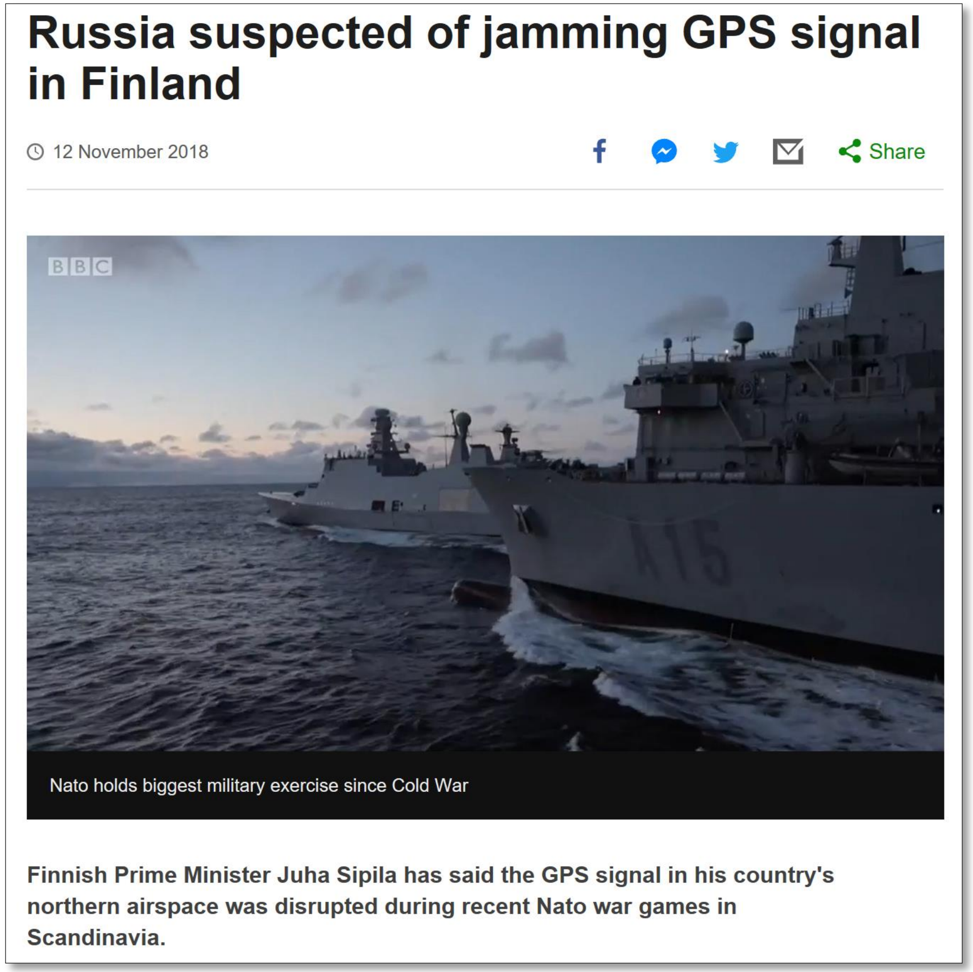
Liliane Landor, acting Director of the BBC World Service Group, has called on the Ethiopian authorities to stop jamming BBC broadcasts in the Middle East and North Africa.

She joined directors from Deutsche Welle, France 24, and the US Broadcasting Board of Directors which oversees the Voice of America, in condemning the flagrant violation of the clearly established international procedures on operating satellite equipment.

Liliane Landor said: “The BBC calls upon the Ethiopian authorities to end this interference. They are disrupting international news broadcasts for no apparent reason. This is a deliberate act of vandalism that tarnishes their reputation.”

During the past week, BBC television and radio broadcasts on the Arabsat satellites have been affected by intentional uplink interference. Many international television broadcasts, including those from France 24 and Deutsche Welle, have been badly affected.

> “This is a deliberate act of vandalism...”
>
> Liliane Landor, acting Director, BBC World Service Group



Russia suspected of jamming GPS signal in Finland

12 November 2018

Share

Nato holds biggest military exercise since Cold War

Finnish Prime Minister Juha Sipila has said the GPS signal in his country's northern airspace was disrupted during recent Nato war games in Scandinavia.

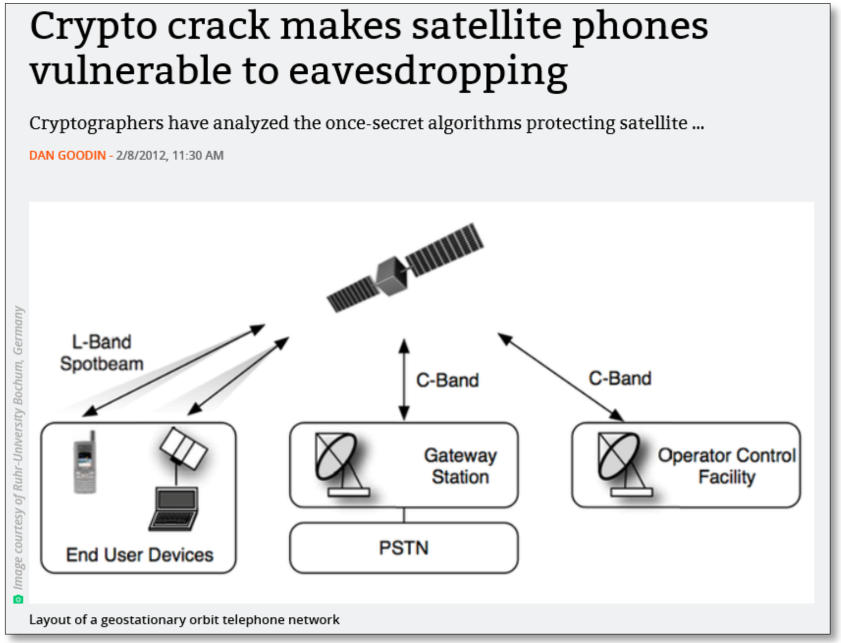
Eavesdrop (interception)

- Intercepting data communicated via satellite

- Attacks only require low cost COTS products:
  - Unauthorised satellite television viewing
  - Intercept satellite telephone conversations
  - Intercept Internet traffic
  - Unauthorised satellite imagery viewing

- Data is often not even encrypted
  - Encrypting satellite signals can cause performance degradation

Real-world Eavesdrop attacks



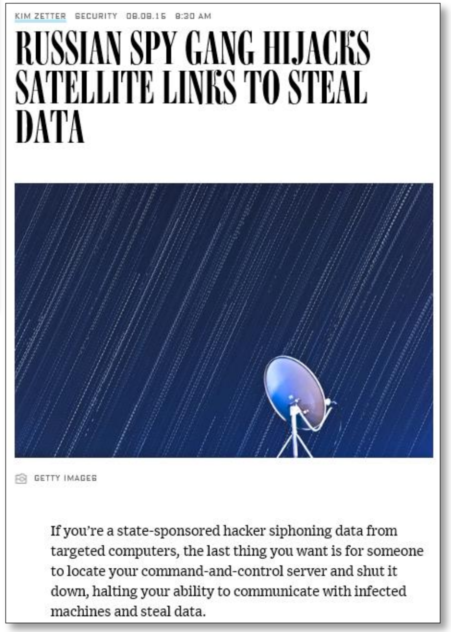
Crypto crack makes satellite phones vulnerable to eavesdropping

Cryptographers have analyzed the once-secret algorithms protecting satellite ...

DAN GOODIN - 2/8/2012, 11:30 AM

Image courtesy of Ruhr-University Bochum, Germany

Layout of a geostationary orbit telephone network

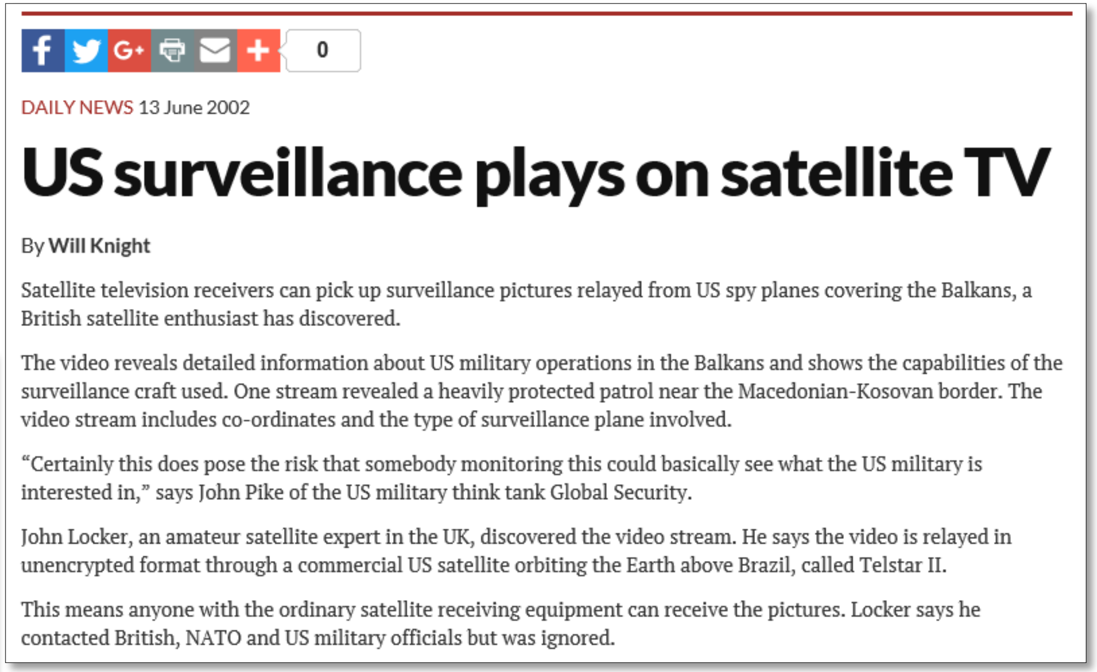


KIM ZETTER SECURITY 08.08.16 8:30 AM

RUSSIAN SPY GANG HIJACKS SATELLITE LINKS TO STEAL DATA

GETTY IMAGES

If you're a state-sponsored hacker siphoning data from targeted computers, the last thing you want is for someone to locate your command-and-control server and shut it down, halting your ability to communicate with infected machines and steal data.



0

DAILY NEWS 13 June 2002

US surveillance plays on satellite TV

By **Will Knight**

Satellite television receivers can pick up surveillance pictures relayed from US spy planes covering the Balkans, a British satellite enthusiast has discovered.

The video reveals detailed information about US military operations in the Balkans and shows the capabilities of the surveillance craft used. One stream revealed a heavily protected patrol near the Macedonian-Kosovan border. The video stream includes co-ordinates and the type of surveillance plane involved.

“Certainly this does pose the risk that somebody monitoring this could basically see what the US military is interested in,” says John Pike of the US military think tank Global Security.

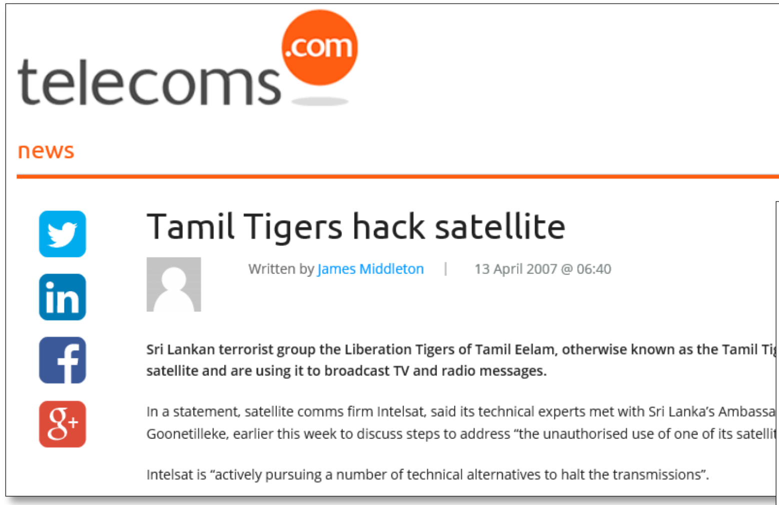
John Locker, an amateur satellite expert in the UK, discovered the video stream. He says the video is relayed in unencrypted format through a commercial US satellite orbiting the Earth above Brazil, called Telstar II.

This means anyone with the ordinary satellite receiving equipment can receive the pictures. Locker says he contacted British, NATO and US military officials but was ignored.

Hijack (re-purpose)

- Unauthorised use of a satellite to transmit the attacker’s signal, potentially manipulating legitimate traffic.
- COTS products used for eavesdropping attacks can also potentially be used for hijacking.
- Similar types of attack in the enterprise world:
  - Wi-Fi theft
  - Web page defacement
  - DNS cache poisoning

Real-world Hijack attacks



telecoms.com

news

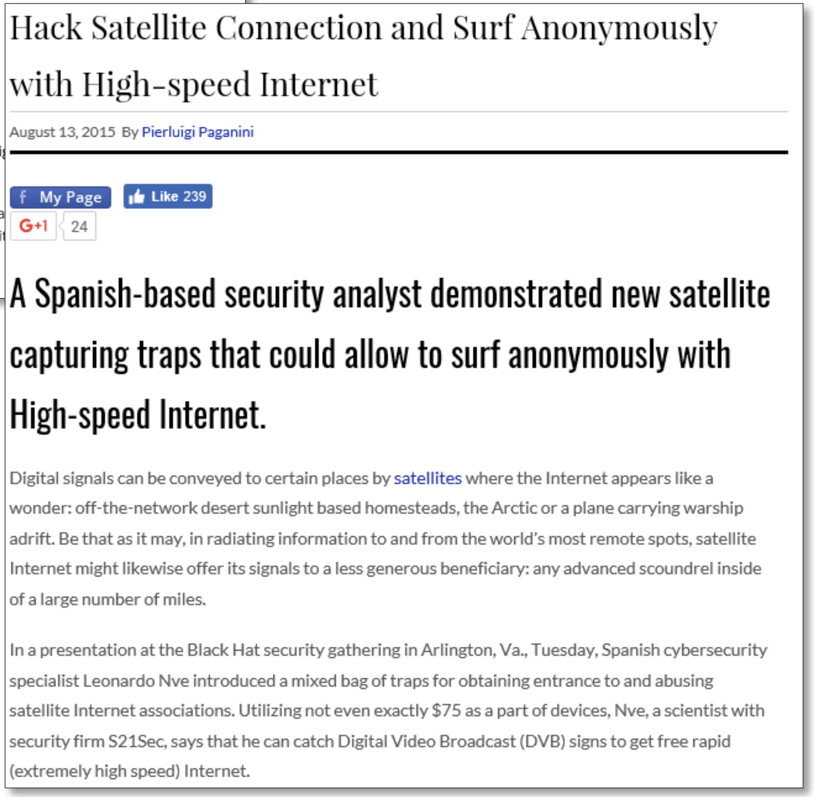
Tamil Tigers hack satellite

Written by James Middleton | 13 April 2007 @ 06:40

Sri Lankan terrorist group the Liberation Tigers of Tamil Eelam, otherwise known as the Tamil Ti satellite and are using it to broadcast TV and radio messages.

In a statement, satellite comms firm Intelsat, said its technical experts met with Sri Lanka's Ambassa Goonetilleke, earlier this week to discuss steps to address "the unauthorised use of one of its satelli

Intelsat is "actively pursuing a number of technical alternatives to halt the transmissions".



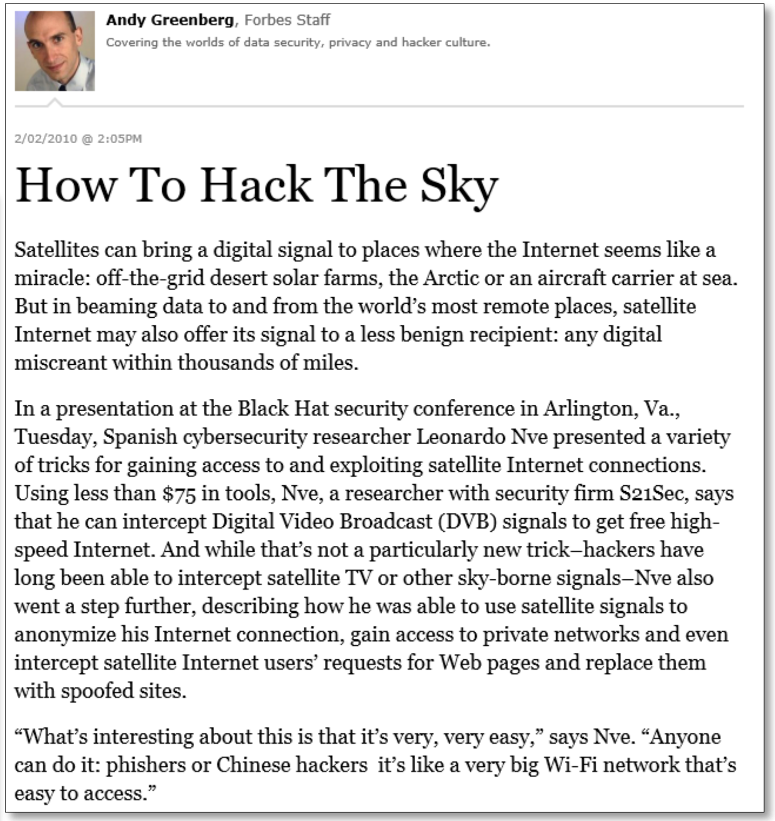
Hack Satellite Connection and Surf Anonymously with High-speed Internet

August 13, 2015 By Pierluigi Paganini

A Spanish-based security analyst demonstrated new satellite capturing traps that could allow to surf anonymously with High-speed Internet.

Digital signals can be conveyed to certain places by satellites where the Internet appears like a wonder: off-the-network desert sunlight based homesteads, the Arctic or a plane carrying warship adrift. Be that as it may, in radiating information to and from the world's most remote spots, satellite Internet might likewise offer its signals to a less generous beneficiary: any advanced scoundrel inside of a large number of miles.

In a presentation at the Black Hat security gathering in Arlington, Va., Tuesday, Spanish cybersecurity specialist Leonardo Nve introduced a mixed bag of traps for obtaining entrance to and abusing satellite Internet associations. Utilizing not even exactly $75 as a part of devices, Nve, a scientist with security firm S21Sec, says that he can catch Digital Video Broadcast (DVB) signs to get free rapid (extremely high speed) Internet.



Andy Greenberg, Forbes Staff
Covering the worlds of data security, privacy and hacker culture.

2/02/2010 @ 2:05PM

How To Hack The Sky

Satellites can bring a digital signal to places where the Internet seems like a miracle: off-the-grid desert solar farms, the Arctic or an aircraft carrier at sea. But in beaming data to and from the world's most remote places, satellite Internet may also offer its signal to a less benign recipient: any digital miscreant within thousands of miles.

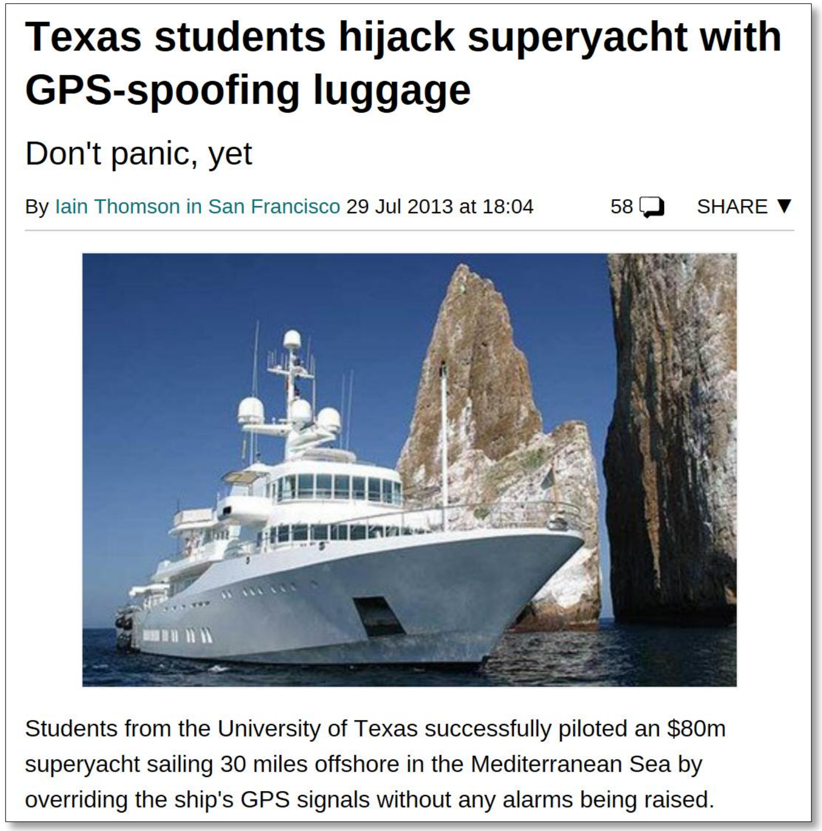
In a presentation at the Black Hat security conference in Arlington, Va., Tuesday, Spanish cybersecurity researcher Leonardo Nve presented a variety of tricks for gaining access to and exploiting satellite Internet connections. Using less than $75 in tools, Nve, a researcher with security firm S21Sec, says that he can intercept Digital Video Broadcast (DVB) signals to get free high-speed Internet. And while that's not a particularly new trick–hackers have long been able to intercept satellite TV or other sky-borne signals–Nve also went a step further, describing how he was able to use satellite signals to anonymize his Internet connection, gain access to private networks and even intercept satellite Internet users' requests for Web pages and replace them with spoofed sites.

"What's interesting about this is that it's very, very easy," says Nve. "Anyone can do it: phishers or Chinese hackers it's like a very big Wi-Fi network that's easy to access."

Spoofing – e.g. GPS

- Virtual Teleportation
  - Spoof location – subtly or to extremes
- Virtual Time Machine
  - Spoof date and time
  - Y2038 bug: 03:14:07 UTC on Tuesday, 19 January 2038
- Intelligent Jamming
  - Malformed ephemeris/almanac data
  - DoS attacks

Real-world Spoofing attacks

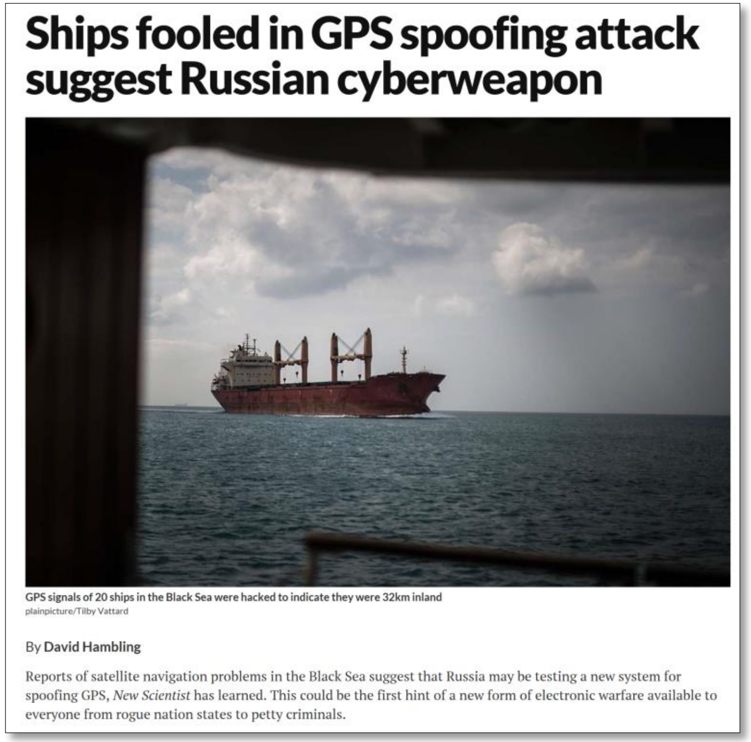


Texas students hijack superyacht with GPS-spoofing luggage

Don't panic, yet

By Iain Thomson in San Francisco 29 Jul 2013 at 18:04 58 SHARE ▼

Students from the University of Texas successfully piloted an $80m superyacht sailing 30 miles offshore in the Mediterranean Sea by overriding the ship's GPS signals without any alarms being raised.



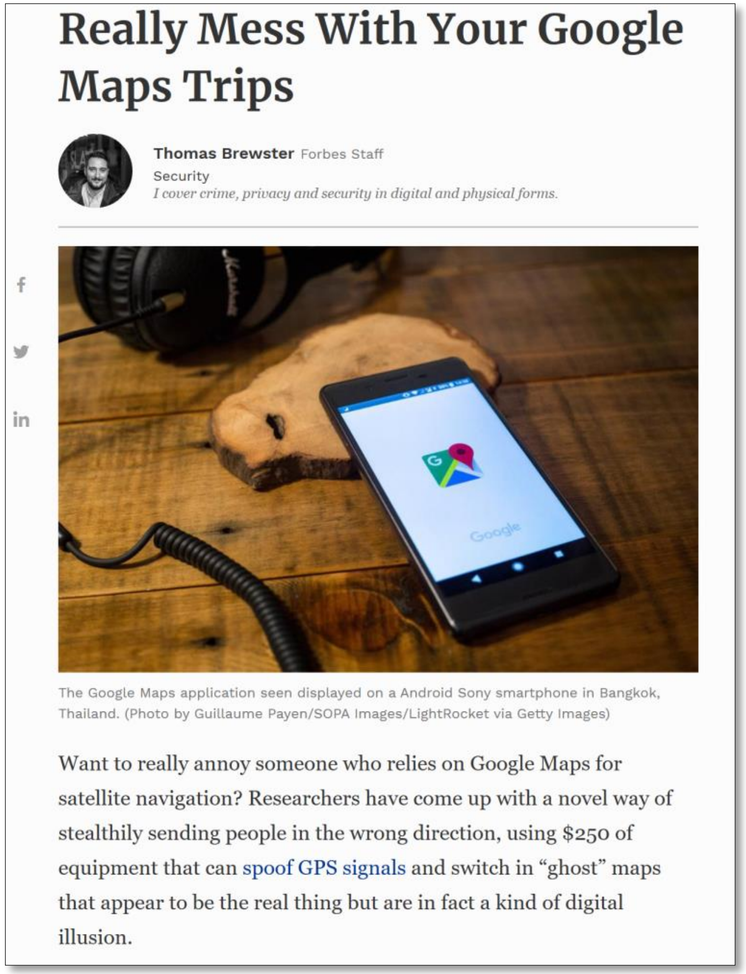
Ships fooled in GPS spoofing attack suggest Russian cyberweapon

GPS signals of 20 ships in the Black Sea were hacked to indicate they were 32km inland

plainpicture/Tilby Vattard

By **David Hambling**

Reports of satellite navigation problems in the Black Sea suggest that Russia may be testing a new system for spoofing GPS, *New Scientist* has learned. This could be the first hint of a new form of electronic warfare available to everyone from rogue nation states to petty criminals.



Really Mess With Your Google Maps Trips

Thomas Brewster Forbes Staff
Security
I cover crime, privacy and security in digital and physical forms.

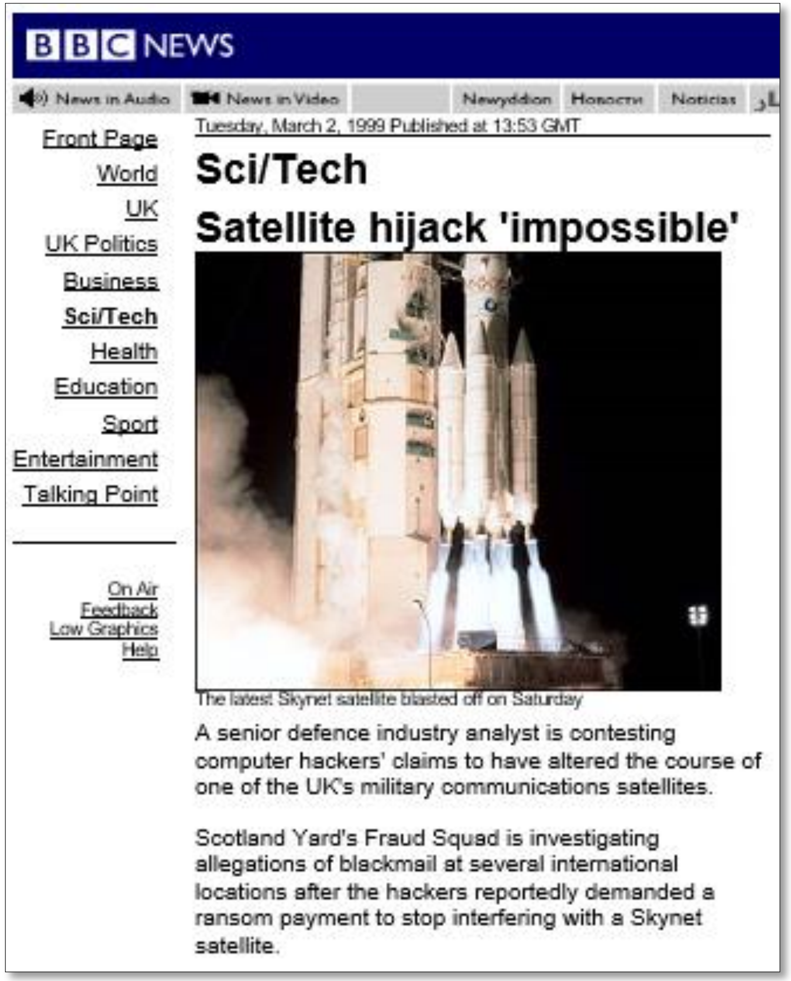
The Google Maps application seen displayed on a Android Sony smartphone in Bangkok, Thailand. (Photo by Guillaume Payen/SOPA Images/LightRocket via Getty Images)

Want to really annoy someone who relies on Google Maps for satellite navigation? Researchers have come up with a novel way of stealthily sending people in the wrong direction, using $250 of equipment that can spoof GPS signals and switch in "ghost" maps that appear to be the real thing but are in fact a kind of digital illusion.

Control (manipulate)

- Take control of the satellite to manipulate its systems, orientation or orbit
- To control a satellite the attacker must breach the TT&C (Tracking, Telemetry and Control) links
- Requires significant knowledge / skill level to achieve

Real-world Control attacks



Tuesday, March 2, 1999 Published at 13:53 GMT

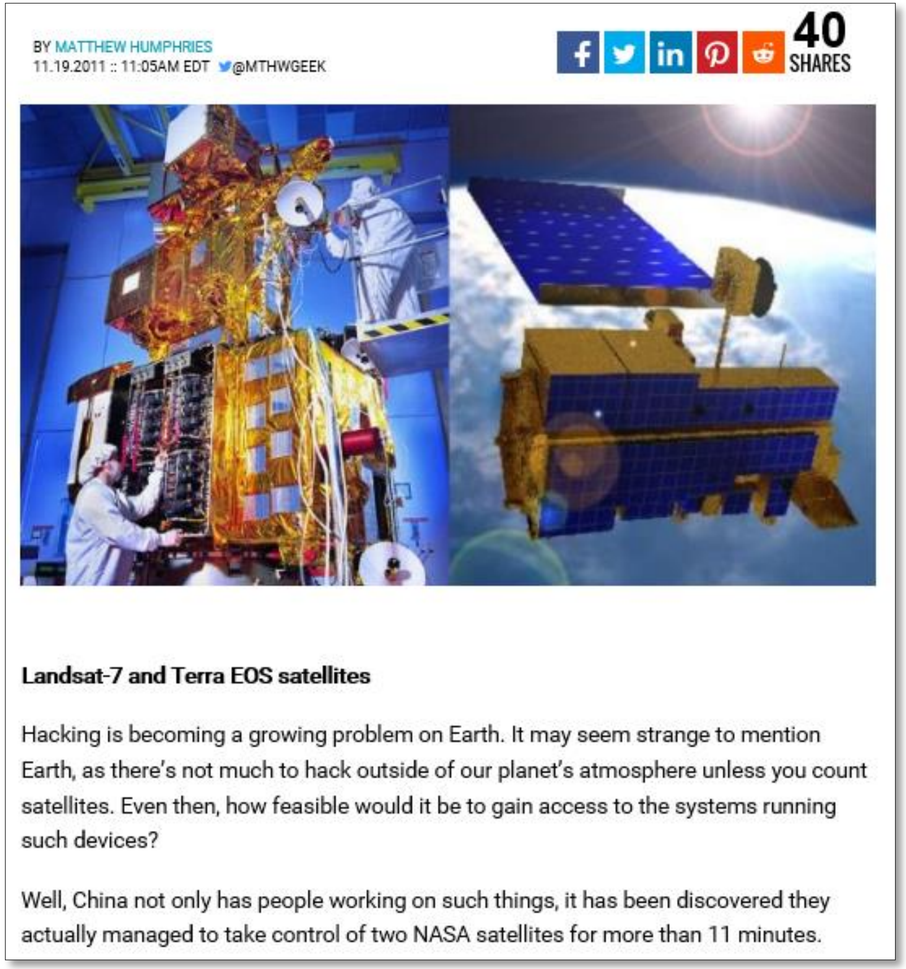
Sci/Tech

Satellite hijack 'impossible'

The latest Skynet satellite blasted off on Saturday

A senior defence industry analyst is contesting computer hackers' claims to have altered the course of one of the UK's military communications satellites.

Scotland Yard's Fraud Squad is investigating allegations of blackmail at several international locations after the hackers reportedly demanded a ransom payment to stop interfering with a Skynet satellite.



BY MATTHEW HUMPHRIES
11.19.2011 :: 11:05AM EDT @MTHWGEEK

Landsat-7 and Terra EOS satellites

Hacking is becoming a growing problem on Earth. It may seem strange to mention Earth, as there's not much to hack outside of our planet's atmosphere unless you count satellites. Even then, how feasible would it be to gain access to the systems running such devices?

Well, China not only has people working on such things, it has been discovered they actually managed to take control of two NASA satellites for more than 11 minutes.

The use of Commercial Off-The-Shelf (COTS) products

Why COTS products?

- **Primarily cost** - *"I worked on a couple of what NASA considered small satellites costing 10–200 million dollars. They're not necessarily physically small, but they're small in cost because normal satellites cost half a billion or billions of dollars."* - Will Marshall, CEO Planet Labs

- COTS devices are attractive due to their **relatively low power consumption** and high processing performance

- Plenty of available **knowledge and expertise** around the use of COTS products for systems development

- **Trade-off: Cost vs Reliability** – depends on mission – fault tolerance through use of redundant components

Brief history of COTS in space

- **1970s:** A group of highly-skilled aerospace researchers working at the University of Surrey, decided to experiment by creating a satellite using COTS components
- **1980s:** The University of Surrey launched UoSat-1 in 1981 with the help of NASA and the mission was a great success, outliving its planned three year life by more than five years.
- **1990s:** California Polytechnic State University (Cal Poly) and Stanford University developed the CubeSat specifications
- **2000s:** 386-based on-board computers running QNX used on the University of Surrey’s UoSat-12
- **2010s:** *“We’re seeing a lot of electronics – imaging technologies, radio technologies, navigation and GPS receivers, and other things we take for granted in our cellphones – moving into space designs.”* - Aaron Q. Rogers, Johns Hopkins University Applied Physics Lab

Automotive cyber security comparisons

- Automotive COTS components now being used in satellites
- Operating Systems such as QNX and Linux used for both applications
- CAN Bus technology used in satellites
- Attacker skillset well established in many technology areas already implemented in automotive

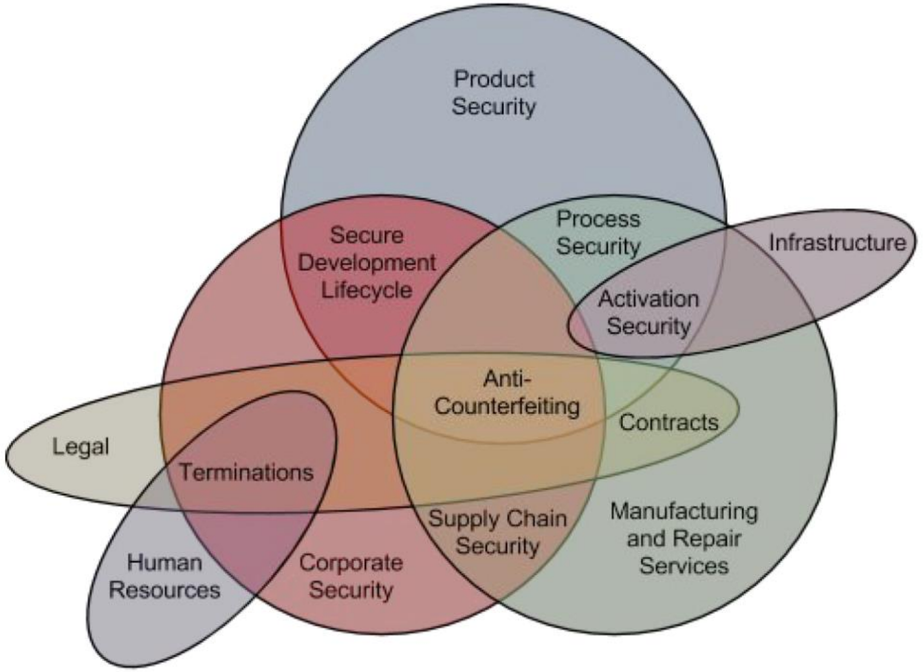
COTS Operating Systems in space

- In the 2018 CVE “Top 50”, Ubuntu Linux is number 3 (with only Android and Debian Linux higher)
- With the rise of IoT attackers are looking for more interesting targets – embedded systems
- Embedded systems mind-set: Security through obscurity
- Increased risk of malware on-board satellites – incident response significantly more tricky!

Supply Chain

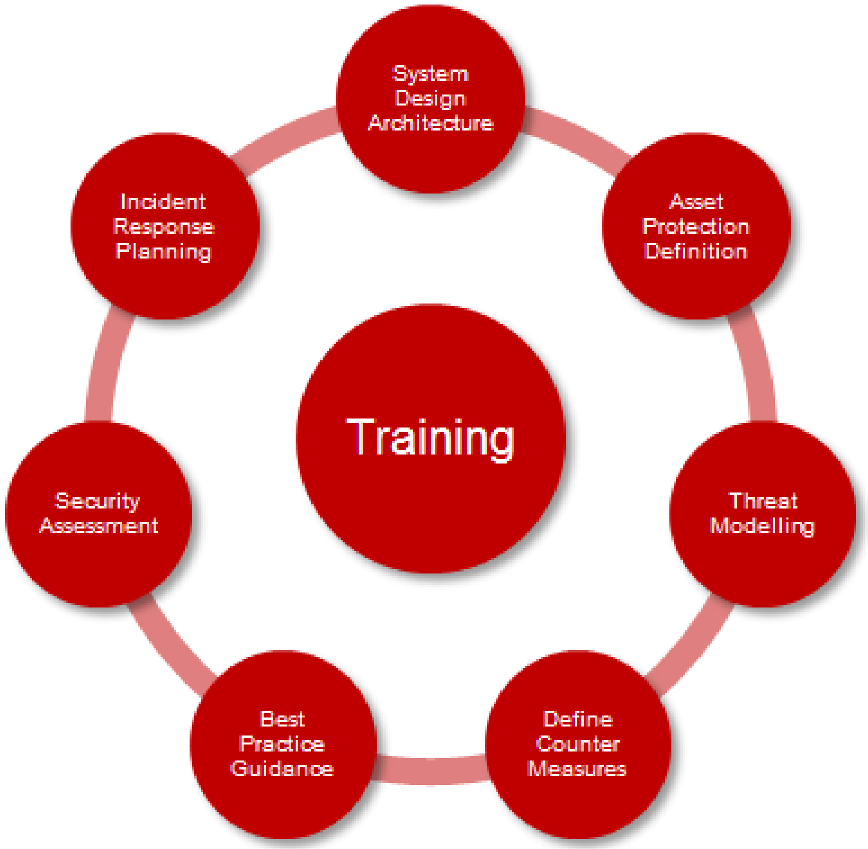
Supply chain attacks

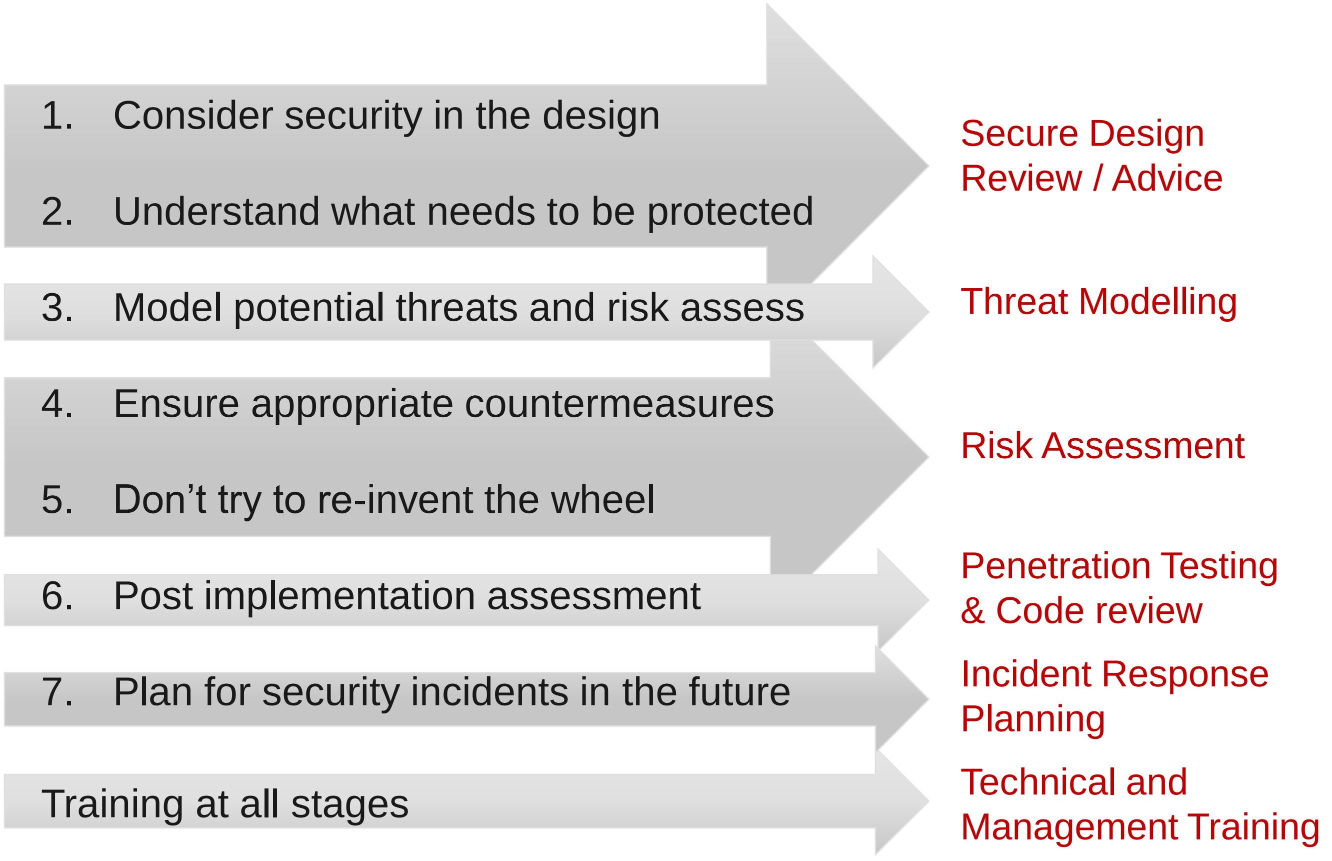
- Attacker Tools and Techniques
  - Chip-Off
  - Leaked Software/Tools/Schematics/Data
  - Third Party Tools
  - Open Source Research
  - Jailbreaking Community
  - Stolen Network Access
  - Vulnerabilities and Exploits
  - Common Components



Risk Reduction

SDL: Secure Development Lifecycle





1. Consider security in the design
2. Understand what needs to be protected

Secure Design Review / Advice

3. Model potential threats and risk assess

Threat Modelling

4. Ensure appropriate countermeasures
5. Don’t try to re-invent the wheel

Risk Assessment

6. Post implementation assessment

Penetration Testing & Code review

7. Plan for security incidents in the future

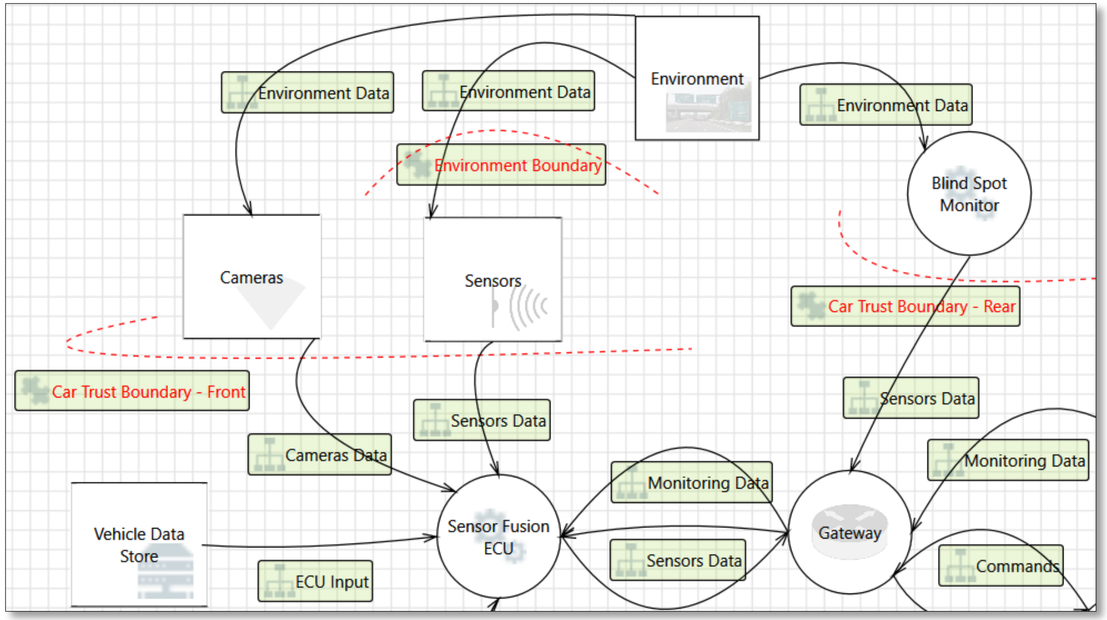
Incident Response Planning

Training at all stages

Technical and Management Training

Threat Modelling

- Identify threats to a design
- Examine interfaces and trust boundaries
- Understand associated risks
- Prioritise risks
- Inform security test plans



NCC Group Automotive Threat Modelling Template

Reducing the risks - summary

- An awareness of the risks needs to be raised with the right stakeholders
- Satellite cyber security standards need to be developed with input from experts
- Satellite manufacturers and their whole supply chain need to develop-in security from day one (Secure Development Lifecycle) – bolt-on solutions are never as effective and often very costly
- Satellite technology must be independently security assessed to ensure that vulnerabilities haven’t been introduced during development or integration

Questions?

+44 (0)161 209 5200

TransportSecurity@nccgroup.trust

www.nccgroup.trust/transport

A global practice offering the full range of Cyber Security and Assurance services to the Transport industry

North America

- Atlanta
- Austin
- Boston
- Chicago
- New York
- San Francisco
- Seattle
- Sunnyvale

Canada

- Waterloo

Middle East

- Dubai

Europe

- Manchester - Head Office
- Amsterdam
- Basingstoke
- Cambridge
- Cheltenham
- Copenhagen
- Edinburgh
- Glasgow
- Leatherhead
- Leeds
- London
- Luxembourg
- Madrid
- Malmö
- Milton Keynes
- Munich
- Vilnius
- Wetherby
- Zurich

Australia

- Sydney

Asia

- Singapore