UNIVERSITY OF OXFORD

SSL
Systems Security Lab

Firefly: Spoofing Earth Observation Satellites through Radio Overshadowing

Edd Salkield [1] Joshua Smailes [1] Sebastian Köhler [1]
Simon Birnbach [1] Richard Baker [1] Martin Strohmeier [2]
Ivan Martinovic [1]

[1] Systems Security Lab, University of Oxford

[2] Cyber-Defence Campus, armasuisse Science + Technology

Trinity Term 2022

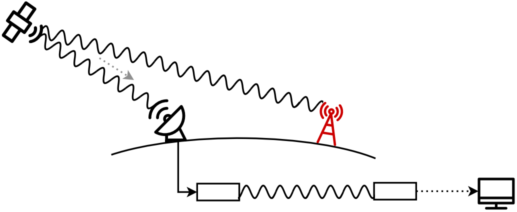
Challenges of unauthenticated satellites

- Many current satellites do not encrypt the downlink, due to:
  - Engineering constraints
  - Desire for public reception
  - Increased power budget and costs
  - Legacy systems, and backwards compatibility with them
- Other satellites are decryptable, due to:
  - Insecure cryptosystems [1]
  - Leaked keys [2]

[1] COMS-1 uses single DES `https://vksdr.com/lrit-key-dec/`
[2] GK-2A keys embedded in published source code `https://vksdr.com/xrit-rx/`

Implications

Data secrecy



Using only an off-the-shelf SDR and open source software, attackers can:

- Read confidential maritime data and internet traffic, Pavur et. al [**?**, **?**]
- Eavesdrop on Iridium traffic and cals [**?**]

Certain satellites designed to be unencrypted, e.g.

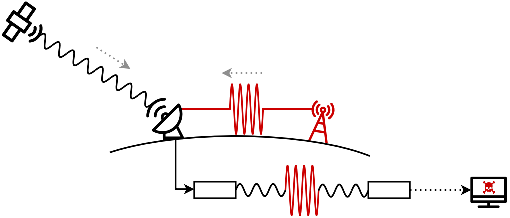
- EOS fleet: Terra, Aqua, Aura, etc.
- Amateur radio satellites e.g. SO-50, QO-100
- Freeview TV

UNIVERSITY OF OXFORD

SSL
Systems Security Lab

Implications

Data authenticity and integrity



Spoofing attacks have been shown against:

- GNSS to manipulate calculated location [**?**, **?**]
- Uplink to hijack the satellite or intrude on TV broadcasts [**?**, **?**]

However, no work considers the consequences of spoofing Earth Observation satellites.

Research question: What can the attacker achieve by exploiting the unauthenticated channel?

Implications

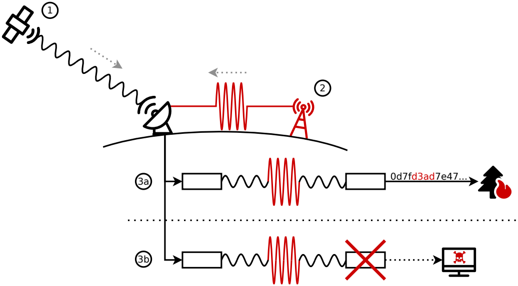
Unencrypted Earth Observation Satellites

Many Earth Observation satellites are unencrypted, including:

- **Fire detection and management** e.g. Terra, Aqua
- Geospatial intelligence e.g. Landsat-7..9
- Weather monitoring e.g. GOES-14..17, NOAA=15,18..21, FengYun series
- Infrared sensing e.g. Metop-A,B
- Climate monitoring e.g. Suomi-NPP

Threat model

Adversary's goal



Attacker transmits counterfeit signals in the vicinity of the receiver, to:

- Affect the satellite-derived datasets
- Exploit or disrupt downlink processing stages

Attacker capabilities

Estimated cost

Hardware component	**Cost**
limeSDR	598 USD
X-Band transmitter	22, 800 EUR
Compatible antenna	6, 400 EUR
Total	~30, 000 EUR

Within the budget of a motivated hobbyist.

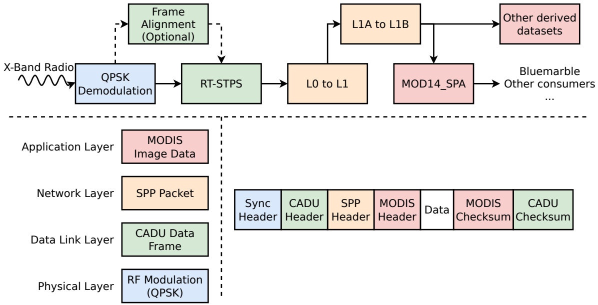
Case Study: Forest fire detection in FIRMS

NASA's global fire detection service

The 2019 Australia bushfires as seen from Aqua's MODIS instrument, annotated with the *Fires and Thermal Anomalies* dataset on NASA's worldview.

Case Study: Forest fire detection in FIRMS

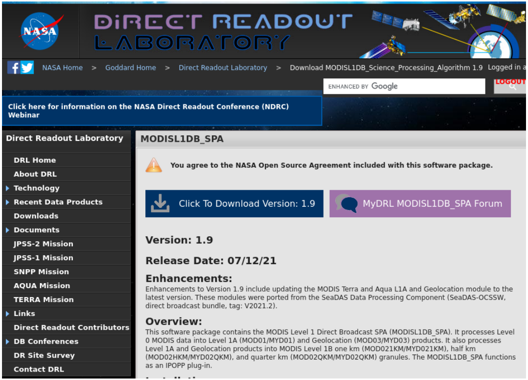
Experiment setup



We set up docker pipeline for the relevant parts of IPOPP

Exploiting processing stages

Obtaining the processing software



With a research account, anyone can download the entire set of decoding software from NASA's *Direct Readout Laboratory*

`https://directreadout.sci.gsfc.nasa.gov/`

Affecting the derived dataset

Key challenges

- Obtaining legitimate data
  - Beforehand – download from NASA distributed data archive
  - Live – set up custom receiver setup
- Processing it to add/remove artefacts
  - Reverse engineer the image format, and write an image manipulation program

Affecting the derived dataset

Data capture

Index of /archive/Science Domain/Level-0/MODIS Level-0/MODIS Aqua C6.1 - Level 0 Raw Instrument Packets (5 minutes)/2015/299/

Download Selected | See wget Download Command | Download Help | View as JSON | View as CSV

Multi-file downloads: Click individual table rows (or hold down Shift key for multiple) to select files followed by clicking "Download Selected" to confirm multi-file download

Select All		Last Modified	Size
.. Parent directory			
MYD00F.A2015299.0000.20152990300.000.PDS.bz2		2017-12-22 06:29	149.0
MYD00F.A2015299.0000.20152990300.001.PDS.bz2		2017-12-22 06:29	68.0 MB

https://ladsweb.modaps.eosdis.nasa.gov/archive/

Affecting the derived dataset

Data processing: image format reversing

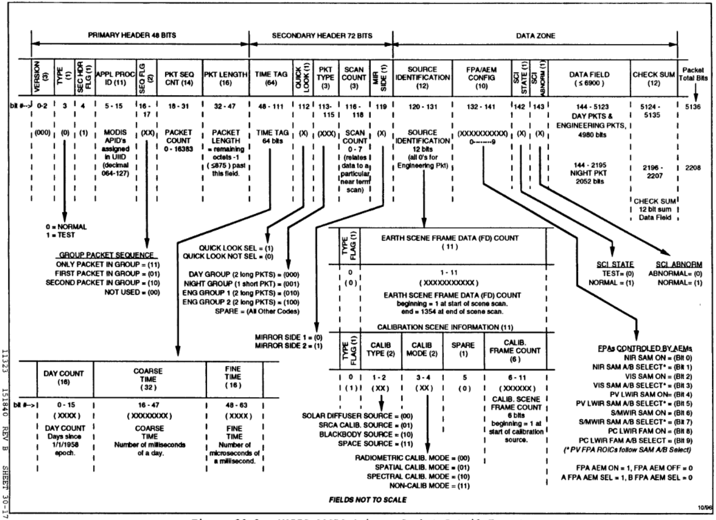


Figure 30-8. MODIS CCSDS Science Packet Detail Format

UNIVERSITY OF OXFORD

SSL
Systems Security Lab

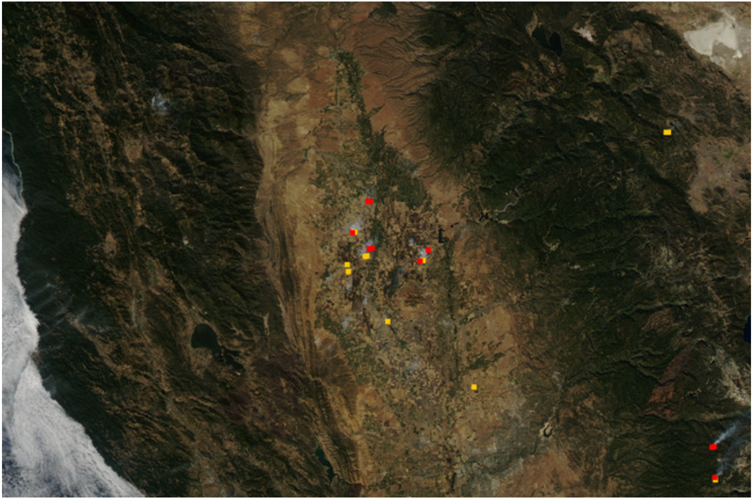
Affecting the derived dataset

Data processing: building protocol manipulation tools

TODO: find way of presenting the tools

Attack consequences

Affecting the derived dataset



Original image.

Attack consequences

Affecting the derived dataset

Masking existing fires.

Attack consequences

Affecting the derived dataset

Fine-grained control over fire injection.

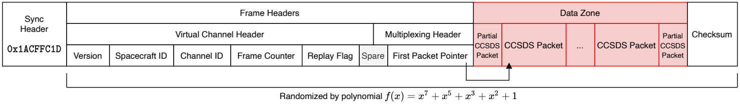
Exploiting processing stages

Key challenges

- Obtain downlink decoder software and perform security audit
  - Look for possible exploits around manual memory management and execution boundaries
- Construct payload packet to trigger vulnerability chain
  - Violate assumptions about the protocol headers

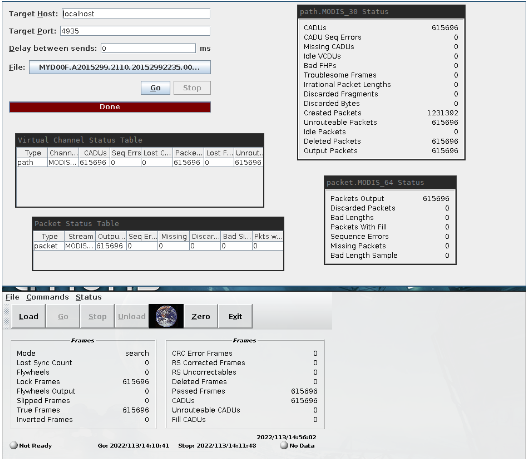
Exploiting processing stages

Construct payload packet



Attack consequences

Exploiting the processing stages

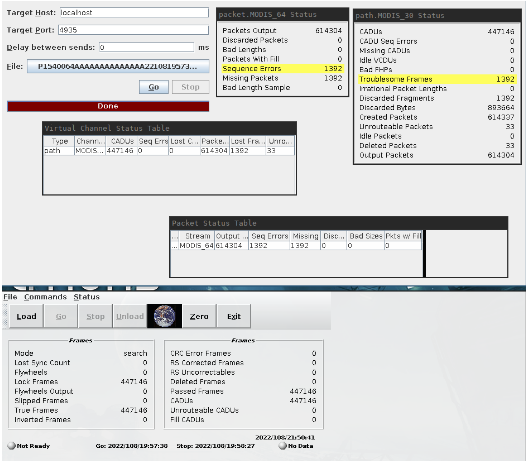


UNIVERSITY OF
OXFORD

SSL
Systems Security Lab

Attack consequences

Exploiting the processing stages



Countermeasures

Multi-receiver data comparison

TODO: citations Look for artefacts of tampering in the packets, and compare packets from multiple groundstations

- Certain systems already have multiple receiver stations
- Protects against decoder exploitation
- Doesn't require any hardware modifications to the receiver

Countermeasures

Timing analysis

- Triangulating the source effective in other systems such as aircraft
- Calculated position can be compared against orbital parameters
- Requires accurate clock synchronisation and multiple receivers

Countermeasures

Physical-layer fingerprinting

- Analyse properties of the legitimate/overshadowed signal
- Only effective on the downlink
- Traditional approaches like analysing signal-to-noise may prove effective
- New ML approaches starting to be created (PAST-AI)

UNIVERSITY OF OXFORD

SSL
Systems Security Lab

Conclusion

Our paper...

- presents a demonstration of byte-level spoofing against NASA's forest fire detection system.
- provides the source code required to manipulate the packet data and structure.
- confirms that only a moderate budget is required to perform these attacks.
- identifies current countermeasures which significantly increase attack difficulty.