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

NDSS SpaceSec 2023

Challenges of unauthenticated satellites

- Many current satellites do not encrypt the downlink, due to:
  - Increased power budget, mission complexity, and cost
  - Legacy systems backwards compatibility
  - Open access data
- 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 leaked in source code `https://vksdr.com/xrit-rx/`

Challenges of unauthenticated satellites

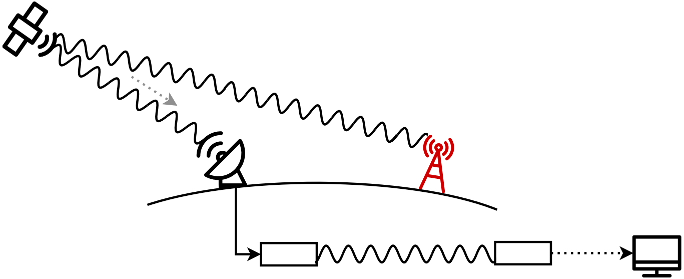
Insecure Earth Observation Satellites

Satellites with insecure downlinks include:

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

Implications

Data secrecy



Using an SDR and open source software, attackers can:

- Read confidential maritime data[1] and internet traffic[2]
- Eavesdrop on Iridium traffic and calls [3]

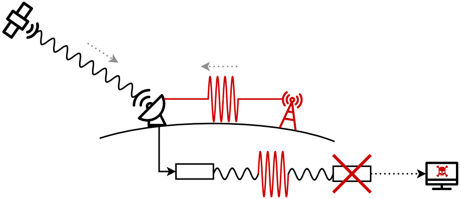
[1] Pavur et al. (2020) "*A Tale of Sea and Sky on the Security of Maritime VSAT Communications*"

[2] Pavur et al. (2019) "*Secrets in the Sky: On Privacy and Infrastructure Security in DVB-S Satellite Broadband*"

[3] muccc "*Iridium Toolkit*" `https://github.com/muccc/iridium-toolkit`

Implications

Data authenticity and integrity



Spoofing attacks have been shown against:

- GNSS to manipulate calculated location[1]
- Uplinks for satellite hijacking[2] or broadcast intrusion[3]

No work considers spoofing Earth Observation satellites

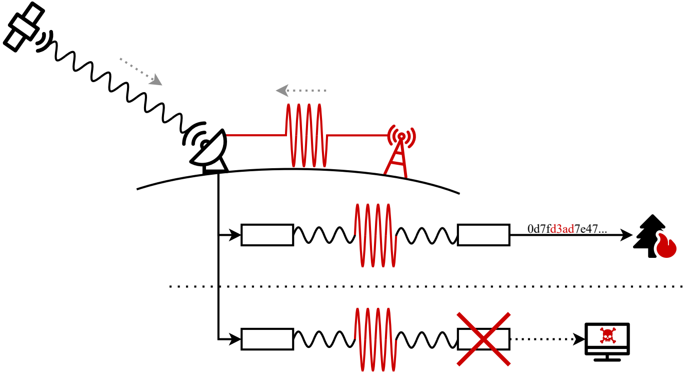
RQ: What can the attacker achieve by exploiting the unauthenticated channel of these specific systems?

[1] Motallebighomi et. al. (2022) "*Cryptography Is Not Enough: Relay Attacks on Authenticated GNSS Signals*"

[2] "*2011 REPORT TO CONGRESS of the U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION*" p.223–224

[3] Broadcasting (1986) "*'Captain Midnight' unmasked*"

Threat model



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**
Software-defined radio	598 USD[1]
X-Band upconverter	~100 USD[2]
X-Band amplifier	1, 638 USD
Compatible antenna	431 USD
Total	~3, 000 USD

Within the budget of a motivated hobbyist

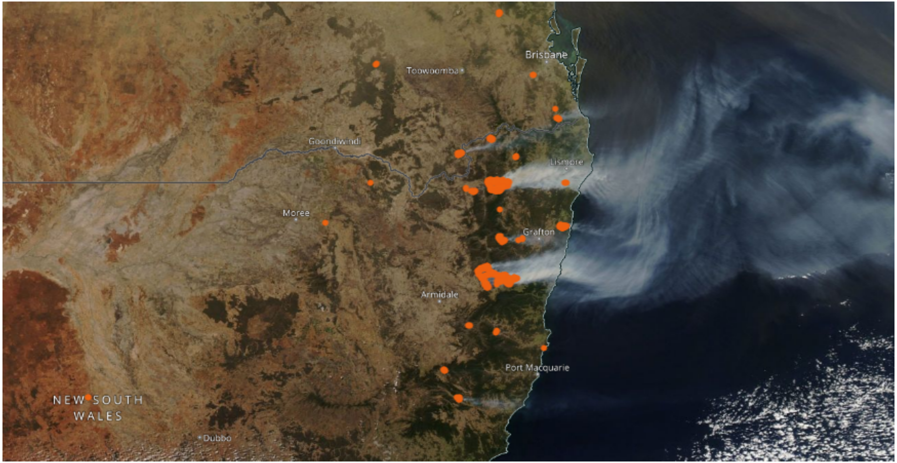
[1] Cost of a LimeSDR

[2] Estimated price from self-built amateur radio equipment

Motivation
Challenges
Implications
Threat model
Attacker capabilities
Case Study: FIRMS
Experiment setup
Attack overview
Affecting the derived dataset
Exploiting the decoder
Countermeasures
Future work
Conclusion

Case Study: Forest fire detection in FIRMS

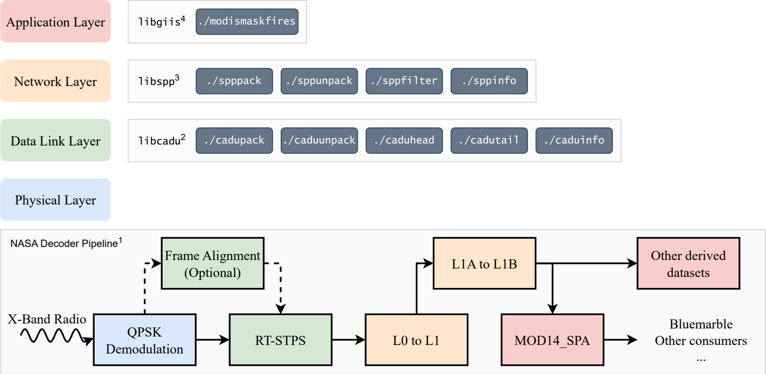
NASA's global fire detection service



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



Application Layer

libgiis[4] ./modismaskfires

Network Layer

libspp[3] ./spppack ./sppunpack ./sppfilter ./sppinfo

Data Link Layer

libcadu[2] ./cadupack ./caduunpack ./caduhead ./cadutail ./caduinfo

Physical Layer

NASA Decoder Pipeline[1]

X-Band Radio

QPSK Demodulation

Frame Alignment (Optional)

RT-STPS

L0 to L1

L1A to L1B

Other derived datasets

MOD14_SPA

Bluemarble
Other consumers
...

[1] NASA source code available with a research account from `https://directreadout.sci.gsfc.nasa.gov/`

[2] Custom tools to pack/unpack CADU frames `https://github.com/ssloxford/libcadu`

[3] Custom tools to pack/unpack SPP packets `https://github.com/ssloxford/libspp`

[4] Custom tools to modify MODIS sensor readings `https://github.com/ssloxford/libgiis`

Attack overview

Our attack

- Obtain legitimate data from digital archive[1]
- Perform security audit on downlink decoder software[2]
  - Determine data integrity checks
  - Identify vulnerabilities where safe input data assumed
- Create maliciously crafted data
  - Reprocess archived data to add/remove artifacts
  - Construct payload packet to trigger vulnerability chain

[1] NASA Distributed Active Archive containing MODIS data: `https://ladsweb.modaps.eosdis.nasa.gov/archive/`

[2] Decoder source code available with an academic account: `https://directreadout.sci.gsfc.nasa.gov/`

UNIVERSITY OF OXFORD

SSL
Systems Security Lab

Motivation

- Challenges
- Implications
- Threat model
- Attacker capabilities

Case Study: FIRMS

- Experiment setup
- Attack overview
- Affecting the derived dataset
- Exploiting the decoder

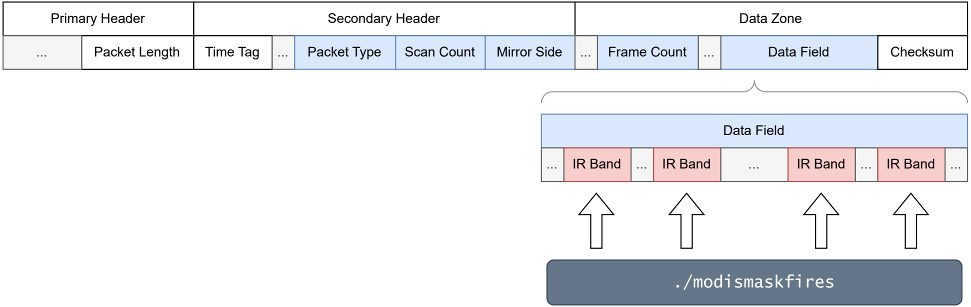
Countermeasures

Future work

Conclusion

Affecting the derived dataset

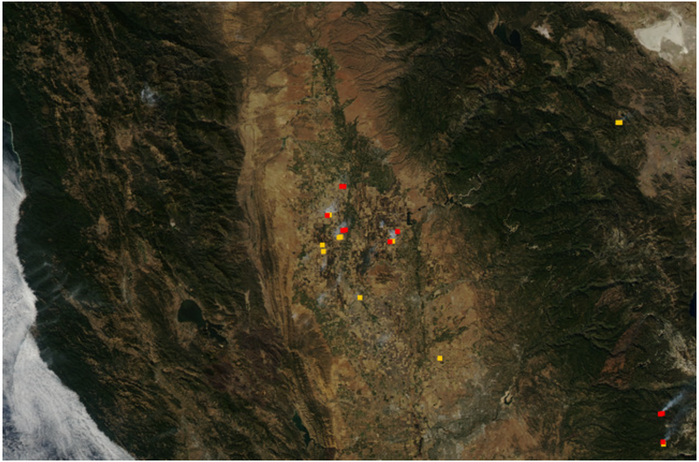
Packet structure



```
./modismaskfires
```

Affecting the derived dataset

Attack consequences



Original image.

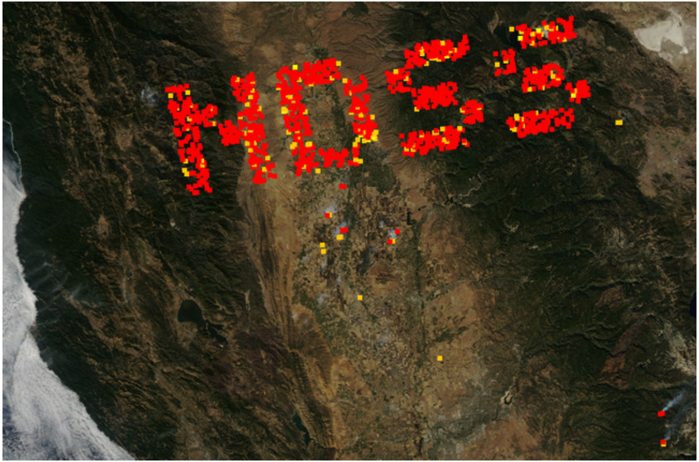
Affecting the derived dataset

Attack consequences

Masking existing fires.

Affecting the derived dataset

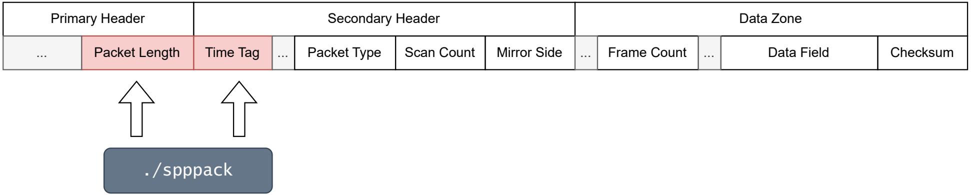
Attack consequences



Fine-grained control over fire injection.

Exploiting the decoder

Packet structure



Primary Header		Secondary Header					Data Zone				
...	Packet Length	Time Tag	...	Packet Type	Scan Count	Mirror Side	...	Frame Count	...	Data Field	Checksum

```
./spppack
```

Exploiting the decoder

Attack consequences

```
$ printf %1337s  | tr " " "f"  | \
  spppack --type-flag telecommand \
            --sec-hdr-flag 1 \
            --app-id aqua_modis \
  > bad_packet.PDS

$ cat bad_packet.PDS good_packet_sequence.PDS \
    > ./data/MYD00F.A2015299...001.PDS

$ ./run_all.sh ./data/
DATA_PATH: /mnt/data
CONTAINER_RUNTIME: docker

### Processing new PDS:
  MYD00F.A2015299.2110.20152992235.001.PDS

### Running modisl1db l1a-geo initial processing
l0fix_modis: Unrecoverable error in l0fix_modis!
```

Further vulnerabilities have been discovered since submission

Countermeasures

Cryptography should be required in future satellites
But existing satellites can't be upgraded

Backwards-compatible countermeasures:

- Multi-receiver data comparison
- Timing analysis[2]
- Physical-layer fingerprinting[3]

Existing countermeasures are effective, but aren't viable in all scenarios

[2] Jedermann et. al. (2021) "*Orbit-based Authentication Using TDOA Signatures in Satellite Networks*"

[3] Oligeri et. al. (2022) "*PAST-AI: Physical-Layer Authentication of Satellite Transmitters via Deep Learning*"

Future research directions

This work confirms the real-world vulnerability of existing Earth Observing systems

Future research is required to:

- Validate this work against real-world receiver hardware
- Comprehensively review other vulnerable satellites
- Analyze the effectiveness of proposed overshadowing countermeasures

Conclusion

We have...

- demonstrated viable spoofing attacks against NASA's forest fire detection system.
- provided the source code required to manipulate the packet data and structure.
- confirmed that only a moderate budget is required to perform these attacks.
- identified current countermeasures which significantly increase attack difficulty.

Thank you for your attention

Any questions?

Reach out to me at
edd.salkield@cs.ox.ac.uk