



UNIVERSITY OF  
OXFORD

**SSL**  
Systems Security Lab

# Firefly: Spoofing Earth Observation Satellites through Radio Overshadowing

*Edd Salkield*<sup>1</sup>    Joshua Smailes<sup>1</sup>    Sebastian Köhler<sup>1</sup>  
Simon Birnbach<sup>1</sup>    Richard Baker<sup>1</sup>    Martin Strohmeier<sup>2</sup>  
Ivan Martinovic<sup>1</sup>

<sup>1</sup>Systems Security Lab, University of Oxford

<sup>2</sup>Cyber-Defence Campus, armasuisse Science + Technology

Trinity Term 2022



UNIVERSITY OF  
OXFORD

**SSL**

Systems Security Lab

### Motivation

Threat model  
Attacker capabilities

### Case Study:

#### FIRMS

Experiment setup  
Affecting the derived  
dataset  
Exploiting processing stages

### Countermeasures

Multi-receiver data  
comparison  
Timing analysis  
Physical-layer fingerprinting

### Conclusion

# 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 <sup>1</sup>
  - Leaked keys <sup>2</sup>

---

<sup>1</sup>COMS-1 uses single DES <https://vkssdr.com/lrit-key-dec/>

<sup>2</sup>GK-2A keys embedded in published source code  
<https://vkssdr.com/xrit-rx/>



UNIVERSITY OF  
OXFORD

**SSL**

Systems Security Lab

## Motivation

Threat model

Attacker capabilities

## Case Study: FIRMS

Experiment setup

Affecting the derived  
dataset

Exploiting processing stages

## Countermeasures

Multi-receiver data  
comparison

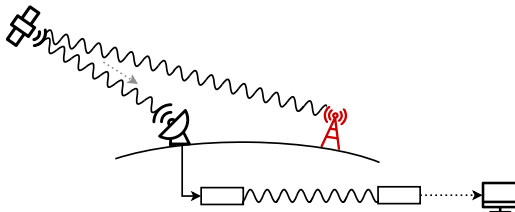
Timing analysis

Physical-layer fingerprinting

## Conclusion

# 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 calls [?]

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

## Motivation

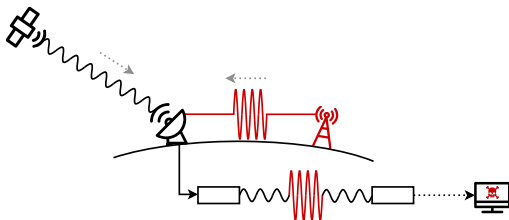
## Case Study: FIRMS

## Countermeasures

## Conclusion

## 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?



UNIVERSITY OF  
OXFORD

SSL

Systems Security Lab

### Motivation

Threat model  
Attacker capabilities

### Case Study: FIRMS

Experiment setup  
Affecting the derived  
dataset  
Exploiting processing stages

### Countermeasures

Multi-receiver data  
comparison  
Timing analysis  
Physical-layer fingerprinting

### Conclusion

# 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

## Motivation

### Threat model

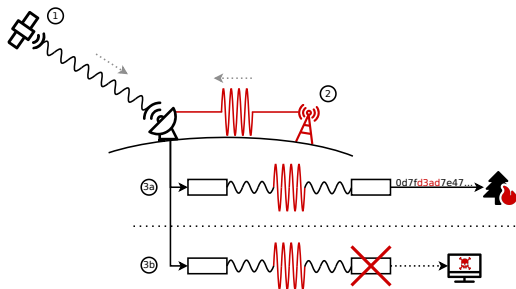
## Case Study: FIRMS

## Countermeasures

## Conclusion

## 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



UNIVERSITY OF  
OXFORD

# SSL

Systems Security Lab

## Motivation

Threat model  
Attacker capabilities

## Case Study: FIRMS

Experiment setup  
Affecting the derived  
dataset  
Exploiting processing stages

## Countermeasures

Multi-receiver data  
comparison  
Timing analysis  
Physical-layer fingerprinting

## Conclusion

# 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.



UNIVERSITY OF  
OXFORD

**SSL**

Systems Security Lab

## Motivation

- Threat model
- Attacker capabilities

## Case Study: FIRMS

- Experiment setup
- Affecting the derived dataset
- Exploiting processing stages

## Countermeasures

- Multi-receiver data comparison
- Timing analysis
- Physical-layer fingerprinting

## 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.





UNIVERSITY OF  
OXFORD

**SSL**  
Systems Security Lab

## Motivation

Threat model  
Attacker capabilities

## Case Study: FIRMS

Experiment setup  
Affecting the derived  
dataset  
Exploiting processing stages

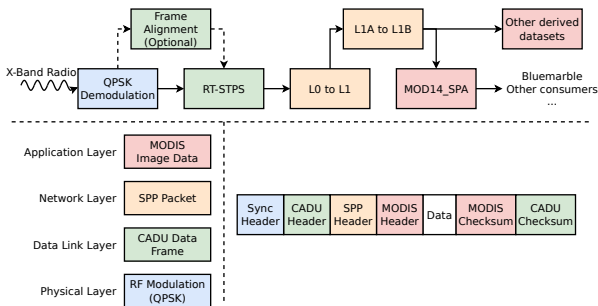
## Countermeasures

Multi-receiver data  
comparison  
Timing analysis  
Physical-layer fingerprinting

## Conclusion

# Case Study: Forest fire detection in FIRMS

Experiment setup



We set up docker pipeline for the relevant parts of IPOPP



UNIVERSITY OF  
OXFORD

**SSL**  
Systems Security Lab

## Motivation

Threat model  
Attacker capabilities

## Case Study: FIRMS

Experiment setup  
Affecting the derived  
dataset  
Exploiting processing stages

## Countermeasures

Multi-receiver data  
comparison  
Timing analysis  
Physical-layer fingerprinting

## Conclusion

# Exploiting processing stages

## Obtaining the processing software

The screenshot shows the NASA Direct Readout Laboratory website. The header includes the NASA logo and the text "DIRECT READOUT LABORATORY". Below the header is a navigation bar with links to "NASA Home", "Goddard Home", "Direct Readout Laboratory", and "Download MODISL1DB\_Science\_Processing\_Algorithm 1.9". A search bar and a "LOGOUT" button are also present. The main content area is titled "MODISL1DB\_SPA" and features a warning icon and the text "You agree to the NASA Open Source Agreement included with this software package." Below this is a "Click To Download Version: 1.9" button and a "MyDRL MODISL1DB\_SPA Forum" button. The page also lists the "Version: 1.9", "Release Date: 07/12/21", and "Enhancements". An "Overview" section describes the software package, which contains the MODIS Level 1 Direct Broadcast SPA (MODISL1DB\_SPA) and processes Level 0 MODIS data into Level 1A (MOD001/MYD001) and Geolocation (MOD003/MYD003) products. It also processes Level 1A and Geolocation products into MODIS Level 1B one km (MOD021KM/MYD021KM), half km (MOD02HKM/MYD02QKM), and quarter km (MOD02QKM/MYD02QKM) granules. The MODISL1DB\_SPA functions as an IPOPP plug-in.

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/>



UNIVERSITY OF  
OXFORD

# Affecting the derived dataset

Key challenges

**SSL**  
Systems Security Lab

## Motivation

Threat model  
Attacker capabilities

## Case Study: FIRMS

Experiment setup  
Affecting the derived  
dataset  
Exploiting processing stages

## Countermeasures

Multi-receiver data  
comparison  
Timing analysis  
Physical-layer fingerprinting

## Conclusion

- 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



UNIVERSITY OF  
OXFORD

# SSL

Systems Security Lab

## Motivation

Threat model

Attacker capabilities

## Case Study: FIRMS

Experiment setup

Affecting the derived  
dataset

Exploiting processing stages

## Countermeasures

Multi-receiver data  
comparison

Timing analysis

Physical-layer fingerprinting

## Conclusion

# 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

<input type="radio"/> Select All	Last Modified	Size
..  Parent directory		
<input type="radio"/>		
MYD00FA2015299.0000.20152990300.000.PDS.bz2	2017-12-22 06:29	149.0
<input type="radio"/>		
MYD00FA2015299.0000.20152990300.001.PDS.bz2	2017-12-22 06:29	68.0 MB

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



UNIVERSITY OF  
OXFORD

# Affecting the derived dataset

Data processing: image format reversing

# SSL

Systems Security Lab

## Motivation

Threat model  
Attacker capabilities

## Case Study: FIRMS

Experiment setup  
Exploiting the derived dataset  
Exploiting processing stages  
Countermeasures  
Multi-receiver data comparison  
Timing analysis  
Physical-layer fingerprinting

## Conclusion

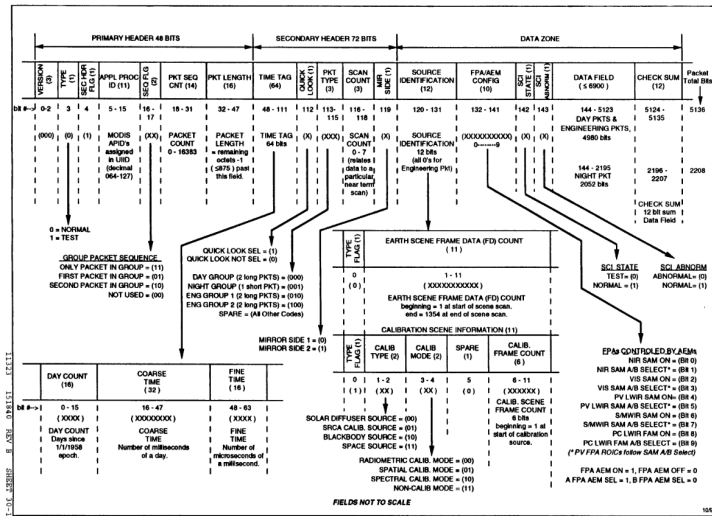


Figure 30-8. MODIS CCSDS Science Packet Detail Format



UNIVERSITY OF  
OXFORD

**SSL**  
Systems Security Lab

### Motivation

Threat model  
Attacker capabilities

### Case Study: FIRMS

Experiment setup  
Affecting the derived  
dataset  
Exploiting processing stages

### Countermeasures

Multi-receiver data  
comparison  
Timing analysis  
Physical-layer fingerprinting

### Conclusion

# Affecting the derived dataset

Data processing: building protocol manipulation tools

**TODO: find way of presenting the tools**



UNIVERSITY OF  
OXFORD

# SSL

Systems Security Lab

## Motivation

- Threat model
- Attacker capabilities

## Case Study: FIRMS

- Experiment setup
- Affecting the derived dataset
- Exploiting processing stages

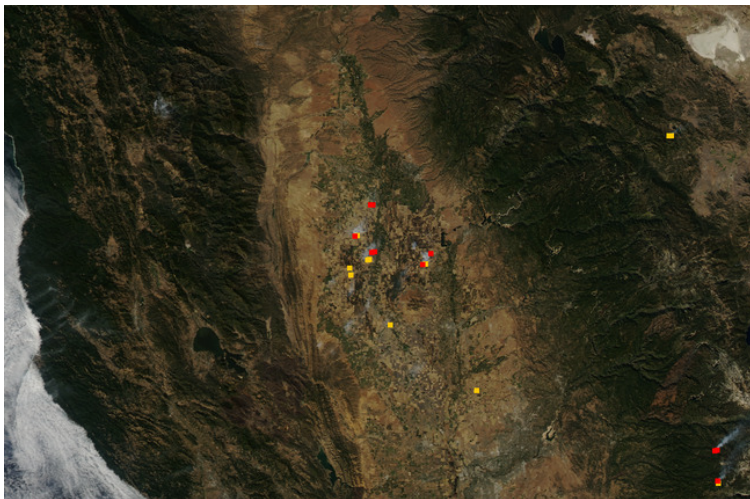
## Countermeasures

- Multi-receiver data comparison
- Timing analysis
- Physical-layer fingerprinting

## Conclusion

# Attack consequences

Affecting the derived dataset



Original image.



UNIVERSITY OF  
OXFORD

# SSL

Systems Security Lab

## Motivation

- Threat model
- Attacker capabilities

## Case Study: FIRMS

- Experiment setup
- Affecting the derived dataset
- Exploiting processing stages

## Countermeasures

- Multi-receiver data comparison
- Timing analysis
- Physical-layer fingerprinting

## Conclusion

# Attack consequences

Affecting the derived dataset



Masking existing fires.





UNIVERSITY OF  
OXFORD

**SSL**  
Systems Security Lab

### Motivation

- Threat model
- Attacker capabilities

### Case Study: FIRMS

- Experiment setup
- Affecting the derived dataset
- Exploiting processing stages

### Countermeasures

- Multi-receiver data comparison
- Timing analysis
- Physical-layer fingerprinting

### Conclusion

# Attack consequences

Affecting the derived dataset



Fine-grained control over fire injection.



UNIVERSITY OF  
OXFORD

# Exploiting processing stages

Key challenges

# SSL

Systems Security Lab

## Motivation

Threat model  
Attacker capabilities

## Case Study: FIRMS

Experiment setup  
Affecting the derived  
dataset  
Exploiting processing stages

## Countermeasures

Multi-receiver data  
comparison  
Timing analysis  
Physical-layer fingerprinting

## Conclusion

- 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



UNIVERSITY OF  
OXFORD

# SSL

Systems Security Lab

# Exploiting processing stages

## Construct payload packet

### Motivation

Threat model

Attacker capabilities

### Case Study: FIRMS

Experiment setup

Affecting the derived  
dataset

Exploiting processing stages

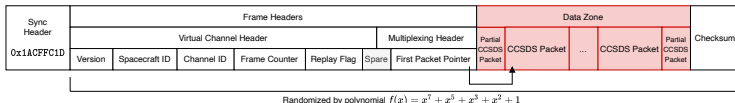
### Countermeasures

Multi-receiver data  
comparison

Timing analysis

Physical-layer fingerprinting

### Conclusion





UNIVERSITY OF  
OXFORD

# SSL

Systems Security Lab

## Motivation

Threat model

Attacker capabilities

## Case Study: FIRMS

Experiment setup

Affecting the derived  
dataset

Exploiting processing stages

## Countermeasures

Multi-receiver data  
comparison

Timing analysis

Physical-layer fingerprinting

## Conclusion

# Attack consequences

Exploiting the processing stages

The screenshot displays the FIRMS application interface, which is used for SSL attack experiments. It features several control panels and status tables.

**Target Configuration:**

- Target Host: localhost
- Target Port: 4935
- Delay between sends: 0 ms
- File: MYD00F.A2015299.Z110.20152992235.00...
- Buttons: Go, Stop
- Status: Done

**Virtual Channel Status Table:**

Type	Chann...	CADUS	Seq Err	Lost C...	Packe...	Lost F...	Unrout...
path	MODIS...	615696	0	0	615696	0	615696

**Packet Status Table:**

Type	Stream	Output...	Seq Er...	Missing	Discar...	Bad SL...	Pits w...
packet	MODIS...	615696	0	0	0	0	0

**path.MODIS\_30 Status:**

CADUS	615696
CADU Seq Errors	0
Missing CADUS	0
Idle VCDUS	0
Bad FHs	0
Troublesome Frames	0
Irrational Packet Lengths	0
Discarded Fragments	0
Discarded Bytes	0
Created Packets	1231392
Unrouteable Packets	615696
Idle Packets	0
Deleted Packets	615696
Output Packets	615696

**packet.MODIS\_64 Status:**

Packets Output	615696
Discarded Packets	0
Bad Lengths	0
Packets With Fill	0
Sequence Errors	0
Missing Packets	0
Bad Length Sample	0

**File Commands Status:**

Buttons: Load, Go, Stop, Unload, Zero, Exit

**Frames:**

Mode	search
Lost Sync Count	0
Flywheels	0
Lock Frames	615696
Flywheels Output	0
Slipped Frames	0
True Frames	615696
Inverted Frames	0
CRC Error Frames	0
RS Corrected Frames	0
RS Uncorrectables	0
Deleted Frames	0
Passed Frames	615696
CADUS	615696
Unrouteable CADUS	0
Fill CADUS	0

2022/11/14:56:02  
Hot Ready Go: 2022/11/14:10:41 Stop: 2022/11/14:11:48 No Data



UNIVERSITY OF  
OXFORD

# Attack consequences

Exploiting the processing stages

## SSL

Systems Security Lab

### Motivation

Threat model  
Attacker capabilities

### Case Study: FIRMS

Experiment setup  
Affecting the derived  
dataset  
Exploiting processing stages

### Countermeasures

Multi-receiver data  
comparison  
Timing analysis  
Physical-layer fingerprinting

### Conclusion

Target Host: localhost  
Target Port: 4935  
Delay between sends: 0 ms  
File: P1540064AAAAAAAAAAAAAAAA2210819573...

Go Stop

**Done**

**Virtual Channel Status Table**

Type	Chann...	CADUs	Seq Errs	Lost C...	Packe...	Lost Fra...	Unro...
path	MODIS...	447146	0	0	614304	1392	33

**packet.MODIS\_64 Status**

Packets Output	614304
Discarded Packets	0
Bad Lengths	0
Packets With Fill	0
Sequence Errors	1392
Missing Packets	1392
Bad Length Sample	0

**path.MODIS\_30 Status**

CADUs	447146
CADU Seq Errors	0
Missing CADUs	0
Idle VCDUs	0
Bad FHPs	0
Troublesome Frames	1392
Irrational Packet Lengths	0
Discarded Fragments	1392
Discarded Bytes	893664
Created Packets	614337
Unrouteable Packets	33
Idle Packets	0
Deleted Packets	33
Output Packets	614304

**Packet Status Table**

Stream	Output	Seq Errors	Missing	Disc...	Bad Sizes	PKts w/ Fill
MODIS_64	614304	1392	1392	0	0	0

File Commands Status

Load Go Stop Unload Zero Exit

**Frames**

Mode	search
Lost Sync Count	0
Flywheels	0
Lock Frames	447146
Flywheels Output	0
Slipped Frames	0
True Frames	447146
Inverted Frames	0

**Frames**

CRC Error Frames	0
RS Corrected Frames	0
RS Uncorrectables	0
Deleted Frames	0
Passed Frames	447146
CADUs	447146
Unrouteable CADUs	0
Fill CADUs	0

2022/10/8/21:50:41  
Not Ready Go: 2022/10/8/19:57:38 Stop: 2022/10/8/19:58:27 No Data



UNIVERSITY OF  
OXFORD

# SSL

Systems Security Lab

## Motivation

Threat model  
Attacker capabilities

## Case Study: FIRMS

Experiment setup  
Affecting the derived  
dataset  
Exploiting processing stages

## Countermeasures

Multi-receiver data  
comparison  
Timing analysis  
Physical-layer fingerprinting

## Conclusion

# 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



UNIVERSITY OF  
OXFORD

# SSL

Systems Security Lab

## Motivation

Threat model  
Attacker capabilities

## Case Study: FIRMS

Experiment setup  
Affecting the derived  
dataset  
Exploiting processing stages

## Countermeasures

Multi-receiver data  
comparison  
Timing analysis  
Physical-layer fingerprinting

## Conclusion

# 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



UNIVERSITY OF  
OXFORD

# SSL

Systems Security Lab

## Motivation

Threat model  
Attacker capabilities

## Case Study: FIRMS

Experiment setup  
Affecting the derived  
dataset  
Exploiting processing stages

## Countermeasures

Multi-receiver data  
comparison  
Timing analysis  
Physical-layer fingerprinting

## Conclusion

# 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

### Motivation

Threat model  
Attacker capabilities

### Case Study: FIRMS

Experiment setup  
Affecting the derived  
dataset  
Exploiting processing stages

### Countermeasures

Multi-receiver data  
comparison  
Timing analysis  
Physical-layer fingerprinting

### Conclusion

# 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.