

# 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

NDSS SpaceSec 2023



Challenges

implicatii

Attacker capabiliti

### Case Study:

Experiment set Attack overvier

Affecting the de dataset

Exploiting the deco

Countermeasures

Future worl

Conclusion

# Challenges of unauthenticated satellites

Many current satellites do not encrypt the downlink, due to:



Challenges

Threat mo

Attacker capabiliti

Case Study:

Experiment sets Attack overview

Affecting the der dataset

Countermeasures

**Future work** 

Conclusion

- Many current satellites do not encrypt the downlink, due to:
  - Increased power budget, mission complexity, and cost



Challenges

Threat mod

Attacker capabiliti

Case Study:

Experiment set

Attack overview Affecting the de

Exploiting the decor

Countermeasures

**Future work** 

Conclusion

- Many current satellites do not encrypt the downlink, due to:
  - Increased power budget, mission complexity, and cost
  - Legacy systems backwards compatibility



Challenges

Threat mod

Attacker capabilitie

Case Study:

Attack overview Affecting the der dataset

Countermeasures

**Future** work

Conclusion

- Many current satellites do not encrypt the downlink, due to:
  - Increased power budget, mission complexity, and cost
  - Legacy systems backwards compatibility
  - Open access data



Challenges

Threat model

Attacker capabilitie

Case Study:

Attack overview
Affecting the derived dataset

Countermeasures

**Future work** 

Conclusion

- 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:



Challenges

Threat mode

Attacker capabilities

Case Study:

Attack overview Affecting the derived dataset Exploiting the decode

Countermeasures

**Future work** 

Conclusion

# 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 <sup>1</sup>

l

<sup>&</sup>lt;sup>1</sup>COMS-1 uses single DES https://vksdr.com/lrit-key-dec/



Challenges

Implications Threat mode

Attacker capabilitie

Case Study:

Experiment setup
Attack overview
Affecting the deri
dataset

Exploiting the decode

Countermeasures

**Future** work

Conclusion

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

<sup>&</sup>lt;sup>1</sup>COMS-1 uses single DES https://vksdr.com/lrit-key-dec/

<sup>&</sup>lt;sup>2</sup>GK-2A keys leaked in source code https://vksdr.com/xrit-rx/



Challenges

Threat model
Attacker capabiliti

Case Study:

FIRMS
Experiment s

Affecting the derived dataset

Countermeasures

**Future work** 

Conclusion

# Challenges of unauthenticated satellites

Insecure Earth Observation Satellites

Satellites with insecure downlinks include:

• Fire detection and management, e.g., Terra, Aqua



Challenges

Threat model Attacker capabilitie

Case Study:

Experiment setu

Affecting the derived dataset Exploiting the decoder

Countermeasures

**Future work** 

Conclusion

# 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



# SSL Systems Security La

#### Motivation

Implications

implicatio

Attackor canabilitio

Attacker capabilities

### Case Study: FIRMS

Attack overview

Affecting the derive

dataset

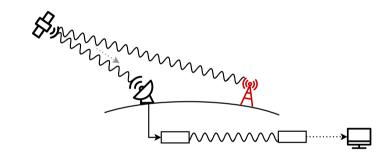
Countermeasur

**Future work** 

Conclusion

# **Implications**

Data secrecy





Challenges Implications

Threat model Attacker capabilit

Case Study:

Experiment set

Affecting the deriv

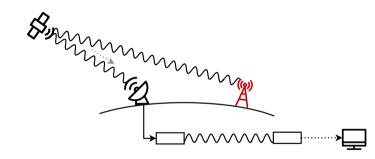
Countermeasures

**Future work** 

Conclusion

# **Implications**

Data secrecy



Using an SDR and open source software, attackers can:



Implications
Threat mode

Attacker capabilit

### Case Study: FIRMS

Affecting the derive dataset Exploiting the decor

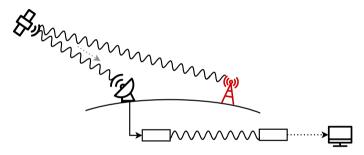
Countermeasures

Future work

Conclusion

# **Implications**

Data secrecy



Using an SDR and open source software, attackers can:

• Read confidential maritime data<sup>1</sup> and internet traffic<sup>2</sup>

<sup>&</sup>lt;sup>1</sup>Pavur et al. (2020) "A Tale of Sea and Sky on the Security of Maritime VSAT Communications"

<sup>&</sup>lt;sup>2</sup>Pavur et al. (2019) "Secrets in the Sky: On Privacy and Infrastructure Security in DVB-S Satellite Broadband"



Implications
Threat mode

rnreat model Attacker capabiliti

### Case Study: FIRMS

Attack overview
Affecting the derived dataset
Exploiting the decode

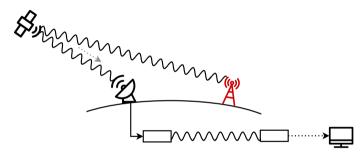
-----

Future work

Conclusion

# Implications

Data secrecy



Using an SDR and open source software, attackers can:

- Read confidential maritime data<sup>1</sup> and internet traffic<sup>2</sup>
- Eavesdrop on Iridium traffic and calls <sup>3</sup>

<sup>&</sup>lt;sup>1</sup> Pavur et al. (2020) "A Tale of Sea and Sky on the Security of Maritime VSAT Communications"

<sup>&</sup>lt;sup>2</sup>Pavur et al. (2019) "Secrets in the Sky: On Privacy and Infrastructure Security in DVB-S Satellite Broadband"

<sup>3</sup> muccc "Iridium Toolkit" https://github.com/muccc/iridium-toolkit





Implications

-----

Attacker capabilities

Case Study:

### FIRMS

Attack overview

Affecting the d

Exploiting the decod

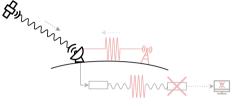
Countermeasure

Future work

Conclusion

### **Implications**

Data authenticity and integrity







Implications

Through man

Attacker capabilities

Casa Studyu

### FIRMS

Attack overview

Affecting the d

Exploiting the decod

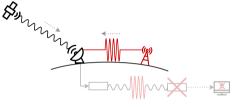
Countermeasure

Future work

#### Conclusion

### **Implications**

Data authenticity and integrity







Implications

Throat man

Attacker capabilities

Case Study

### FIRMS

Attack overview

Affecting the d

Exploiting the decod

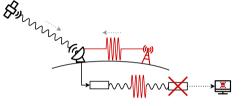
Countermeasure

Future work

Conclusion

### **Implications**

Data authenticity and integrity





Implications

Attacker capabilities

Case Study:

### FIRMS

Experiment sets Attack overview

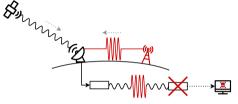
dataset

Countermeasur

**Future worl** 

# **Implications**

Data authenticity and integrity



Spoofing attacks have been shown against:



Implications
Threat mode

Attacker capabilities

Case Study: FIRMS

Attack overview
Affecting the derived dataset
Exploiting the decode

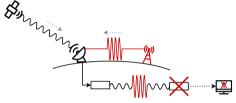
Countermeasures

**Future work** 

Conclusion

### Implications

Data authenticity and integrity



Spoofing attacks have been shown against:

GNSS to manipulate calculated location<sup>1</sup>

<sup>&</sup>lt;sup>1</sup> Motallebighomi et. al. (2022) "Cryptography Is Not Enough: Relay Attacks on Authenticated GNSS Signals"



Implications
Threat mode

Case Study:

### FIRMS

Affecting the derived dataset
Exploiting the decode

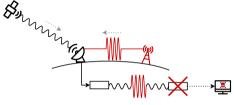
Countermeasures

**Future work** 

Conclusion

# Implications

Data authenticity and integrity



Spoofing attacks have been shown against:

- GNSS to manipulate calculated location<sup>1</sup>
- Uplinks for satellite hijacking<sup>2</sup> or broadcast intrusion<sup>3</sup>

<sup>&</sup>lt;sup>1</sup> Motallebighomi et. al. (2022) "Cryptography Is Not Enough: Relay Attacks on Authenticated GNSS Signals"

<sup>2&</sup>quot;2011 REPORT TO CONGRESS of the U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION" p.223–224

<sup>&</sup>lt;sup>3</sup>Broadcasting (1986) "'Captain Midnight' unmasked"



Implications
Threat mode

Case Study:

### FIRMS

Attack overview
Affecting the derived
dataset
Exploiting the decoder

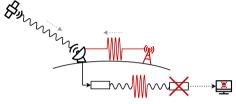
Countermeasure

Future work

Conclusion

# Implications

Data authenticity and integrity



Spoofing attacks have been shown against:

- GNSS to manipulate calculated location<sup>1</sup>
- Uplinks for satellite hijacking<sup>2</sup> or broadcast intrusion<sup>3</sup>

No work considers spoofing Earth Observation satellites

<sup>&</sup>lt;sup>1</sup> Motallebighomi et. al. (2022) "Cryptography Is Not Enough: Relay Attacks on Authenticated GNSS Signals"

<sup>&</sup>lt;sup>2</sup>"2011 REPORT TO CONGRESS of the U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION" p.223-224

<sup>&</sup>lt;sup>3</sup> Broadcasting (1986) "'Captain Midnight' unmasked"



Implications
Threat mode

### Case Study:

Attack overview
Affecting the derived dataset
Exploiting the decoder

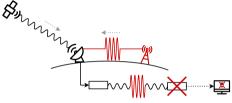
Countermeasures

Future work

Conclusion

# Implications

Data authenticity and integrity



Spoofing attacks have been shown against:

- GNSS to manipulate calculated location<sup>1</sup>
- Uplinks for satellite hijacking<sup>2</sup> or broadcast intrusion<sup>3</sup>

No work considers spoofing Earth Observation satellites

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

<sup>&</sup>lt;sup>1</sup> Motallebighomi et. al. (2022) "Cryptography Is Not Enough: Relay Attacks on Authenticated GNSS Signals"

<sup>&</sup>lt;sup>2</sup>"2011 REPORT TO CONGRESS of the U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION" p.223-224

<sup>&</sup>lt;sup>3</sup> Broadcasting (1986) "'Captain Midnight' unmasked"



Challenge

Threat model

Attacker capabilitie

### Case Study:

Experiment set

Affecting the d

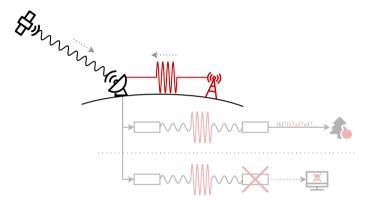
Exploiting the deco

Countermeasures

Future wo

Conclusion

### Threat model



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



Challenges Implication

Threat model

ttacker capabilitie

#### Case Study: FIRMS

Attack overvie Affecting the o

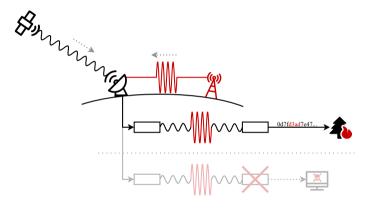
Exploiting the deco

Countermeasures

**Future work** 

Conclusion

### Threat model



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

Affect the satellite-derived datasets



Challenges Implication

Threat model

Attacker capabilitie

### Case Study: FIRMS

Attack overview
Affecting the der
dataset

Exploiting the decoder

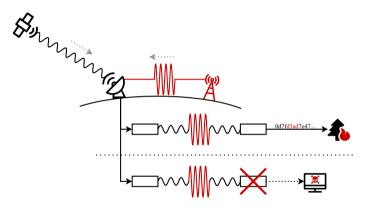
Countermeasures

Future work

i dedie woi

Conclusion

### Threat model



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

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



# Systems Sec

Motivation

Implications
Threat mode

Threat model

Attacker capabilities

Case Study:

Attack overview

Affecting the derive dataset

Countermeasu

Future wor

onclusion

# Attacker capabilities

Estimated cost

Hardware component	Cost
Software-defined radio	598 USD <sup>1</sup>
X-Band upconverter	$\sim 100~\mathrm{USD^2}$
X-Band amplifier	$1,638\mathrm{USD}$
Compatible antenna	431 USD
Total	~3,000 USD

<sup>&</sup>lt;sup>1</sup>Cost of a LimeSDR

<sup>&</sup>lt;sup>2</sup>Estimated price from self-built amateur radio equipment



# Systems Sec

#### Motivation

Implications
Threat mode

Threat model

Attacker capabilities

Case Study:

Attack overview
Affecting the derive dataset

Countermeasure

Future work

Conclusion

# Attacker capabilities

Estimated cost

Hardware component	Cost
Software-defined radio	598 USD <sup>1</sup>
X-Band upconverter	$\sim 100~\mathrm{USD^2}$
X-Band amplifier	$1,638\mathrm{USD}$
Compatible antenna	431 USD
Total	~3,000 USD

Within the budget of a motivated hobbyist

<sup>&</sup>lt;sup>1</sup>Cost of a LimeSDR

<sup>&</sup>lt;sup>2</sup>Estimated price from self-built amateur radio equipment



# SSL Systems Security Lat

#### Motivation

Challenges Implications Threat model

Threat model

Attacker capabilitie

### Case Study: FIRMS

Experiment setup

Affecting the d

Exploiting the de

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.





Challenges Implications Threat mod

Attacker capabilitie

Case Study: FIRMS

Experiment setup

Attack overview

Affecting the derived dataset

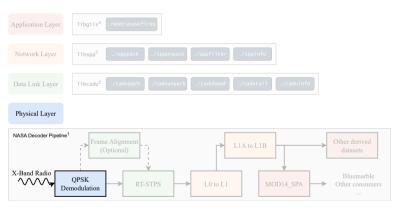
Exploiting the decoder

Countermeasures

**Future work** 

Conclusion

### Case Study: Forest fire detection in FIRMS



 $<sup>^{1} \</sup>text{NASA source code available with a research account from $\texttt{https://directreadout.sci.gsfc.nasa.gov/} \\$ 



SSL Systems Security La

Motivation

Challenges Implications Threat mode

Case Study:

FIRMS
Experiment setup

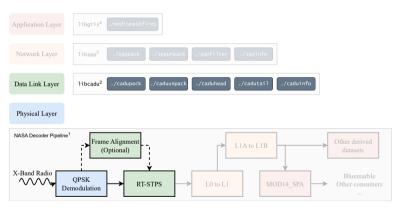
Affecting the derived dataset
Exploiting the decode

Countermeasures

Future work

Conclusion

### Case Study: Forest fire detection in FIRMS



 $<sup>^{1} \</sup>text{NASA source code available with a research account from $\texttt{https://directreadout.sci.gsfc.nasa.gov/}$$ 

 $<sup>{}^2 \</sup>hbox{Custom tools to pack/unpack CADU frames $\tt https://github.com/ssloxford/libcadu}$ 





Challenges
Implications
Threat mode

Case Study: FIRMS

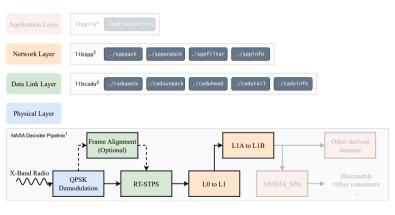
Experiment setup
Attack overview
Affecting the derived dataset
Exploiting the decoder

Countermeasures

**Future work** 

Conclusion

### Case Study: Forest fire detection in FIRMS



 $<sup>^{1} \</sup>text{NASA source code available with a research account from $\texttt{https://directreadout.sci.gsfc.nasa.gov/}$$ 

<sup>&</sup>lt;sup>2</sup>Custom tools to pack/unpack CADU frames https://github.com/ssloxford/libcadu

 $<sup>^3</sup>$  Custom tools to pack/unpack SPP packets https://github.com/ssloxford/libspp





Challenges Implications Threat mode Attacker cap

#### Case Study: FIRMS

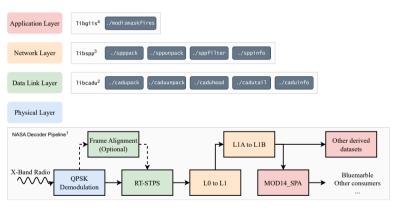
Experiment setup
Attack overview
Affecting the derived dataset
Exploiting the decoder

Countermeasures

**Future work** 

Conclusion

### Case Study: Forest fire detection in FIRMS



 $<sup>^{1} \</sup>text{NASA source code available with a research account from $\texttt{https://directreadout.sci.gsfc.nasa.gov/}$$ 

<sup>&</sup>lt;sup>2</sup>Custom tools to pack/unpack CADU frames https://github.com/ssloxford/libcadu

<sup>&</sup>lt;sup>3</sup>Custom tools to pack/unpack SPP packets https://github.com/ssloxford/libspp

<sup>&</sup>lt;sup>4</sup>Custom tools to modify MODIS sensor readings https://github.com/ssloxford/libgiis



Challenges Implications

Attacker capabilitie

### Case Study:

Attack overview
Affecting the der

Exploiting the deco

Countermeasure

Future wor

Conclusion

### Attack overview

Our attack

Obtain legitimate data from digital archive<sup>1</sup>

<sup>&</sup>lt;sup>1</sup>NASA Distributed Active Archive containing MODIS data: https://ladsweb.modaps.eosdis.nasa.gov/archive/



Challenges Implications Threat mode

nreat modei ttacker capabilitie

### Case Study: FIRMS

Attack overview

Affecting the deri

Exploiting the decor

Countermeasures

**Future work** 

Conclusion

### Attack overview

Our attack

- Obtain legitimate data from digital archive<sup>1</sup>
- Perform security audit on downlink decoder software<sup>2</sup>

<sup>&</sup>lt;sup>1</sup> NASA Distributed Active Archive containing MODIS data: https://ladsweb.modaps.eosdis.nasa.gov/archive/

<sup>&</sup>lt;sup>2</sup> Decoder source code available with an academic account: https://directreadout.sci.gsfc.nasa.gov/



Challenges Implications Threat model

Case Study:

### FIRMS

Attack overview

Attack overview

dataset

Countermeasures

**Future work** 

Conclusion

### Attack overview

Our attack

- Obtain legitimate data from digital archive<sup>1</sup>
- Perform security audit on downlink decoder software<sup>2</sup>
  - Determine data integrity checks

<sup>&</sup>lt;sup>1</sup> NASA Distributed Active Archive containing MODIS data: https://ladsweb.modaps.eosdis.nasa.gov/archive/

<sup>&</sup>lt;sup>2</sup> Decoder source code available with an academic account: https://directreadout.sci.gsfc.nasa.gov/



Challenges Implications Threat model

ttacker capabilities

### Case Study:

FIKMS

Experiment setu

Attack overview

Exploiting the decod

Countermeasures

**Future work** 

Conclusion

### Attack overview

Our attack

- Obtain legitimate data from digital archive<sup>1</sup>
- Perform security audit on downlink decoder software<sup>2</sup>
  - Determine data integrity checks
  - Identify vulnerabilities where safe input data assumed

<sup>1</sup> NASA Distributed Active Archive containing MODIS data; https://ladsweb.modaps.eosdis.nasa.gov/archive/

<sup>&</sup>lt;sup>2</sup> Decoder source code available with an academic account: https://directreadout.sci.gsfc.nasa.gov/



Challenges Implications Threat model

Attacker capabilities

## Case Study: FIRMS

Attack overview
Affecting the derived dataset

Countermeasures

**Future** work

Conclusion

## Attack overview

Our attack

- Obtain legitimate data from digital archive<sup>1</sup>
- Perform security audit on downlink decoder software<sup>2</sup>
  - Determine data integrity checks
  - Identify vulnerabilities where safe input data assumed
- Create maliciously crafted data

<sup>1</sup> NASA Distributed Active Archive containing MODIS data: https://ladsweb.modaps.eosdis.nasa.gov/archive/

<sup>&</sup>lt;sup>2</sup> Decoder source code available with an academic account: https://directreadout.sci.gsfc.nasa.gov/



Challenges Implications Threat model

ttacker capabilities

### Case Study:

Attack overview

Affecting the der

Exploiting the decod

Countermeasures

**Future work** 

Conclusion

## Attack overview

Our attack

- Obtain legitimate data from digital archive<sup>1</sup>
- Perform security audit on downlink decoder software<sup>2</sup>
  - Determine data integrity checks
  - Identify vulnerabilities where safe input data assumed
- Create maliciously crafted data
  - Reprocess archived data to add/remove artifacts

<sup>1</sup> NASA Distributed Active Archive containing MODIS data: https://ladsweb.modaps.eosdis.nasa.gov/archive/

<sup>&</sup>lt;sup>2</sup> Decoder source code available with an academic account: https://directreadout.sci.gsfc.nasa.gov/



Challenges Implications Threat model

Case Study:

### FIRMS

Attack overview

Affecting the derived dataset

Exploiting the decoder

Countermeasures

**Future work** 

Conclusion

## Attack overview

Our attack

- Obtain legitimate data from digital archive<sup>1</sup>
- Perform security audit on downlink decoder software<sup>2</sup>
  - 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

<sup>&</sup>lt;sup>1</sup> NASA Distributed Active Archive containing MODIS data: https://ladsweb.modaps.eosdis.nasa.gov/archive/

<sup>&</sup>lt;sup>2</sup> Decoder source code available with an academic account; https://directreadout.sci.gsfc.nasa.gov/



SSL Systems Security La

Motivation Challenges

Implications
Threat mode

Attacker capabiliti

## Case Study: FIRMS

Attack overview

Affecting the derived

Exploiting the decode

Countermeasure

Future work

Conclusior

## Affecting the derived dataset

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



## SSL Systems Security L

Motivation
Challenges

Threat model

Attacker capabiliti

## Case Study: FIRMS

Attack overview

Affecting the derived

Exploiting the decode

Countermeasure

Future work

Conclusior

## Affecting the derived dataset

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



## SSL Systems Security La

Motivation Challenges

Threat model

Attacker capabilitie

## Case Study: FIRMS

Experiment setu Attack overview

Affecting the derived

Exploiting the decod

Countermeasure

Future work

Conclusion

## Affecting the derived dataset

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





SSL Systems Security L

Motivation Challenges

Threat model

Attacker capabilitie

#### Case Study: FIRMS

Attack overview

Affecting the derived dataset

Exploiting the deco

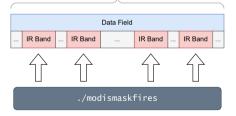
Countermeasure

Future work

Conclusio

## Affecting the derived dataset

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





## SSL Systems Security La

#### Motivation

Challenges

implication

acker capabilitie

## Case Study: FIRMS

Experiment setu

Attack overview

Affecting the derived dataset

Exploiting the deco

Future work

## Affecting the derived dataset



Original image.



## SSL Systems Security Lab

#### Motivation

Challenges

Threat model

## Case Study: FIRMS

Experiment setu

Affecting the derived

Exploiting the deco

Countermeasure

Future worl

Conclusion

## Affecting the derived dataset



Masking existing fires.



## SSL Systems Security Lat

#### Motivation

Challenges

Threat model

Attacker capabilitie

## Case Study: FIRMS

Experiment setu

Attack overview

Affecting the derived

dataset

Countermeasur

**Future work** 

Conclusion

## Affecting the derived dataset



Fine-grained control over fire injection.



## SSI Systems Security I

#### Motivation

Implications
Threat mod

Attacker capabilities

#### Case Study: FIRMS

Attack overview

Affecting the deri

Exploiting the decoder

Countermeasure

Future work

Conclusior

## Exploiting the decoder

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



## Systems Sec

#### Motivation

Implications
Threat mode

Attacker capabilities

#### Case Study: FIRMS

Attack overview
Affecting the deri

Exploiting the decoder

Countermeasure

Future work

Conclusior

## Exploiting the decoder

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



## SSL Systems Security La

#### Motivation

Implication

rnreat model Attacker capabilities

#### Case Study: FIRMS

Experiment setup Attack overview Affecting the der dataset

Exploiting the decoder

Countermeasure

Future work

Conclusio

## Exploiting the decoder

Packet structure

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



./spppack





#### Motivation Challenges

Implications
Threat mode

Attacker capabiliti

## Case Study: FIRMS

Attack overview
Affecting the deri
dataset

Exploiting the decoder

Countermeasures

Future work

Conclusion

## Exploiting the decoder





## Motivation Challenges Implications

Threat model Attacker capabilitie

## Case Study: FIRMS

Attack overview
Affecting the der

Exploiting the decoder

Countermeasures

**Future work** 

Conclusion

## Exploiting the decoder



## SSL Systems Security Lat

Motivation
Challenges
Implications
Threat model

Attacker capabilitie

Case Study:

#### FIRMS

Attack overview
Affecting the deriv

Exploiting the decoder

Countermeasures

Future work

Conclusion

## Exploiting the decoder



## SSL Systems Security Lat

Motivation
Challenges
Implications
Threat model

Attacker capabilitie

Case Study:

## FIRMS Experiment setu

Attack overview
Affecting the deriv

Exploiting the decoder

Countermeasures

Future work

Conclusion

## Exploiting the decoder

```
$ printf %1337s | tr
  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:
  MYDOOF, A2015299, 2110, 20152992235, 001, PDS
```





# Motivation Challenges Implications Threat model

Attacker capabilitie

Case Study:

#### FIRMS

Attack overview

Affecting the derividateset

Exploiting the decoder

Countermeasures

Future work

Conclusion

## Exploiting the decoder

```
$ printf %1337s | tr
  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:
  MYDOOF, A2015299, 2110, 20152992235, 001, PDS
### Running modisl1db l1a-geo initial processing
10fix_modis: Unrecoverable error in 10fix_modis!
```





# Motivation Challenges Implications Threat model

Threat model Attacker capat

## Case Study:

Experiment setup
Attack overview
Affecting the deriv

Exploiting the decoder

Countermeasures

Future work

Conclusion

## Exploiting the decoder

Attack consequences

```
$ printf %1337s | tr
  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:
  MYDOOF, A2015299, 2110, 20152992235, 001, PDS
### Running modisl1db l1a-geo initial processing
10fix_modis: Unrecoverable error in 10fix_modis!
```

Further vulnerabilities have been discovered since submission



## Systems Secu

#### Motivation

Implication

Threatme

Attacker capabiliti

#### Case Study:

Attack overview

Affecting the derive dataset

xploiting the decor

#### Countermeasures

Future wor

Conclusion

## Countermeasures

Cryptography should be required in future satellites



Challenges Implications

Threat mod

Attacker capabiliti

Case Study:

FIRMS

Attack overview

Affecting the derive dataset

Countermeasures

Future worl

Conclusion

## Countermeasures

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



#### Motivation Challenges

Implications
Threat model

Attacker capabiliti

## Case Study: FIRMS

Attack overview
Affecting the derividataset
Exploiting the decident

Countermeasures

Future work

Conclusion

### Countermeasures

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

Backwards-compatible countermeasures:



## Motivation Challenges Implications

implications Threat model Attacker capabili

Case Study:

Experiment setu

Affecting the derive dataset Exploiting the decoc

Countermeasures

**Future work** 

Conclusion

## Countermeasures

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

Backwards-compatible countermeasures:

Multi-receiver data comparison



## Motivation Challenges Implications

Threat model Attacker capabilitie

Case Study:

FIRMS

Attack overview
Affecting the derived
dataset
Exploiting the decode

Countermeasures

**Future** work

Conclusion

### Countermeasures

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

Backwards-compatible countermeasures:

- Multi-receiver data comparison
- Timing analysis<sup>2</sup>

<sup>&</sup>lt;sup>2</sup> Jedermann et. al. (2021) "Orbit-based Authentication Using TDOA Signatures in Satellite Networks"



### Countermeasures

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

Backwards-compatible countermeasures:

- Multi-receiver data comparison
- Timing analysis<sup>2</sup>
- Physical-layer fingerprinting<sup>3</sup>

## Challenges Implications Threat model

Threat model Attacker capabilitie

Case Study:

Experiment setup Attack overview

Affecting the derived dataset Exploiting the decode

Countermeasures

**Future work** 

Conclusion

<sup>&</sup>lt;sup>2</sup> Jedermann et. al. (2021) "Orbit-based Authentication Using TDOA Signatures in Satellite Networks"

<sup>&</sup>lt;sup>3</sup>Oliqeri et. al. (2022) "PAST-AI: Physical-Layer Authentication of Satellite Transmitters via Deep Learning"



### Countermeasures

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

Backwards-compatible countermeasures:

- Multi-receiver data comparison
- Timing analysis<sup>2</sup>
- Physical-layer fingerprinting<sup>3</sup>

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

## Motivation Challenges

Implications Threat model Attacker capabilitie

Case Study:

Experiment setup
Attack overview

Attack over view Affecting the derived dataset Exploiting the decoder

Countermeasures

Future work

Conclusion

<sup>&</sup>lt;sup>2</sup> Jedermann et. al. (2021) "Orbit-based Authentication Usina TDOA Signatures in Satellite Networks"

<sup>&</sup>lt;sup>3</sup> Oligeri et. al. (2022) "PAST-Al: Physical-Layer Authentication of Satellite Transmitters via Deep Learning"



Challenge Implicatio

Threat mode

Attacker capabilit

#### Case Study:

Experiment set Attack overview

Affecting the deri dataset

Exploiting the decod

Countermeasures

**Future work** 

Conclusion

## Future research directions

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



### Case Study:

Countermeasures

**Future work** 

Conclusion

## Future research directions

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

Future research is required to:



Challenges Implications Threat model

Attacker capabiliti

Case Study:

Attack overview
Affecting the derived dataset

Countermeasures

Future work

Conclusion

## 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



Challenges Implications Threat model

rnreat modei Attacker capabiliti

### Case Study:

Attack overview

Affecting the deri

Affecting the derived dataset Exploiting the decode

Countermeasures

**Future work** 

Conclusion

## 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



#### Motivation Challenges

Implications
Threat model

Case Study:

#### Experiment setup Attack overview

Affecting the derived dataset Exploiting the decode

Countermeasures

**Future work** 

Conclusion

## 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



## Systems Secu

#### Motivation

tombination

---

Attacker capabilitie

\_ \_ \_

#### FIRMS

Attack overview

Affecting the der dataset

Exploiting the decod

Countermeasure

Future work

Conclusion

## Conclusion



### Conclusion

#### We have...

 demonstrated viable spoofing attacks against NASA's forest fire detection system.

## Motivation Challenges

Threat model
Attacker capabilitie

Case Study:

Attack overview
Affecting the deridataset
Exploiting the dec

Countermeasure

Future wor

Conclusion



mplications hreat model stacker capabilities

Attacker capabilities

Case Study:

Attack overview
Affecting the derived dataset
Exploiting the decode

Countermeasures

**Future work** 

Conclusion

## Conclusion

- demonstrated viable spoofing attacks against NASA's forest fire detection system.
- provided the source code required to manipulate the packet data and structure.



#### Motivation Challenges

mplications hreat model attacker capabilities

Attacker capabilitie

Case Study:

Attack overview
Affecting the derive
dataset
Exploiting the decor

Countermeasures

**Future work** 

Conclusion

## Conclusion

- 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.



#### Challenges Implications

mplications Threat model Attacker capabilities

Case Study:

Attack overview Affecting the deriv dataset

Countermeasures

**Future work** 

Conclusion

## Conclusion

- 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.



Challenges

implication

Attacker capabilitie

Case Study:

#### FIRMS

Experiment set

Affecting the de

Exploiting the decod

Countermeasures

Future work

Conclusion

## Thank you for your attention

Any questions?

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