

# 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



Challenges

Implication:

Attacker capabili

## Case Study

Experiment set

Affecting the derive dataset

Countermeasure

Conclusion

# Challenges of unauthenticated satellites

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



#### Challenges

Implications

Attacker canabilit

## Case Study:

FIRMS

Attack overview

Affecting the deriv

Exploiting the decode

Countermeasures

Conclusion

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



#### Challenges

Implications

Attacker capabilit

# Case Study: FIRMS

Experiment sets

Attack overview Affecting the deriv dataset

Countermeasures

Conclusion

- Many current satellites do not encrypt the downlink, due to:
  - Increased power budget and costs
  - Open access data



### Challenges

Implications

Attacker capabiliti

## Case Study: FIRMS

Attack overview

Affecting the deriv

Countermeasures

Conclusion

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



### Challenges

Implications

Attacker capabilit

## Case Study:

Attack overview

Affecting the deriv
dataset

Exploiting the decoder

Countermeasures

Conclusion

- Many current satellites do not encrypt the downlink, due to:
  - Increased power budget and costs
  - Open access data
  - Legacy systems backwards compatibility
- Other satellites are decryptable, due to:



## Challenges

Implications

Attacker capabilit

## Case Study:

Experiment setup Attack overview Affecting the derive dataset

Exploiting the decoder

Countermeasures

Conclusion

- Many current satellites do not encrypt the downlink, due to:
  - Increased power budget and costs
  - Open access data
  - Legacy systems backwards compatibility
- Other satellites are decryptable, due to:
  - Insecure cryptosystems <sup>1</sup>

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



### Challenges

Implications
Threat model

Case Study:

## FIRMS

Experiment setup Attack overview Affecting the derive dataset

Countermeasures

Conclusion

- Many current satellites do not encrypt the downlink, due to:
  - Increased power budget and costs
  - Open access data
  - Legacy systems backwards compatibility
- 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://vksdr.com/lrit-key-dec/

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



#### Motivation Challenges

Implications Threat model

Case Study:

## FIRMS

Attack overview
Affecting the deriv

Countermeasures

Conclusion

# Challenges of unauthenticated satellites

Insecure Earth Observation Satellites

Satellites with insecure downlinks include:

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



Challenges Implications

Threat model Attacker capabiliti

Case Study:

FIRMS
Experiment setu

Attack overview

Affecting the derived

Countermeasures

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



# Challenges of unauthenticated satellites

Insecure Earth Observation Satellites

#### Challenges Implications

Threat model

Case Study:

## FIRMS

Attack overview
Affecting the derive
dataset

Countermeasures

Conclusion

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

Further details available in the paper



# SSL Systems Security Lab

#### Motivation

#### Motivati

#### Implications

Threat model

Attacker capabil

### Case Study

Evporiment cat

Experiment se

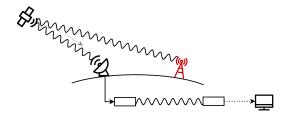
Affecting the deriv

. .

Conclusion

# Implications

Data secrecy





#### MOLIVALIC

#### Implications

Case Study:

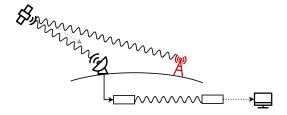
## FIRMS

Attack overview
Affecting the derividataset

Conclusion

# Implications

Data secrecy



Using an SDR and open source software, attackers can:



#### MOLIVALIC

Implications

Threat model

Attacker capab

## Case Study:

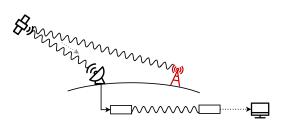
Experiment setup Attack overview Affecting the deriv dataset

Countermeasures

Canalusia

# 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"



#### Motivatio

Implications

Threat model

. . .

# Case Study: FIRMS

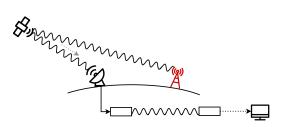
Attack overview
Affecting the deriv

Countermeasures

Conclusio

# 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



SSL Systems Security La

#### Motivation

#### Motivatio

#### Implications

i nreat model

Attacker capab

#### Case Study FIRMS

Experiment set

Affacting the dark

dataset

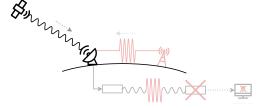
. .

Countermeasure

Conclusion

# **Implications**

Data authenticity and integrity





SSL Systems Security Lab

#### Motivation

#### Motivatio

#### Implications

Illieat model

Case Study

## FIRMS

Experiment set

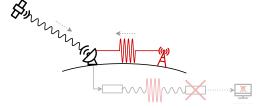
Affecting the deriv

Englisher de de la col

Conclusion

# **Implications**

Data authenticity and integrity





# SSL Systems Security Lat

#### Motivation

#### Motivatio

#### Implications

inreat model

C--- C4...4.

## FIRMS

Experiment set

Attack overview

Affecting the deriv

Affecting the deriv dataset

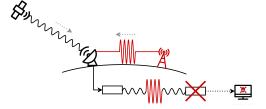
Exploiting the decode

Countermeasures

Conclusion

# **Implications**

Data authenticity and integrity





#### Motivatio

#### Implications

i nreat model

ricuenci capab

### FIRMS

Experiment setu

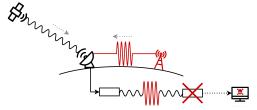
Attack overview Affecting the deriv dataset

Exploiting the decoc

Conclusion

# Implications

Data authenticity and integrity



Spoofing attacks have been shown against:



## Systems Sec

### Motivation

Implications

Attacker conch

Case Study:

## FIRMS

Attack overview
Affecting the derive dataset

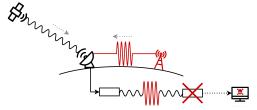
Exploiting the decoc

Countermeasure

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"



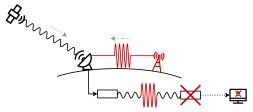
Implications

### Case Study:

Countermeasures

# **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> Motallebiqhomi et. al. (2022) "Cryptography Is Not Enough: Relay Attacks on Authenticated GNSS Signals" <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"



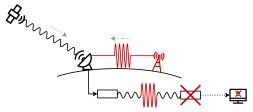
Implications

Case Study:

Countermeasures

# **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> Motallebiqhomi 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

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



#### Motivatio

Implications

Attacker capabil

Case Study:

### FIRMS

Attack overview

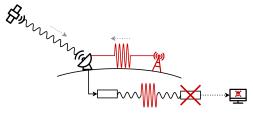
Affecting the derive dataset

Countermeasures

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?

<sup>&</sup>lt;sup>1</sup> Motallebighomi et. al. (2022) "Cryptography Is Not Enough: Relay Attacks on Authenticated GNSS Signals" <sup>2</sup>"2011 REPORT TO CONGRESS of the U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION" p.223–224

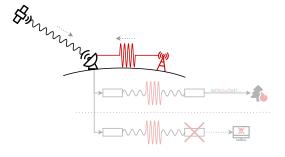
<sup>&</sup>lt;sup>3</sup> Broadcasting (1986) "'Captain Midnight' unmasked"



Threat model

Conclusion

# Threat model



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



Challenge

Threat model

Attacker capab

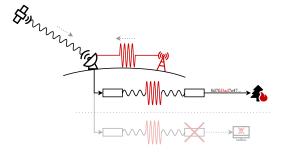
## Case Study

Experiment setup Attack overview Affecting the deriv dataset

Countermeasures

Conclusion

# Threat model



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

• Affect the satellite-derived datasets



Challenge

Threat model

Attacker capab

## Case Study:

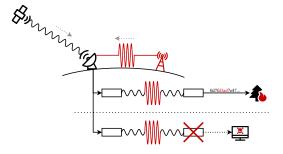
Attack overview

Affecting the deriv

Countermeasures

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



Implications
Threat model
Attacker capabilities

Case Stud

### FIRMS

Experiment setup Attack overview Affecting the deriv dataset

Exploiting the decode

Countermeasure

Conclusion

# Attacker capabilities

Hardware component	Cost
limeSDR	598 USD
X-Band upconverter	100 USD <sup>1</sup>
X-Band amplifier	$1,638\mathrm{USD}$
Compatible antenna	431 USD
Total	$3,000\mathrm{USD}$

<sup>&</sup>lt;sup>1</sup> Estimated price from self-built amateur radio equipment



Threat model

Attacker capabilities

Case Stud

### FIRMS

Attack overview

Affecting the deriv

Exploiting the decode

Countermeasure

Conclusion

# Attacker capabilities

Hardware component	Cost
limeSDR	598 USD
X-Band upconverter	100 USD <sup>1</sup>
X-Band amplifier	$1,638\mathrm{USD}$
Compatible antenna	431 USD
Total	$3,000\mathrm{USD}$

<sup>&</sup>lt;sup>1</sup> Estimated price from self-built amateur radio equipment



Implications
Threat model
Attacker capabilities

Caco Stud

### Case Stud

Attack overview

Affecting the derive
dataset

Exploiting the decode

Countermeasure

Conclusion

# Attacker capabilities

Hardware component	Cost
limeSDR	598 USD
X-Band upconverter	100 USD <sup>1</sup>
X-Band amplifier	$1,638\mathrm{USD}$
Compatible antenna	431 USD
Total	$3,000\mathrm{USD}$

<sup>&</sup>lt;sup>1</sup>Estimated price from self-built amateur radio equipment



Implications
Threat model
Attacker capabilities

Case Stud

FIRMS

Attack overview

Affecting the deri

Exploiting the decode

Countermeasure

Conclusion

# Attacker capabilities

Hardware component	Cost
limeSDR	598 USD
X-Band upconverter	100 USD <sup>1</sup>
X-Band amplifier	$1,638\mathrm{USD}$
Compatible antenna	431 USD
Total	$3,000\mathrm{USD}$

<sup>&</sup>lt;sup>1</sup> Estimated price from self-built amateur radio equipment



Implications
Threat model
Attacker capabilities

Case Stud

### FIRMS

Attack overview

Affecting the deriv

Exploiting the decode

Countermeasure

Conclusion

# Attacker capabilities

Hardware component	Cost
limeSDR	598 USD
X-Band upconverter	100 USD <sup>1</sup>
X-Band amplifier	$1,638\mathrm{USD}$
Compatible antenna	431 USD
Total	$3,000\mathrm{USD}$

<sup>&</sup>lt;sup>1</sup> Estimated price from self-built amateur radio equipment



Implications
Threat model
Attacker capabilities

Caco Stud

#### Case Study

Attack overview

Affecting the deriv
dataset

. .

Conclusion

# Attacker capabilities

Estimated cost

Hardware component	Cost
limeSDR	598 USD
X-Band upconverter	100 USD <sup>1</sup>
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>Estimated price from self-built amateur radio equipment



### Madiusk

Motivation

Challenges

Threat model

Attacker capab

# Case Study: FIRMS

Experiment setup

Attack overvie

Cuplaiting the deer

Countermeasures

Conclusio

# 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.



Implicatio

Threat model

Attacker capab

Case Study:

# FIRMS Experiment setup

Attack overview
Affecting the der

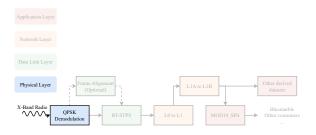
Exploiting the decor

Countermeasures

Conclusion

# Case Study: Forest fire detection in FIRMS

Experiment setup



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/



Implication

Threat model Attacker capab

## Case Study:

FIRMS
Experiment setup

Attack overview Affecting the de

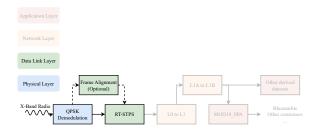
Exploiting the decor

Countermeasures

Conclusion

# Case Study: Forest fire detection in FIRMS

Experiment setup



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/



Implication

Threat model Attacker capab

## Case Study:

# FIRMS Experiment setup

Attack overview
Affecting the der

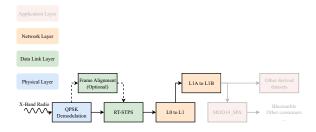
Exploiting the decod

Countermeasures

Conclusion

# Case Study: Forest fire detection in FIRMS

Experiment setup



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/



Implicati

Threat model

Case Study:

## FIRMS

Attack overview

dataset

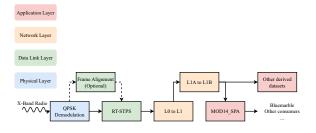
Exploiting the decod

Countermeasures

Conclusion

# Case Study: Forest fire detection in FIRMS

Experiment setup



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/



#### ivio civa ci

Implicati

Threat model

Attacker capabili

# Case Study: FIRMS

rnoriment se

Attack overview

Affacting the day

dataset

Conclusion

# Attack overview

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

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



#### MOLIVALIO

Implications

Attacker canabilit

# Case Study:

IIIIII

Attack overview

Affecting the der

dataset

Exploiting the decode

Countermeasures

Conclusio

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

<sup>1</sup> https://ladsweb.modaps.eosdis.nasa.gov/archive/

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



Challenges

Threat model

Case Study:

### FIRMS

Experiment se

Attack overview Affecting the de

dataset

Countermeasures

Conclusio

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

<sup>1</sup>https://ladsweb.modaps.eosdis.nasa.gov/archive/

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



Challanger

Implications

Threat model Attacker capabilit

#### Case Study: FIRMS

Experiment set

Attack overview

Affecting the deriv

Endowe do londo

Countermeasures

Conclusion

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

https://directreadout.sci.gsfc.nasa.gov/, with an academic account



Implications

Threat model Attacker capabilit

#### Case Study: FIRMS

Experiment sets

Attack overview

Affecting the deriv

Exploiting the decoder

Countermeasures

Conclusion

- 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
- Process data to add/remove artifacts<sup>3</sup>

<sup>1</sup> https://ladsweb.modaps.eosdis.nasa.gov/archive/

<sup>2</sup>https://directreadout.sci.gsfc.nasa.gov/, with an academic account

<sup>&</sup>lt;sup>3</sup>Code provided in the paper



Implications
Throat model

Threat model Attacker capabili

#### Case Study: FIRMS

Experiment setu

Attack overview

Affecting the derive

Exploiting the decode

Countermeasures

Conclusion

- 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
- Process data to add/remove artifacts<sup>3</sup>
  - Edit image format to insert fictitious data

<sup>1</sup> https://ladsweb.modaps.eosdis.nasa.gov/archive/

<sup>2</sup>https://directreadout.sci.gsfc.nasa.gov/, with an academic account

<sup>&</sup>lt;sup>3</sup>Code provided in the paper



Implications
Threat model

Attacker capabili

#### Case Study: FIRMS

Experiment setup
Attack overview

dataset

loiting the decode

Countermeasures

Conclusion

- 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
- Process data to add/remove artifacts<sup>3</sup>
  - Edit image format to insert fictitious data
  - Construct payload packet to trigger vulnerability chain

<sup>1</sup> https://ladsweb.modaps.eosdis.nasa.gov/archive/

<sup>2</sup>https://directreadout.sci.gsfc.nasa.gov/, with an academic account

<sup>&</sup>lt;sup>3</sup>Code provided in the paper



#### Case Study: **FIRMS**

Affecting the derived dataset

Conclusion

# Affecting the derived dataset Packet structure

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



#### Case Study: **FIRMS**

Affecting the derived dataset

Conclusion

# Affecting the derived dataset Packet structure

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



#### Case Study: **FIRMS**

Affecting the derived dataset

Conclusion

# Affecting the derived dataset

Packet structure

Prima			Secondary	Header		Data Zone								
	Packet Length	Time Tag		Packet Type	Scan Count	Mirror Sid	ie	F	rame (	Count .	. Da	ta Field		Checksum
								Data Field						
								IR Ban	id	IR Band		IR Band		IR Band



# Case Study:

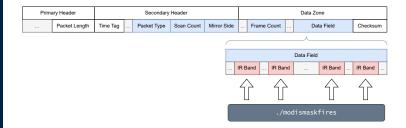
## **FIRMS**

Affecting the derived dataset

Conclusion

# Affecting the derived dataset

Packet structure





# Affecting the derived dataset

Attack consequences



Original image.

# SSL Systems Security Lab

# Motivation

Challenge

Threat model

Attacker capabili

#### Case Study: FIRMS

Experiment se

Attack overview

Affecting the derived dataset

Exploiting the decod

. .

Countermeasure



# Affecting the derived dataset

Attack consequences



### Motivation

Challenge

Threat model

Attacker capabil

# Case Study: FIRMS

Experiment se

Attack overview

Affecting the derived dataset

Exploiting the decod

Countermeasu



Masking existing fires.



# Affecting the derived dataset

Attack consequences



### Challenges

Challenges Implication

Threat model

Case Study:

# FIRMS

Experiment se

Affecting the derived dataset

Exploiting the decod

Countermeasure



Fine-grained control over fire injection.



#### Motivati

Challenges

Throat mode

Attacker capabili

#### Case Study: FIRMS

Experiment setu

Affecting the derive dataset

Exploiting the decoder

Countermeasure

Conclusion

# 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



#### Motivati

Implications

Threat model

Attacker capabili

#### Case Study: FIRMS

Experiment setup Attack overview

dataset

Exploiting the decoder

. .

Conclusion

# Exploiting the decoder

Prim	1 IIIIIe		Secondary	Header			Data Zone	Data Zone			
		Packet Length	Time Tag	 Packet Type	Scan Count	Mirror Side	 Frame Count	 Data Field	Checksum		



#### Case Study: **FIRMS**

Exploiting the decoder

Conclusion

# Exploiting the decoder Packet structure

D-4- 7---

FIIII	ary neader		Secondary	neadel		Data Zone				
	Packet Length	Time Tag	Packet Type	Scan Count	Mirror Side		Frame Count		Data Field	Checksum
	Î	Î								

0----



#### Case Study: FIRMS

Exploiting the decoder

Conclusion

# Exploiting the decoder

Attack consequences

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





Challenges

Threat model

Attacker capabiliti

# Case Study: FIRMS

Attack overview

Affecting the deriv

dataset Exploiting the decoder

Countermeasures

Conclusion

# Exploiting the decoder

Attack consequences



# SSL Systems Security Lab

#### Motivation

Implication:

Threat model Attacker capabiliti

# Case Study: FIRMS

Attack overview
Affecting the derive

Exploiting the decoder

Countermeasures

Conclusion

# Exploiting the decoder

Attack consequences

CONTAINER\_RUNTIME: docker



# SSL Systems Security Lab

### Motivation

Implication

Threat model Attacker capabilit

# Case Study: FIRMS

Attack overview

Affecting the derive dataset

Exploiting the decoder

Countermeasures

Conclusion

# 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



# SSL Systems Security Lab

## Motivation

Implications Threat model

Case Study:

# FIRMS

Attack overview

Affecting the deriver dataset

dataset Exploiting the decoder

Countermeasures

Conclusion

# Exploiting the decoder

Attack consequences

```
$ ./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!



Challeng

Threat model

Attacker capabil

## Case Study

Experiment setu

Affecting the derive dataset

. . . . . . . .

Countermeasures

Conclusion

# Countermeasures

Cryptography should be required in future satellites



#### MOLIVALIO

Implicat

Threat model

## FIRMS

Attack overview
Affecting the derived dataset

Countermeasures

Conclusion

# Countermeasures

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



Challenges

Threat model

## Case Study:

Attack overview

Affecting the deriver dataset

Countermeasures

Conclusion

# Countermeasures

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

Backwards-compatible countermeasures:



Implications
Threat model

Threat model Attacker capabiliti

# Case Study: FIRMS

Attack overview
Affecting the derivi

Countermeasures

Conclusion

# Countermeasures

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

Backwards-compatible countermeasures:

Multi-receiver data comparison



Implications
Threat model

Case Study:

FIRMS

Attack overview

Affecting the derived dataset

Exploiting the decode

Countermeasures

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"



Case Study:

Countermeasures

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>
- Physical-layer fingerprinting<sup>3</sup>

<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> Oligeri et. al. (2022) "PAST-AI: Physical-Layer Authentication of Satellite Transmitters via Deep Learning"



Challenges Implications

Attacker capabilit

# Case Study: FIRMS

Experiment setup Attack overview Affecting the derived dataset

Countermeasures

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>
- Physical-layer fingerprinting<sup>3</sup>

Comparative analysis presented in the paper

<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>Oligeri et. al. (2022) "PAST-Al: Physical-Layer Authentication of Satellite Transmitters via Deep Learning"



# Conclusion

Our paper...

### Motivation



Conclusion

# Conclusion

# Our paper...

presents a demonstration of byte-level spoofing against NASA's forest fire detection system.



Implications
Threat model

Case Study:

# FIRMS

Attack overview Affecting the deriv dataset

Countermeasures

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.



Case Study:

Countermeasures

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.



Implications
Threat model

Case Study:

# FIRMS

Attack overview
Affecting the derive dataset

Countermeasures

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.



#### Challers

Implicat

Threat model

### Case Study

# FIRMS

Attack overview

Affecting the de dataset

. .

Conclusion

# Thank you for your attention

Any questions?

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