UNIVERSITY OF OXFORD

SSL
Systems Security Lab

Firefly: Spoofing Earth Observation Satellites through Radio Overshadowing

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

[1] Systems Security Lab, University of Oxford

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

Trinity Term 2022

Challenges of unauthenticated satellites

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

Challenges of unauthenticated satellites

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

Challenges of unauthenticated satellites

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

Challenges of unauthenticated satellites

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

Challenges of unauthenticated satellites

- 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 of unauthenticated satellites

- 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 [1]

[1] COMS-1 uses single DES `https://vksdr.com/lrit-key-dec/`

Challenges of unauthenticated satellites

- 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 [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

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

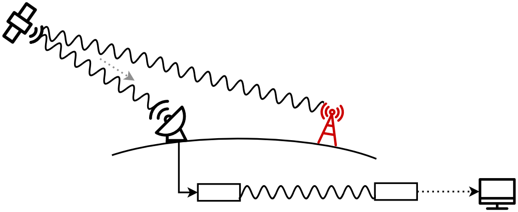
Satellites with insecure downlinks include:

- **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

Implications

Data secrecy

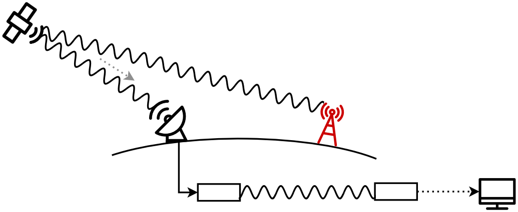


UNIVERSITY OF OXFORD

SSL
Systems Security Lab

Implications

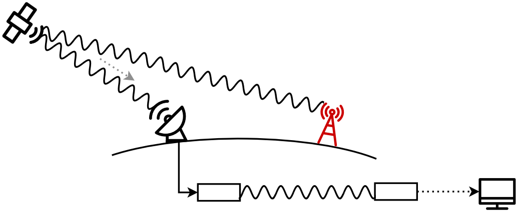
Data secrecy



Using an SDR and open source software, attackers can:

Implications

Data secrecy



Using an SDR and open source software, attackers can:

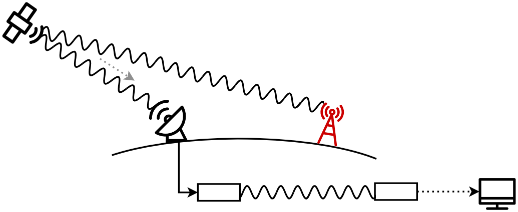
- Read confidential maritime data[1] and internet traffic[2]

[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*"

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]

---

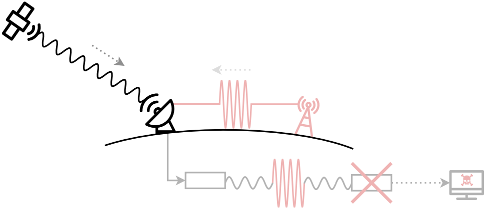
[1] Pavur et al. (2020) "*A Tale of Sea and Sky on the Security of Maritime VSAT Communications*"

[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`

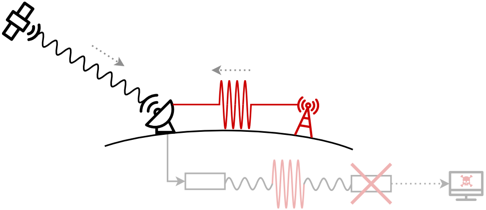
Implications

Data authenticity and integrity



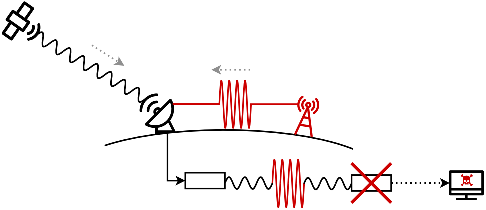
Implications

Data authenticity and integrity



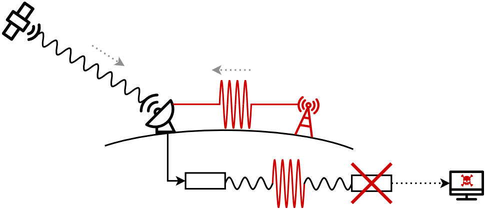
Implications

Data authenticity and integrity



Implications

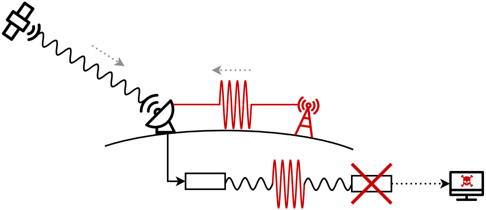
Data authenticity and integrity



Spoofing attacks have been shown against:

Implications

Data authenticity and integrity



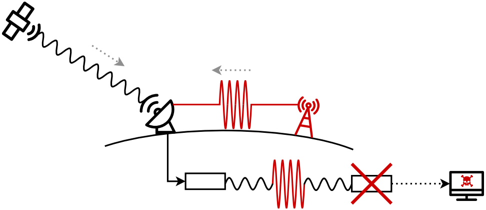
Spoofing attacks have been shown against:

- GNSS to manipulate calculated location[1]

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

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]

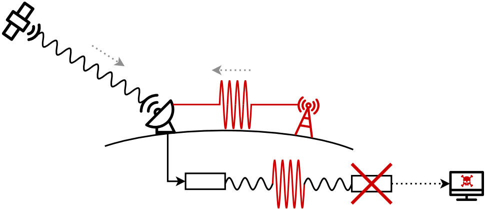
[1] Motallebighomi et. al. (2022) "*Cryptography Is Not Enough: Relay Attacks on Authenticated GNSS Signals*"

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

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

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

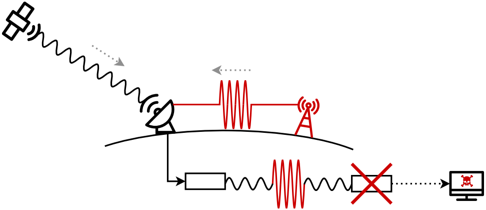
[1] Motallebighomi et. al. (2022) "*Cryptography Is Not Enough: Relay Attacks on Authenticated GNSS Signals*"

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

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

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

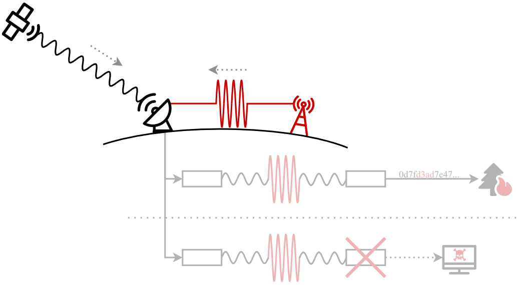
RQ: What can the attacker achieve by exploiting the unauthenticated channel?

[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

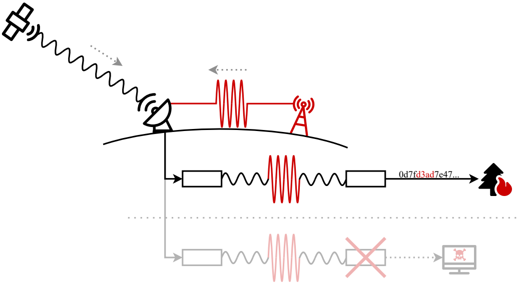
[3] Broadcasting (1986) "*'Captain Midnight' unmasked*"

Threat model



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

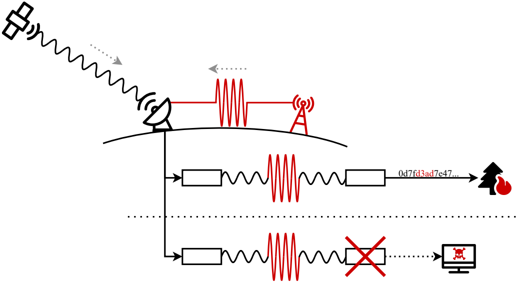
Threat model



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

- Affect the satellite-derived datasets

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**
limeSDR	598 USD
X-Band upconverter	100 USD[1]
X-Band amplifier	1,638 USD
Compatible antenna	431 USD
Total	3,000 USD

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

Attacker capabilities

Estimated cost

Hardware component	Cost
limeSDR	598 USD
X-Band upconverter	100 USD[1]
X-Band amplifier	1,638 USD
Compatible antenna	431 USD
Total	3,000 USD

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

Attacker capabilities
Estimated cost

Hardware component	**Cost**
limeSDR	598 USD
X-Band upconverter	100 USD[1]
X-Band amplifier	1,638 USD
Compatible antenna	431 USD
Total	3,000 USD

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

Attacker capabilities

Estimated cost

Hardware component	**Cost**
limeSDR	598 USD
X-Band upconverter	100 USD[1]
X-Band amplifier	1,638 USD
Compatible antenna	431 USD
Total	3,000 USD

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

Attacker capabilities

Estimated cost

Hardware component	**Cost**
limeSDR	598 USD
X-Band upconverter	100 USD[1]
X-Band amplifier	$1,638$ USD
Compatible antenna	431 USD
Total	$3,000$ USD

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

Attacker capabilities

Estimated cost

Hardware component	Cost
limeSDR	598 USD
X-Band upconverter	100 USD[1]
X-Band amplifier	$1,638$ USD
Compatible antenna	431 USD
Total	$3,000$ USD

Within the budget of a motivated hobbyist

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

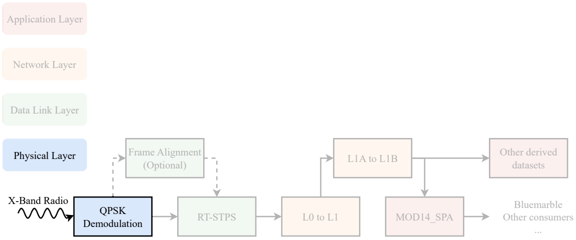
Case Study: Forest fire detection in FIRMS

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

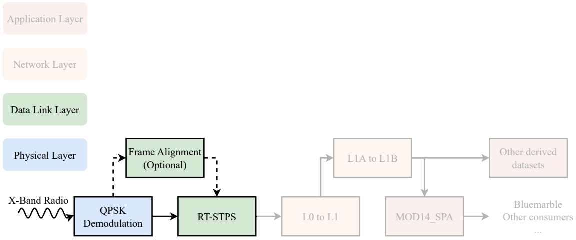
Experiment setup



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/`

Case Study: Forest fire detection in FIRMS

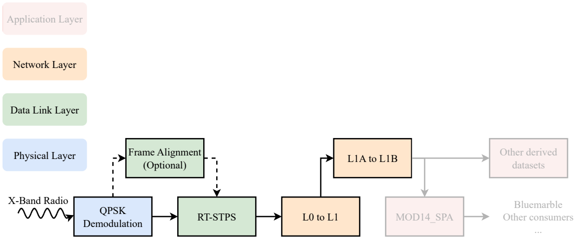
Experiment setup



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/`

Case Study: Forest fire detection in FIRMS

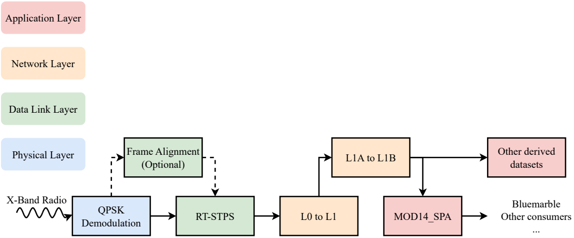
Experiment setup



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/`

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/`

Attack overview

- Obtain legitimate data from digital archive[1]

[1] `https://ladsweb.modaps.eosdis.nasa.gov/archive/`

Attack overview

- Obtain legitimate data from digital archive[1]
- Perform security audit on downlink decoder software[2]

[1] `https://ladsweb.modaps.eosdis.nasa.gov/archive/`

[2] `https://directreadout.sci.gsfc.nasa.gov/`, with an academic account

Attack overview

- Obtain legitimate data from digital archive[1]
- Perform security audit on downlink decoder software[2]
  - Determine data integrity checks

[1] `https://ladsweb.modaps.eosdis.nasa.gov/archive/`

[2] `https://directreadout.sci.gsfc.nasa.gov/`, with an academic account

Attack overview

- 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

[1] `https://ladsweb.modaps.eosdis.nasa.gov/archive/`

[2] `https://directreadout.sci.gsfc.nasa.gov/`, with an academic account

Attack overview

- 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
- Process data to add/remove artifacts[3]

---

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

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

3 Code provided in the paper

Attack overview

- 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
- Process data to add/remove artifacts[3]
  - Edit image format to insert fictitious data

[1] `https://ladsweb.modaps.eosdis.nasa.gov/archive/`

[2] `https://directreadout.sci.gsfc.nasa.gov/`, with an academic account

[3] Code provided in the paper

Attack overview

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

[1] `https://ladsweb.modaps.eosdis.nasa.gov/archive/`

[2] `https://directreadout.sci.gsfc.nasa.gov/`, with an academic account

[3] Code provided in the paper

Affecting the derived dataset

Packet structure

<table>
<tr><td colspan="2">Primary Header</td><td colspan="6">Secondary Header</td><td colspan="6">Data Zone</td></tr>
<tr><td>...</td><td>Packet Length</td><td>Time Tag</td><td>...</td><td>Packet Type</td><td>Scan Count</td><td>Mirror Side</td><td>...</td><td>Frame Count</td><td>...</td><td>Data Field</td><td>Checksum</td></tr>
</table>

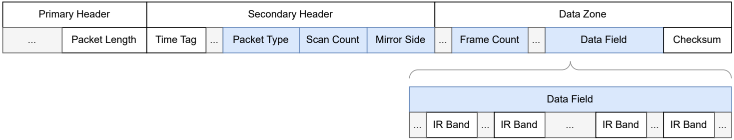
Affecting the derived dataset

Packet structure

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

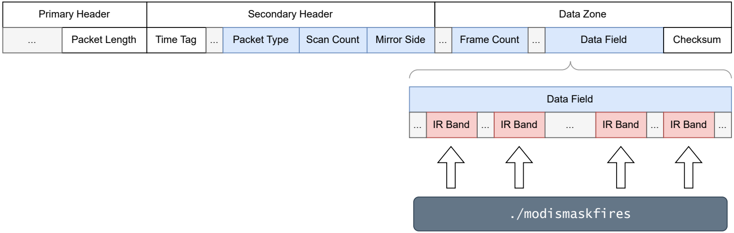
Affecting the derived dataset

Packet structure



Affecting the derived dataset

Packet structure

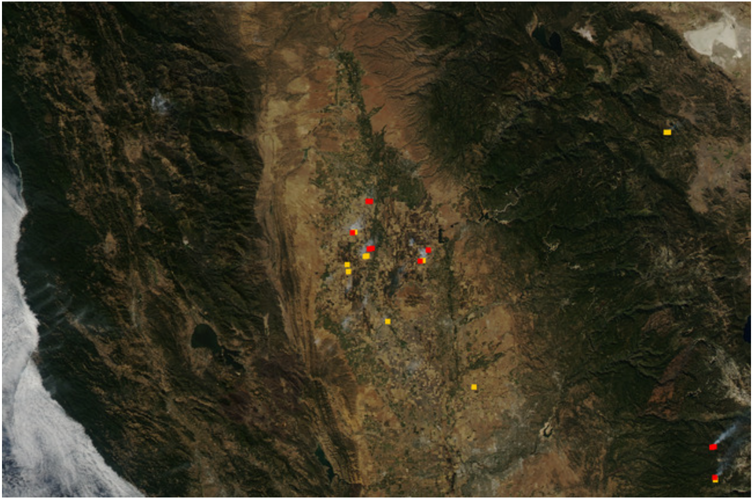


UNIVERSITY OF OXFORD

SSL
Systems Security Lab

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

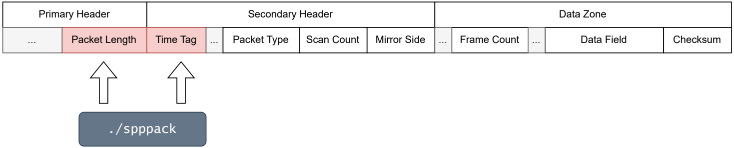
Exploiting the decoder

Packet structure

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

Exploiting the decoder

Packet structure



Exploiting the decoder

Attack consequences

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

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
```

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
```

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
```

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!
```

Countermeasures

Cryptography should be required in future satellites

Countermeasures

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

Countermeasures

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

Backwards-compatible countermeasures:

Countermeasures

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

Backwards-compatible countermeasures:

- Multi-receiver data comparison

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]

[2] 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[2]
- Physical-layer fingerprinting[3]

---

[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*"

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]

Comparative analysis presented in the paper

[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*"

Conclusion

Our paper...

Conclusion

Our paper...

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

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.

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.

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.

Thank you for your attention

Any questions?

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