2023-02-27

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]

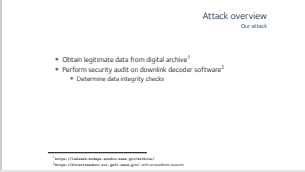
[1] Systems Security Lab, University of Oxford
[2] Cyber-Defence Campus, armasuisse Science + Technology

Although satellite data is increasingly relied upon, many satellites don't have authenticated downlinks, which opens the door for spoofing attacks. My name's Edd Salkield, and I'm from the Systems Security Lab at the University of Oxford. I'm presenting Firefly, an analysis of the vulnerability and effects of spoofing attacks against current Earth observation satellite systems. In particular, we'll consider the effects of a motivated, modern adversary against NASSA's real-time forest fire API.

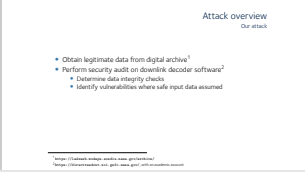
The current situation in space is that…

All the tools used in our attack will be published alongside our paper

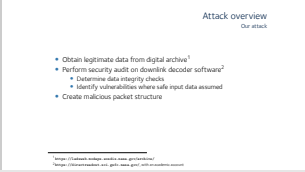
All the tools used in our attack will be published alongside our paper



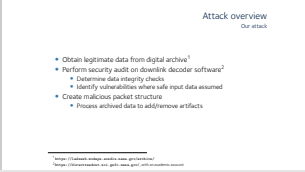
All the tools used in our attack will be published alongside our paper



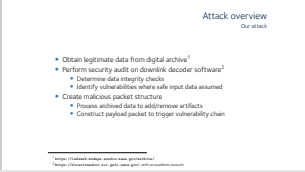
All the tools used in our attack will be published alongside our paper



All the tools used in our attack will be published alongside our paper



All the tools used in our attack will be published alongside our paper



All the tools used in our attack will be published alongside our paper

Cryptography should be required in future satellites

We discuss the countermeasures in context

Multi-receiver data comparison

- Certain systems already have multiple receiver stations
- Protects against decoder exploitation
- Doesn't require any hardware modifications to the receiver

Timing analysis

- Triangulating the source effective in other systems such as aircraft
- Calculated position can be compared against orbital parameters
- Requires accurate clock synchronisation and multiple receivers

Physical-layer fingerprinting

- Analyse properties of the legitimate/overshadowed signal
- Only effective on the downlink

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

We discuss the countermeasures in context

Multi-receiver data comparison

- Certain systems already have multiple receiver stations
- Protects against decoder exploitation
- Doesn't require any hardware modifications to the receiver

Timing analysis

- Triangulating the source effective in other systems such as aircraft
- Calculated position can be compared against orbital parameters
- Requires accurate clock synchronisation and multiple receivers

Physical-layer fingerprinting

- Analyse properties of the legitimate/overshadowed signal
- Only effective on the downlink

Countermeasures

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

Backwards-compatible countermeasures:

We discuss the countermeasures in context

Multi-receiver data comparison

- Certain systems already have multiple receiver stations
- Protects against decoder exploitation
- Doesn't require any hardware modifications to the receiver

Timing analysis

- Triangulating the source effective in other systems such as aircraft
- Calculated position can be compared against orbital parameters
- Requires accurate clock synchronisation and multiple receivers

Physical-layer fingerprinting

- Analyse properties of the legitimate/overshadowed signal
- Only effective on the downlink

Countermeasures

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

Backwards-compatible countermeasures:
- Multi-receiver data comparison

We discuss the countermeasures in context

Multi-receiver data comparison

- Certain systems already have multiple receiver stations
- Protects against decoder exploitation
- Doesn't require any hardware modifications to the receiver

Timing analysis

- Triangulating the source effective in other systems such as aircraft
- Calculated position can be compared against orbital parameters
- Requires accurate clock synchronisation and multiple receivers

Physical-layer fingerprinting

- Analyse properties of the legitimate/overshadowed signal
- Only effective on the downlink

└Countermeasures

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) "DVB-Vessel Authentication Using TDOG Signatures in Satellite Networks"

We discuss the countermeasures in context

Multi-receiver data comparison

- Certain systems already have multiple receiver stations
- Protects against decoder exploitation
- Doesn't require any hardware modifications to the receiver

Timing analysis

- Triangulating the source effective in other systems such as aircraft
- Calculated position can be compared against orbital parameters
- Requires accurate clock synchronisation and multiple receivers

Physical-layer fingerprinting

- Analyse properties of the legitimate/overshadowed signal
- Only effective on the downlink

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) "DVB-Vessel Authentication Using TDOA Signatures in Satellite Networks"
[3] Degen et. al. (2022) "NIST: AI: Physical Layer Authentication of Satellite Transmitters via Deep Learning"

We discuss the countermeasures in context

Multi-receiver data comparison

- Certain systems already have multiple receiver stations
- Protects against decoder exploitation
- Doesn't require any hardware modifications to the receiver

Timing analysis

- Triangulating the source effective in other systems such as aircraft
- Calculated position can be compared against orbital parameters
- Requires accurate clock synchronisation and multiple receivers

Physical-layer fingerprinting

- Analyse properties of the legitimate/overshadowed signal
- Only effective on the downlink

└Countermeasures

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

Backwards-compatible countermeasures:

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

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

[2] Jedermann et. al. (2017) "DVB-Vessel Authentication Using TDOA Signatures in Satellite Networks"
[3] Degen et. al. (2022) "REFI-AI: Physical Layer Authentication of Satellite Transmitters via Deep Learning"

We discuss the countermeasures in context

Multi-receiver data comparison

- Certain systems already have multiple receiver stations
- Protects against decoder exploitation
- Doesn't require any hardware modifications to the receiver

Timing analysis

- Triangulating the source effective in other systems such as aircraft
- Calculated position can be compared against orbital parameters
- Requires accurate clock synchronisation and multiple receivers

Physical-layer fingerprinting

- Analyse properties of the legitimate/overshadowed signal
- Only effective on the downlink

Future research directions

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

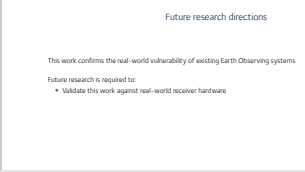
Review of vulnerable satellites: dovetails with other conference work e.g. SAR systems

Future research directions

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

Future research is required to:

Review of vulnerable satellites: dovetails with other conference work e.g. SAR systems



Review of vulnerable satellites: dovetails with other conference work e.g. SAR systems

Review of vulnerable satellites: dovetails with other conference work e.g. SAR systems

Review of vulnerable satellites: dovetails with other conference work e.g. SAR systems