Edd Solfeidf ¹ Joshus Smalles ¹ Sebastian Köhler ¹ Simon Birnbach ¹ Richard Baker ¹ Martin Strohmeier ² Ivan Martinovic ¹ ¹Symma Security List, University of Oxford ²Cyber-Oxforce Comput, armassian 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...

¹ kerge://ladeath.milege.emdis.nam.grs/s

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

Attack overview

Ohtain lenitimate data from dinital archive¹

tys://kalesch.molega.amdis.nam.gov/archina/

Obtain legitimate data from digital archive¹
 Perform security audit on downlink decoder software²

Attack overview

ps://ladewh.nologe.undis.nasa.gov/arthina/ ps://kinetreadov.nti.gols.nasa.gov/.nih.anadovic.noonti

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

Attack overview

- Perform security audit on downlink decoder software²

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

Attack overview

- Obtain legitimate data from digital archive¹
 Perform security audit on downlink decoder software²
 - Determine data integrity checks
 Identify vulnerabilities where safe input data assumed

pr//indexh misps smilis nam gr/arshirs/

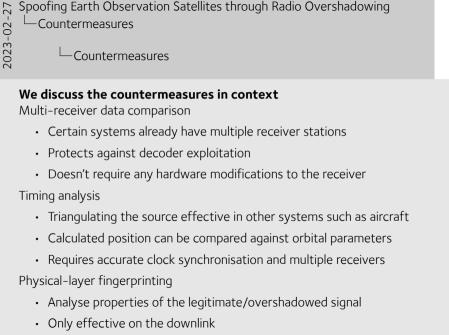
2023-02-

. Ohtain lenitimate data from dinital archive 1 Perform security audit on downlink decoder software²

 Determine data integrity checks Identify vulnerabilities where safe input data assumed

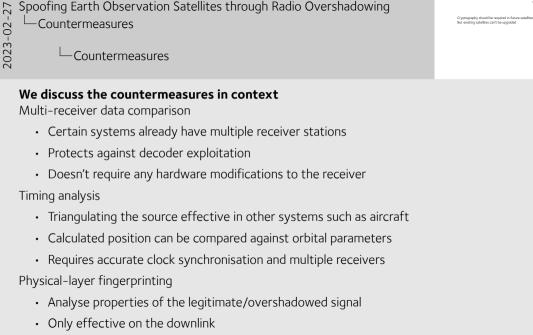
. Process archived data to additemous artifacts Construct payload packet to tripper vulnerability chain

. Create malicious packet structure

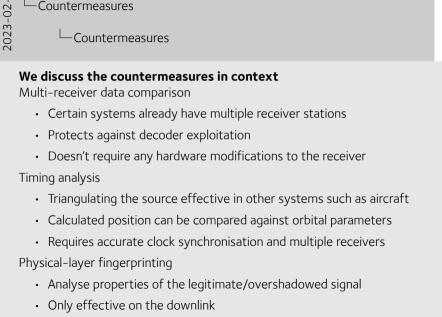


Countermeasures

Cruntography should be required in future satellites



Countermeasures



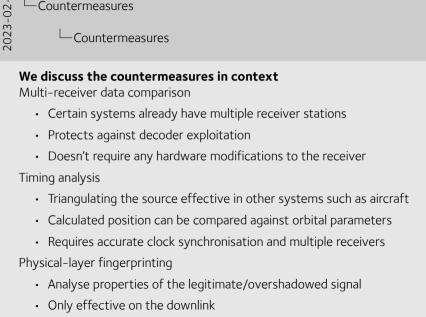
Spoofing Earth Observation Satellites through Radio Overshadowing

Countermeasures

Cruntography should be required in future satellites

But existing satellites can't be upgraded

Backwards-compatible countermeasures

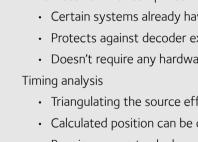


Spoofing Earth Observation Satellites through Radio Overshadowing

But existing satellites can't be upgraded Backwards-compatible countermeasure: • Multi-receiver data comparison

Cruntography should be required in future satellites

Countermeasures



Countermeasures

Countermeasures

2023-02

Cruntography should be required in future satellites But existing satellites can't be upgraded Backwards-compatible countermeasures: Multi-receiver data comparison Timing analysis²

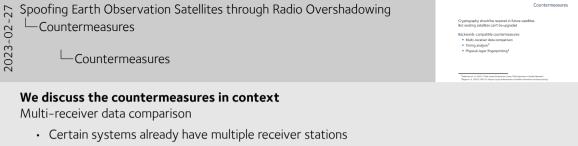
Countermeasures

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

Spoofing Earth Observation Satellites through Radio Overshadowing

- - 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



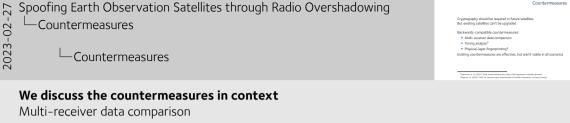
- Protects against decoder exploitation
- Doesn't require any hardware modifications to the receiver

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

nequires decurate cloc

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



- 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

Obvisical layor fingerprinting

- 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

Future research is required to:

Future research directions

and a standard and a

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

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
 Compethensively review other unlearable satellites

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