# Spread Spectrum Satcom Hacking

## Attacking the Globalstar Simplex Data Service

Colby Moore
@colbymoore - colby@synack.com

# Motivation

- Satellite hacking talks never deliver
- RF world largely neglected by hacker community
- So much legacy tech in critical systems
- Spark interest in satellite security research

# What are we going to learn?

- Overview of basic RF signals and modulation
- What is spread spectrum - how does it work and how do we work with it
- Picking a target and reverse engineering it
- Exploiting that target
- Next steps

# Analog RF Modulation

- Amplitude Modulation (AM)
- Frequency Modulation (FM)

# Digital RF Modulation

- Amplitude Shift Keying (ASK / OOK)
- Frequency Shift Keying (FSK)
- **Phase Shift Keying (PSK)**

# Spread Spectrum Modulation

- What is Spread Spectrum Special?  WiFi, Bluetooth, Most modern RF Communication

# Spread Spectrum Modulation

- Frequency Hopping Spread Spectrum (FHSS)
- Direct Sequence Spread Spectrum (DSSS)

# Selecting a Target

- Consumer Accessible
- Cheap
- Popular
- High Impact

# Introducing SPOT

- SPOT

- But wait… this tech is used… everywhere. Goldmine.

# Who uses it?

- Flight Planning Services
- Consumers
- SCADA
- Big Gas and Oil

# How does it work?

- LEO non-geosynchronous Bend Pipe Architecture

# Intel Gathering

- Google
- FCC Database
- Academic Papers
- Integrator Spec Sheets

# Intel Gathering Continued

- What we know:
- PN = 255 Chip M-Sequence
- 1.6xx ghz
- 144 bit message

# Hardware and Validation

- USRP B200
- GQRX
- GNURADIO

# Decoding Theory

- Mix signal with PN sequence and the BPSK signal will drop out

# Packet Format Contd.

- Wait a second… There is no signing… No encryption.

- We can create packets if we known how to reproduce the checksum.

- Reverse engineering the checksum

# Transmitting

- Strictly Theoretical - Do not attempt

- This is the easy part

# Impact of Transmission

- Spoof communications
- Disrupt critical services

# Signal Interception Demo

- DEMO

# Future Research

- Code optimization
- Custom hardware
- Widespread reception

# Slides and Code

- Updated slides, resources, and code to be posted online after the presentation.