SSL
Systems Security Lab

Firefly: New Experimental Design

Edd Salkield [1] Joshua Smailes [1] Richard Baker [1]
Martin Strohmeier [2] Ivan Martinovic [1]

[1] Systems Security Lab, University of Oxford

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

Michaelmas Term 2022

SSL
Systems Security Lab

Firefly 2.0

Research questions

Understanding the barriers to entry for signal injection attacks against the downlink

What are the main factors to consider regarding…

- an attacker getting their signal into the victim antenna?
- an attacker knowing that their signal will cause the intended harm?
- the downstream effects that an attacker can expect to cause?

Firefly: overall paper structure

Experimental method

(1) Validate antenna attenuation model in the real world

(2) Understand how common protocols/decoders are weak to downlink injection

(3) End-to-end attack demonstration through amateur radio satellite

(4) Analyse downstream attack consequences

Section 1: Validate antenna attenuation model

Summary

Validate antenna attenuation model and understand the key factors affecting injection capability

Emit amateur-frequency signals at various antennas in real world settings and measure the gain/SNR

SSL
Systems Security Lab

Section 1: Physical layer

Experiment: Out-of-band angular emission

Method:

- Set up several antenna types in a real world setting
- Emit repeated, distinct legal out-of-band signals at the dish in amateur frequency bands
- Filter down to just the band that we emit, and measure signal gain before/after emission

SSL
Systems Security Lab

Section 1: Physical layer

Experiment: Out-of-band angular emission

Outcomes:

- A number of meaurements of gain/SNR in multiple injection settings
- Compare against the polar plots we get from simulation
- Understand how accurately the model lets an attacker estimate equipment needed beforehand

SSL
Systems Security Lab

Section 2: Analyse weak protocols

Summary

Outcome: Understand how common protocols/decoders are weak to injection on the downlink

Summary: Reverse several protocols/decoders to determine packets that break things if injected

Proposed work:

- Terra/Aqua (completed)
- Johannes' decoders
- Meteosat
- Iridium packets

SSL
Systems Security Lab

Section 3: End-to-end attack demonstration

Summary

Outcome: End-to-end attack to understand the key protocol factors affecting injection capability

Summary: Overshadow reflected bent-pipe signal from QO-100 or equivalent at antenna gains calibrated to mirror the real-world setup, causing erroneous bytes to be decoded

SSL
Systems Security Lab

Section 3: End-to-end attack demonstration

Experiment: overshadowing amateur satellite

Method:

- Create encoded physical-layer satellite signals
- Modulate the signals onto the uplink
- Overshadow the downlink with a calibrated signal
- Pipe the resulting decoding software into modems/decoding software

Section 3: End-to-end attack demonstration

Transmitting

Section 3: End-to-end attack demonstration

Overshadowing

Requirements:

- SDR (already in lab)
- X-band upconverter
- Amplifier

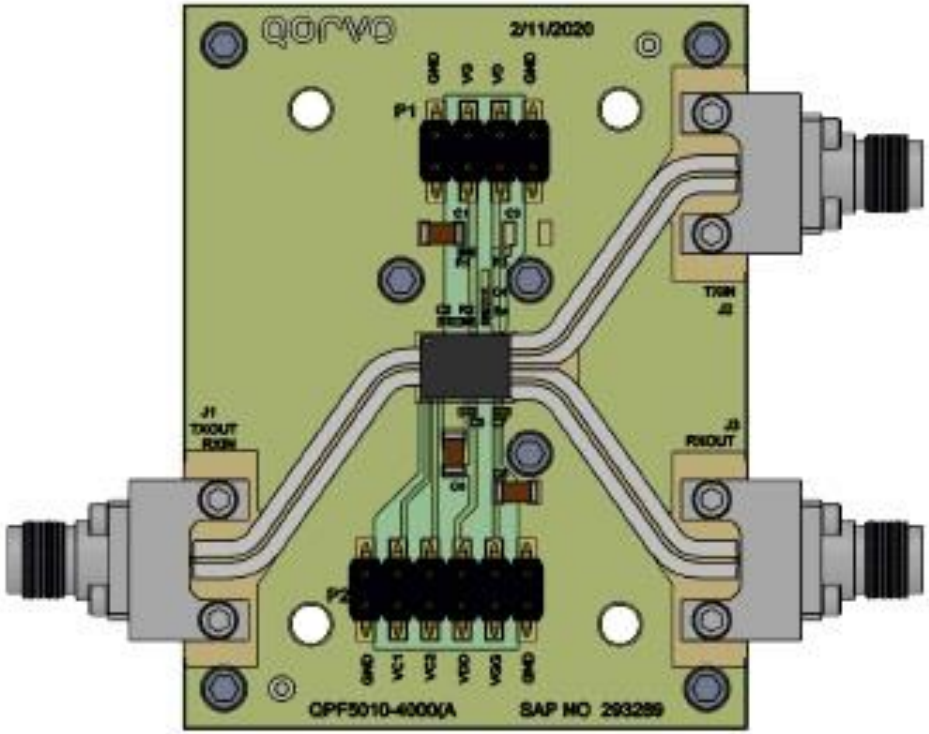
Options:

- COTS Dartcom X-Band system: 90,000GBP[1]
- Qorvo QPF5005EVB1: 1600GBP
- Qorvo QPF5005: 200GBP

[1] https://www.dartcom.co.uk/products/x-band-eos-system/technical-summary

Section 3: End-to-end attack demonstration

Overshadowing



Section 3: End-to-end attack demonstration

Receiving