RF Replay

The Short Version

RF replay attacks should be a dead meme but, like Rick Rolling, just won't die. It involves intercepting the remote control signal, recording it and replaying it. The code is always the same and there's no validation.

The Long Version

These alarms have remotes. They use **fixed (AKA static) codes**, where the **code doesn't change.** They are **vulnerable to replay attacks**.

Rolling codes are where the **code changes every time** using an algorithm shared between transmitter and receiver. A **used code is invalidated** once used. Any **modern system** should use rolling codes. Ideally, the system should also use **encryption and bidirectional communication** between remote and receiving unit.

Note that trying to attack systems with rolling codes risks causing remotes to go out of sync with the receiver unit. This should be considered like lock picking where you only test systems you have permission to test and aren't relied upon. Styx Security has a policy which states if you want us to test a live system, a service engineer must be available to rectify any problems.

Even though the alarms here use static codes, there are actually quite a lot of steps:

1) First you have to figure out the frequency and modulation in use.
2) Then you have to intercept the correct arm/disarm/silence signal.
3) You may have to try this several times.
4) Then you can replay it.

You therefore need **several transmissions** to do this with the **Flipper** and this kind of limitation is why it's **not a serious tool for enabling criminals**. Software defined radios can do all of this far quicker. They lack a Dolphin and require far greater knowledge and skill, however.

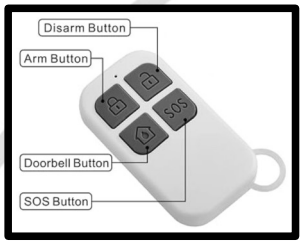
There are several transmitters and alarms on which to try a replay attack.

Enquiries@StyxSecurity.org

We don't knock.

Raw Replay - Flipper

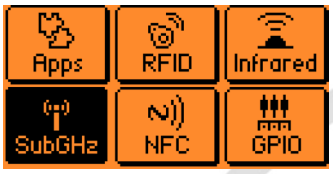
RF Replay



You'll need the remote and the corresponding alarm. They are labelled.

Pick a signal to clone. I suggest disarm.

1

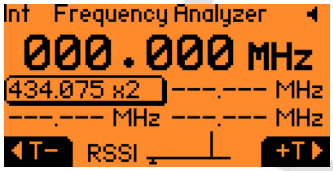


1. Open SubGHz

2

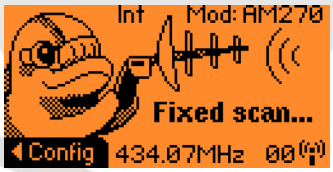
2. Select Frequency Analyzer

3



3. Press remote and find frequency. Look for high RSSI as this environment likely has a few transmitters. Select the right frequency.

4

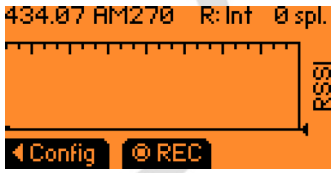


4. You can try this, it won't work on these remotes.

5

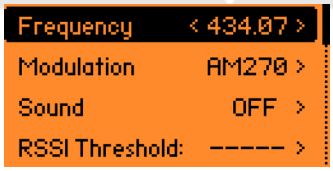
5. Press back and select "read RAW"

6



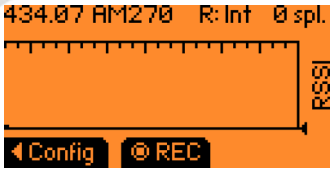
6. On this page select "config"

7



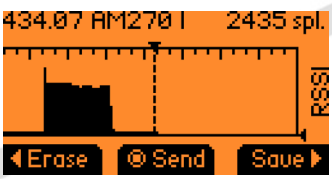
7. The settings should be like this. Press "back".

8



8. Press "REC" and press the remote button.

9



9. Ensure you capture the whole signal.

10

10. Send it!

Enquiries@StyxSecurity.org

We don't knock.

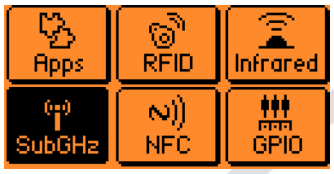
Replay Attack - Flipper

RF Replay

You'll need the remote.

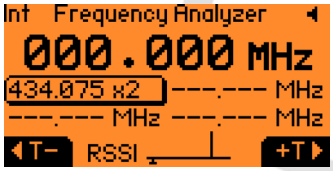
The receiver for this exercise is in the black box with the LED strips.

This one activates red and blue LEDs.

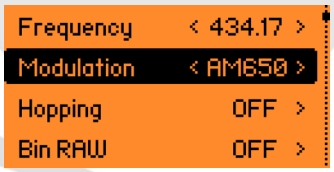


1. Open SubGHz

2. Select Frequency Analyzer

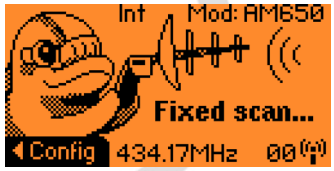


3. Press remote and find frequency. Look for high RSSI as this environment likely has a few transmitters. Select the right frequency.



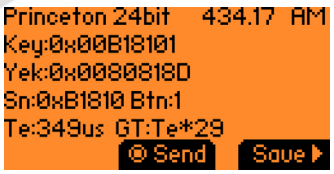
4. You'll need to change the modulation to AM650.

5. Press back and select "read"



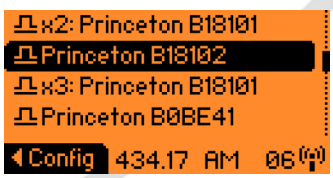
6. It's now receiving. Press buttons on remotes to capture.

7. You'll get a list of signals you have captured.



8. Select a signal to see more.

9. Press the middle button to replay the signal.



10. Save a few signals and look through them to see the differences.

Enquiries@StyxSecurity.org

We don't knock.

IR Replay - Flipper

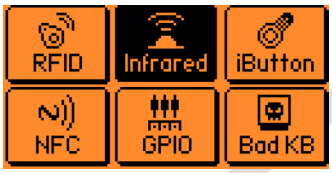
IR Replay

You'll need the remote.

The receiver for this exercise is the PIR alarm.

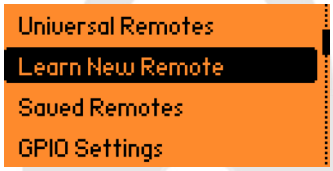
This remote arms and disarms it.

1



1. Open Infrared

2



2. Select Learn New Remote

3

3. Keep the remote a few centimetres from the IR sensor on the Flipper (black rectangle).

4

4. Keep the remote a few centimetres from the sensor on the Flipper.

5

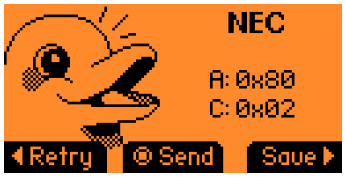
5. You may have to press the remote several times before it captures.

6

6. Press centre button to send and see if it works.

You will probably find the alarm is toggled on and off repeatedly.

The Flipper doesn't recognise the remote (e.g. right), which simply doesn't behave as expected.



The Flipper is a multitool and there are better tools out there for almost everything it does.

It's a balance of power and accessibility.

Enquiries@StyxSecurity.org

We don't knock.