ESP Key

The Short Version

The ESP key sits between reader and door controller, intercepting the communication. It has a WiFi interface. We can collect information to make our own cards, replay cards already presented and DOS the reader to stop it working.

The Long Version

The ESP key **taps into four wires** – positive, negative, D0 and D1.

It doesn't need the positive to read, but it uses it to **steal power from the system**.

It works as **a MITM attack**, reading all the data that comes from the reader and is sent to the door controller. In a **Wiegand based system**, all the fancy cryptographic operations happen within the reader and the **data is sent** to the controller in the **same format as in the 1970s**.

As a result, we can pop a reader off the wall, tap into the wires and collect all the card reads that go through.

There are **tamper systems** on the readers but often they **aren't connected** and, if they are, it's not hard to look up the model and figure out how to bypass. **Security screws** can be used but you can usually get the bits from Aldi.

The ESP Key can **intercept** the Wiegand data, **replay** it and also try to **disable a door**.

The reader connected to the ESP Key is marked. You can see the wires on the **back of the reader board.**

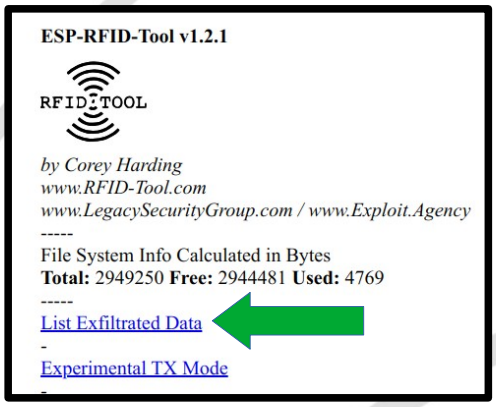
There is a laptop connected to the ESP key. You can scan cards and replay them – the door will open.

Try the ESP Key on the laptop.

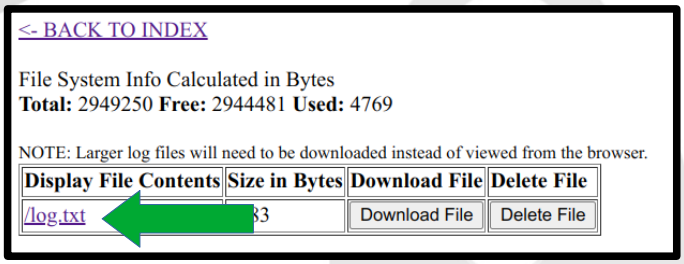
Enquiries@StyxSecurity.org

We don't knock.

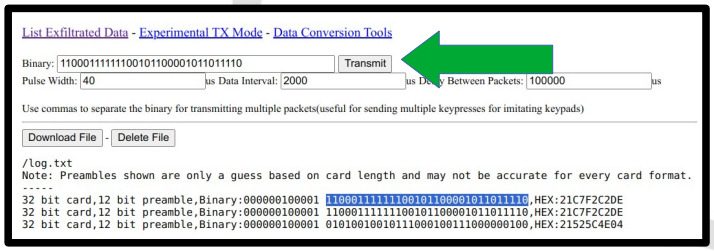
Intercept and Replay ESP Key



Go to the home page for the ESP key and click “**List Exfiltrated Data**”



Click on the **log file** to open it.

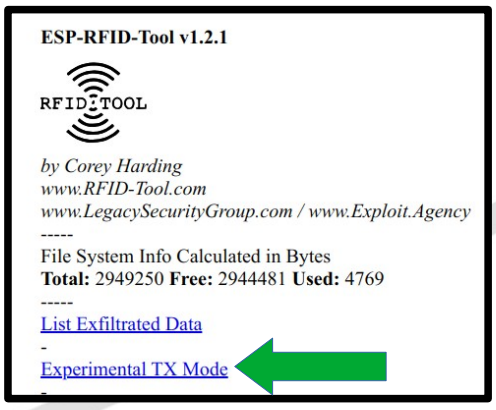


Present a card to the reader with the ESP key and **refresh** the page.

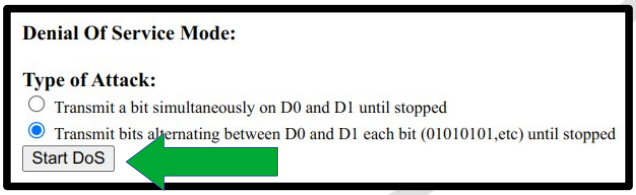
You’ll see the intercepted data appear on the list. You can **copy the binary data** into the box and **transmit** it. The door should open.

Denial of Service

Please don’t leave this running.



When you start the DOS attack, the reader will not be able to communicate with the controller. The door can’t be unlocked.



Enquiries@StyxSecurity.org

We don’t knock.