BINGHAMTON
UNIVERSITY
STATE UNIVERSITY OF NEW YORK

Final Project

Replay attack on the ID card reader

Professor Emrah Akyol

Mohsen Hatami

22nd Dec 2022

Before any survey on the possibility of a reply attack and reading data of an ID card, it is important to deep into RFID since ID cards are considered RFID tags and work in the HF radio frequency band to analyze the possibility of reading data from a long distance from ID cards.

What is RFID?

RFID is an acronym for "radio-frequency identification" and refers to a technology whereby digital data encoded in RFID tags or smart labels (defined below) are captured by a reader via radio waves. RFID is analogous to barcoding therein data from a tag or label are captured by a tool that stores the information in a very database. RFID, however, has several advantages over systems that use barcode asset tracking software. The foremost notable is that RFID tag data will be read outside the road of sight, whereas barcodes must be aligned with an optical scanner.

How does RFID work?

RFID could be a group of technologies called Automatic Identification and Data Capture (AIDC). AIDC methods automatically identify objects, collect data about them, and enter those data directly into computer systems with little or no human intervention. RFID methods utilize radio waves to accomplish this. At a straightforward level, RFID systems include three components: an RFID tag or smart label, an RFID reader, and an antenna. RFID tags contain a computer circuit and an antenna, which are wont to transmit data to the RFID reader (also called an interrogator). The reader then converts the radio waves to a more usable kind of data. Information collected from the tags is then transferred through a communications interface to a bunch automatic data processing system, where the information is often stored in an exceedingly database and analyzed at a later time.

RFID frequency options for passive chip tags

Chip tags are usually made to work at specific frequencies which are license free. These are:

- Low Frequency (LF) 125-135 KHz
- High Frequency (HF) 13.56 MHz
- Ultra-High Frequency (UHF) 868-930 MHz
- Microwave 2.45 GHz
- Microwave 5.8 GHz

All have various advantages and disadvantages and affect not only the performance and size of the tag but also the price of the tags and readers. Further, the tolerated power levels and regulations for these vary from country to country. For example, the maximum permitted legal power level (the power level at which the interrogator is set) for 2.45 GHz in the USA is higher than in Europe. This creates a difference in read range.

Low-frequency (LF) Tags

The low-frequency range includes frequencies from 30 to 300 KHz but only 125 KHz and 134 KHz (actually, 134.2 KHz) are used for RFID. This range has been in use for RFID tags for animal tracking since 1979 and is the most mature range in use. It is available for RFID use all over the world. The tags in this range are generally called LF tags. They use near-field inductive coupling to obtain power and communicate with the interrogator. The LF tags are passive (no battery and transmitter on the tag) and have a short read range of a few inches. They have the lowest data transfer rate among all the RFID frequencies and usually store a small amount of data. The LF tags have no or limited anti-collision capabilities; therefore, reading multiple tags simultaneously in the IZ is impossible or very difficult. The tag antennas are usually made of a copper coil with hundreds of turns wound around a ferrous core. They are expensive to manufacture, and

tags using them are thicker than others at higher frequencies. The LF tags can be easily read while attached to objects containing water, animal tissues, metal, wood, and liquids.

LF tags have the largest installed base. They are used in access control, asset tracking, animal identification, automotive control, vehicle immobilizers, healthcare, and various point-of-sale applications (such as Mobil/Exxon SpeedPass). The automotive industry is the largest user of LF tags. For example, in an automobile vehicle immobilizer system, an LF tag is embedded inside the ignition key. When that key is used to start the car, an RFID interrogator placed around the key slot reads the tag ID. If the tag ID is correct, the car can be started. If the ID is incorrect or no tag is found, the car cannot be started.

High-Frequency (HF) Tags

The high-frequency range includes frequencies from 3 to 30 MHz but only one frequency, 13.56 MHz, is used for RFID applications. This frequency is now available for RFID applications worldwide with the same power level. Tags and interrogators using 13.56 MHz are generally called HF tags and HF interrogators. They, like the LF tags, also use near-field inductive coupling to obtain power and communicate with the interrogator. HF tags are passive tags and have a short read range, of less than 3 feet. They have a lower data transfer rate than the UHF frequencies but a higher data rate than the LF. The HF tags may have anti-collision capability that facilitates the reading of multiple tags simultaneously in the IZ. Since the read range of many HF tags and interrogators is small, they usually do not implement anti-collision. This reduces the complexity and cost. Some HF tags can store up to 4K of data. HF tags are more mature than UHF tags and many standards are in place.

Ultra-High Frequency (UHF) Tags

The ultra-high frequency range includes frequencies from 300 to 1000 MHz, but only two frequency ranges, 433 MHz and 860–960 MHz are used for RFID applications. The 433 MHz frequency is used for active tags, while the 860–960 MHz range is used mostly for passive tags and some semi-passive tags. The frequency range of 860–960 MHz is often referred to as a single frequency of 900 or 915 MHz. Tags and interrogators in this range are called UHF tags and UHF interrogators. The passive and the semi-passive tags in this frequency range use far-field radiative coupling or backscatter coupling. The UHF tags have a read range of about 15 to 20 feet. All the protocols in the UHF range have some type of anti-collision capability, allowing multiple tags to be read simultaneously in the IZ. The new Gen 2 protocol for UHF tags is designed for reading several hundred tags per second. UHF interrogators are usually costlier than HF interrogators, but UHF tags are becoming more economical.

The UHF tag antennas are usually made of copper, aluminum, or silver deposited on the substrate. Their effective length is approximately 6.5 inches, which is approximately equal to one-half the wavelength of 900 MHz radio waves. The optimum length of a UHF antenna is equal to one-half the wavelength of the carrier wave, though, with proper design, the length can be reduced. The UHF antennas are thin and easy to manufacture, allowing tags to be very thin, less than 100mm, and almost two-dimensional. The UHF tags cannot be easily read while attached to objects containing water and animal tissues because water absorbs UHF waves. The UHF tags get detuned when they are attached to metal objects. Separating UHF tags from metal objects or objects with liquid improves their performance. UHF tags cannot be read if water or any conductive material is placed between the interrogator antenna and the tags.

Microwave Tags

The microwave frequency range includes frequencies from 1 to 10 GHz, but only two frequency ranges around 2.45 GHz and 5.8 GHz are used for RFID applications. Almost all microwave tags use 2.45 GHz. Microwave tags are available as passive, semi-passive, and active types. The passive and semi-passive tags

use backscatter coupling to communicate with interrogators, and active types use their transmitters to communicate. Passive microwave tags are usually smaller than passive UHF tags and have the same read range of about 15 feet. The semi-passive microwave tags have a read range of about 100 feet, while the active microwave tags have a read range of about 350 feet. Passive microwave tags, due to low demand, are more expensive than passive UHF tags, but they share the same advantages and disadvantages. Only a few manufacturers make this type of tag. Japan is the largest user of passive microwave tags.

Frequency Bands	Antenna	Data & Speed	Read Range	Usage
Low Frequency (LF) 125 kHz – 134 kHz	Induction Coil on Ferrite Core, or flat many turns	Low Read Speeds – Small Amount of Data (16 bits)	Short to Medium 3-5 feel	– Access Control – Animal Tagging – Inventory Control – Car Immobilizer
High Frequency (HF) 13.56 MHz	Induction Coil flat 3-9 turns	Medium Read Speed Small to Medium Amounts of Data	Short 1-3 feet	– Smart Cards – Item or Case level Tagging – Proximity Cards – Vicinity Cards
Very High Frequency (VHF) 433 Mhz – Active Tags	Internal Custom Design	High Read Speed Large Amount of Data	High 1-1000 feet	– Asset Tracking – Locationing – Container Tracking
Ultra-High Frequency (UHF) 860 MHz – 960 MHz	Single or Double Dipole	High Read Speed Small to Medium Amount of Data	Medium 1-30 feet	– Pallet or Case Level Tagging – DOD & Walmart Mandates
Microwave Frequency 2.45 GHz & 5.4 GHz	Single Dipole	High Read Speed Medium Amount of Data	High 1-300 feet	– Container Rail Car – Auto Toll Roads – Pallet Level Tracking

Table1. RFID tag characteristics overview based on the frequency

RFID Tags and Smart Labels

As stated above, an RFID tag consists of a computer circuit and an antenna. The tag is additionally composed of a protective material that holds the pieces together and shields them from various environmental conditions. The protective material depends on the appliance. for instance, employee ID badges containing RFID tags are typically made up of durable plastic, and also the tag is embedded between layers of plastic. RFID tags are available in a spread of shapes and sizes and are either passive or active. Passive tags are the foremost widely used, as they're smaller and less expensive to implement. Passive tags must be “powered up” by the RFID reader before they'll transmit data. Active RFID tags have an onboard power supply, enabling them to transmit data in the least bit of time.

Smart labels differ from RFID tags in this they incorporate both RFID and barcode technologies. They’re products of an adhesive label embedded with an RFID tag inlay, and they may additionally feature a barcode and/or other printed information. Smart labels are often encoded and printed on-demand using desktop label printers, whereas programming RFID tags are more time-consuming and need more advanced equipment.

RFID Applications

RFID technology is used in many industries to perform such tasks as:

- Inventory management
- Asset tracking
- Personnel tracking
- Controlling access to restricted areas
- ID Badging
- Supply chain management
- Counterfeit prevention
- RFID APPLICATIONS

The demand for RFID equipment is increasing rapidly, all around the world specially by companies tracking their products by using RFID. Whether or not RFID compliance is required, applications that currently use barcode technology are good candidates for upgrading to a system that uses RFID or some combination of the 2. RFID offers many advantages over the barcode, particularly the fact that an RFID tag can hold far more data about an item than a barcode can. additionally, RFID tags don't seem to be liable for the damages which will be incurred by barcode labels, like ripping and smearing.

How to read the info on an RFID tag from a protracted distance for UHF and Microwave band frequency?

Some hardware is intended to maximize read range, while others are designed to limit read range. it's important to own the acceptable hardware in situ for the application. Six important factors must be taken into consideration for hardware.

Antenna Gain: First and foremost, the more read range, the upper the gain antennas. Vice versa, the less read range, the lower the gain antennas.

> **The details:** Simply put, a better gain antenna increases the facility received from the reader. Some environments and applications require a tightly controlled configuration. for instance, in systems where the tag will always be the identical short distance far from the antenna, a high-gain antenna simply isn't needed. In short, the upper the gain, the upper the range of the antenna, and vice-versa. Additionally, lower-gain antennas are smaller in size than high-gain antennas.

Antenna Polarization: If tags are aligned with the antenna's polarization, linear polarized antennas will read farther than circular polarized antennas. If tags don't seem to be aligned with the antenna's polarization, then circular polarized antennas will read farther than linear polarized antennas.

> **The details:** Polarization refers to a sort of electromagnetic field the antenna is generating. Linear polarization refers to radiation along one plane. a really simple thanks to considering a linearly polarized RFID antenna's beam is to imagine swinging a sword straight up and down or side to side. Circular Polarization refers to antennas that split the radiated power across two axes and so "spin" the sphere to hide as many planes as possible. an easy thanks to imagining a circularly polarized RFID antenna's field is to imagine a "tornado" emitting from the surface of the antenna. because of the character of the antenna's field, tag orientation becomes far more important with linear antennas than with circular antennas. Additionally, because the ability isn't split across quite one axis, a linear antenna's field will extend farther than a circular antenna with comparable gain, thus with an extended read range when aligned with the RFID tag. See our article further explaining circular vs. linear polarization.

Fig1. RFID antenna

Tag SOAP (Size/Orientation/Angle/Placement): As a general rule of thumb, small tags will have shorter read ranges, and huge tags will have longer read ranges. to induce the simplest, range from any RFID tag, confirm that the tag is fully facing the antenna and pay particular attention to tag orientation when using linearly polarized antennas. Lastly, when tagging objects with high liquid or high metallic content, take care to decide on RFID tags designed for mounting on such objects.

The details:

- **Tag Size:** Passive RFID tags can vary in reading range from some inches to 50+ feet. RFID tags contain antennas and since larger antennas will broadcast farther than smaller antennas, generally speaking, the larger the tag, the longer the read range.
    - **RFID Tags** Radio Frequency Identification (RFID) tags or transponders are small devices that utilize low-power radio waves to receive, store, and transmit data to nearby readers. RFID tags are comprised of the subsequent main components: a microchip or computer circuit (IC), an antenna, and a substrate or protective material layer that holds all the components together.
        - **There are three basic sorts of RFID tags:** passive, active, and semi-passive or battery-assisted passive (BAP). Passive RFID tags don't have an enclosed power source, rather, they're powered by the electromagnetic energy transmitted from an RFID reader. Active RFID tags have their transmitter and power source onboard the tag. Semi-passive or battery-assisted passive (BAP) tags are comprised of an influence source incorporated into a passive tag configuration. Additionally, RFID tags operate in three frequency ranges: Ultra-High Frequency (UHF), High Frequency (HF), and Low Frequency (LF).
    - RFID tags may be affixed to a spread of surfaces and are widely available in various sizes and styles.
    - RFID tags also are available in a good array of form factors including but not limited to wet inlays, dry inlays, labels, wristbands, hard tags, cards, stickers, and fobs.
- **Tag Orientation and browse Angle:** to elucidate the tag orientation and browse angle, picture an RFID tag lying flat on a stool. Then, picture an RFID antenna on the ceiling facing downward above the stool. during this scenario, the tag is in two important ways and both have major ramifications on reading range.
- **Rotating the RFID tack on the stool (tag orientation):** To clarify, now only matters for antennas with linear polarization. For the circular polarized antenna, the tag's orientation shouldn't matter. However, with linear antennas, tag rotation does matter. Imagine that the seat

of the stool may be a face. With a linear antenna, if the tag is in the same direction as the antenna, the reader can read data from the tag, however, if the rotation of the tag changes antenna cannot receive data from the tag. this can be a fast test that mainly applies to tags with one dipole. Some RFID tags have dual dipoles which can help mitigate problems caused by this movement.

- **Flipping the RFID tag onto its side (read angle**): Reading any RFID tag from an angle (vs. straight on) will hurt the read range. To harness the foremost energy possible from the RFID antenna, the RFID tag should directly face the antenna. think about the antenna extended as an X, Y plane, and therefore the tag (aligned with the antenna) also extended as an X, Y plane. the 2 are separated by some Z distance, and they never touch. In short, to urge the simplest range when reading the tag face-on - the steeper the read angle, the more the read range will decrease. Some RFID tags, like the embeddable RFID wire tag, have a 360-degree read profile which mitigates the read angle concern.
- **Tag Placement:** UHF RFID tags are strongly full of objects containing metal (reflection of RF energy) or water (absorption of RF energy). Choosing the proper tag for the thing, the read range may be greatly reduced, or might not be able to read the tag in the slightest degree. There are metal-mount RFID tags with a special backing designed to be applied on metal (or objects containing water). These styles of tags will frequently perform better on metal than they are doing off metal. As a general rule, unless a tag is marketed as a background insensitive or on-metal RFID tag, assume that it can't be applied to metal or water-filled objects. Additionally, to the composition of the item being tagged, each item will usually contain a "sweet spot" that may maximize the read range when the tag is placed within it. Sweet spots vary tremendously from item to item and might only be identified via testing.

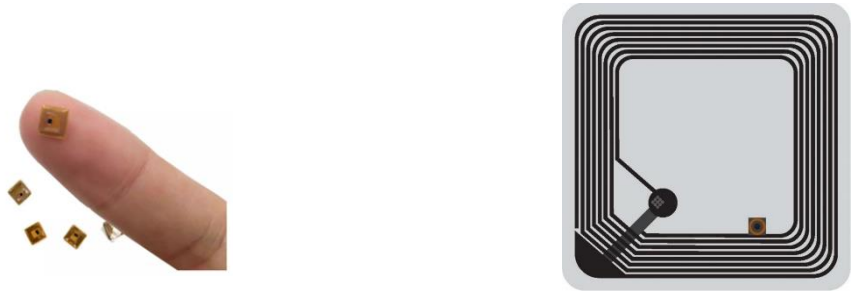

Fig2. Different types of tags

Reader Settings: Higher power settings will end in a greater read range, while lower power settings will end in decreased read range. Also, to maximize read range, make sure that the reader is ready to its highest receive sensitivity.

The details: All RFID readers can control what proportion of power they send through the cables to the antennas. the upper the quantity, the more the read range is increased, and vice-versa. it's important to notice that, because the ability is measured in decibels (dB), the ability will double (or be cut in half) for increasing every 3 dB (or decrease). for instance, 27 dB is twice as powerful as 24 dB, and 30 dB is twice as powerful as 27 dB. Although the facility doubles with every increase in 3 dB that does not mean the read range is doubled. Finally, the sensitivity of the reader; If the reader is ready to maximum sensitivity, it'll report a weaker tag; a lower sensitivity setting will ignore the weaker signals, thus decreasing the read range. Bottom line: the quickest and simplest way to maximize read range is to confirm that reader is ready to its full power and highest receive sensitivity.

Cable Length, Multiplexers, and Adapters: The longer the cable, the upper the loss, and using adapters and/or multiplexers inserts additional loss into the RFID system. for max read range, connect the antenna to the reader with the shortest cables.

The details:

- Length of cables: The antenna cables connecting the antennas to the RFID reader "leak" energy. The longer the cable, the more energy it'll lose, eventually losing most that the antenna won't receive enough power to come up with a robust RF field (regardless of the antenna gain).
- **Adapters & Multiplexers:** Sometimes it's necessary to convert the top of an antenna cable from one type to a different adapter is required. However, note that for every adapter there'll be 1/3 dB of loss within the system.

Environmental Factors: Many environmental factors can affect read range. When attempting to maximize read range, take care to account for various sorts of interference and test, test, test!

The details: Different environmental conditions can affect the performance of UHF RFID systems. Water, metal, florescent lighting, large machinery, and competing frequencies (other radio waves) may adversely affect UHF RFID read ranges. the most effective thanks to maximizing read range is to notice the varied possible types of interference and try to mitigate that interference by testing, making changes to the system, and retesting.

What is the NFC?

NFC or Near Field Communications is a short-range wireless connectivity technology that allows two compatible devices to communicate without contact. This two-way wireless communication technology uses radio waves operating at a base frequency of 13.56 MHz. This technology provides wireless communication between a pair of NFC-enabled devices (reader & tag) at a distance of less than 30 cm.

NFC delivers data speeds of 106 Kb/s, 212 Kb/s, 424 Kb/s, or 848 Kb/s which is enough to move small pieces of information almost instantaneously. NFC is very similar to RFID however the biggest difference between the two technologies is that RFID provides one-way communication while NFC provides two-way wireless communication.

An active NFC device can work in three modes: peer-to-peer, read/write mode, and card emulation. Peer-to-peer mode (P2P): In this mode, two NFC-enabled active devices (for example, two smartphones) directly share files and information. While one smartphone sends data, the other one act as receiving device. In this mode, both devices generate the radio wave alternatively at a carrier frequency of 13.56 MHz.

Read/write mode: In this mode, an NFC-enabled active device reads data from an NFC-enabled passive device (tag) or writes data on the tag by generating the radio wave alternatively at a carrier frequency of 13.56 MHz.

Card emulation mode: In this mode, the NFC-enabled active device acts as a passive device to communicate with the receiver terminal. The active device does not generate any radio waves, but it responds to the receiver terminal for requested data transfer.

Applications of NFC: NFC allows one-way or two-way wireless communications and is used in many applications such as paying bills, passports & ID cards, exchanging business cards, downloading coupons, or sharing a research paper, social networking for sharing photos/videos/files, gaming, and sports applications.

Reading NFC tags with Smartphones

Both android and apple now offer their customers the ability to use their smartphones to read NFC tags. Smartphones have a piece of hardware to work as an active NFC device that can read data from RFID tags, especially passive tags, and emulate a passive tag to respond to the reader. Therefore, using smartphones are much easier to use since it does not require external hardware to read tags.

Fig3. Resing NFC tags with Smartphones

Attacks on NFC

In the last few years, many big companies are adding NFC (Near Field Communication) support to all sorts of devices to allow consumers to make monetary transactions. Some of these companies are protecting themselves by implementing tokenization as part of payment technology. However, it is well documented that it is possible to bypass these technologies using simple mechanisms. With all these changes in the NFC ecosystem, the information security field is not well prepared to protect against the increasing new attacks in this area. Relay and replay attacks are becoming more common in the payment industry. Getting more complex and sophisticated day by day. We are not just seeing simple skimming techniques but complex attack vectors that are a combination of technologies and implementations involving SDR (Software-Defined Radio), NFC, APDU (Application Protocol Data Unit), hardware emulation design, specialized software, tokenization protocols, social engineering.

Replay Attacks

A replay attack is a technique where a malicious user could implement a device to intercept an NFC transaction and redeem it later, using another device or even in a different location.

Vulnerability

NFC (Near Field Communication) protocol is the technology that mostly is used for different purposes, from payment to the identification. By default, the protocol has different layers of security to avoid or protect against replay or downgrade attacks. When a person wants to make an NFC data exchange with the NFC reader, an attacker could intercept the NFC data transmission. The malicious user can manipulate the intercepted transaction in a different location and with different hardware as well. So, that intercepted data could be saved and replayed it later with another device.

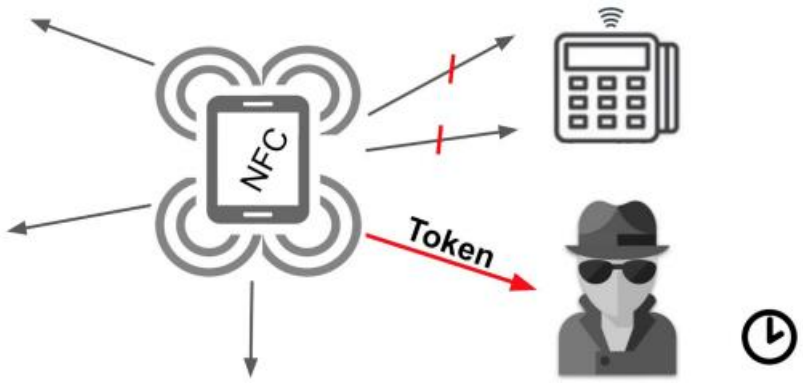

Fig4. Replay attack schematic

Relay Attack

The relay attack is a technique where a malicious user implements a man-in-the-middle attack. The attacker (APDUer) is capable to intercept, manipulate and change the transaction in real-time to take advantage of it. On the left side, we have a device with NFC technology, capable to make digital transactions. On the right side, we have a PoS(Point of Sale System) with NFC technology as well.

The APDUer could design an exclusive communication channel implementing SDR (Software-defined radio) instead of Wi-Fi to avoid interruptions, lag, or delays. EMV states that an NFC transaction has to be completed in 500ms, but the terminal is not restricted to finishing the transaction if it takes longer. So, this flexibility could be abused with many variable factors; the most important is the difficulty to design a time-bounding protocol to protect this.

Fig5. Relay attack schematic

Since the read range of the NFC tags is less than 30cm even 10cm, to apply any attack on these devices there must be two parts to have a successful attack without being noticed in the environment. One part can be a smartphone and the other part is compact hardware to be installed exactly somewhere that can read data from the ID card. For instance, nowadays hackers design a frame which can be installed exactly on any door lock or any payment card reader to collect data of many ID/Payment cards. Then this piece of hardware can transfer data in a long range to a smartphone and make it an emulator. The following figure represents how this system can work.

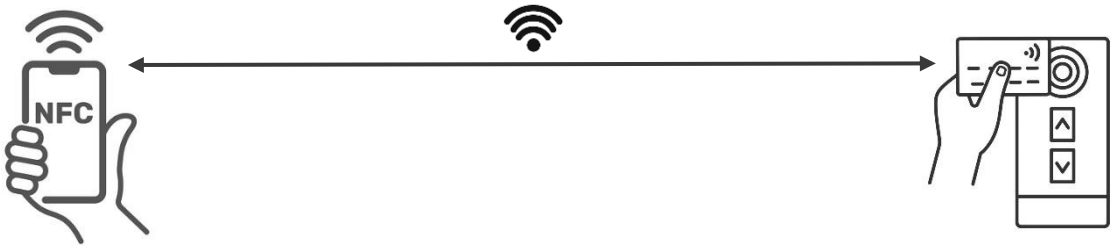

Fig6. Proposed design is based on Relay/Replay attack

The hardware contains separate parts; ESP32 Wemos D1, HID Card RW module, Battery charger, Battery, and Antenna. The hardware should be assembled in a box that is similar to a door lock or an NFC card reader that can be installed on that device. In this way, no one can understand the presence of a new thing over the main NFC card reader.

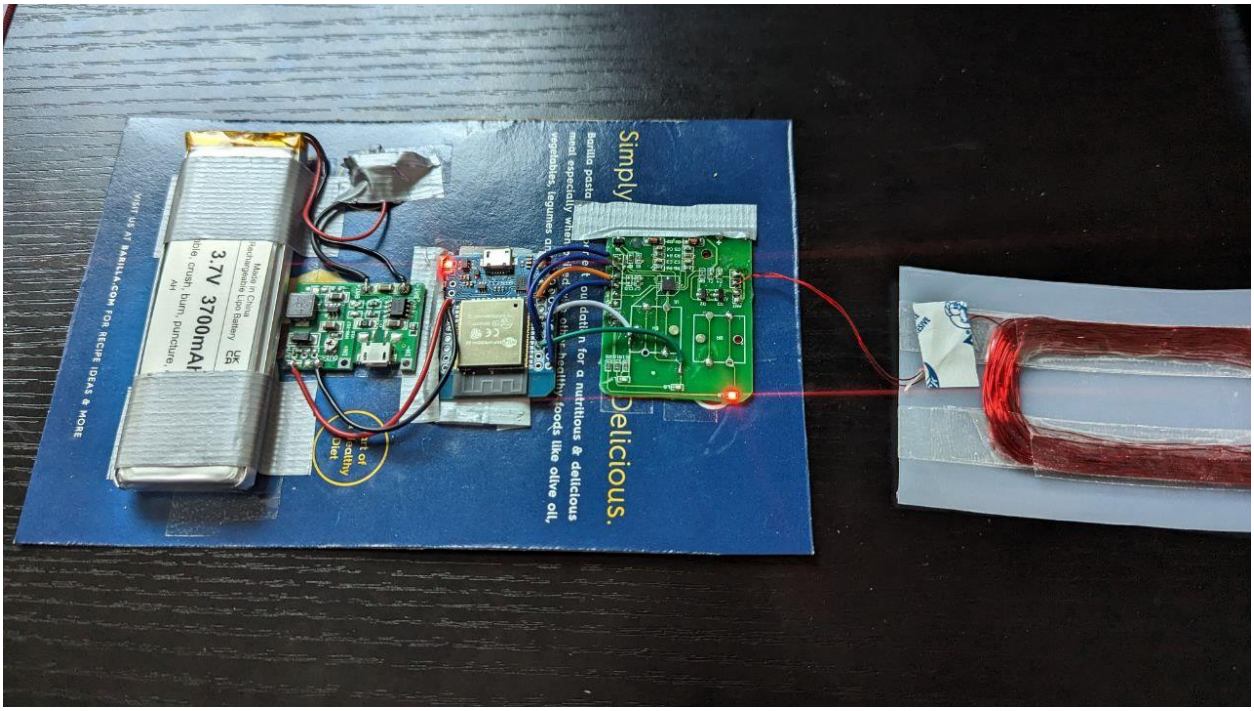

Fig7- Replay attack hardware sample (HID duplicator)

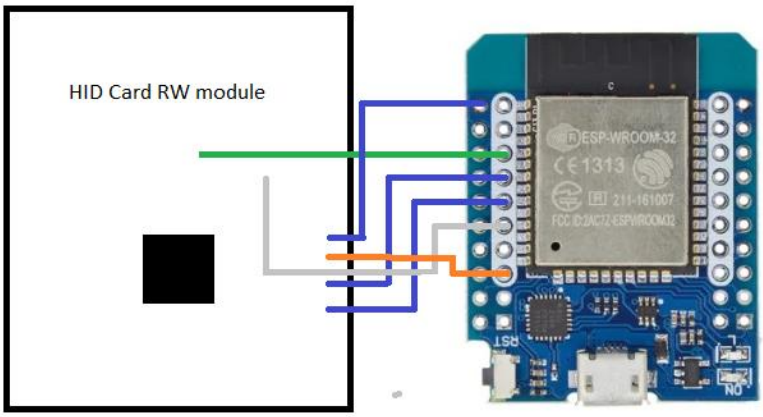

Fig8-Wiring diagram between ESP32 module and HID RW module

How does it work?

When the switch is on, the ESP32 creates a Mesh network, then the application tries to connect to the ESP32. When the Mesh network is available, the application connects to the network and can control the hardware from a remote distance.

When the connection is established between the application and the hardware, the start button will appear. By pressing the start button in the application, the hardware tries to read any cards in front of the antenna. Whenever any card appears in front of the antenna, the data of the card will be stored and the hacker can come and copy the card after minutes or hours.

Whenever any card approaches the antenna, the copy button will appear in the application and the attacker can reach the location, and copy the card data on a new fake card.

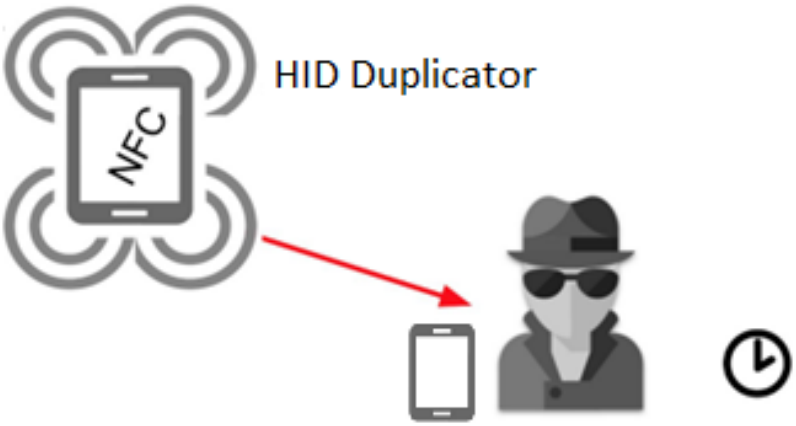

Fig9-Attacker waiting for reading data of a car remotely

After successful reading of data, the attacker notices that they can copy data from the card, so the attacker comes back to the location and detaches the HID duplicator from a card reader, and copies data from the card on a new fake card.

How it can be improved?

Using a better HID RW module, a power Antenna, capability to connect to the internet and send data over the internet instead of saving data on the hardware are the main improvements that can be done to this concept. In addition, to make this concept clear, a 3D print can be used to create a thin cover box to assemble the hardware inside of it.