Introduction to RFID Security

By Abdul Rasheed and Rajesh Thadethilmelathil

@nullDubai

Our efforts are to spread the awareness and purely for Education purpose only.

Agenda

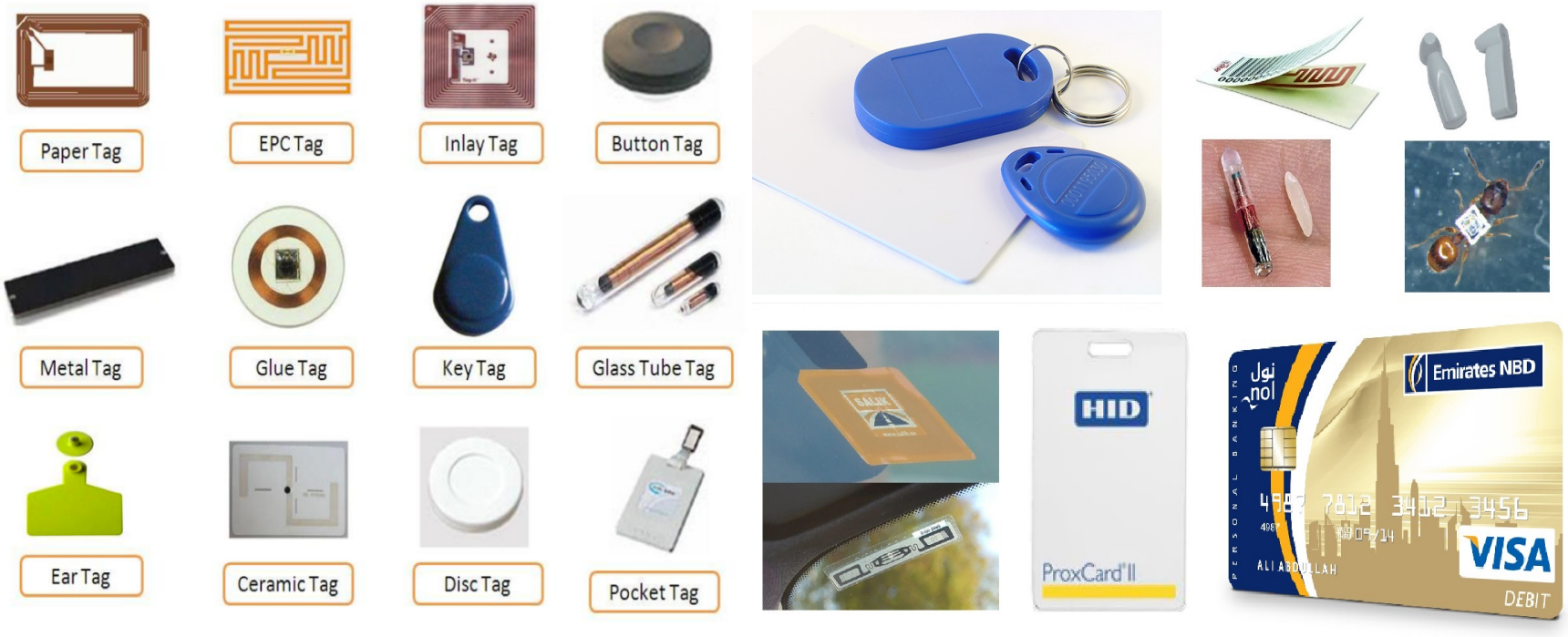
- What is RFID technology
- Usage and examples of RFID
- How RFID works
- Operating frequencies and standards
- RFID authentication methods
- Security and privacy concerns
- Demo
  - Proxmark3 and RFID Reader
    - Understanding and tampering of RFID reader
    - Reading, Writing, Simulating, Spoofing,& Cloning Attacks on RFID Tags
- Shielding & Protection Against RFID Attacks
- References
- Q&A

What is RFID

- Works on radio frequency range
- Information is transferred between reader and tag
- Identify & track objects
- It can be both passive and active
- Used in various industries from healthcare to defense

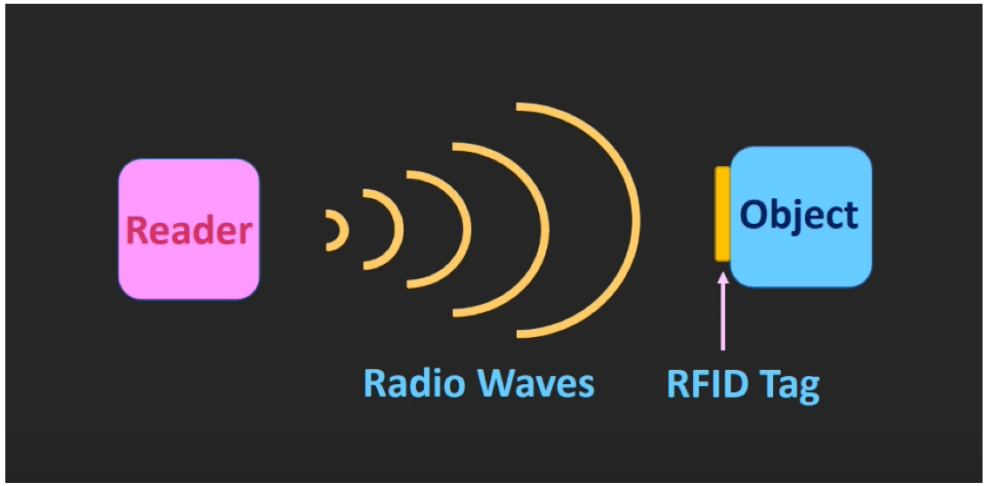
Example – RFID Reader

Example - RFID Tags



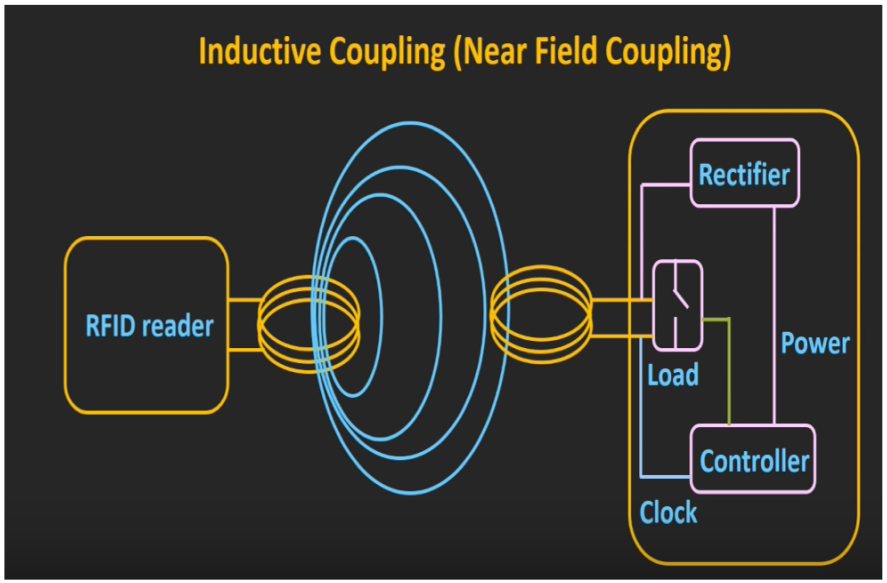
How Does it Work?

- The reader sends beacon broadcasts to tags
- The radio waves from the readers power up the tags
- The tags will respond to the beacons

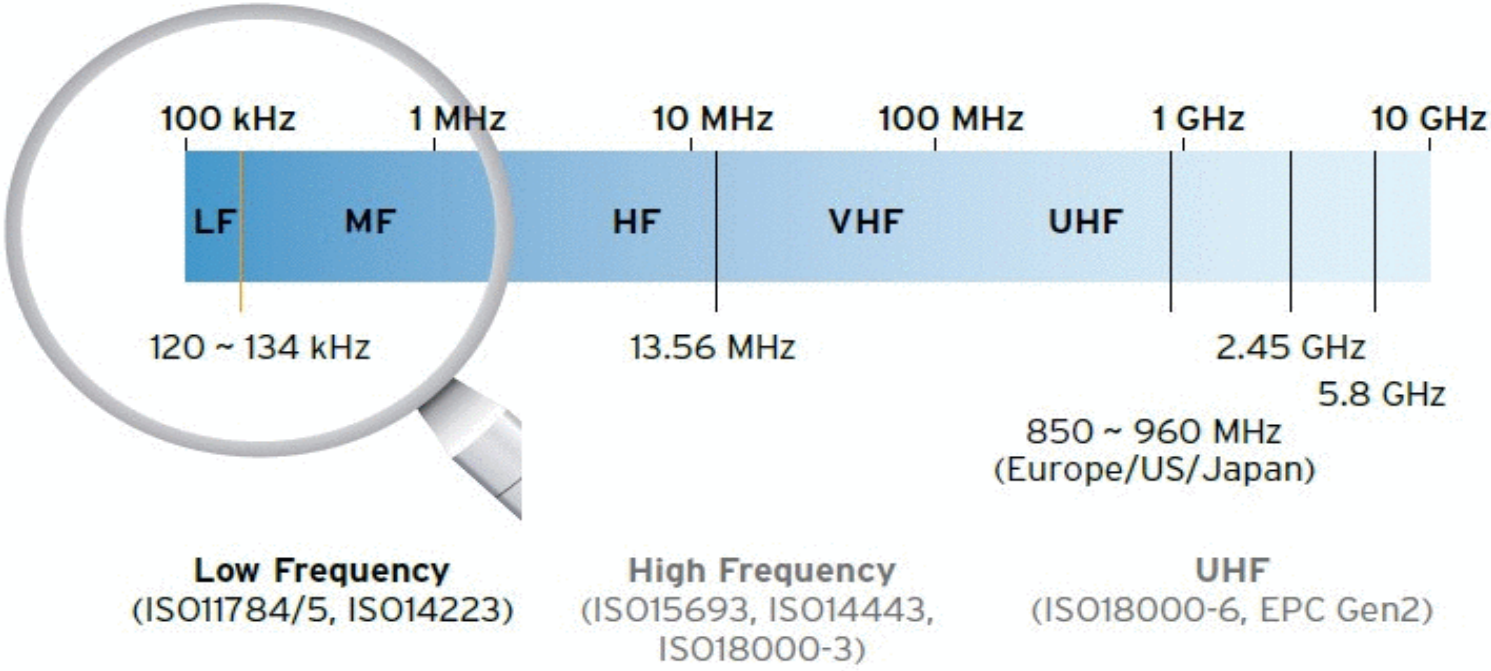


Working Principle

- Uses inductive coupling
- RFID tags works from 10 cm to 500 meter range
- The reader and tag gets coupled and voltage is generated
- The voltage will be used as power supply for tag



Operating Frequencies & Standards



Security, Encryption & Authentication

Security and Encryption

The data stored in the memory of an RFID tag can be shared with the various tag users (clients, suppliers, etc.). This naturally enables data exchange without a need to share anything but the object itself. This obviously raises the question of data security. Although the memory of an RFID tag is small, it can be organized in the same way as any other digital memory. Zones can therefore be reserved for certain users and password-protected. There can be several levels of authorization (read-only, read and write, delete, etc.). There is nothing to stop users encrypting the data they enter onto the tag (it is even advisable)

Security, Encryption & Authentication

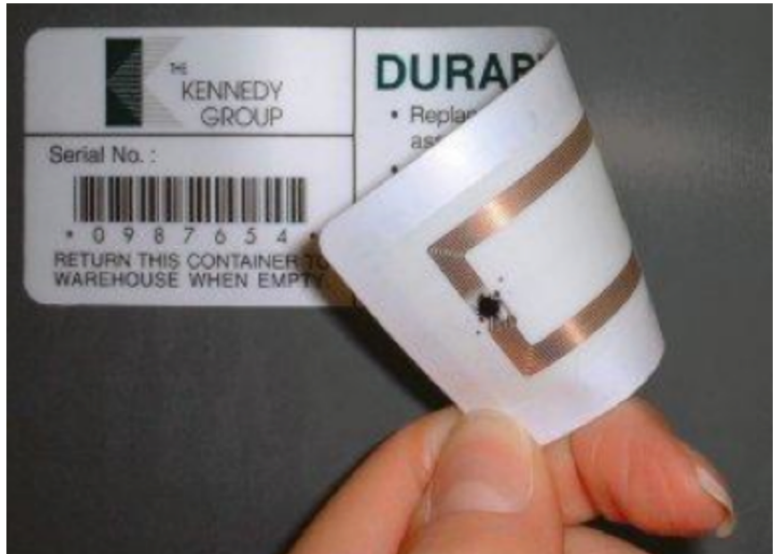
- By nature, RFID technologies are identification and not authentication technologies. Authentication of a reader or tag requires a common secret (key), known only to the players, to be shared at the moment communication is established, and before data can be exchanged.
- Currently, only RFID tags with microcontrollers have sufficient computation resources to use authentication techniques. These can be found in government applications (e-passport), or payment or ticketing applications (public transport, for example)
- The ISO/JTC1/SC31 committee is in the process of establishing new standards for RFID systems with microchips that use hard-wired logic (sequential state machines). These standards could soon allow the use of simple authentication and encryption algorithms.

Fundamental RFID privacy issues

- RF transmissions are hard to secure
- RFID tags can hold much information – unique static identifier allows tracking
- RFID tags are often promiscuous – respond to any compatible reader
- RFID systems are stealthy – how do ordinary people exert control?
- Privacy Leakage

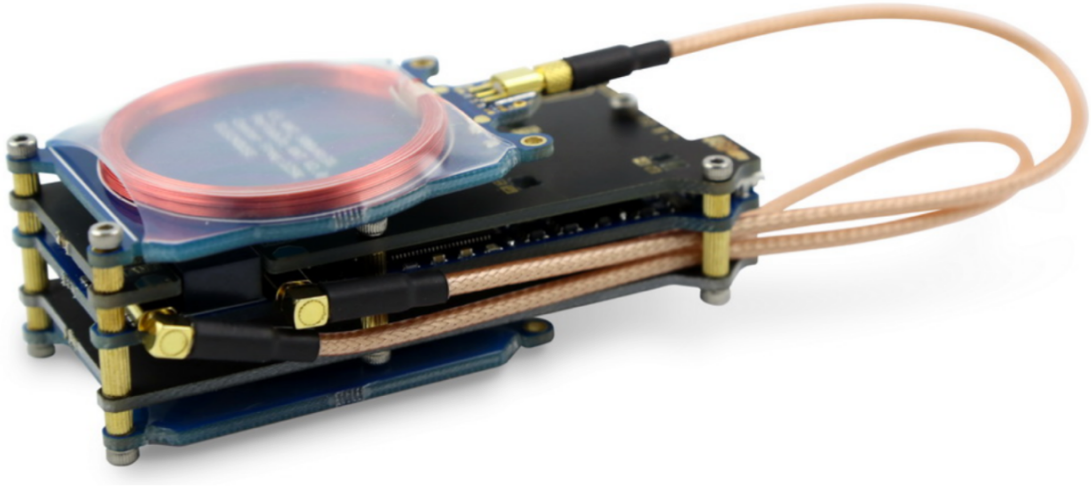
Common Attacks against RFID Systems

- Data manipulation
- Disable traceability
- Deletion of tag data
- RFID card cloning
- Jamming RFID frequencies



Tools of the Trade

- Proxmark3
  - Read, Write, Spoof, Simulate & Clone RFID Tags



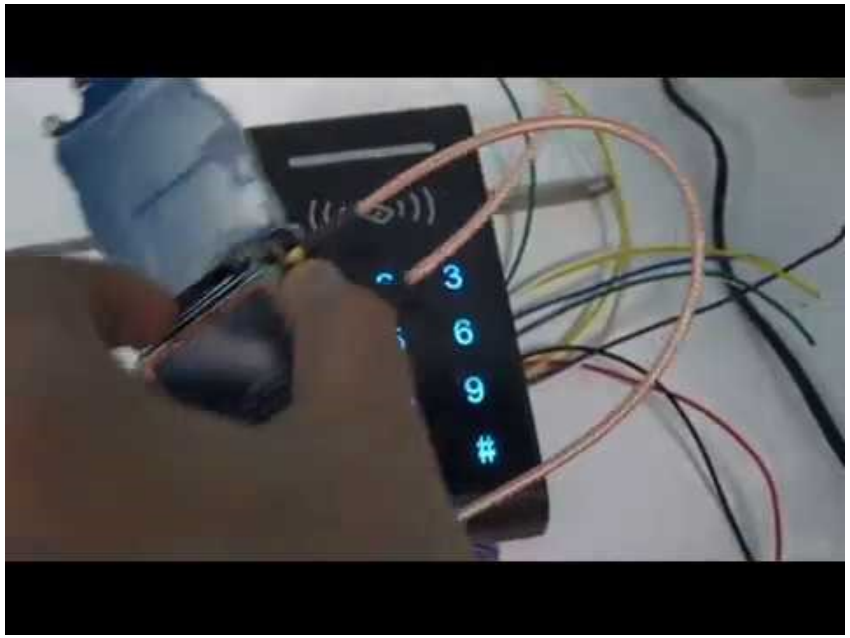
Demo

1.Tuning hardware

2.Reading tags

3.Spoofing and Emulating

4.Cloning.



Protection Against RFID Attacks

- Watermarking & physical unclonable function (PUF)
- Deploying CCTV surveillance for monitoring the RFID entrances
- RFID wallets and shielded badge holders for access cards.

PROTECTION AGAINST RFID Attacks – Demo ☺

REFERENCES

- https://en.wikipedia.org/wiki/Radio-frequency_identification
- http://www.proxmark.org/
- https://github.com/Proxmark/proxmark3/wiki/commands
- https://www.blackhat.com/presentations/bh-usa-06/BH-US-06-Grunwald.pdf
- https://www.youtube.com/watch?v=Ukfpq71BoMo

Note: We have used media and some content from many resources to make this presentation, we warmly thanks to all resources.

Special Thanks to nullDubai for giving this opportunity and GBM for hosting a venue.

Thanks!

Any Questions?

Reach us:

Abdul Rasheed fb.com/rash1253

Rajesh TV fb.com/raj3sh.tv

What's next? Hacking more Radio frequencies with another hardware soon.. Stay tuned @nullDubai