Exploitation of Radio Frequency Technologies Through the use of Microcontrollers

Author and Presenter Contact Information:
DJ Joachim
Lord Fairfax Community College
Email: djj2985@email.vccs.edu

Daniel Joachim is employed by Navy Federal Credit Union in desktop support services, supporting critical infrastructure. He is working toward his Associates of Applied Science Degree in Cybersecurity from Lord Fairfax Community College and plans to continue on to earn his Bachelors Degree in Cybersecurity. He has received two scholarships from the LFCC Foundation: Dorothy Margaret Overcash Memorial Scholarship and the Jeffrey L. Ross Memorial Endowed Scholarship. During the National Cyber League Competition, he placed in the top 3 percent of 5,600 competitors. Daniel is also serving as the Cybersecurity CTF Competition Team Captain and the Delta Phi Chapter of Epsilon Pi Tau's Competition Officer.

Radio Frequency Identification (RFID)

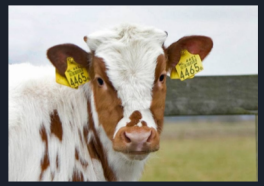
First application During WW2

- Signal is generated by transmission station
- Signal is modulated by device (aircraft)
- Authenticity is validated by evaluating the modulated result
- Example of passive RFID

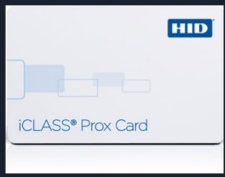
Tags, Token, Cards, Fobs (LF / HF / UHF)

- Invented in 70s, adopted in 80s, are used internationally YTD.
- Enabled contactless communication / authorization
- Tags consist of Memory, UID, Controller Circuit and Antenna
- Preinstalled amounts of memory (size varies on tag architecture)
- UID (unique ID) programmed by manufacturer
- Reader must interface with card modulation/encryption standards to be read
- Passive, semi-active and active tags

Low-Frequency 125/134 kHz tags : HID Prox , Indala , flex ioProx



High-Frequency 13.56MHz - NXP Semiconductors (MIFARE : Mini, Classic 1k , Ultralight, Plus, DESFire , DESFire EV1 , PLUS), iCLASS



Ultra-High-Frequency 860-960Mhz / 3.1+ Ghz : nedap, ezPass, ePassport, Omni-ID(Ultra, Max, Flex, Prox)

RFID Standards and Features

Low Frequency

- ISO 14223 + ISO/IEC18000-2
- EM4100 standard (non programmable chips)
- Low frequency = low proximity (10cm)
- Supports no encryption
- Animal tracking
- Slower read speeds
- Less sensitive to interference
- Average cost per tag = 1$

High Frequency

- ISO 14443(A,B)
- Contactless Payments
- Data transfer
- Inventory Tagging
- Access Control
- Adapted internationally
- Average cost per tag = .50$

Ultra High Frequency

- 860-960Mhz / 3.1+ Ghz
- ISO 18000-6C standard (Global Gen2)
- Passports
- Long range 10m+
- Fast DTR
- Average cost per tag = 5$
- Multiple usages due to wide frequency range

Access Control Systems

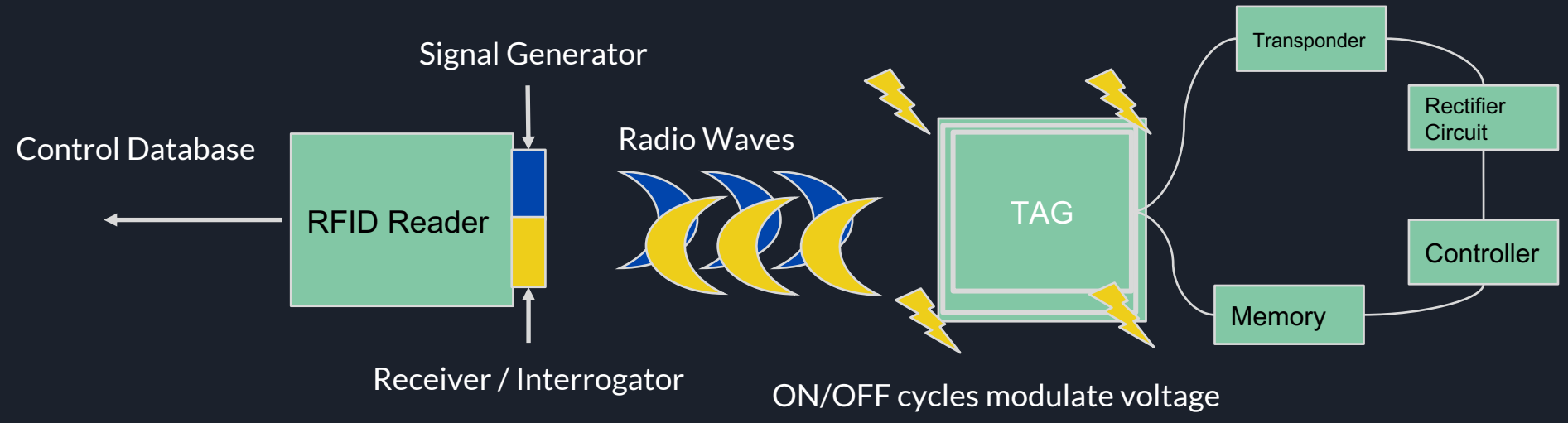
What are they?

Systems implemented to restrict physical access to private resources. Access is granted upon validation of identification.

- Gated communities
- Organizational entry
- Government access
- Transit systems
- Educational institutes
- Hotels
- Nursing homes

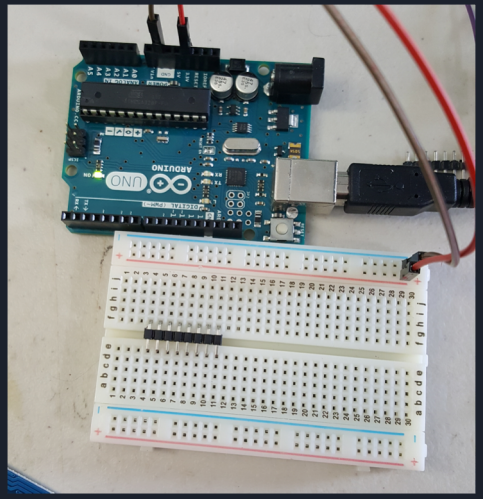
Access Control Systems - Component Information

Utilizes Inductive Coupling to exchange information from Tag to Reader

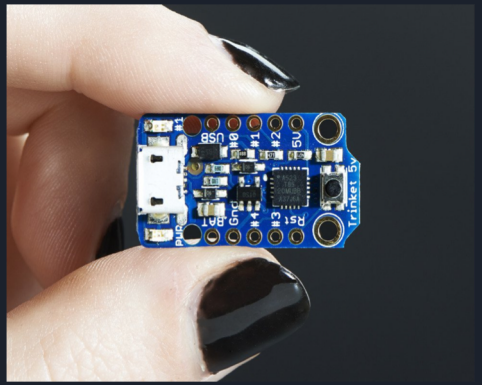


Microcontroller Boards

Arduino Raspberry Pi Adafruit Trinket



- Noiseless IC (Integrated Circuit) boards that allow modular sensory devices to connect to them
- Low profile/ Low power
- Perform only one {set} specific task
- Easily Programmable Read Only Memory (EPROM) flashed for each application
- Libraries, schematics, intelligence, software and components are open source.
- Average cost < 30$
- Power any IoT device e.g. Smart Devices.



Key Information

Table 2. NXP Contactless Card IC Feature Overview

	MIFARE Ultralight	MIFARE Ultralight C	MIFARE Classic	MIFARE Plus	MIFARE Plus EV1	MIFARE DESFire	DIF (like SmartMX)
HW Crypto	-	3DES	Crypto1	Crypto1, AES	Crypto1, AES	3DES, AES	3DES, AES, PKE
EEPROM	512 bit	1536 bit	320 Bytes, 1k Bytes, 4k Bytes	2k Bytes, 4k Bytes	2k Bytes, 4k Bytes	2k Bytes, 4k Bytes, 8k Bytes	4k Bytes – 144k Bytes
Special Features	-	-	-	MIFARE Classic compatible	MIFARE Classic compatible	-	MIFARE Classic compatible
Certification	-	-	-	CC EAL 4+	CC EAL 5+	CC EAL 4+	CC EAL 5+
Contactless interface	ISO/IEC 14443A	ISO/IEC 14443A	ISO/IEC 14443A	ISO/IEC 14443A	ISO/IEC 14443A	ISO/IEC 14443A	ISO/IEC 14443A

Table 3. NXP Contactless Card IC compliance overview

ISO layer	MIFARE Ultralight	MIFARE Ultralight C	MIFARE Classic	MIFARE Plus	MIFARE Plus EV1	MIFARE DESFire	SmartMX platform
ISO/IEC 14443 -4				✓	✓	✓	✓
ISO/IEC 14443 -3	✓	✓	✓	✓	✓	✓	✓
ISO/IEC 14443 -2	✓	✓	✓	✓	✓	✓	✓

1.1 Terms and Abbreviations

Table 1 shows the terms and abbreviation used in this document. All the "Type A" related definitions are used and described in the ISO/IEC 14443 documents.

Table 1. Abbreviations

Abbreviation	
ATQA	Answer To Request acc. to ISO/IEC 14443-4
ATS	Answer To Select acc. to ISO/IEC 14443-4
DIF	Dual Interface (cards)
COS	Card Operating System
CL	Cascade Level acc. to ISO/IEC 14443-3
CT	Cascade Tag, Type A
n.a.	not applicable
NFC	Near Field Communication
PCD	Proximity Coupling Device ("Contactless Reader")
PICC	Proximity Integrated Circuit ("Contactless Card")
PKE	Public Key Encryption (like RSA or ECC)
REQA	Request Command, Type A
SAK	Select Acknowledge, Type A
Select	Select Command, Type A
RID	Random ID, typically dynamically generated at Power-on Reset (UID0 = "0x08", Random number in UID1… UID3)
RFU	Reserved for future use
UID	Unique Identifier, Type A
NUID	Non-Unique Identifier

Penetration Resources

Proxmark 3
→ copier / writer / reader / emulator
→ De-Facto penetration / exploitation tool for RFID Technologies
→ Average price ~$300

HFeng Handheld cloner
→ Inexpensive ~$17
→ Cannot copy EM4100 Tags

MFOC Library (GNU Linux) / RFDump
→ Library designed for cracking RFID cards
→ Open source

NFC-Tools (GNU Linux)
→ Installed in most Android phones
→ Open source

Magic cards (T5577)
→ Programmable UID
→ Some readers disable card (security implementation)
→ Inexpensive ~ $.50 per card

References

1. Single Contactless Access system: https://www.google.com/imgres?imgurl=https%3A%2F%2Fwww.business.com%2Fimages%2Frev%2Fprod%2F2_1141_Access_Control_Systems.jpg&imgrefurl=https%3A%2F%2Fwww.business.com%2Fcategories%2Fbest-access-control-systems%2F&docid=Dy5s5oAIIdPDEM&tbnid=oPpnEXg-dULLIM%3A&vet=10ahUKEwjoxq_7ssPhAhVnmeAKHZ_pAWMQMwjlASgAMAA..i&w=5184&h=3456&bih=931&biw=1920&q=access%20control%20systems&ved=0ahUKEwjoxq_7ssPhAhVnmeAKHZ_pAWMQMwjlASgAMAA&iact=mrc&uact=8
2. Implementing Access control through multiple means. https://www.google.com/imgres?imgurl=http%3A%2F%2Fzafatech.com%2Fwp-content%2Fuploads%2F2017%2F06%2Faccess_header-1100x400.jpg&imgrefurl=http%3A%2F%2Fzafatech.com%2Four-solutions%2Faccess-control-systems%2F&docid=hE99g8SP2LLk8M&tbnid=tx4LlQGTuq4GtM%3A&vet=10ahUKEwjW5NmHtMPhAhWimuAKHYwyAUIQMwjsASgHMAc..i&w=1100&h=400&bih=931&biw=1920&q=access%20control%20systems&ved=0ahUKEwjW5NmHtMPhAhWimuAKHYwyAUIQMwjsASgHMAc&iact=mrc&uact=8
3. Civilian entry access control : https://lotgroup.eu/wp-content/uploads/2016/09/AFC_Implemented_Metro_Baku-3.jpg
4. Adafruit Trinket : https://cdn-shop.adafruit.com/1200x900/1501-12.jpg
5. WW2 Fighter Plane : https://nationalinterest.org/sites/default/files/styles/desktop__1486_x_614/public/main_images/messerschmitt.jpg?itok=9USXfMKG
6. Military Radio Tower : http://www.27east.com/assets/Article/59908/_DSC0701.JPG
7. Low-Frequency Ear Tag : https://gaorfid.com/wp-content/uploads/2014/12/112002.png
8. iCLASS Prox Card : https://cdn3.volusion.com/cyoas.tvrdt/v/vspfiles/photos/HID-202X-2.jpg?1427203537
9. UHF Windshield Tag : https://www.nedapidentification.com/wp-content/uploads/2017/12/windshield-tag.png
10. UHF Medical Prox Card : https://www.google.com/url?sa=i&source=images&cd=&cad=rja&uact=8&ved=2ahUKEwjK_orfh8fhAhWld98KHZfhCvUQjRx6BAgBEAU&url=https%3A%2F%2Fwww.starnfc.com%2Fproduct%2Fuhf-epc-gen2-rfid-cards860-960mhz%2F&psig=AOvVaw3LS8udlA8gMAZCD8m5VOxO&ust=1555038433021313
11. EZ Pass : https://www.google.com/url?sa=i&source=images&cd=&cad=rja&uact=8&ved=2ahUKEwjXuaOPi8fhAhWHl-AKHXkkC94QjRx6BAgBEAU&url=https%3A%2F%2Fwww.amazon.com%2FFree-Thought-Designs-Transponder-Holder%2Fdp%2FB06XD7MP47&psig=AOvVaw1Nv8lFDe5IKChh4Nl_r6Z5&ust=1555039298660230
12. Livestock tracking LRFID : https://ae01.alicdn.com/kf/HTB1jI1dRXXXXXXhXpXXq6xXFXXXF/Animal-Livestock-Tracking-ID-Tags-rfid-ear-tag-cheap-long-range-passive-cattle-rfid-tag.jpg_640x640.jpg
13. Raspberry Pi : https://www.raspberrypi.org/app/uploads/2018/03/770A5842-462x322.jpg
14. Proxmark 3 RDV2 : https://images-na.ssl-images-amazon.com/images/I/61HKXTMNdtL._SL1500_.jpg\
15. 125Khz Tag Cloner : https://images-na.ssl-images-amazon.com/images/I/61siwIBh%2BvL._SL1000_.jpg
16. Magic Cards : https://www.google.com/url?sa=i&source=images&cd=&cad=rja&uact=8&ved=2ahUKEwj0sJaPysjhAhVlp1kKHbeeAS4QjRx6BAgBEAU&url=https%3A%2F%2Fwww.aliexpress.com%2Fitem%2F13-5MHZ-UID-Changeable-MF-S50-1K-Standard-NFC-Card-FM11RF08-MF1-S50-Clone-Copy-Backup%2F32806266837.html&psig=AOvVaw2bN0yyGU6XIkpNa5y1J0t3&ust=1555090610093766