Case Study on RFID (proximity cards) hacking

-Sarwar Jahan M

-Ashwath Kumar

Disclaimer: All the views/data presented are our own and do not reflect the opinions of our current/past employer.

Who are we

Sarwar Jahan M

Consultant at Cigital Asia Pvt. Ltd (subsidiary of Synopsys Inc.)

- @sarwarjahanm
- https://in.linkedin.com/in/sarwar-jahan-m-70289795
- Interested in Secure Code Review, Web Application Sec, Mobile App Sec
- Synack & Bugcrowd leaderboard: Top 10 researcher (2016)

Ashwath Kumar

Associate Principal Consultant at Cigital Asia Pvt. Ltd (subsidiary of Synopsys Inc.)

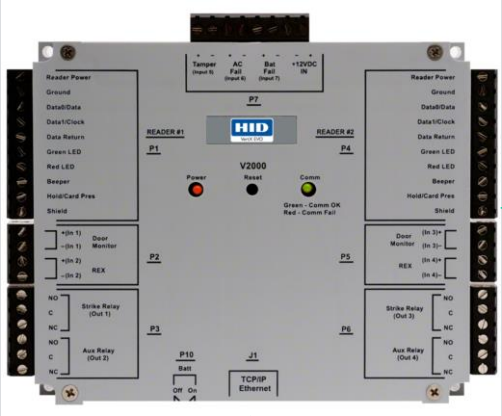
- @ka3hk
- https://in.linkedin.com/in/ashwath-kumar-5a4383b
- Interested in Red Teaming, Threat Modeling, Cloud Security
- Former Security Engineer at Microsoft

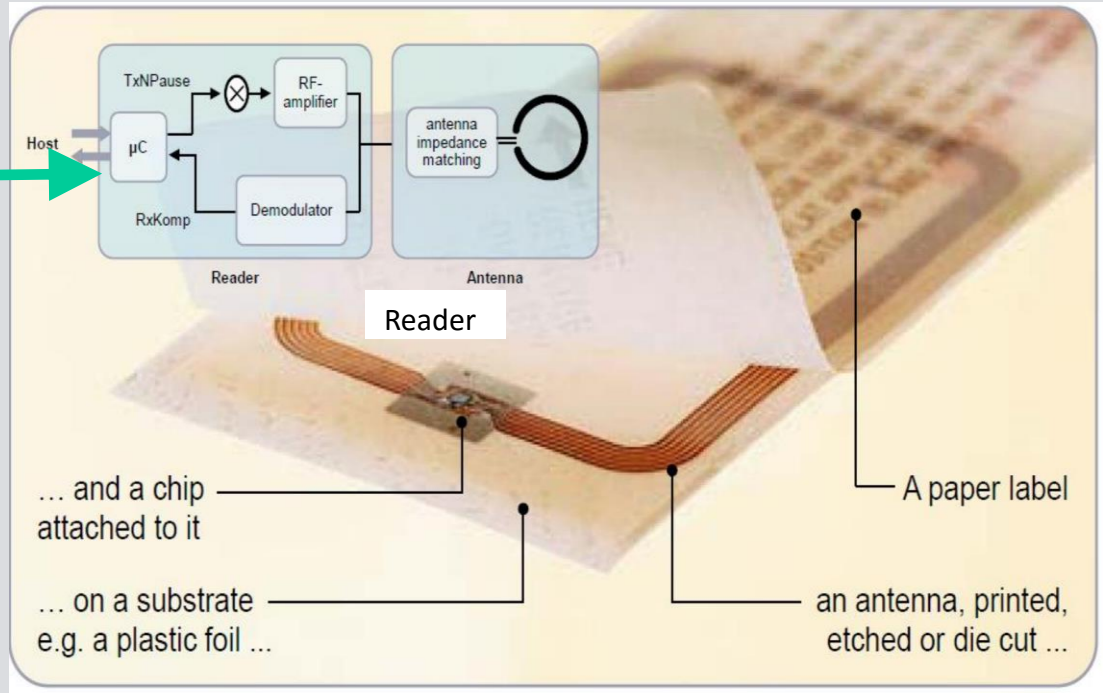
Outline

- How we got started
- RFID Introduction
- Security aspect
- Tools available
- Case study details
- Industry wide usage
- Remediation
- Conclusion

RFID Introduction - Basics

Controller

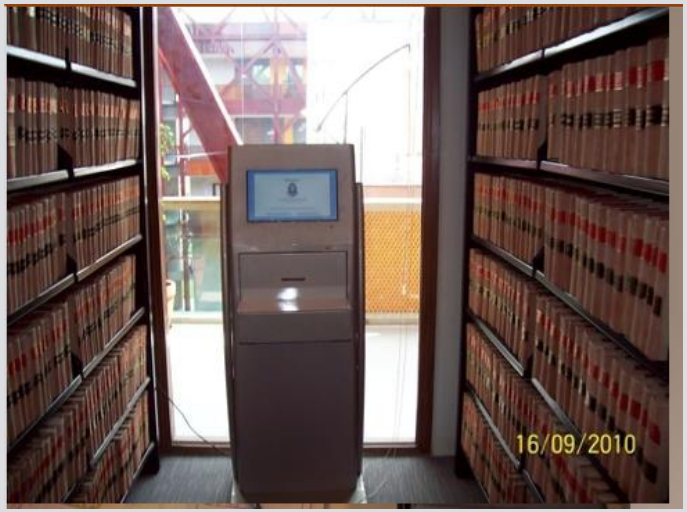




Host PC

http://rfip.eu/papers/hid_frequency_selection_guide.pdf

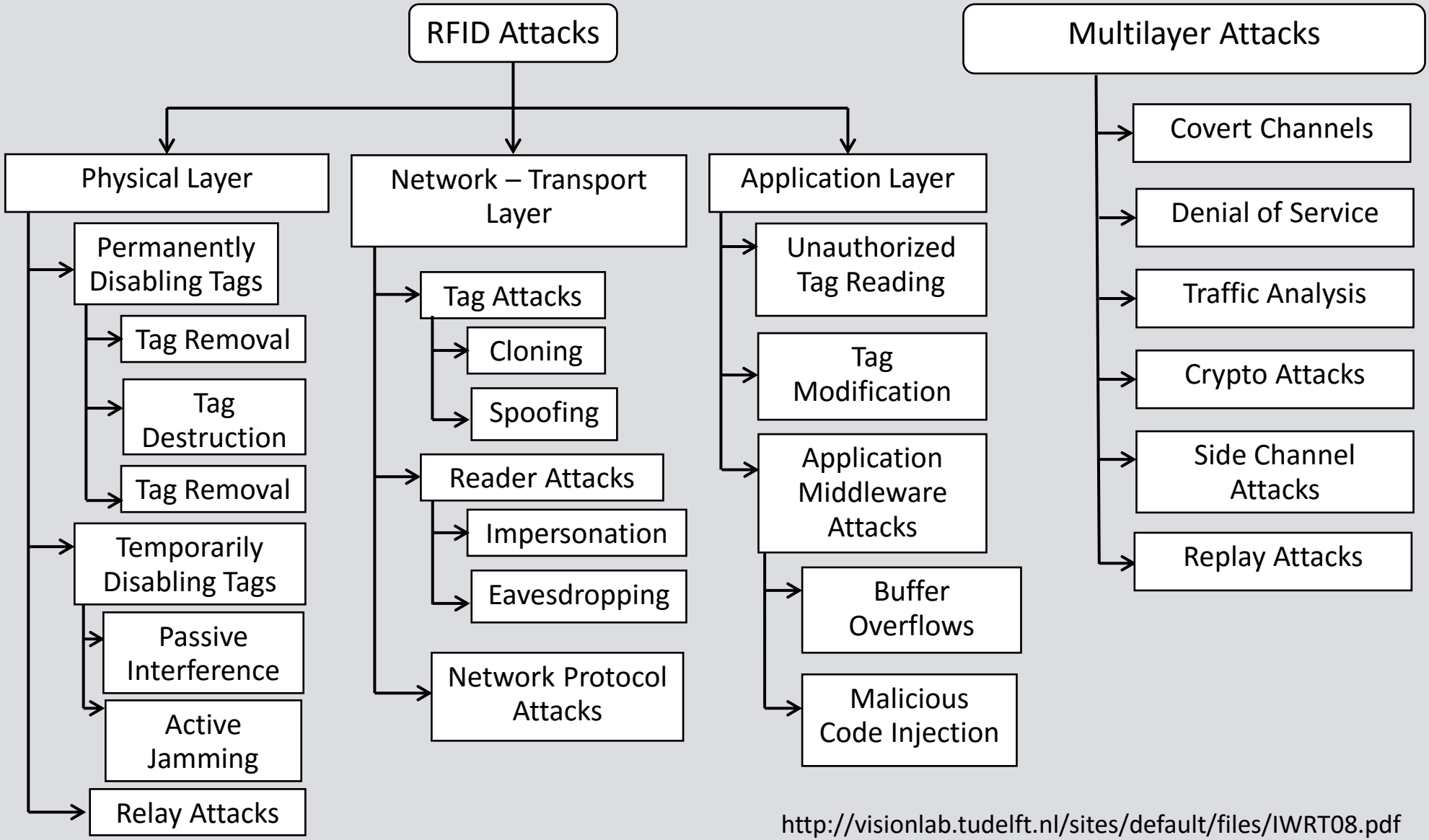
RFID Introduction - Usage



RFID Frequency Comparison

Area	Low Frequency (LF)	High Frequency (HF)	Ultra High Frequency (UHF)
Frequency	125kHz, 134.2kHz	13.56MHz	860MHz – 960MHz 865MHz – 867MHz (India)
Physical Concept	Inductive coupling Antenna - Coil	Inductive coupling Antenna - Coil	EM – wave propogation Antenna – Dipole/loop
Distance	Upto 3 ft	Upto 3 ft	~25 ft
Memory/Storage	64 to 2048 bit	896 bit to 8 KB	EPC: 96 to 128 bit / TID: 64 to 96 bit / User: 128 to 8192 bit
No. of items read	1	1-2	~200 at a time
Usual applications	Access control, Animal identification, Industrial environment,	Access control, Libraries, Public Transport, Product Identification	Vehicle toll booths Container Fashion Electronics
Environmental	No influence on metal	No influence on metal	Interference with metal & liquid
Standards	ISO 11784 / ISO 11785 (Animals) ISO 14223 (RTF, TTF) ISO 18000-2 (Item management)	ISO 15693 (Vicinity card) ISO 14443 (Proximity) ISO 18000-3 (Item management) HF EPC Gen2	ISO 18000-6C

Security Aspect



http://visionlab.tudelft.nl/sites/default/files/IWRT08.pdf

Security aspect - Attack Remediation

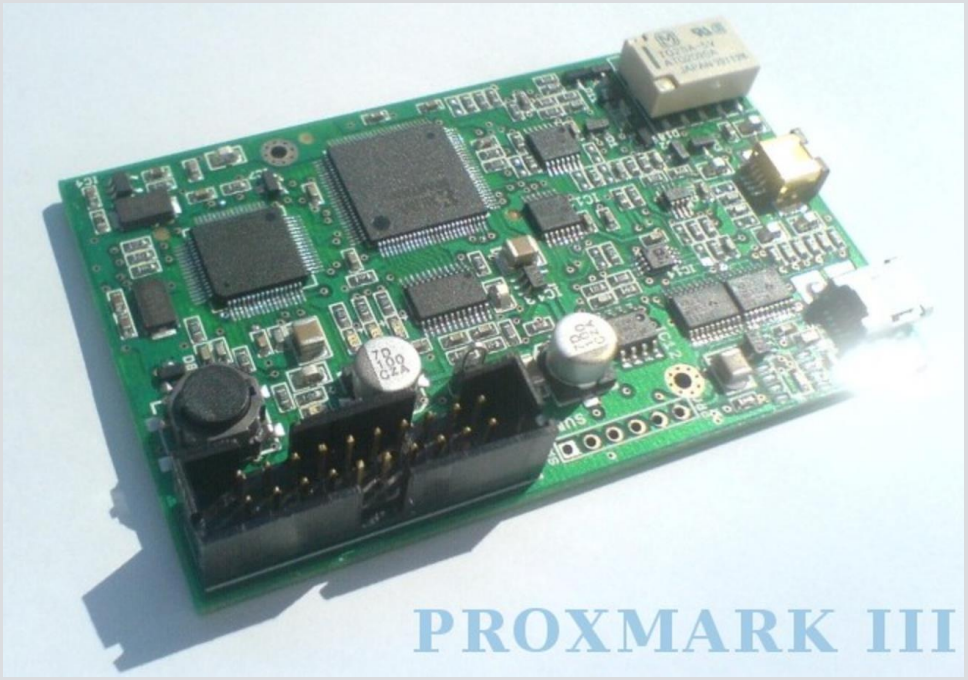
Class of attack	Attack	Remediation
Badge attacks	Cloning Spoofing	Authentication, Recognize duplicates Install Field Detectors, Frequency Division/Hopping
	Unauthorized read/write	Authentication, Install Field Detectors, Use Read-only Tags
	Reverse Engineering	Optical Tamper Sensor, Chip Coating
Reader attacks	MITM / Replay	Authentication, Encryption / Challenge response
	Eavesdropping	Encryption, Shift data to backend
	Jamming /Blocking Tags	Authentication, Encryption. Can't be remediated at all times, can be monitored
	Tracking Abuse of Kill	Kill Function Authentication
Controller attacks	Unauthorized access	Network lockdown of ports, change default credentials, update patches. Monitor activity

http://visionlab.tudelft.nl/sites/default/files/IWRT08.pdf

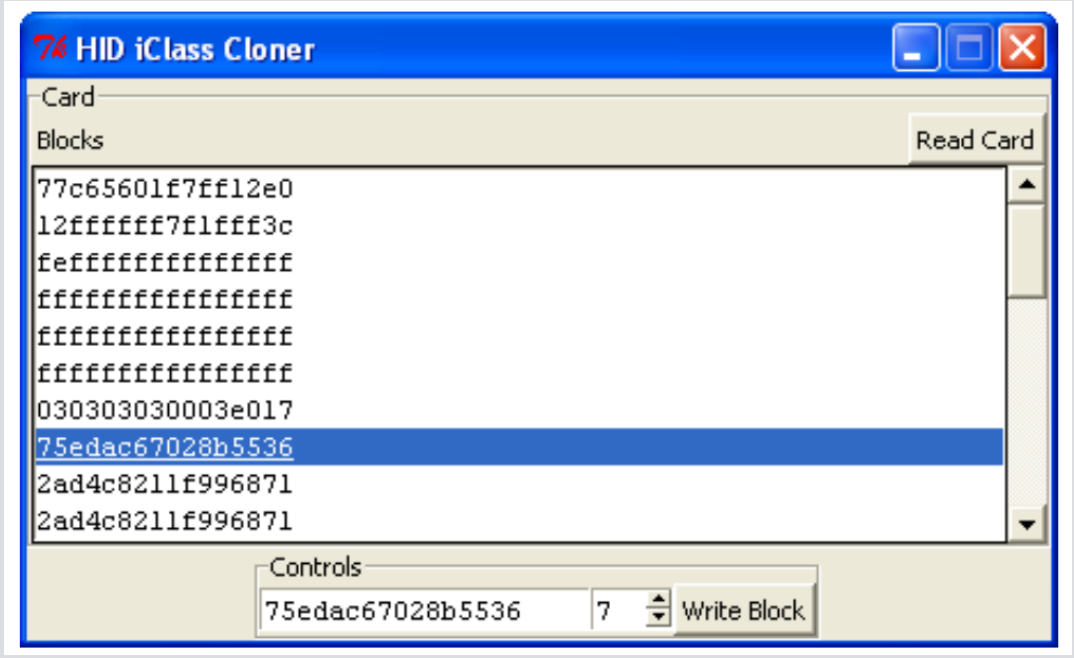
Security aspect – Frequency based

Frequency	Technology	Security Issues	Attacks
LF	125KHz, 134kHz	No/Weak encryption	Copy, clone, spoof Eavesdropping Wormhole attacks Jamming, overwriting cards Reader, Controller attacks
HF (13.56 Mhz)	MiFare Classic	Weak encryption	Nested key Bruteforce attack Reader, Controller attacks Wormhole attacks
	MiFare Desfire		Side channel attacks (Power analysis) Reader, Controller attacks Wormhole attacks
UHF	Class1 Gen1	No security features	Copy, clone, spoof. Reader, controller attacks
	Class1 Gen2		(TID, Passwords, Access Code introduced.) Bruteforce attacks, reader, controller attacks

Tools - 1

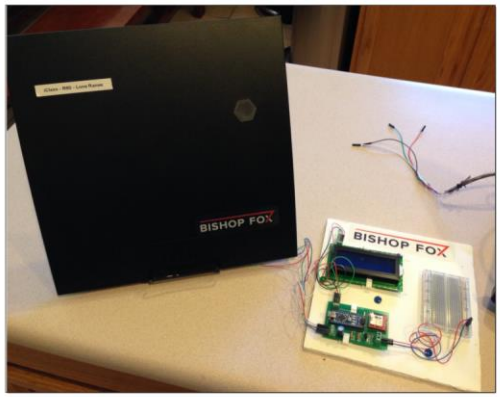


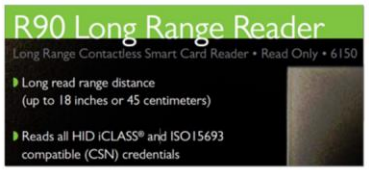
Proxmark 3 – Rs. 20,000



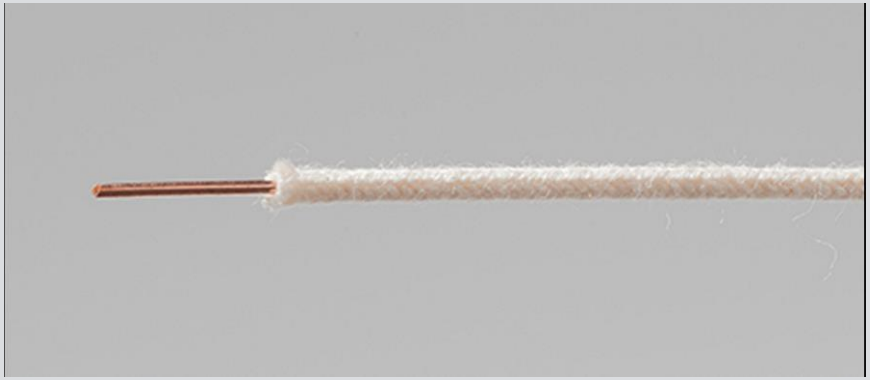
iClass Cloner – Rs. 12,500

Tools - 2





Tastic RFID - ~Rs. 13,000



Copper wire – Rs.50

RFIdiot– Adam Laurie

BLEKey – Rs.700

Demo - 1

Copying & cloning card data

Demo - 2

Wormhole attack

Case Study - **Requirements**

Let us say we are a startup

- There are **100** employees (100 cards)
- We have one door where 1 card reader has to be installed
- We need 1 controller

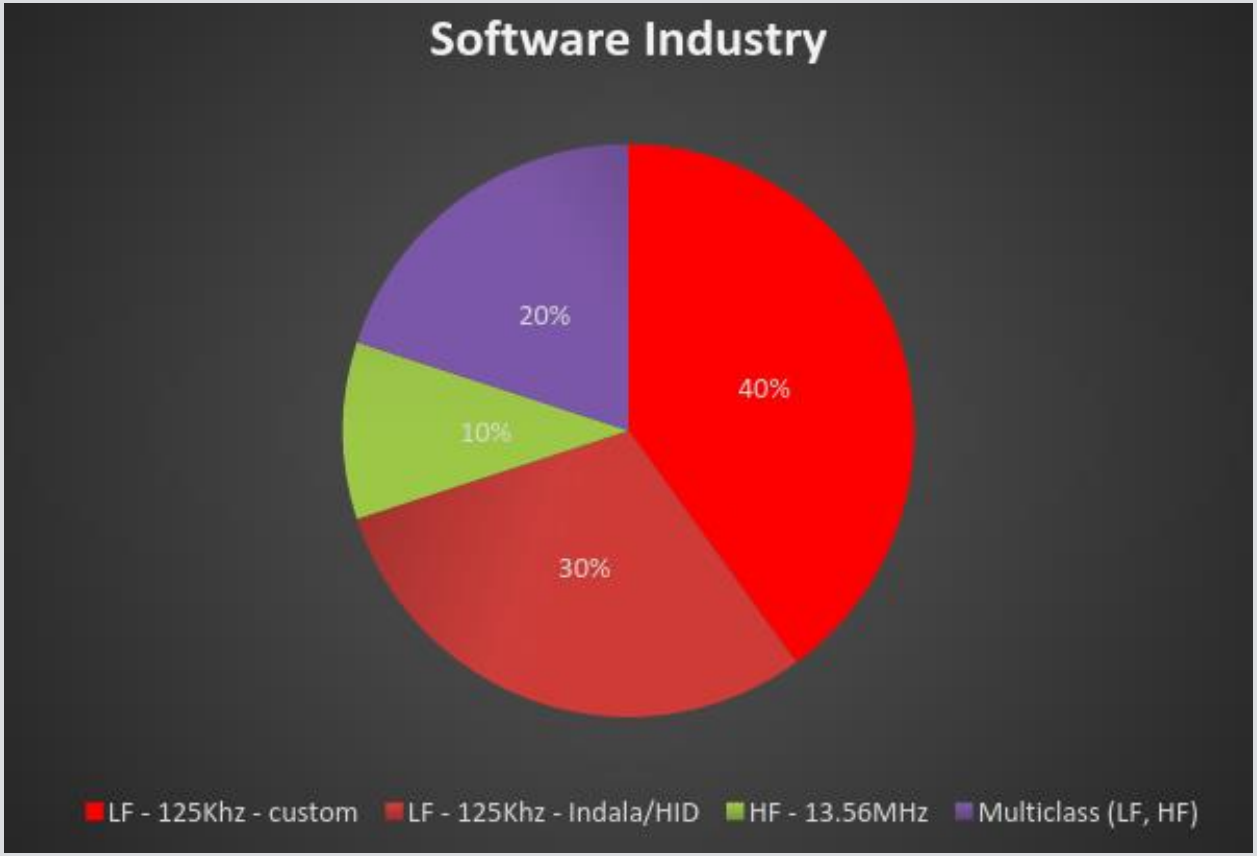
Case Study - Cost Comparison (Approx.)

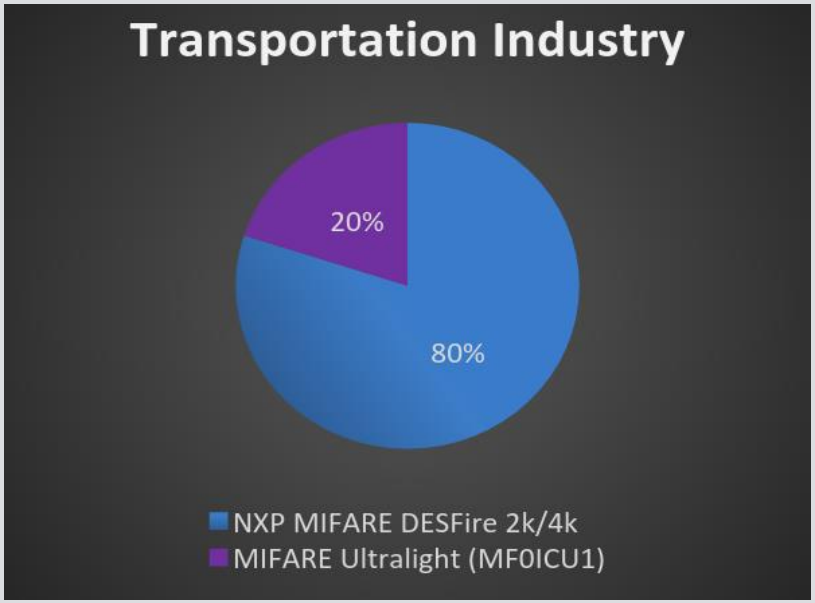
Type	Card reader	Reader Cost(single)	Controller cost	Cards cost (100 cards)	Total Approx. Cost
Low frequency	125 kHz LF Passive	4200 INR	5000 INR	1100 INR	10300 INR
	134 kHz LF Passive	4800 INR	5400 INR	1300 INR	11500 INR
	125 kHz LF Passive (HID Prox Reader)	7950 INR	12400 INR	4900 INR	25250 INR
High frequency	13.56 MHz HF Passive	11500 INR	15900 INR	2900 INR	30300 INR
	13.56 MHz HF Passive (HID)	24000 INR	16000 INR	5500 INR	45500 INR
Ultra High frequency	Gen 2 UHF 865-868 MHz Passive	52000 INR	44000 INR	3200 INR	99200 INR
	Gen2 UHF 902-928 MHz Passive	70000 INR	46800 INR	3500 INR	120300 INR
Active	433 MHz Active	36000 INR	30000 INR	2200 INR	68200 INR
	2.45 GHz Active	68000 INR	48000 INR	6500 INR	122500 INR

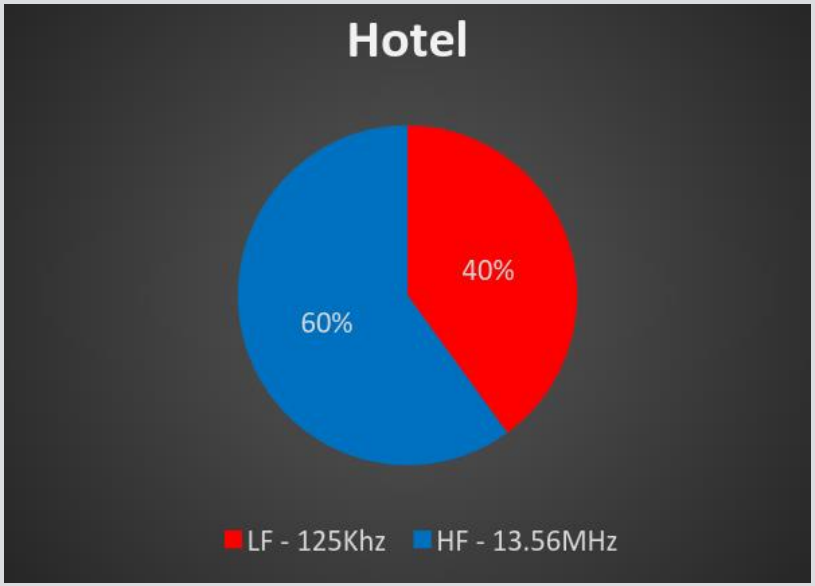
Industry wide usage -1

Name	Description	Card type used
Public Transport	Metro Cards, Travel Cards	MIFARE DESFire 4k | DESFire EV1 2k/4k/8k | Plus 2k/4k SL3 MIFARE Ultralight (MF0ICU1)
Hotels	Hotel Room Access keys, Employee IDs	Ultralight S50 SRI 512 Mifare 1K
Banks	Employee access cards, Debit/Credit cards	EM4001 EM410x Ultralight JCOP J2A040 chip card(TK4100,T5567/5577,S50/70)
Tech Companies	Access Cards, Identification Badges	EM410x Indala MIFARE Classic 1k
Recreation Clubs/ Gyms	Membership cards	Ultralight ICODE SLI(1KB)/ICODE SLI-S(2KB) Ultralight(512bits)/ Ultralight C(193bytes) Tag-it HF-1 Plus(TI 2K)
Tolls	Vehicle ID	Alien Higgs 3 UHF Card EPCglobal Class 1 Gen 2

Industry wide usage - 2



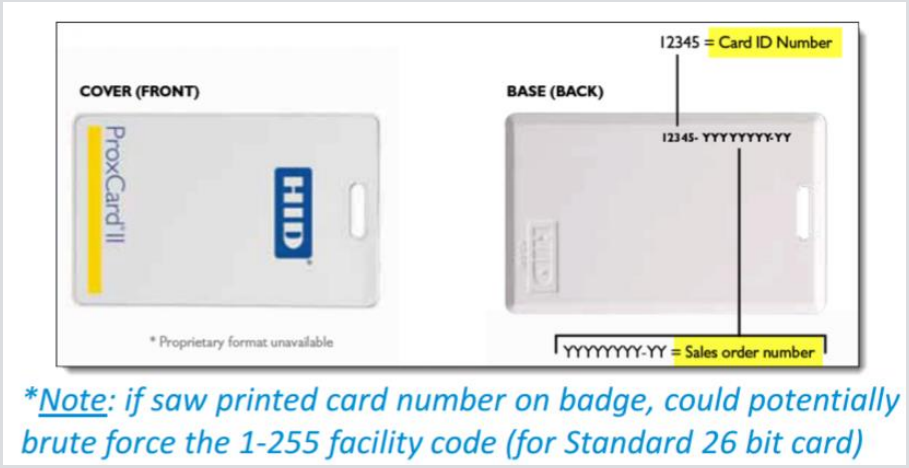




From a survey we conducted by visiting different organizations

Remediation - Users

- Be aware of your surroundings
- Have an RFID safe wallet
- Mask the code if present on your card



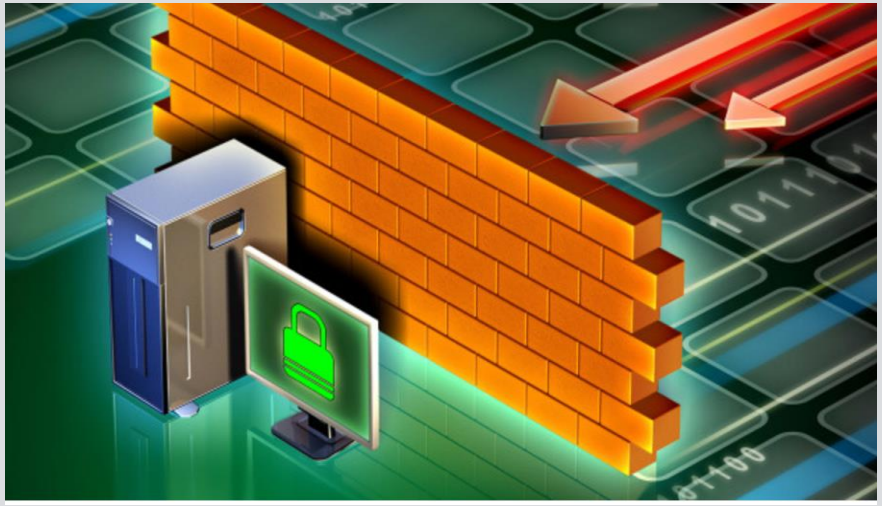
*Note: if saw printed card number on badge, could potentially brute force the 1-255 facility code (for Standard 26 bit card)

DEFCON-21 talk by Francis Brown RFID-Hacking-Updated

Remediation – Organizations - 1

Easy fixes

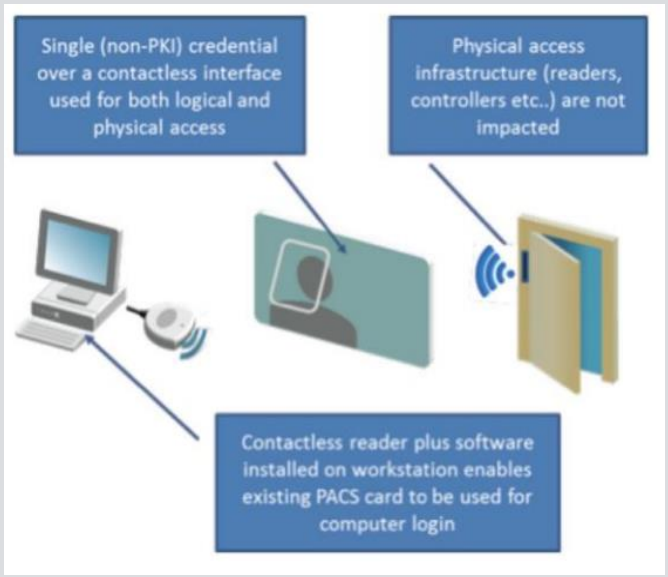
- Provide secure badge holder to employees
- Restrict network access to the RFID Infrastructure
- Add Video monitoring to the RFID readers



Remediation – Organizations - 2

Hard fixes

- Use a secure family of cards/readers
- Second form of authentication – PIN or One time password
- Active RFID that uses encryption, mutual authentication & has replay protection



http://visionlab.tudelft.nl/sites/default/files/IWRT08.pdf

Conclusion – Key takeaways

- Find out the frequency of your card
  - LF is not secure
  - Plan on migration if insecure card technology is being used

- Cost consideration
  - LF (HID) is 2.5 times the cost of LF (standard)
  - HF (secure) is 4.5 times the cost of LF (standard)

- Remediation
  - [Individual]: Buy an RFID Wallet
  - [Organization]: Secure badge technology

THANK YOU

-Sarwar
(@sarwarjahanm)

-Ashwath
(@ka3hk)