DEI
DIPARTIMENTO DI
INGEGNERIA DELL'INFORMAZIONE

UNIVERSITÀ
DEGLI STUDI
DI PADOVA

University of Padua – Department of Information Engineering

Bachelor's Degree in Information Engineering

Final Report

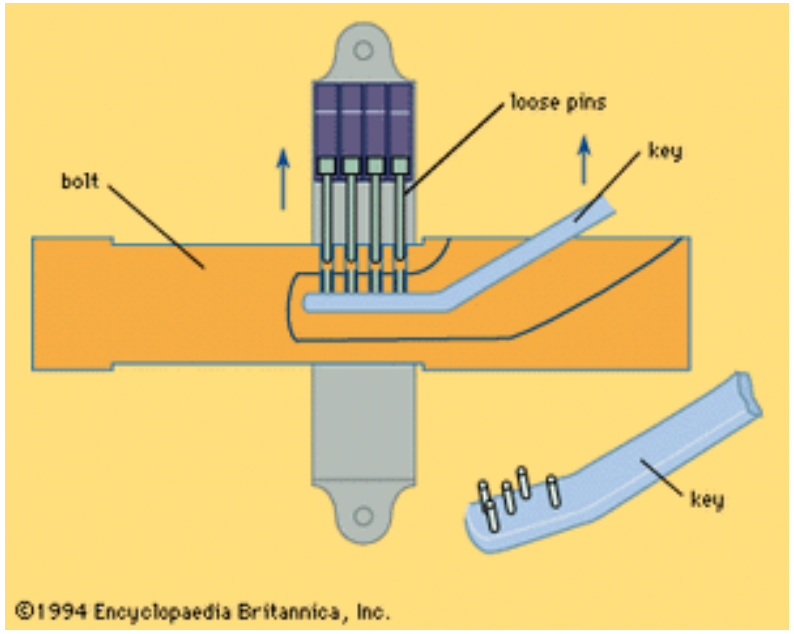
Electronic Control Access: A passing trend or a new standard?

Supervisor: Prof. Matteo Meneghini

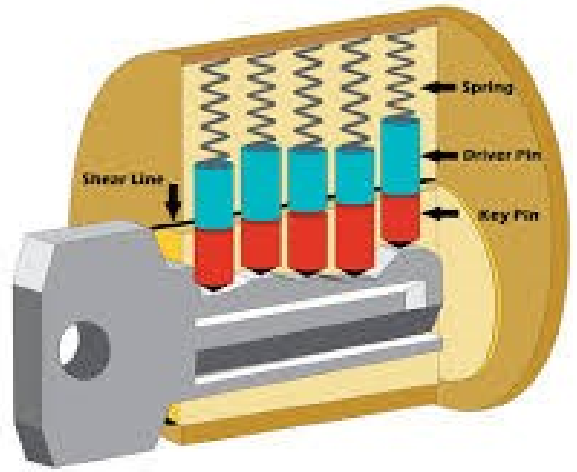
Graduate Student: Jovan Mijovic
Student ID: 2081286

Padua, 13/3/2026

INTRODUCTION



Among the earliest instances of usage of locks, Egyptian lock



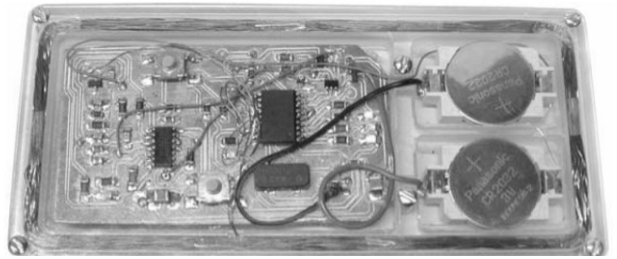
Modern pin tumbler lock, designed after the mechanism of the Egyptian lock

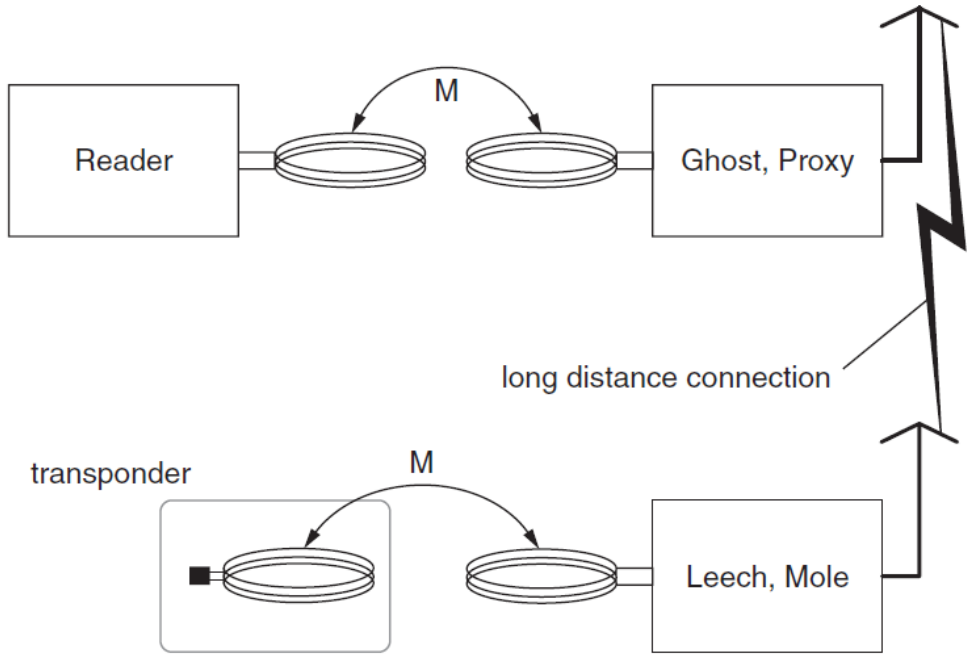
RFID for Control Access

- RFID stands for Radio Frequency IDentification
- First used in WWII as part of the IFFF system
- The system consists of tags/cards, readers, and backend database
- Many variations of RFID systems exist
- Reader supplies power, and the clock cycle to be used to transmit the data from the tag to identify the user

Potential attacks on RFID Control Access System

- Spoofing attack
  - Potential solution: Encryption (Mutual symmetric authentication)

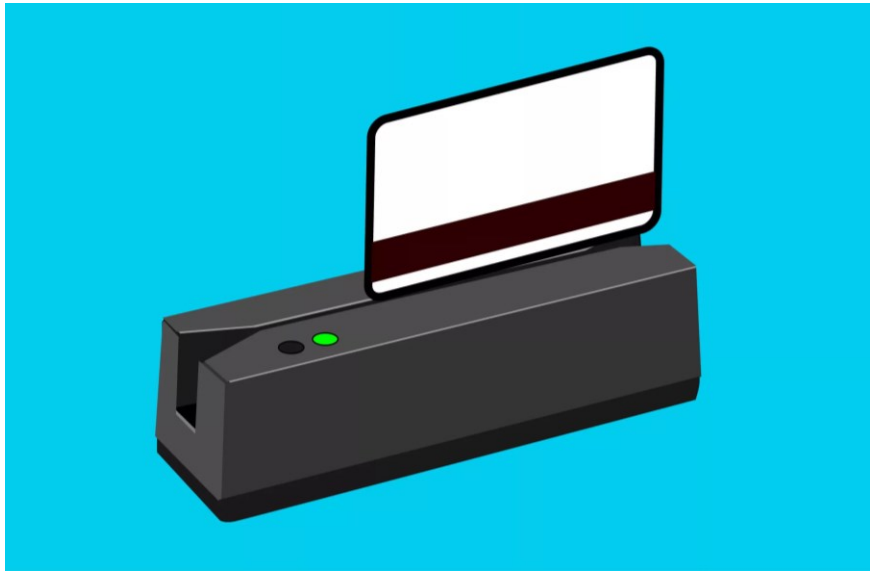


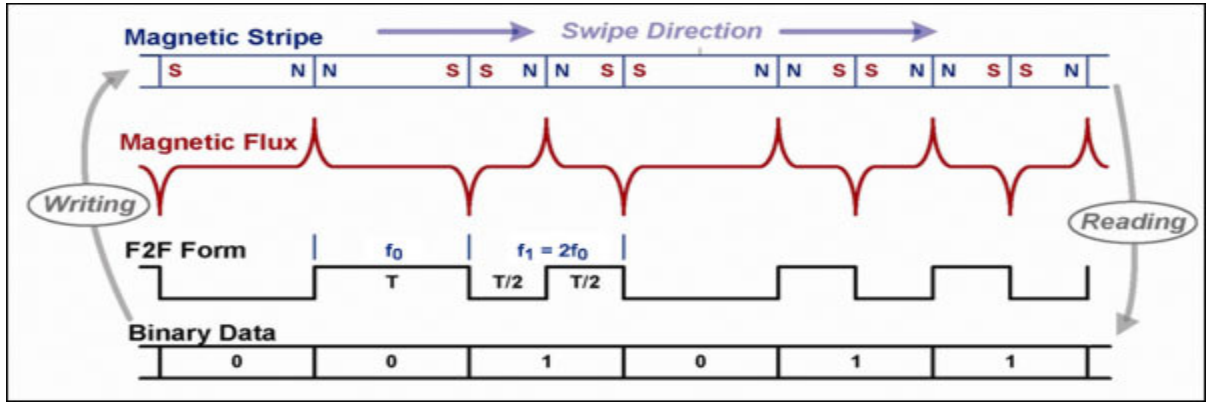


- Relay attack
  - Potential solution: Distance bounding protocols

Magnetic Stripe for Control Access

- First used for speech recording
- Uses multiple tracks
- Coercivity (Oersted)
- Differential Manchester encoding (F2F)



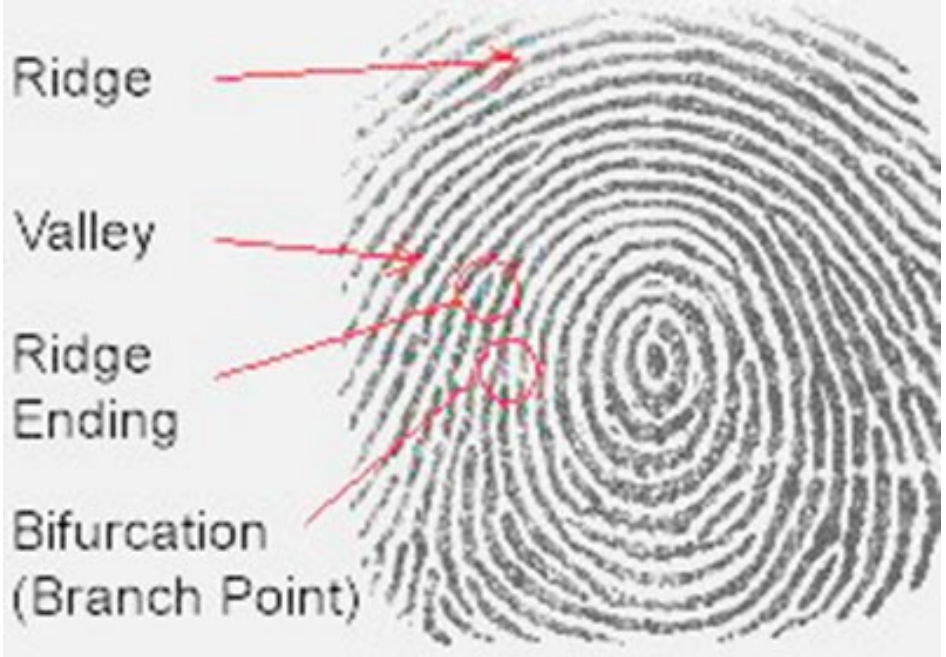


Potential attacks on Magnetic Stripe Control Access System

- Main way of attack is skimming
- Pin code skimming
- Potential solution: Image processing

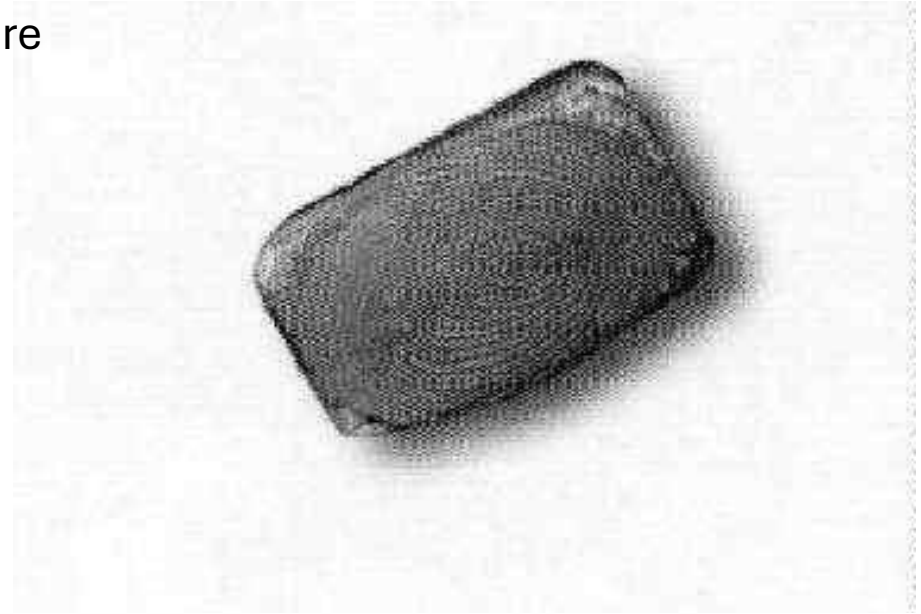
Biometrics (Fingerprint recognition) for Control Access

- First used in ancient Babylon to identify merchants
- Sensor scans the fingerprint (optical, thermal)
- Minutiae
- Types, coordinates and direction
- Comparison
- Threshold check



Potential attacks on Biometrics (Fingerprint recognition) Control Access System

- Presentation attack (copying a fingerprint without cooperation)
- Potential solution: Pairing with another identification procedure



- Hill climbing attack
- Potential solution: Quantization of the matching score

Comparison

	Traditional locks	RFID	Magnetic stripe	Fingerprints
Distance of the attacker	Physical/ Completely remote	~10m	Physical	Physical/ Completely remote
Upgradability of the system	Security pins	Encryption/ Distance bounding protocol	Limited	Minutiae matching/ Non uniform quantization
Drawbacks	Granting access to a large amount of people	Completely remote attacks	Demagnetization	False rejections

CONCLUSIONS

- No lock is unbreakable, no system unbeatable
- Control access mechanisms are just a part of the system
- Combination of systems is preferable
- Important to consider alternative bypass methods
- Educating the consumer on potential dangers

Pictures from:

https://www.britannica.com/technology/lock-security

https://www.southord.com/blogs/news/understanding-the-anatomy-of-different-lock-types

https://www.vergetechnologies.ca/home

Finkenzeller, K. (2010). *RFID handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication*. John Wiley & Sons.

https://www.szhcct.com/what-do-you-know-about-magnetic-stripe-card-reader_n139

https://www.analog.com/cn/resources/app-notes/improve-magnetic-card-reading-in-the-presence-of-noise.html

https://www.ricreditunion.org/information-resources/fraud-and-security-center/atm-skimming/

https://atmeye.com/blog/atm-skimmer/

http://www.sciencedirect.com/science/book/9781597499897

https://www.securityinfowatch.com/access-identity/article/53069444/ai-advanced-analytics-that-bring-value-to-access-control-systems