Advanced Cyber Security

SFWRTECH 4NS3

Social Engineering and Physical Penetration Testing

McMaster University ENGINEERING

W BOOTH SCHOOL OF ENGINEERING PRACTICE AND TECHNOLOGY

Lecture Overview

- Social Engineering
  - Vectors
  - Motivation Techniques
- Physical Penetration Testing
  - Doors
  - Locks
  - RFID Cards
- Let's have a (Ka)hoot together!

Social Engineering

Weakest Link (2000-2012), BBC

Social Engineering

- Vectors
  - Pretexting
    - Impersonation to create a situation in which a target divulges information (elicitation)
  - Phishing
    - Sending a link or attachment that appears to be from a trusted source
  - Spear phishing
    - Directly targeting specific individuals or companies with a customized email
  - Smishing
    - SMS phishing, messages sent with links or malware
  - Vishing
    - Voice phishing by conducting an attack via telephone
  - Whaling
    - Similar to spear phishing, but targeted at senior executives or key individuals

Social Engineering

- Vectors (continued)
  - Pharming
    - Redirecting a target from a valid site to a malicious one
  - Malvertising
    - Malicious ad on a trusted or legitimate website
  - Watering hole
    - Compromising a site that is trusted and regularly visited by a victim
  - Baiting
    - Leaving malware-infected media to be found
  - Tailgating
    - Following someone into a secured location
  - Quid pro quo
    - "Something for something"

Social Engineering

- Motivation Techniques
  - Authority
    - Projecting confidence and authority
  - Curiosity
    - Exploiting the natural curiousness of people
  - Empathy
    - Appealing to a moral obligation
  - Familiarity
    - The concept of likeability or similarity
  - Frugality
    - Related to greed
  - Intimidation
    - Leveraging fear

Social Engineering

- Motivation Techniques (continued)
  - Scarcity
    - Limiting quantities
  - Social proof
    - Leveraging a desire to conform or groupthink
  - Temptation
    - Appealing to illicit or taboo desires
  - Trust
    - Pretending to be a trusted person or source
  - Urgency
    - Creating a time constraint

Social Engineering

Live Free or Die Hard (2007), 20th Century Fox

Social Engineering

Mr. Robot (2015), NBCUniversal

Suspicious sign-in attempt prevented.

SS

Security Service <no-reply@mcmaster.ca>
To [redacted]@mcmaster.ca

Someone recently used wrong passwords to try to sign in your [redacted]@mcmaster.ca account.
We prevented the sign-in attempt in case this was a hijacker trying to access your account.

Please review the details of the sign-in attempt.
http://ajuniperjupiter.com/tnx3
Click or tap to follow link.

If you do not recognize this sign-in attempt, someone else might be trying to access your account.
You should check activity.

TJ

Thu 4/5/2018 10:36 PM

Timothy J.Taylor <tim1989@yahoo.com>

Updated Resume

To Herman Poon

TT_Application.zip.html
264 bytes

Hi Herman,

John in your department recommended that I reach out to you as you could possibly be of assistance. I am a recent graduate of McMaster and am reaching out to see if there are any openings in your department or any other areas in the University,

I'm very excited to hear about any opportunities that Mac may have. I would love to hear back from you about any current or future position.

Attached is my current resume. Please let me know what you think and when we can connect for a face-to-face interview. Hope you have a great day, thanks,

Regards
Timothy AllenTaylor

Migrate your account in order to use it

Outlook.Web.App@pinegw06.uts.mcmaster.ca
To [redacted]@mcmaster.ca

Reply | Rep

Outlook Web App

We're happy to let you know that your email account is ready for update.

We are migrating all email accounts into Outlook Web App 2020 and as such all active Account Holder are to verify and Log in for the update and migration to take effect now.This is done to improve the security and efficiency due to recent spam emails received.

Remember, if you don't update your account in 24 hours,your email address will be closed without any chance of backup.

To update your account,simply click on the update and migrate button below.
http://rekify.com/vendor/outlook-web-app/migrate/
Click or tap to follow link.
ake sure to sign in on the migration page.

Update and Migrate »

2020 Outlook Web App

REQUEST..

DF

David Farrar <excutivmannagment@gmail.com>
To [redacted]

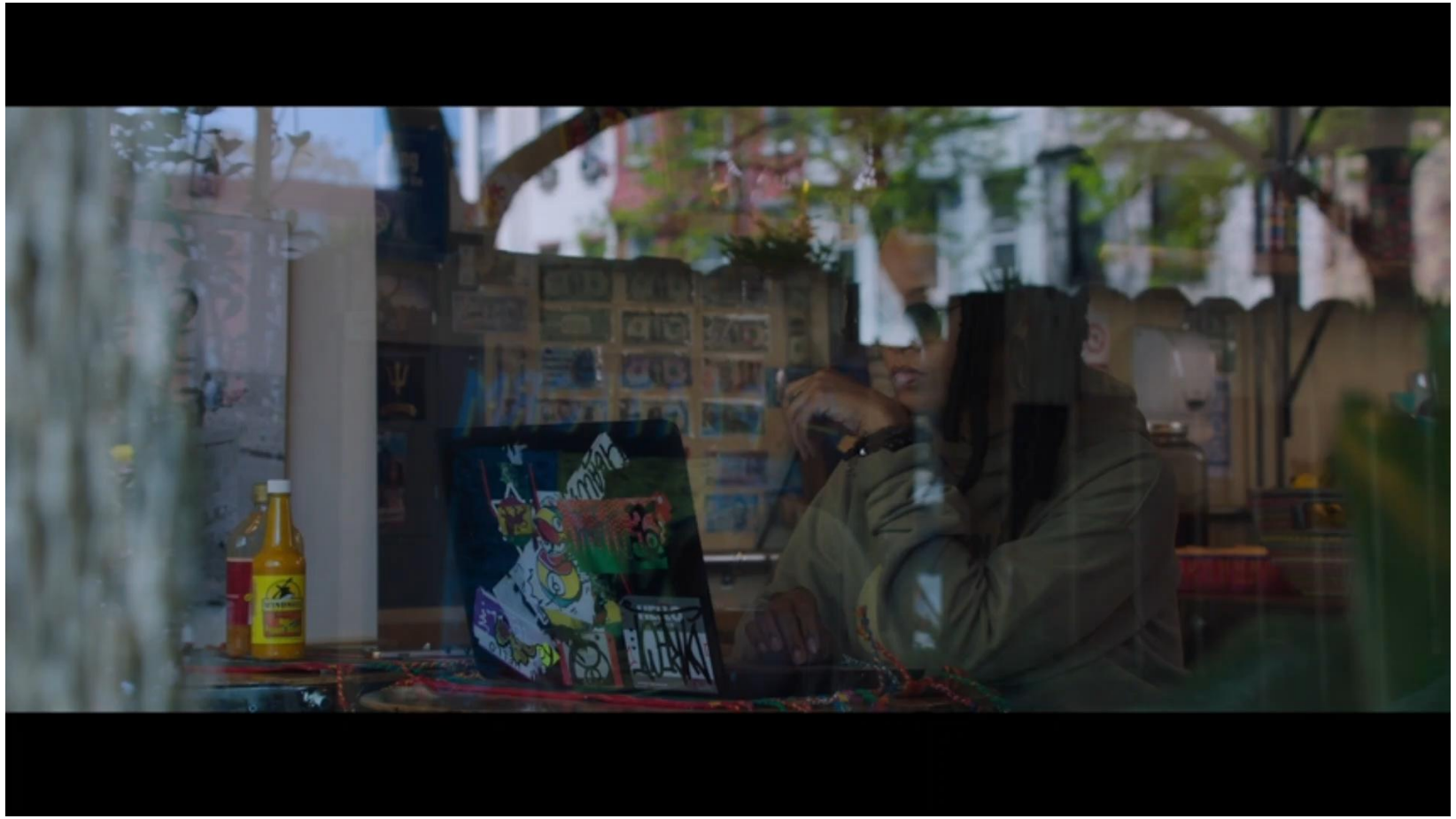
I have a task you need to handle immediately, confirm your availability.

Thanks.
David

Social Engineering

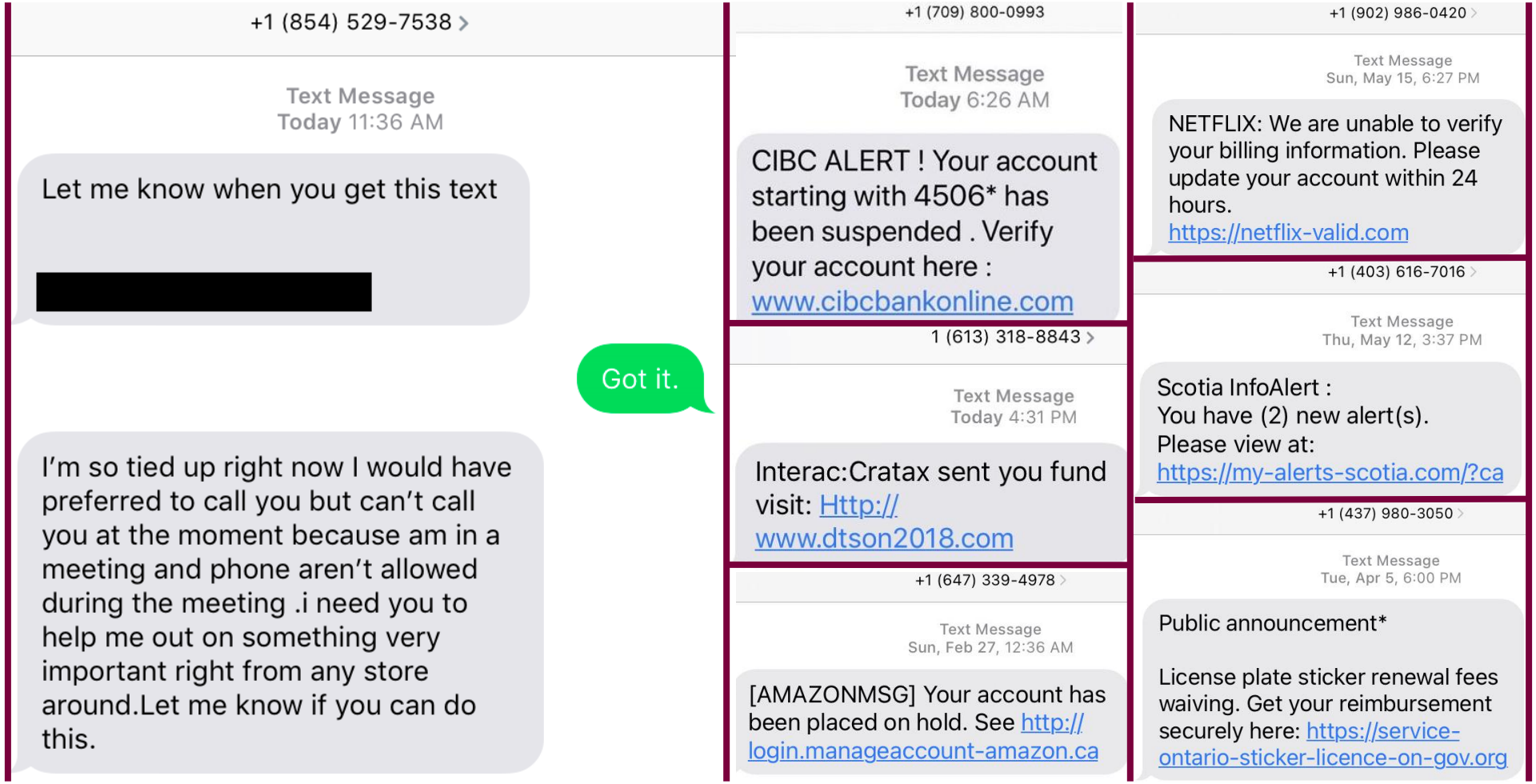
Sneakers (1992), Universal Pictures

Social Engineering



Ocean's 8 (2018), Warner Bros.

Social Engineering



Social Engineering

Mr. Robot (2015), NBCUniversal

Role-playing Scenario

Social Engineering Exercise

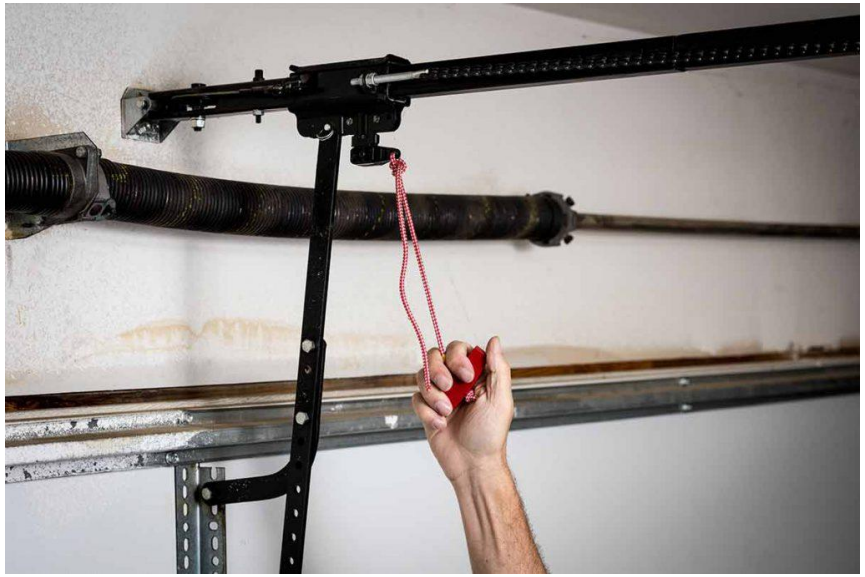
- Breakout Room Exercise/Discussion
  - Approximately 15-20 minutes will be provided in the breakout rooms
  1. In your group, choose an organization from a specific (but any) vertical
     - E.g. higher education institution, government (municipal/provincial/federal), non-profit, technology, engineering, manufacturing, financial, construction, health care, retail, legal, etc.
  2. Decide who your target is (e.g. what employee role) for your social engineering attack
  3. Decide what information you want to obtain and/or what action you want the target to perform
  4. Focus on **one** specific vector to deliver your attack
     - Vectors: Pretexting, Phishing, Spear phishing, Smishing, Vishing, Whaling, Pharming, Malvertising, Watering hole, Baiting, Tailgating, Quid pro quo
  5. Identify the motivation techniques you will leverage to plausibly achieve your objective via that vector
     - Motivation Techniques: Authority, Curiosity, Empathy, Familiarity, Frugality, Intimidation, Scarcity, Social proof, Temptation, Trust, and Urgency
  6. Elect someone from your group to post a summary to the discussion forum after the class

Physical Penetration Testing

- Reminder re: Disclaimer from Lecture 01
- Warning – physical penetration testing is **dangerous**!
- Physical Security Domains
  - Premises: perimeter, lighting, locks, access control, environmental, surveillance, guards, etc.
  - Technical: authentication, authorization, power, EMI/RFI, etc.
  - Operational: policies and procedures, logging, auditing, etc.
- MITRE Command Attack Pattern Enumerations and Classifications (CAPEC)
  - CWE: the root cause of a vulnerability
  - CVE: a specific instance of a weakness resulting in a vulnerability
  - CAPEC: how a weakness can be exploited

Physical Penetration Testing

- Doors
  - Hinges
  - Handles
  - Latches
  - Garages



Physical Penetration Testing

- Doors
  - Crash bars
  - REX sensors

Security Astragal

Mullion

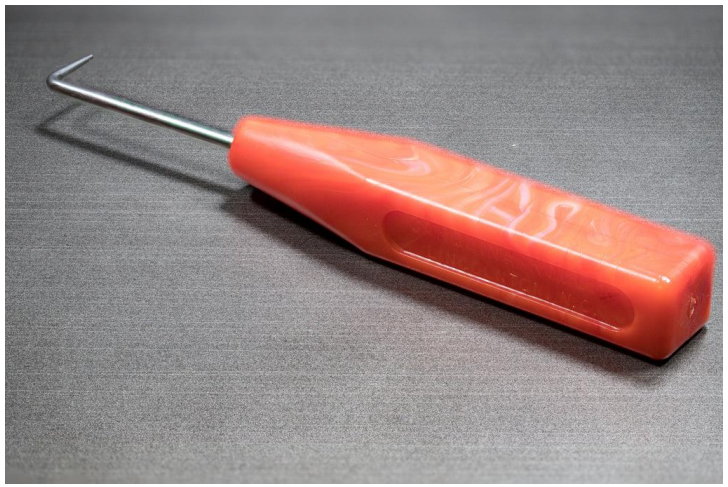
Physical Penetration Testing

https://www.youtube.com/watch?v=o8T-L4SNGmU

Physical Penetration Testing

- Common Bypass Tools for Loiding Latches

Traveler hook (Shrum tool)



Jim tool

Plastic shims

Physical Penetration Testing

- Locks and Lock Picking – Criminal Code of Canada
- Section 351, Possession of break-in instrument

(1) Every person who, without lawful excuse, has in their possession any instrument suitable for the purpose of breaking into any place, motor vehicle, vault or safe knowing that the instrument has been used or is intended to be used for that purpose,

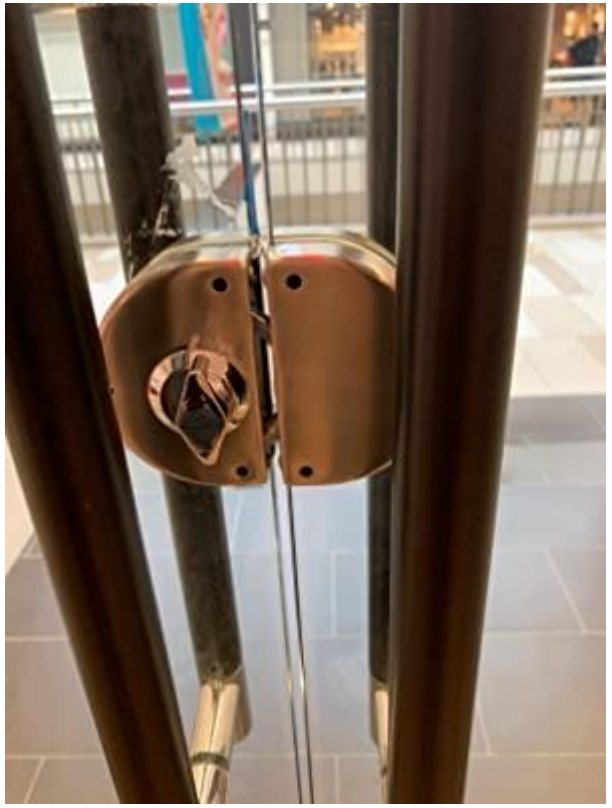
(a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years; or

(b) is guilty of an offence punishable on summary conviction.

Physical Penetration Testing

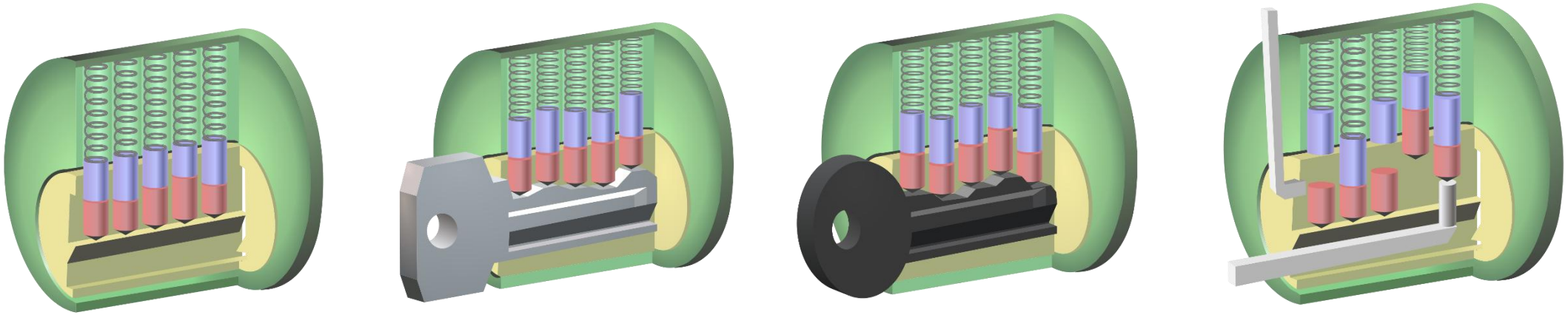
- Keyed Locks
  - Entry lock vs. deadbolt

Thumb turn tool



Physical Penetration Testing

- Keyed Locks
  - Pin tumbler design and operation
  - Bumping



Physical Penetration Testing

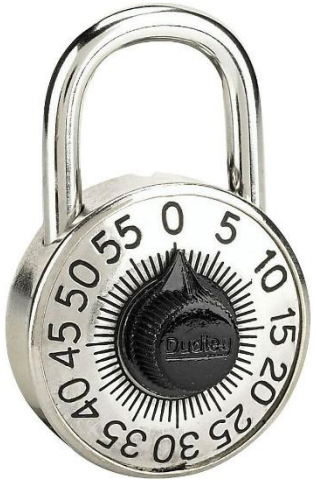
- KABA Simplex Series 1000
  - Mechanical, keyless operation
  - Push-button door lock
  - Susceptible to bypass with a strong magnet

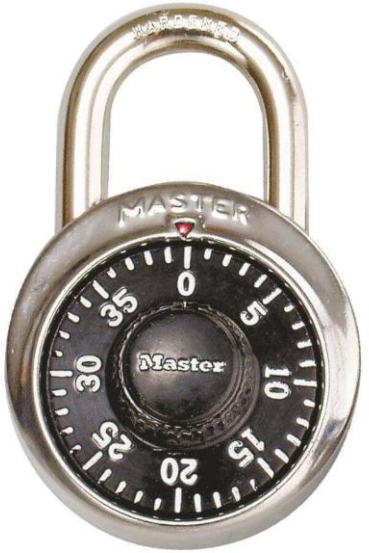
Physical Penetration Testing

https://www.youtube.com/watch?v=c2DcfJLquOk

Physical Penetration Testing

- Combination Padlocks
  - Typically all susceptible to some form of bypass or shortcut; no need to brute-force!

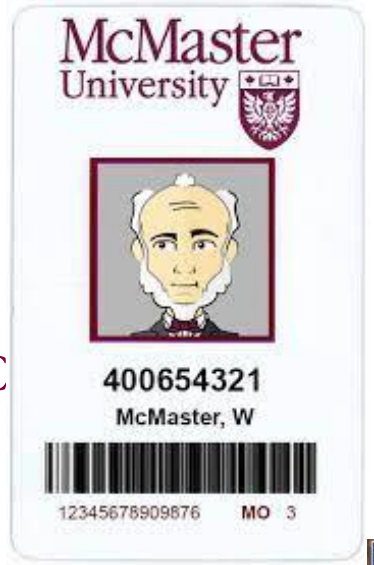


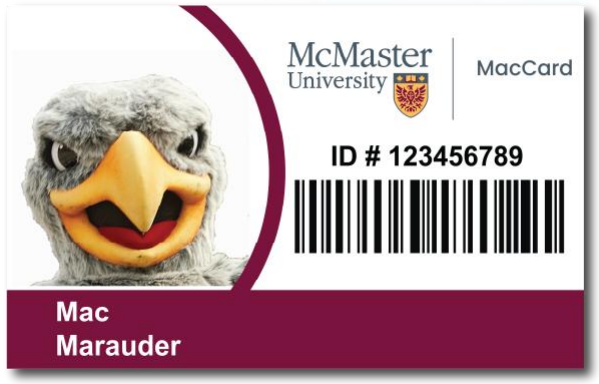


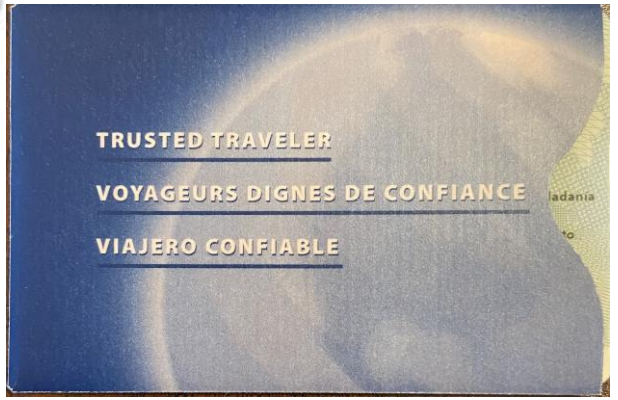
Physical Penetration Testing

- RFID Cards
  - Proximity cards

Regular PVC cards







Physical Penetration Testing

- RFID Cards
  - Proximity card
    - Passive or active, 125 kHz (low-frequency)
    - Standard 26-bit Wiegand format (or other various formats with additional storage)

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
P	Facility Code (8 bits)									Card Number (16 bits)															P

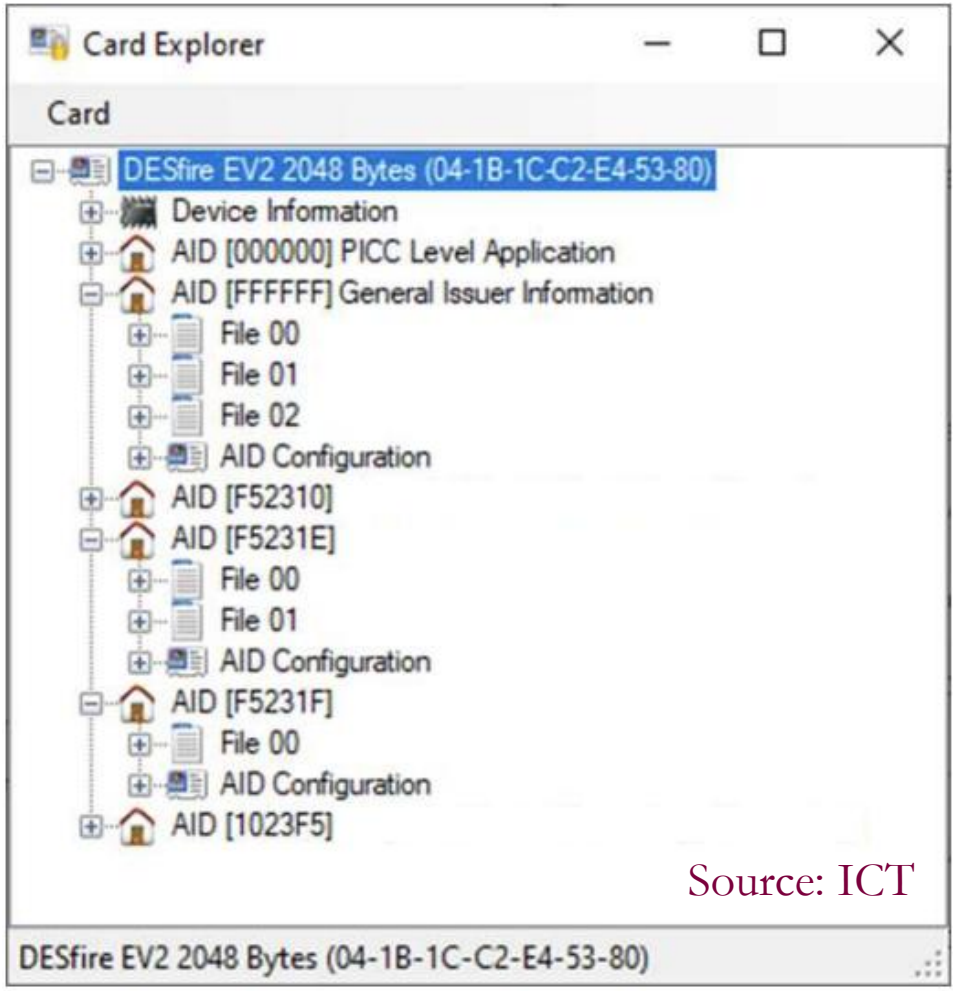
    - P: leading and trailing parity bits
    - Facility Code is "unique" to an organization to help avoid duplication

Physical Penetration Testing

- RFID Cards
  - Contactless smartcard
    - ISO/IEC 14443 standard (contactless IC cards)
    - 13.56 MHz (high-frequency)
    - Storage typically ranging from 2 kiB to 8 kiB
    - Data rates typically ranging from 106 to 848 kbps
    - Support cryptographic protocols such as 3DES, AES
    - Debit/credit cards are typically the EMV (chip+PIN) format
    - PRESTO Card is a MIFARE DESFire EV1 format
      - Applications typically secured by symmetric encryption key
    - UID/CSN: readable by anyone

Physical Penetration Testing

- RFID Cards
  - Contactless smartcard
    - MIFARE DESFire
    - Separate applications identified by AIDs
      - EV1: max 28, EV2/EV3 limited only by storage
    - Each application has one or more Files which can store data, identified by FIDs (max 32)
    - Multiple keys can be assigned to applications
    - Files can have different keys to read, write, or read/write
    - Keys may be diversified (unique to the card)



Source: ICT

Physical Penetration Testing

https://www.youtube.com/watch?v=gbn3JtoFdPg

Lecture Summary

- We have learned about:
  - A variety of attack vectors for performing social engineering
  - Several motivation techniques to convince targets to becoming victims
  - Physical security considerations for doors, locks, and RFID cards
- Chapter 5 Readings
- Additional references:
  - CAPEC-390, Bypassing Physical Security: https://capec.mitre.org/data/definitions/390.html
  - TheNotSoCivilEngr: https://www.youtube.com/user/amihirata/videos
  - LockPickingLawyer: https://www.youtube.com/c/lockpickinglawyer/videos
  - Lockpicking by Deviant Ollam: https://deviating.net/lockpicking/

Game Time!

Let's have a Kahoot! together!

- Open your web browser and go to: kahoot.it
- Game PIN: enter as shown/instructed
- Nickname: you will receive a randomly-assigned name