Written by Thapanapong Rukkanchanunt

Updated by Prakarn Unachak

Internet Security

Online Threats

- There are many dangers from using the web (and computer in general).
- One should watch out for **malware**, automated programs designed to cause harm to you, your data, and your system.
- You are also vulnerable from attacks by **hackers**, those who seeks and exploits weaknesses in a computer system or computer network.
  - This include human using them!
- https://www.youtube.com/watch?v=AuYNXgO_f3Y

Malware

- Virus/Worm
  - Self-replicating. Can spread through e-mail, malicious link, USB drive, etc
  - Can reside in (sometime important) part of hard drives
- Trojan horse
  - Imitate a legitimate program

- Malware can:
  - Damage files
  - Use up memory
  - Display annoying popups
  - Stealing data
  - Create backdoor
  - Gain control to your computer (creating “zombie” or “bot”)
  - Hold your data/computer hostage (“Ransomware”)

Hackers

- Someone who seeks and exploits weaknesses in a computer system or computer network.
  - Can be for good cause (“White Hat”): educational, or security concern
    - Can alert weakness to owner of software/website for “bounty”
    - https://www.facebook.com/whitehat
  - Sometime illegally for personal gain (“Black Hat”): blackmail, data theft, entertainment, political or other causes (“Hacktivist”)
  - And sometime both (“Grey Hat”)

Example of Attacks

- Using computer systems with no authority to gain such access
- Other examples from the media
  - Employees steal time on company computers to do personal business
  - Intruders break into government Web sites and change information displayed
  - Thieves steal credit card numbers and buy merchandise
- Hackers gain access by
  - Using software weakness at the target (“exploit”)
  - Trick people work at/for the target to give access (“Social Engineering”)

Example of Attacks (cont.)

- Denial-of-service (DOS) or Distributed DOS (DDOS)
  - Attempt to make a machine or network resource unavailable to its intended users.
  - Usually by repeatedly trying to connect/ request service to the target, disrupting it.
  - DDoS will consist of many computers under attackers' control ("bot/zombie farm")

Example of Attacks (cont.)

- Cyber Stalking
  - Use of computer/network technologies to stalk or harass one or more persons
  - Activities
    - Defamation
    - Gathering information
    - Identity theft
    - Monitoring (esp. on Social Network)
    - Threats

Example of Attacks (cont.)

- Identity Theft: Pretending to be someone else, for malicious purpose
  - Criminal Identity Theft
    - Pretend to be someone else when arrested
  - Financial Identity Theft
    - Credit card, loans, etc
  - Identity cloning
    - Living as someone else
  - Medical Identity Theft
    - Using other's ID to obtain drug
  - Child Identity Theft
    - Using Child's ID
- Use information gather (partially) from the web

Example of Attacks (cont.)

- Phishing
  - Attempt to obtain sensitive information, often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.
  - Information can be: username/password, credit card details, ID, bank account, etc.
  - Usually comes in the form of e-mail pretending to be from back/government agency/school/etc.
    - Ask you to "log in"/ provide personal information on the website with the URL provided in the e-mail.
    - Website is fake, created to collect your personal information

Internet Security

- Internet Security is the protection of messages communicating within the Internet from theft and forgery
- There are two categories of protection
  - Authentication: Identify the sender/receiver
  - Authorization: Limit accessibility for individual entities

Authentication

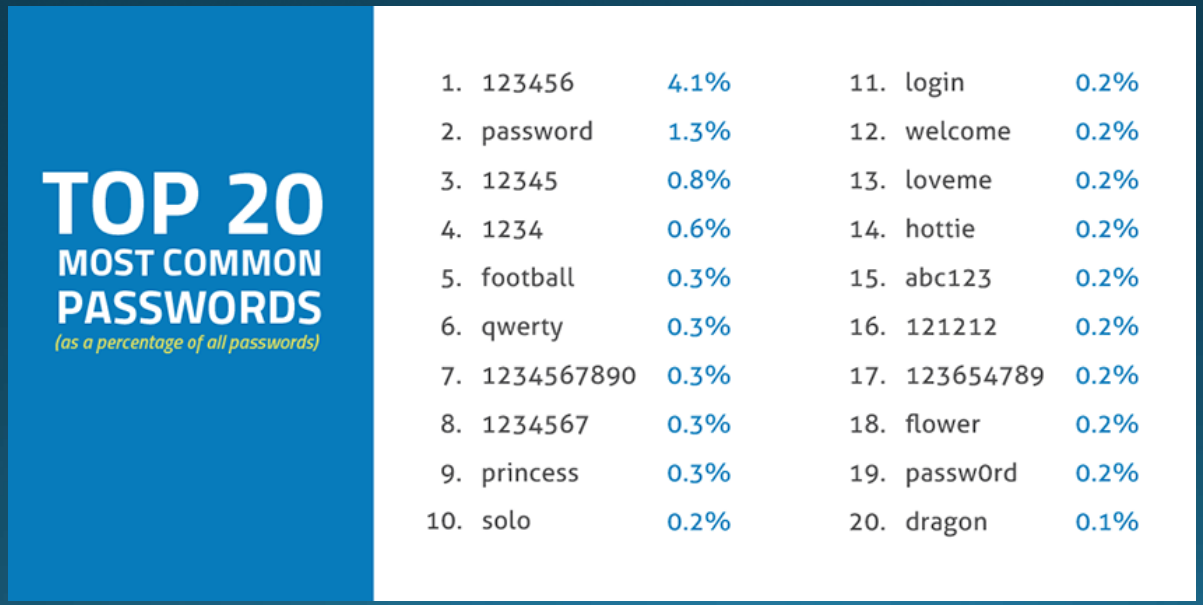
- Authentication is an identification process that verifies that a person who wishes to access the data is the real user
- There are 3 techniques used in authentication
  - Possession
  - Memorization
  - Physicality
- Also, the more secure way of authentication is to required **Two-factor Authentication**, performing two different authentications at once.

Possession

- Use manmade objects to verify the identity such as
  - ID Card / Credit Card
  - Authenticator that generates random number with pre-determined seed

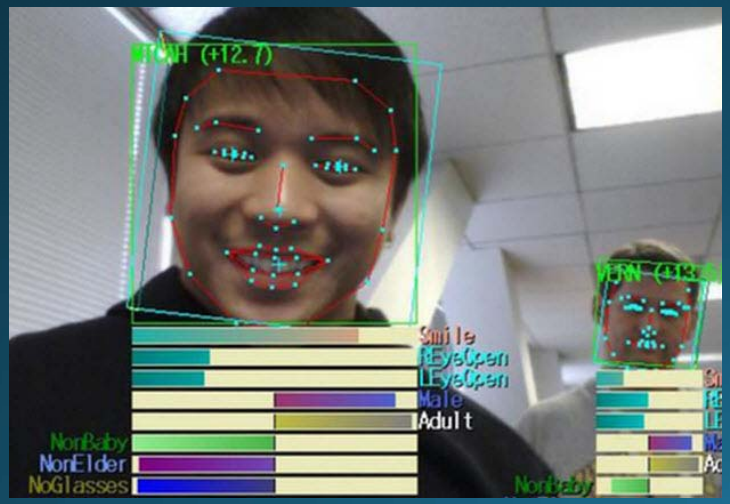
Memorization

- Use password



Physicality

- Use human physical appearance (dictated by DNA) such as face, eye, fingerprint, palm, voice or a combination of those



Limitation

- Limitation of Possession
  - Theft / Renewable
  - Forgery / Duplicable
- Limitation of Memorization
  - Easily guessed weak password / Hard-to-memorize strong password
  - Risk of scamming from public use
- Limitation of Physicality
  - Need special equipment / can be forged (but take effort)

Authorization

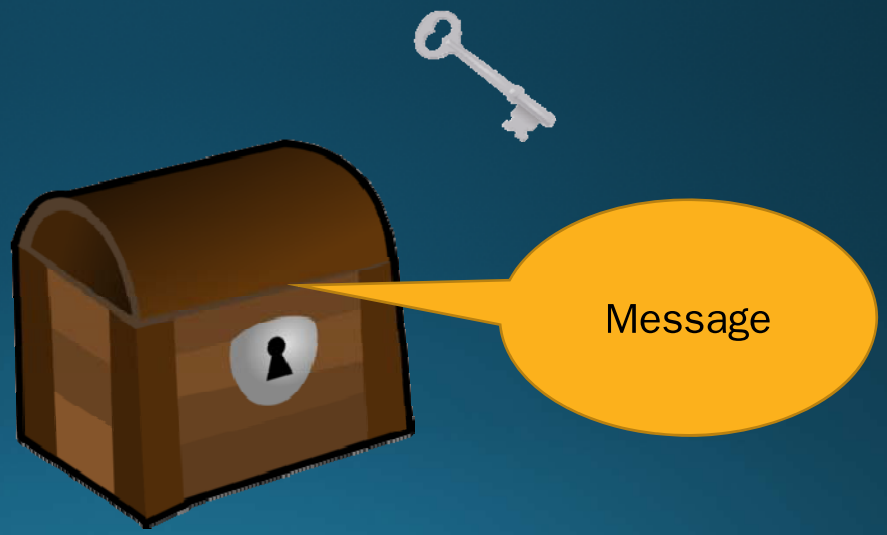
- Authorization assigns different access permission to different individuals based on their rank or importance
- Users of the same rank cannot access each other data
- Users with higher rank may be able to see lower rank data but should not be able to modify it without consent from lower rank user
- Should Mark Zuckerberg be able to see our relationship status on Facebook while our friends cannot?

Encryption and Decryption

- There is no guarantee that our message sent to the Internet cannot be bugged so we need a way to hide our message and make sure that only our friends can reveal it
- We use the method called Public Key Cryptography to encrypt our message
- https://www.youtube.com/watch?v=ZghMPWGXexs

Key and Lock analogy

- Let’s say that we put our message into a chest
- We lock the chest using a KEY
- We send the chest to your friend
- How would your friend open it?

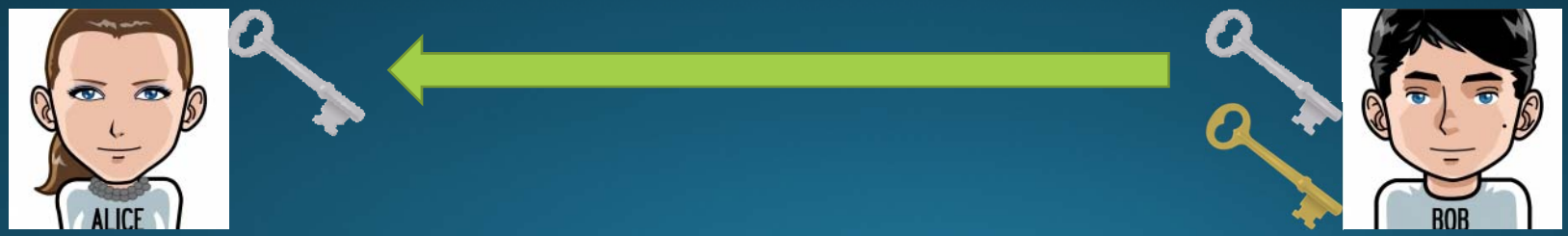


Twin keys

- In real world, we use the same key that locks the chest to open the chest
- In the Internet, we can create what is called twin keys
- One key can open the chest only if its twin locks the chest
- That means that if we lock the chest with one key, that key cannot open the chest

Encryption with twin keys

- Alice wants to send a message to Bob
- Bob creates twin keys, say gold key and silver key
- Bob distributes silver key to everyone

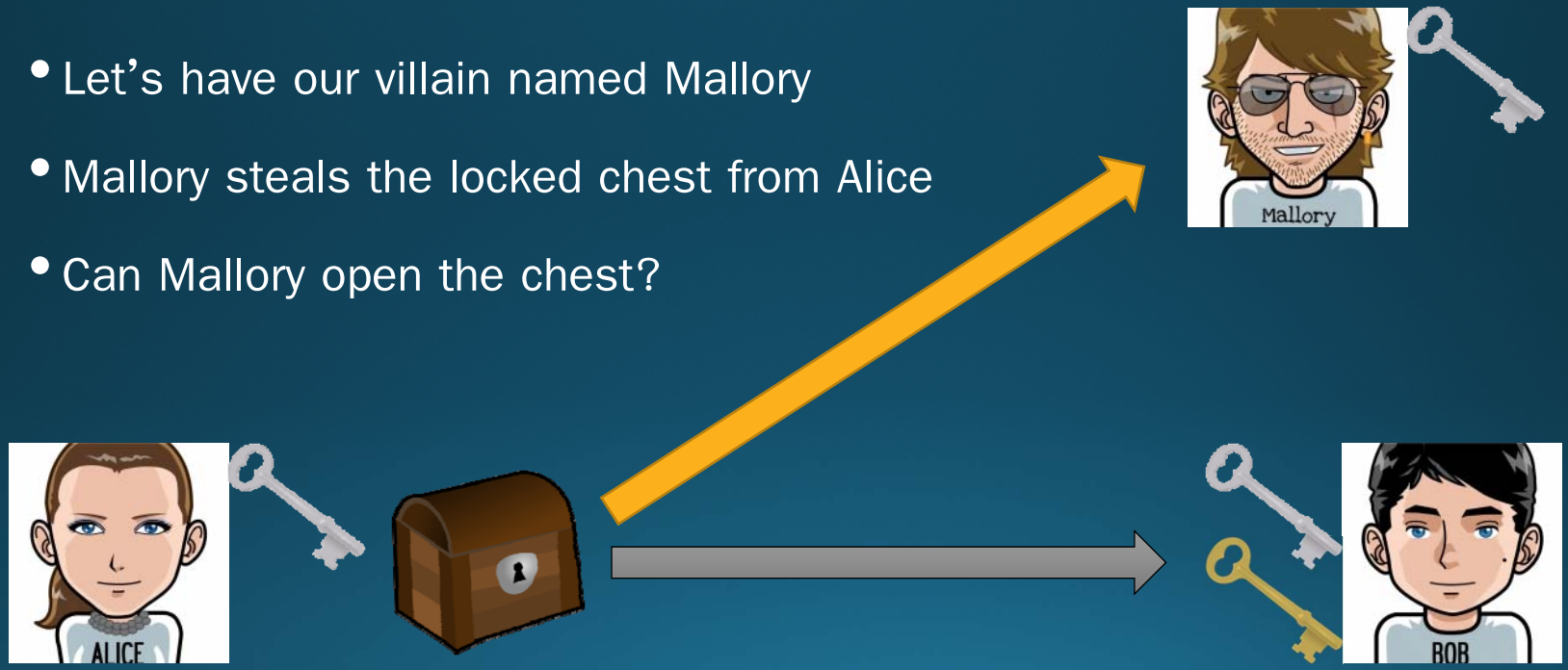


Encryption with twin keys (2)

- Alice uses silver key to lock the chest containing her message
- Alice sends the locked chest to Bob
- Bob opens the lock with gold key and retrieves the message

Why is it safe?

- Let's have our villain named Mallory
- Mallory steals the locked chest from Alice
- Can Mallory open the chest?



Twin keys creation and their security

- Do twin keys really exist? If so, how do one create them?
- Twin keys uses concept of Mathematics, specifically number theory
- Basically twin keys are two magic numbers that related in some way
- Knowing one number cannot help deducing another number
- The time to guess gold key using silver key is beyond the age of the universe!!!

Dark Side of Encryption: Cryptowall/Ransomware

- Malware that uses encryption to lock you out of your system/data
- Usually disguised as harmless attachments on e-mails, tricking you to open them.
- Once activated, the cryptowall encrypts files on your computers (and sometime those in the same network)
- Usually, cryptowall works as **ransomware**: a ransom note if left on your computer, detailing how to pay the ransom to get your files decrypted.

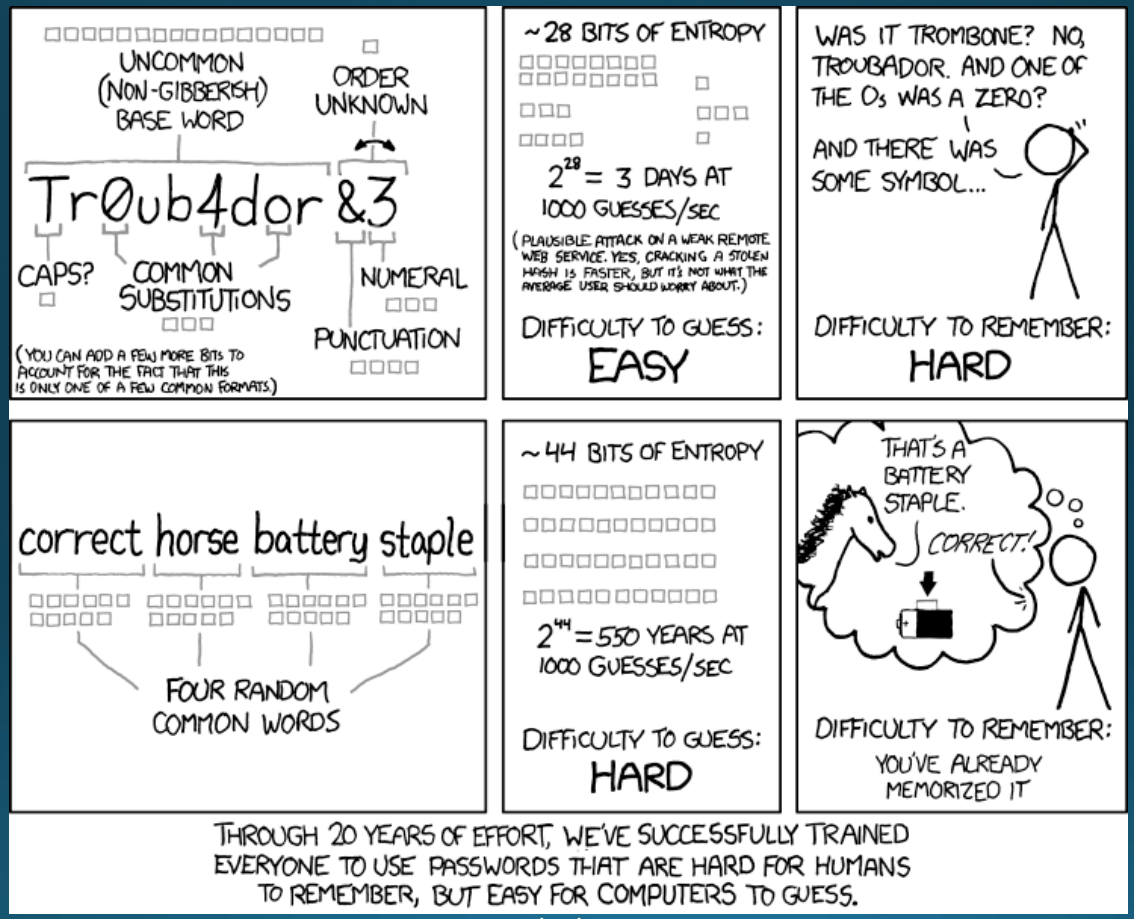
Stay safe online

1. Take cautions before clicking any attachment/ link
2. Take EXTRA cautions before sharing any personal information (or anything else)
3. Set privacy setting on social network properly
4. Install (trustworthy) security programs
   - Antivirus/ Antispyware/ Backup/ Firewall
5. Practice Password Discipline
6. Logout from Facebook/Google/etc. after you're done using public computer
7. Set password for lockout screen for your PC/Phone/Tablet

- https://www.youtube.com/watch?v=GCWBf7WKYyA

Password Security

- **NEVER SHARE PASSWORD**
- Change password often
- Use different password for different sites
  - In case one got hacked
- Use strong password
  - Hard to guess, even if the attacker know your personal information
  - (Should not be so hard that you can't remember it)
  - Avoid: `123456`, *password*, *admin*, pet's name
- Secret Question
  - Option to recover your account
  - Should you use correct answer?



source:xkcd.com