CS1102
Lecture 7
Privacy, Security, and Ethics

Semester A, 2020-2021
Department of Computer Science
City University of Hong Kong

Concerns with Computer Technology

- Technology can have both positive and negative impacts on people
- Effective implementation of computer technology involves maximizing its positive effects while minimizing its negative effects
- Most significant concerns are:
  1. Privacy
     - What are the threats to personal privacy and how can we protect ourselves?
  2. Security
     - How can access to sensitive information be controlled, and how can we secure hardware and software?
  3. Ethics
     - How do the actions of individual users and companies affect society?

Privacy

- Privacy concerns the collection and use of data about individuals
- Three primary privacy issues:
  1. Accuracy
     - the responsibility of those who collect data to ensure that the data is correct
  2. Property
     - the ownership of the data
  3. Access
     - the responsibility of those who have data to control who is able to use that data

Large Databases

- Large organizations are constantly compiling information about us
- Data is gathered about us everyday and stored in large databases, e.g.,
  - Telephone companies compile lists of numbers we call and our locations
  - Credit card companies track cardholder purchases, payments and credit records
  - Supermarkets record what we buy, when we buy, how much we pay
  - Financial institutions record how much money we have, what we use it for, how much we owe
  - Search engines record search histories of their users including search topics and sites visited
- The size and number of databases are exploding. This ever-growing volume of data is referred to as **big data**

Electronic Profiles

- Electronic profiles
  - Are highly detailed and personalized descriptions of individuals such as name, address, phone number, bank account numbers, credit card numbers, shopping patterns, etc.
  - Created by information resellers, also known as information brokers, using publicly available databases and in many cases nonpublic databases as well
- Information resellers sell electronic profiles to direct marketers, fund-raisers, etc.

Issues with Electronic Profiles

- Important issues to note regarding electronic profiles:
  - Collecting public, but personally identifying, information
  - Spreading information without personal consent
  - Spreading inaccurate information
    - E.g., a mistaken identity in which the electronic profile of one person is switched with another

http://www.mirror.co.uk/tech/man-caught-embarrassing-photo-google-8753179

Most of us don't walk around our hometowns ready to have our photograph taken at any moment.

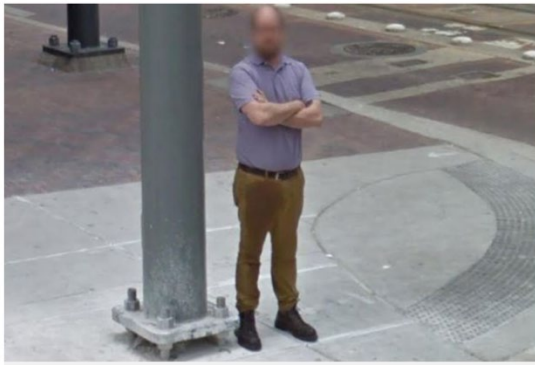
And if someone did happen to snap a pic, it probably wouldn't be the most flattering.

Spare a thought for this man who had his photo taken by the **Google Street View** van - and it's been splashed all over the internet.

It wouldn't be so bad, except he was snapped looking a bit like he'd wet himself.

But the man completely denies that he'd had an accident and instead shared a perfectly rational explanation.

In fact, he even predicted the embarrassing incident coming.



Oh no he didn't...

Two months before the photo was uploaded to Street View, the man in question wrote on Facebook "I just poured half a cleaning keg all over my pants.

"Went outside to stand in the sun ... as a Google maps car drove by. Look for me on Street View soon. I'll be the guy that looks like he p***ed himself," **the Houstonia Mag reports.**

CHINA REAL TIME REPORT

Wrong Number: Chinese Man Mistaken for Corruption Buster Gets Flooded With Calls

Sep 12, 2014 7:23 pm HKT

0 COMMENTS

AGENCE FRANCE-PRESSE/GETTY IMAGES

It was the best of pranks. It was also, given China's current political climate, the worst of pranks.

This week, Chinese media lit up with the story of a clothing entrepreneur whose phone number was posted online last month along with a message identifying him as a member of the central government's anti-corruption investigative team.

The man, surnamed Shi, has since been deluged with hundreds of phone calls and text messages from citizens hoping to vent.

"Regarding online rumors that I'm a the head of a central government inspection group, it's already been 31 days, and just as before, it's continued to seriously disrupt my life and work, the pain is too much to suffer!" Mr. Shi wrote in a Sept. 6 post on the Tecent Weibo microblogging site. "A cellphone number that I've used for 14 years—for a small-scale businessman to change it abruptly, would be a disaster!"

https://blogs.wsj.com/chinarealtime/2014/09/12/wrong-number-chinese-man-mistaken-for-corruption-buster-gets-flooded-with-calls/

The Facebook data leak: What happened and what's next

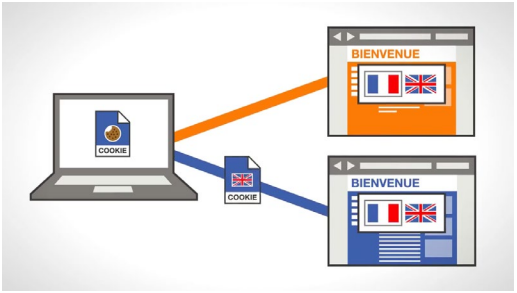
https://www.euronews.com/2018/04/09/the-facebook-data-leak-what-happened-and-what-s-next

Privacy over Internet and Web

- Many people think that as long as they are using their own computer and are selective about disclosing their names or other personal information while online, then little can be done to invade their personal privacy
  - This is known as **illusion of anonymity**
  - When you browse the web, your browser stores critical information onto your hard disk, typically without you being aware of
    - History files include the locations (addresses) of sites that you have recently visited
    - Temporary Internet files, also known as browser cache, contain web page content and instructions to display the content so that they can be quickly redisplayed when you revisit the webpage
    - Cookies are small data files that are deposited on your hard disk from websites you have visited (more details on next slide)
- Ways to protect privacy over web browsing:
  - Browsers now offer an easy way to delete browsing history
  - Most browsers also offer a privacy mode, which ensures that your browsing activity is not recorded on your hard disk, e.g., Incognito Mode from Chrome and Private Browsing from Safari

What is a Cookie?
https://www.youtube.com/watch?v=I01XMRo2ESg

Cookies



- A cookie can be first-party or third-party
- First-party cookie
  - Only generated by the website you are currently visiting
  - Used by many websites to store information about the current session, your general preferences, and your activity on the site
  - The purpose is to provide a personalized experience on a particular site, e.g., present you with sales and promotions that interest you
- Third-party cookie
  - Usually generated by an advertising company that is affiliated with the website you are currently visiting
  - Used by the advertising company to keep track of your web activity as you move from one site to the next, thus third party-cookies are also known as tracking cookies
  - The purpose is to deliver ads that interest you

Web Bugs

- Web bugs, also called web beacons, are invisible images or HTML code hidden within a webpage or email message that can be used to transmit information without your knowledge, e.g., web bug from an email sends to server to verify that the email address is active
- Defense: many email programs now block images and HTML code from unknown senders and let users decide whether to allow blocked content to be displayed

Spyware

- Spyware is a wide range of programs designed to secretly record and report an individual's activities on the Internet
- Keystroke logger is one type of computer monitoring software that records every activity and keystroke made on your computer system
- Computer monitoring software can be deposited onto your hard drive without your knowledge by a malicious website or by someone installing the program directly onto your computer
- Spywares will run in the background, invisible to average user, or disguises itself as useful software such as security program
- Defense
  - Exercise caution when visiting new websites and downloading software from an unknown source
  - Use antispyware or spy removal programs which are designed to detect and remove various types of privacy threats

Security

- Security involves protecting individuals and organizations from theft and danger
- Computer security specifically focuses on protecting information, hardware, and software from unauthorized use, as well as preventing or limiting the damage from intrusions, sabotage, and natural disasters
- Cybercrime or computer crime is any criminal offense that involves a computer and a network and can take various forms, including
  - Creation of malicious programs
  - Denial of service attacks
  - Rogue Wi-Fi hotspots
  - Data manipulation
  - Identity theft
  - Internet scams
  - Cyberbullying

Malware

- Malware
  - short for malicious software
  - specifically designed to damage or disrupt a computer system
  - created and distributed by computer criminal called cracker
- Three most common types of malware:
  1. Viruses
  2. Worms
  3. Trojan horses
- Defenses
  - Use antivirus programs that offer services to keep track of viruses on a daily basis
  - Never open an email attachment from an unknown source
  - Exercise great care in accepting new programs and data from any source

Viruses

- Programs that migrate through networks and operating systems
- Most attach themselves to different programs and databases
- The destructive viruses can alter and/or delete files

Flashback Friday: The Melissa virus

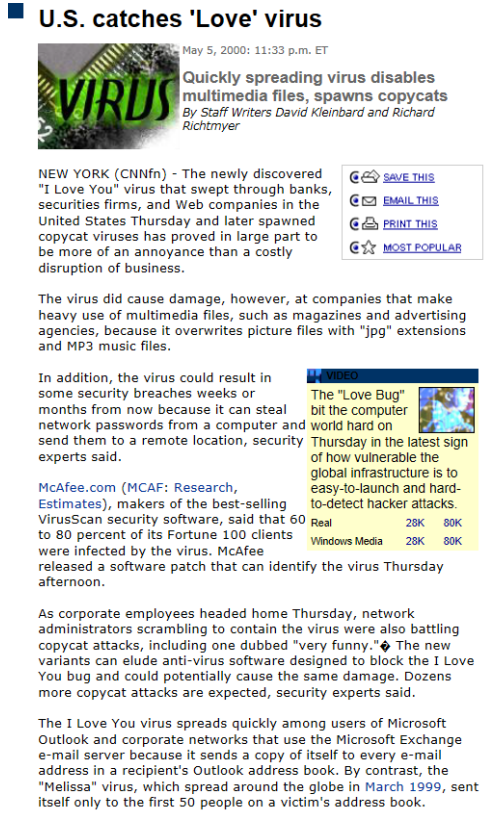
BY EDITOR POSTED 15 JUL 2016 - 01:30PM

VIRUS

The year was 1999. The month March. There was already lots of talk about the Y2K bug, budgets being allocated to computer and software updates, bunkers being prepared for the end of the world. Meanwhile, for many, it was business as usual. You still have to go to work. Pay the bills. Buy groceries.

For David L. Smith, however, things were less routine. The American, hitherto unknown to many, was preoccupied with what would be his most and only infamous creation. Eventually, on or around 26th, he let loose the Melissa virus (officially known as W97M/Melissa.A@mm).

https://www.welivesecurity.com/2016/07/15/flashback-friday-melissa-virus/



U.S. catches 'Love' virus

May 5, 2000: 11:33 p.m. ET

Quickly spreading virus disables multimedia files, spawns copycats

By Staff Writers David Kleinbard and Richard Richtmyer

NEW YORK (CNNfn) - The newly discovered "I Love You" virus that swept through banks, securities firms, and Web companies in the United States Thursday and later spawned copycat viruses has proved in large part to be more of an annoyance than a costly disruption of business.

SAVE THIS
EMAIL THIS
PRINT THIS
MOST POPULAR

The virus did cause damage, however, at companies that make heavy use of multimedia files, such as magazines and advertising agencies, because it overwrites picture files with "jpg" extensions and MP3 music files.

In addition, the virus could result in some security breaches weeks or months from now because it can steal network passwords from a computer and send them to a remote location, security experts said.

VIDEO

The "Love Bug" bit the computer world hard on Thursday in the latest sign of how vulnerable the global infrastructure is to easy-to-launch and hard-to-detect hacker attacks.

Real 28K 80K
Windows Media 28K 80K

McAfee.com (MCAF: Research, Estimates), makers of the best-selling VirusScan security software, said that 60 to 80 percent of its Fortune 100 clients were infected by the virus. McAfee released a software patch that can identify the virus Thursday afternoon.

As corporate employees headed home Thursday, network administrators scrambling to contain the virus were also battling copycat attacks, including one dubbed "very funny."• The new variants can elude anti-virus software designed to block the I Love You bug and could potentially cause the same damage. Dozens more copycat attacks are expected, security experts said.

The I Love You virus spreads quickly among users of Microsoft Outlook and corporate networks that use the Microsoft Exchange e-mail server because it sends a copy of itself to every e-mail address in a recipient's Outlook address book. By contrast, the "Melissa" virus, which spread around the globe in March 1999, sent itself only to the first 50 people on a victim's address book.

http://money.cnn.com/2000/05/05/technology/loveyou/

Worms

- Programs that simply replicate themselves over and over again
- The self-replicating activity clogs computers and networks until their operations are slowed or stopped
- Worm does not attach itself to a program but can carry a virus

The Terrifying U.S.-Israeli Computer Worm That Could Cause World War III

Alex Gibney's new doc 'Zero Days' chronicles the Stuxnet worm, a piece of malware the west used against Iran, and its even more dangerous sister virus: "Nitro Zeus."

NICK SCHAGER 07.09.16 5:51 AM ET

In 2007's *Live Free or Die Hard*, Timothy Olyphant's evil cyber-terrorist Thomas Gabriel initiates a paralyzing attack on the nation's technological infrastructure—seizing control of its transportation, communication, military, and power systems—which Justin Long's nerdy hacker dubs a "fire sale" due to the fact that in such an assault, "everything must go." As befitting an entry in the popular action franchise, this catastrophe concludes with Bruce Willis's cop John McClane saving the day through acts of superhuman physical heroism. Replete with Gabriel using his high-tech gadgetry as a way to soothe his damaged ego and steal lots of money, it's a familiar Hollywood saga, albeit with a modern digital twist. Except that, according to Alex Gibney's new documentary, *Live Free or Die Hard* is anything but outlandish fantasy.

In *Zero Days*, Gibney provides a comprehensive overview of the Stuxnet worm—a sophisticated piece of malware that, on June 17, 2010, was found by a Belarus security expert on one of his client's machines in Iran. Though it was immediately apparent that the virus was deadly, it would take considerably more analysis—including by Symantec security response professionals Eric Chien and Liam O'Murchu—before its true potential was revealed. Those revelations were at once awe-inspiring and unsettling, as Stuxnet turned out to be a complex program designed to infiltrate, target, and sabotage the centrifuges at Iran's Natanz nuclear facility. It was equipped to do this even though Natanz's systems were disconnected from the internet. And it was to perform its mission without "command and control" input—meaning that its groundbreaking code would initiate and carry out its tasks wholly on its own (or as Chien says, "There was no turning back once Stuxnet was released").

https://www.thedailybeast.com/the-terrifying-us-israeli-computer-worm-that-could-cause-world-war-iii

Trojan Horses

- Programs that appear to be harmless but contain malicious programs
- Most common types of Trojan horses appear as free computer games and free screensaver programs that can be downloaded from Internet
- Trojan horses are not viruses but can carry viruses that can be installed secretly on the computer system when a user installs a Trojan horse program
- Trojan horse may claim to provide free antivirus programs for user to download and install, then it installs a virus that locates and disables any existing virus protection programs before depositing other viruses

Don't bank on your phone - it could be hacked by Zeus 'trojan horse'

Malware attacks Android phones to steal financial data as security experts warn of 'fraudsters' heaven'

Using a smartphone to access free Wi-Fi in a public place such as a cafe puts you at risk of a security attack. Photograph: Pixellover RM 7 /Alamy

No one knows who lies behind Zeus. Security experts believe he or she is Russian, but no one is completely sure. But what they all agree is that Zeus is the most pernicious "trojan horse" - a destructive program disguised as an application - on the internet. During the last four years it has infected millions of PCs, taking control of the computer and stealing personal banking details.

Microsoft has fought a running battle against Zeus, which is one of the most difficult types of malware to detect - but the great fear among cybercrime experts is no longer your home computer. A new strain of Zeus, dubbed "Zitmo" (it stands for "Zeus in the mobile") has begun to exploit a huge hole in personal banking security: the smartphone in your pocket.

https://www.theguardian.com/money/2011/jul/22/smartphones-hacked-zeus-malware

Botnet

- Zombies are computers infected by a virus, worm or Trojan horse that allows them to be remotely controlled for malicious purpose
- A botnet, or robot network, is a collection of zombie computers
  - Botnets harness the combined power of many zombies for malicious activities like password cracking or sending junk email
  - Botnets are hard to shut down even after they are detected because they are formed by many computers distributed across the Internet

Denial of Service

- A denial of service (DoS) attack attempts to slow down or stop a computer system or network by flooding a computer or network with requests for information and data
- The targets are usually Internet service providers (ISPs) and specific websites
- Once under attack, the servers at the ISP or the website become overwhelmed with requests for services and are unable to respond to legitimate users

Cybersecurity

A third of the internet is under DoS attack

Published 3 November 2017

Share

For the first time, researchers have carried out a large-scale analysis of victims of internet denial-of-service (DoS) attacks worldwide. And what they found is, in a phrase from their study, "an eye-opening statistic." The researchers found that about one-third of the IPv4 address space was subject to some kind of DoS attacks, where a perpetrator maliciously disrupts services of a host connected to the internet. IPv4 is the fourth version of an Internet Protocol (IP) address, a numerical label assigned to each device participating in a computer network.

Study by SDSC's CAIDA group finds millions of network addresses subjected to denial-of-service attacks over two-year period

For the first time, researchers have carried out a large-scale analysis of victims of internet denial-of-service (DoS) attacks worldwide. And what they found is, in a phrase from their study, "an eye-opening statistic."

Spanning two years, from March 2015 to February 2017, the researchers found that about one-third of the IPv4 address space was subject to some kind of DoS attacks, where a perpetrator maliciously disrupts services of a host connected to the internet. IPv4 is the fourth version of an Internet Protocol (IP) address, a numerical label assigned to each device participating in a computer network.

http://www.homelandsecuritynewswire.com/dr20171103-a-third-of-the-internet-is-under-dos-attack

Rogue Wi-Fi Hotspots

- Rogue Wi-Fi hotspots imitate free Wi-Fi networks
- They operate close to the legitimate free hotspots and typically provide stronger signals that many users unsuspectingly connect to
- Once connected, the rogue networks capture any and all information sent by the users to legitimate sites including user names and passwords

Beware of fake Wi-Fi hotspots
https://www.youtube.com/watch?v=cMFyL38OB3g

Data Manipulation

- Unauthorized access of a computer network and copying files to or from the server, e.g.,
  - Making a post in Facebook when logged in as someone else
  - Feeding a company false reports to change their business practices
- Can occur for months, or even years, without the victims being aware of the security breach, making it hard to detect

'Zombies ahead', warns electronic road sign

Pranksters in at least three US states have figured out how to alter the text on electronic road signs, posting notices of "Nazi zombies" and "raptors ahead" instead of legitimate messages detailing traffic problems.

Road sign, Austin, Texas Photo: AP

7:00AM GMT 05 Feb 2009

The latest breach came on Tuesday during the morning rush hour near Collinsville, Illinois, where hackers changed a sign along southbound Interstate 255 to read, "DAILY LANE CLOSURES DUE TO ZOMBIES."

A day earlier in Indiana's Hamilton County, the electronic message on a board in Carmel's construction zone warned drivers of "RAPTORS AHEAD."

Signs in Austin, Texas, recently flashed: "NAZI ZOMBIES! RUN!!!" and "ZOMBIES IN AREA! RUN."

Officials in Illinois are concerned the rewritten signs distract motorists from heeding legitimate hazards down the road. The hacked sign on Tuesday originally warned drivers of crews replacing guardrails.

"We understood it was a hoax, but at the same time those boards are there for a reason," said Joe Gasaway, an Illinois Department of Transportation supervisory field engineer. "We don't want (drivers) being distracted by a funny sign."

http://www.telegraph.co.uk/news/newstopics/howaboutthat/4518092/Zombies-ahead-warns-electronic-road-sign.html

Identity Theft

- Identity theft is the illegal assumption of someone's identity for the purposes of economic gain
- Once an identity is stolen, the criminal applies for and obtains new credit cards in the victim's name and then uses the cards to purchase clothes, cars and even a house
- Identity thieves look for anything that can help steal your identity such as from social networking sites
- Defenses
  - Exercise caution when providing information on social networking sites
  - Use privacy settings and controls that are provided by the social networking sites

Internet Scams

- Internet scams are scams using the Internet
- Almost all the scams are initiated by a mass mailing to unsuspecting individuals

Type	Description
Advance fee loans	Guaranteed low-rate loans available to almost anyone. After applicant provides personal loan-related information, the loan is granted subject to payment of an "insurance fee."
Auction fraud	Merchandise is selected and payment is sent. Merchandise is never delivered.
Fake antivirus software	A website or e-mail warns you that you are at risk of being infected by a computer virus and you need to download and install the security software they recommend. Ironically, the security software is fake and will install malicious software on your computer.
Nigerian Scam	A classic e-mail scam. The recipient receives an e-mail from a wealthy foreigner in distress who needs your bank account information to safely store their wealth, and for your troubles you will receive a large amount of money. Of course, once the scammer has your bank account information, your accounts will be drained and they will disappear

Social Engineering - Phishing

- Social engineering is the practice of manipulating people to divulge private data, which has played a key role in identity theft, Internet scams, and data manipulation
- A technique often employed by scammers is phishing which tricks Internet users into thinking a fake but official-looking website or email is legitimate

Social Engineering - Phone Scams

News / Hong Kong / Law & Crime / TELEPHONE SCAMS

Taken for a ride: Three Hong Kong university students lose HK$250,000 in telephone scams

PUBLISHED : Friday, 23 October, 2015, 7:00am
UPDATED : Friday, 23 October, 2015, 7:00am

COMMENTS: 8

Clifford Lo

15 SHARES

Three university students, including two mainlanders, have become the latest victims of cross-border phone scams after they were duped out of HK$250,000.

The 18-year-old Hong Kong girl and two mainlanders – a man, 22, and a woman, 21 – lodged complaints on Tuesday and Wednesday, according to police.

They separately received calls from someone claiming to be an employee of a postal organisation or courier company informing them that parcels they sent were carrying forged documents, police said.

READ MORE: From street con-artists to phone fraud: A history of Hong Kong scams ... and how to avoid becoming another victim →

http://www.scmp.com/news/hong-kong/law-crime/article/1871178/taken-ride-three-hong-kong-university-students-lose

Phone Scams Getting More Sophisticated

Posted May 5, 2015

Even folks who know better can fall for sophisticated phone scams that leverage personal information.

SHARE

Download our in-depth report: The Ultimate Guide to IT Security Vendors

By Rod Simmons, BeyondTrust

I was talking to a friend who is a pretty technical guy, and he told me about a call he got from someone posing as Dell technical support. Normally he would hang up on this type of call, but he had a couple minutes to kill and decided to toy with the caller. A few minutes into the call and his jaw almost hit the floor, because the caller knew too much information to be a classic "you have a virus" scam.

What made this call different was that the scammer offered to prove he was from Dell technical support. He was able to share the date of his last technical support call and details about what the call was for -- and surprisingly all the information was accurate. If that was not enough, they read to him his Service Tag Number and Express Service Code. All my friend could think was, "How do they know all of this?"

Sophisticated Scam

My friend realized this was not the normal scam call stating "this is Microsoft technical support." Companies like Microsoft and Dell never initiate support calls with their customers, so whoever was on the other end must have been using compromised information.

https://www.esecurityplanet.com/network-security/phone-scams-getting-more-sophisticated.html

Cyberbullying

- Cyberbullying is the use of Internet, smartphones, or other devices to send or post content intended to hurt or embarrass another person
- Cyberbullying may include the following activities:
  - Sending repeated unwanted emails to individuals who has stated that he/she wants no further contact with the sender
  - Ganging up on victims in electronic forums
  - Posting false statements designed to injure the reputation of another
  - Maliciously disclosing personal data about a person that could lead to harm to that person
  - Sending any type of communication that is threatening or harassing

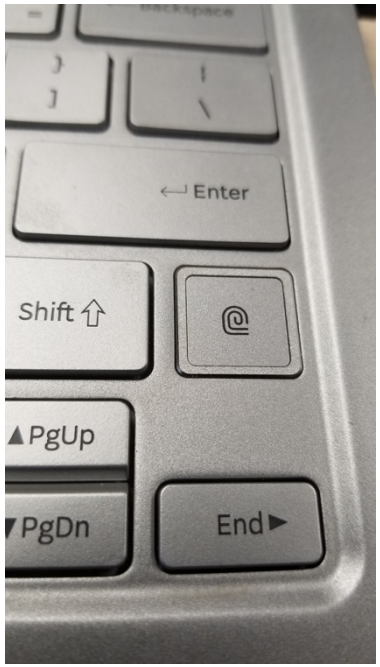
Measures to Protect Computer Security

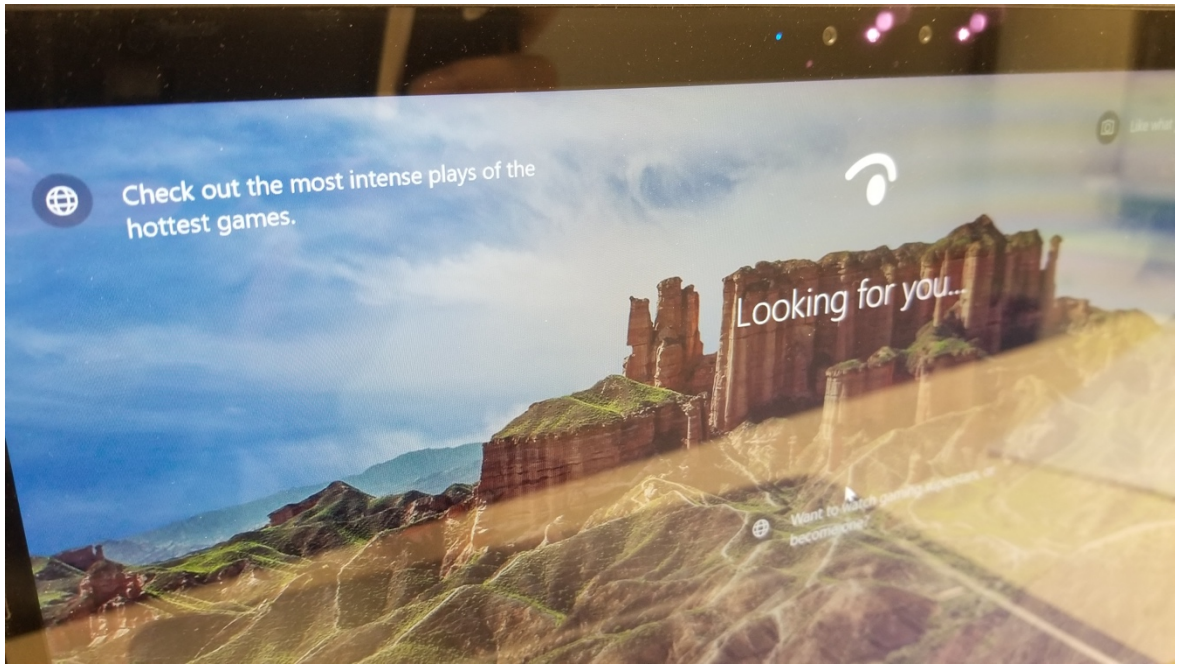
- Some principal measures to ensure computer security:

1. Restricting access
2. Encrypting data
3. Anticipating disasters
4. Preventing data loss

Restricting Access (1)

- Putting guards on a company computer rooms and checking the identification of everyone admitted
- Using biometric scanning devices such as fingerprint and iris scanners
- Using face recognition to allow access to a computer system





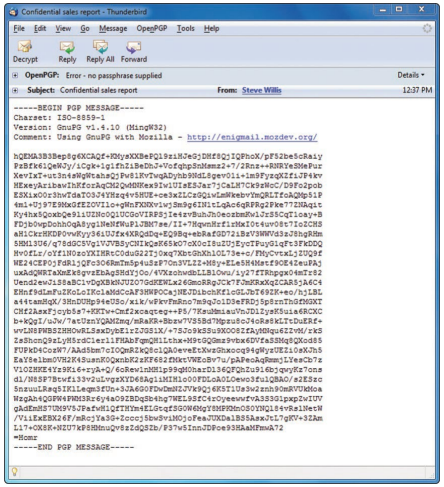
Restricting Access (2)

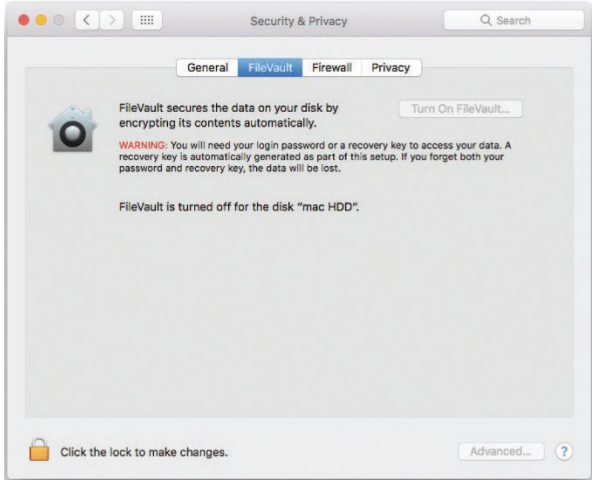
- Using strong passwords
  - Passwords are secret words or phrases that must be keyed into a computer system to gain access
  - The strength of a password depends on how easily it can be guessed

    Illustration: https://howsecureismypassword.net/
  - A dictionary attack uses software to try thousands of common words sequentially in an attempt to gain unauthorized access to a user's account so words, names, and simple numeric patterns make weak or poor passwords
- Denying access to unauthorized communications using firewalls that act as security buffer between a corporate's private network and all external networks

Encrypting Data

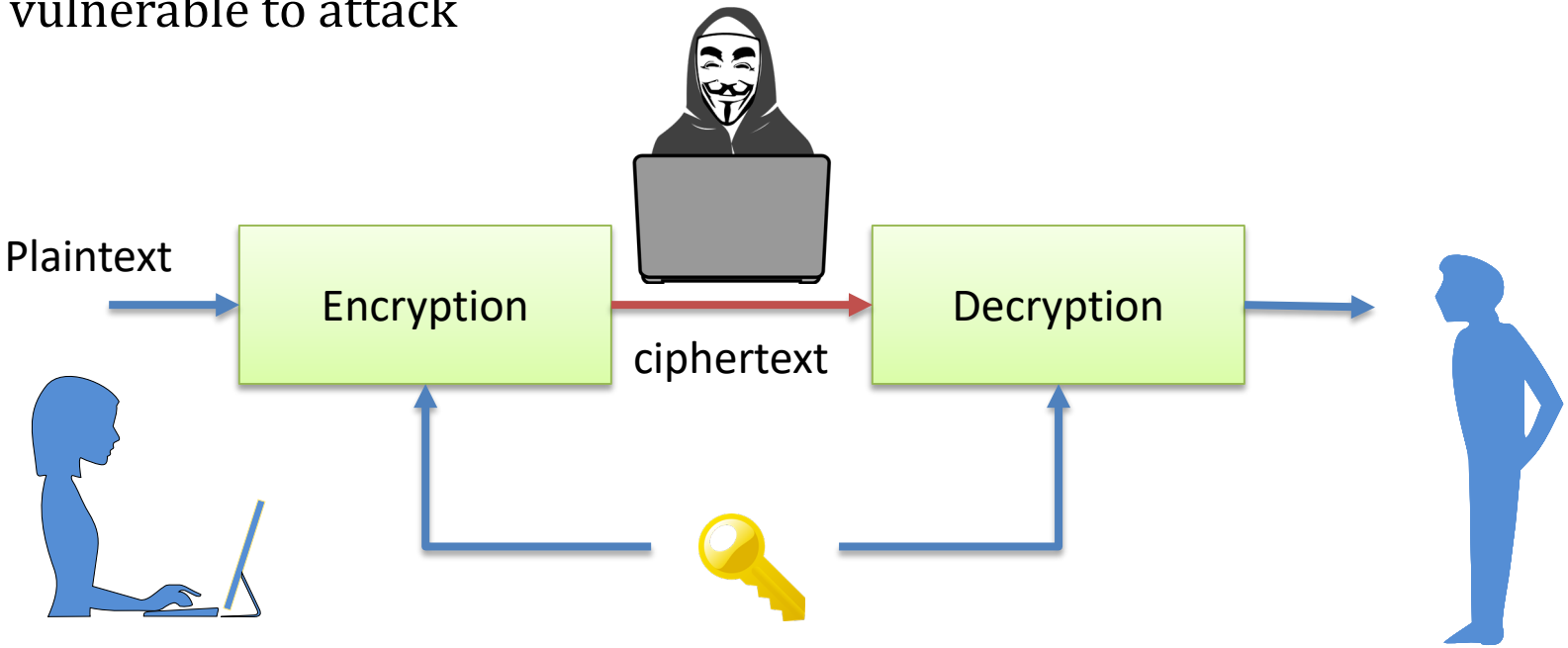
- Encryption is the process of coding information to make it unreadable except to those who have a special piece of information known as an encryption key, or simply, a key
- Some common uses of encryption
  - Email encryption
  - File encryption
  - Website encryption
    - https is the most widely used Internet protocol
  - Virtual Private Network (VPN)
    - encrypts connections between company networks and remote users such as workers connecting from home
  - Wireless network encryption
    - WPA2 (Wi-Fi Protected Access) is the most widely used wireless network encryption for home wireless networks





Symmetric Key Encryption

- Uses the same key for encryption and decryption, e.g. AES.
- Requires the key to be distributed before someone else can read the ciphertext
- Problem: someone else can capture the key which makes it vulnerable to attack

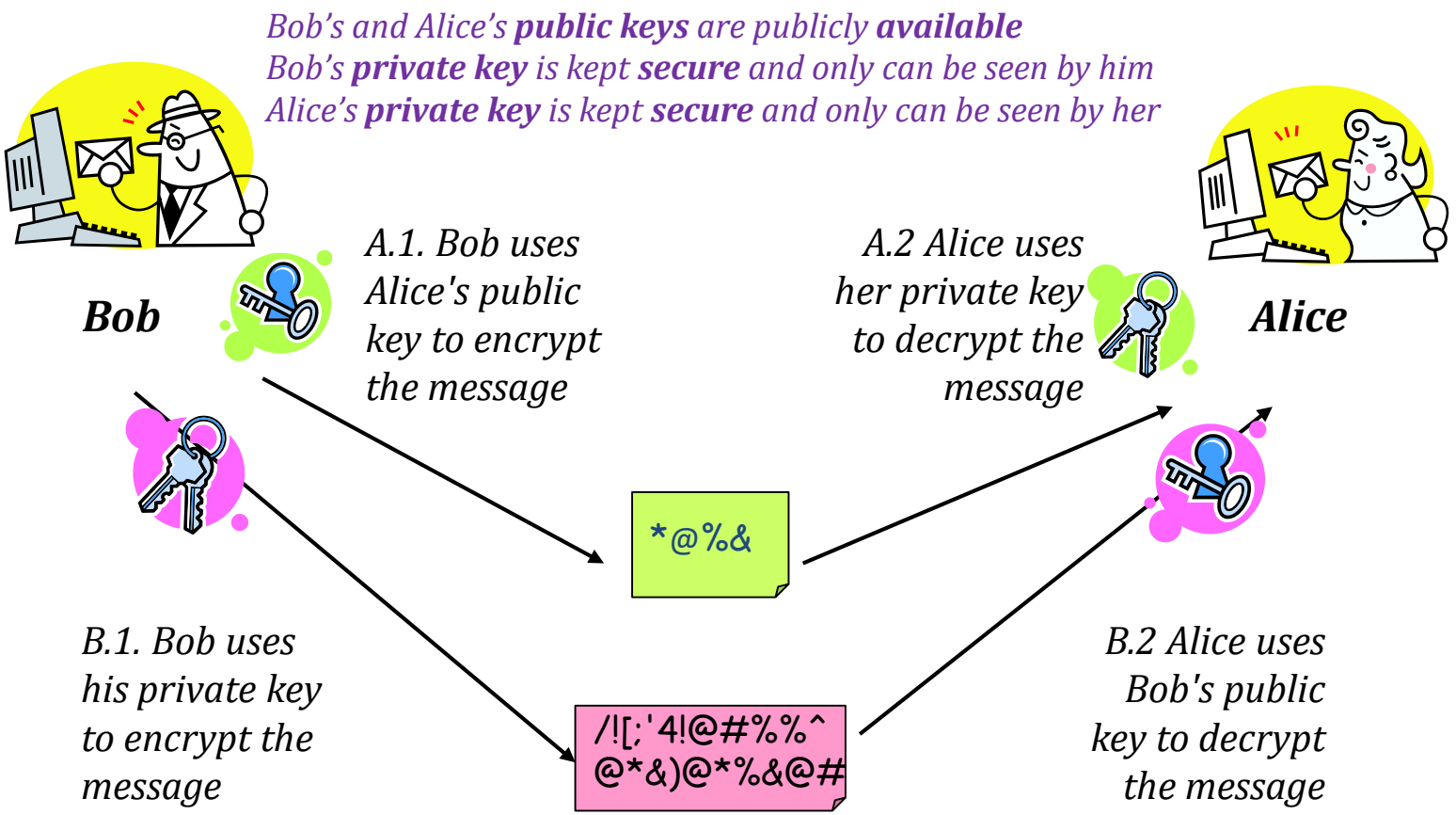


Asymmetric Key Encryption (1)

Also known as public key encryption

- Uses a pair of different keys
  - A public key is a widely distributed one
  - A private key is kept secure
  - The public/private keys are constructed with very large prime numbers. They have a mathematical property that they can decode each other but one cannot use the public key to derive the private key or vice versa (hence no worry in releasing the public key)
- Encryption can be done by either key, with the other key used for decryption

Asymmetric Key Encryption (2)



Which one is right? A1+A2 vs. B1 + B2

Asymmetric encryption – Simply explained
https://www.youtube.com/watch?v=AQDCe585Lnc

Anticipating Disasters

- Physical security is concerned with protecting hardware from possible human and natural disasters
- Data security is concerned with protecting software and data from unauthorized tampering or damage
- Most large organizations have disaster recovery plans that describe ways to continue operating until normal computer operations can be restored

Preventing Data Loss

- Most companies have ways of trying to keep software and data from being tampered with in the first place
  - Careful screening of job applicants
  - Guarding of passwords
  - Auditing of data and programs from time to time
- Some systems use redundant storage to prevent loss of data even when a hard drive fails
- Making frequent backups of data is essential to prevent data loss
- Backups are often stored at an off-site location to protect data in case of theft, fire, flood, or other disasters

Ethics

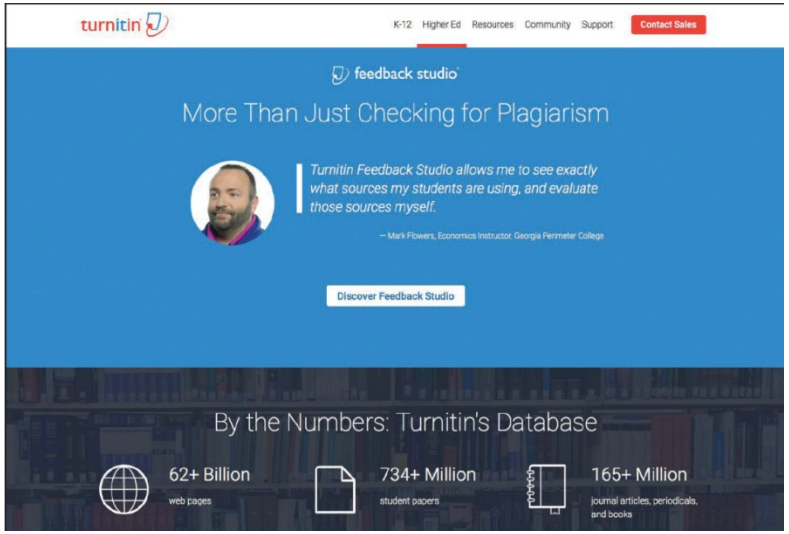
- Ethics are standards of moral conduct
- Computer ethics are guidelines for the morally acceptable use of computers in our society
- Two important issues in computer ethics where average users have a role:
  1. Copyright and Digital Rights Management
  2. Plagiarism

Copyright and Digital Rights Management

- Copyright is a legal concept that gives content creators the right to control use and distribution of their work, e.g., paintings, books, music, films, etc.
  - Making unauthorized copies of digital media violates copyright
- Software piracy is the unauthorized copying and/or distribution of software
- To prevent copyright violations, corporations often use digital rights management (DRM). Typically DRM is used to
  - Control the number of access to electronic media and files
  - Limit the kinds of devices that can access a file

Plagiarism

- Plagiarism means representing some other person's work and ideas as your own without giving credit to the original source http://www6.cityu.edu.hk/ah/case_study.htm
- Computer technology has made plagiarism easier say by copying and pasting content directly
- Computer technology has also made it easier to recognize and catch plagiarists



Lesson Summary

- The most significant concerns for effective implementation of computer technology are privacy, security and ethics
- Electronic profiles contain highly detailed and personalized descriptions of individuals are created by information resellers from large databases
- Cookies, web bugs and spyware pose further threats to our privacy over Internet and web
- Computer security specifically focuses on protecting information, hardware, and software from unauthorized use, as well as preventing or limiting the damage from intrusions, sabotage, and natural disasters
- Computer ethics are guidelines for the morally acceptable use of computers in our society
- It is important to know how we can protect our privacy, defend against computer security threats, and be ethical in using computer technology

Reading

- Computing Essentials 2019
  - Chapter 9

Reference

[1] HowStuffWorks.com - Computer Virus

- http://computer.howstuffworks.com/virus.htm

[2] Ronald B. Standler - Examples of malicious programs

- http://www.rbs2.com/cvirus.htm

[3] Wikipedia - Botnet

- https://en.wikipedia.org/wiki/Botnet

[4] Wikipedia - Denial-of-service attack

- https://en.wikipedia.org/wiki/Denial-of-service_attack

[5] CMU.edu – Security: passwords

- https://computing.cs.cmu.edu/security/security-password.html

[6] Wikipedia - Public key cryptography

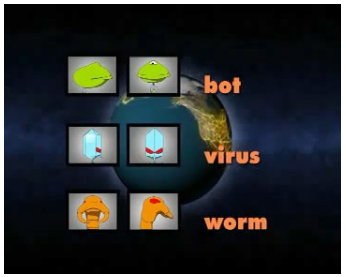
- http://en.wikipedia.org/wiki/Public-key_cryptography

[7] Wikipedia - HTTP cookie

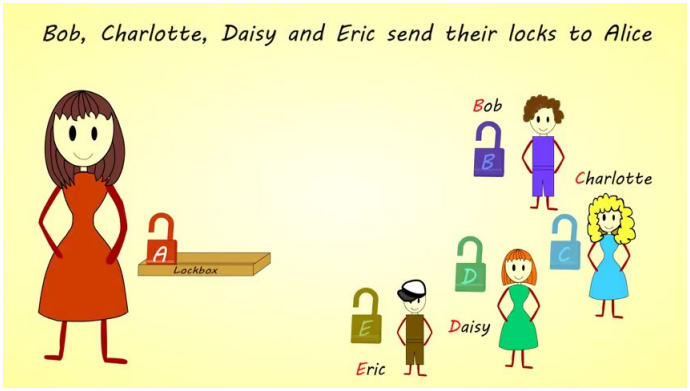
- https://en.wikipedia.org/wiki/HTTP_cookie

Video

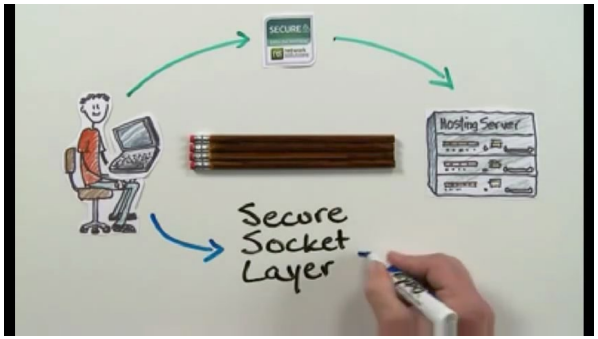
Difference Between Viruses, Worms, Malware, Trojans, Ransomware, and Spyware
https://www.youtube.com/watch?v=n8mbzU0X2nQ



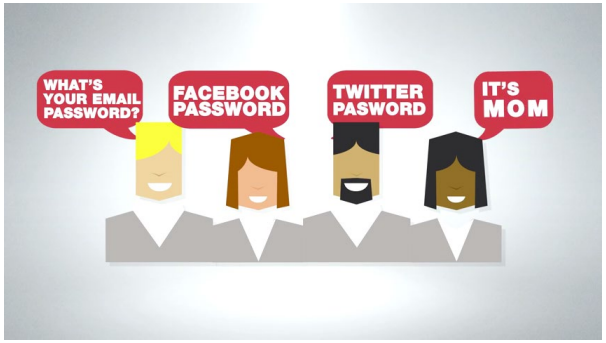
Viruses, Worms and Botnet Explained
https://www.youtube.com/watch?v=LJAb7unURho



How asymmetric encryption works
https://www.youtube.com/watch?v=E5FEqGYLL0o



SSL Certificate Explained
https://www.youtube.com/watch?v=SJJmoDZ3il8



Social Engineering
https://www.youtube.com/watch?v=hM6l0BehFgE