CRIME AND SECURITY

COMPUTER CRIME

- A computer crime is a crime like any other crime, except that in this case the illegal act must involve a **computer system** either as an **object of a crime**, **an instrument used** to commit a crime, or **a repository of evidence** related to a crime.

- Have you been cheated in cyberspace? Con artists and crooks have ample opportunities to cheat unsuspecting people in cyberspace----→these scams are almost unchanging from their pre-web forms; phony business investment opportunities, some weird lotteries and games for awards, pyramid schemes, sales of counterfeit luxury goods etc

  Always remember that if an investment or bargain looks too good to be true, it probably is

- These scams are constantly evolving to take advantage of characteristics of online, interconnected and mobile activities;
  - recent scam of an elderly man almost being robbed by being enticed to disclose his pin number through the mobile phone
  - Online dating scams that use fake identity to develop relationships with people and later convince their victims to send them money

Hacking

- What is hacking?
- What are the different kind of hacking? Is all hacking wrong?
- What are the motives of the different hackers?
- What can we do as professionals or individual users, to reduce hacking risks?

- Hackers Documentaries
  - https://www.youtube.com/watch?v=CuESlhKLhCY
  - https://www.youtube.com/watch?v=olrWxQPYRmU
  - Many more on youtube

What is Hacking?

- This is an irresponsible, destructive action performed by a criminal (Blackhat) or is a responsible , constructive action performed by skilled individuals in protecting the systems from black hat hackers (white hat)
- Black hat hackers break into computer systems and intentionally release computer viruses.
- They steal money and sensitive personal, business and government information
- Crash websites, destroy files and disrupt businesses
- The Evolution of Hacking
  - Era 1—the early years (1960s and 1970s), when hacking was a positive term *(The joy of programming)*
  - Era 2—from the late 1970s to the late 1990s, when hacking took on its more negative meanings *(The rise of hacking's dark side)*
  - Era 3—from late 1990s to today, with the growth of the Web, e-commerce, and the number of online devices (such as medical devices and automobiles)----- *(Hacking as a destructive and criminal tool)*

Why do they do what they do?

1. For monetary gain, especially when it involves breaking into systems with the specific purpose of stealing credit card numbers or manipulating banking systems.
2. Some hackers act for egoistic motives; to increase their reputation within the hacker subculture, leaving their signatures on the system or network after a breach.
3. Corporate spies allow organizations to possess information on services and products that may be hijacked or used as a leverage within the marketplace.
4. Some hackers do it for patriotic reasons; as in state-sponsored cyber attacks during wartime.

Hacker Tools

Hackers use different tools to gain access; we discuss some of the tools

- **Virus**— software that attaches or adds itself to other software. Often a virus is a small portion of a program that can replicate itself and perform other functions such as deleting files or sending emails. Viruses often spread when someone runs an infected program or opens an infected attachment.
- **Worm**— similar to a virus, but does not need to attach itself to another program in order to function. Worms are designed to exploit specific system flaws. Once a worm has gained access to a host system, it scans nearby systems for similar flaws so that it can spread to those systems.
- **Trojan horse**— malware that appears to be a benign software application but carries a malicious component. The user believes the program is safe and launches it. When the application runs, in addition to its normal functionality, it performs malicious activities such as installing a virus or sending spam to all contacts in the user's address book.
- **Social engineering**— the manipulation of people into releasing information or performing a task that violates security protocols. A hacker might impersonate someone from the technical support office in your organization and call you and ask for login credentials or other important information. Hackers have used social engineering since the early days of computers, and it has been very successful.

Hacker Tools

Hackers use different tools to gain access; we discuss some of the tools

- **Phishing**: fraudulent spam called phishing (in the case of email) and smishing (in the case of text messaging) is used to send millions of messages fishing for information to use to impersonate someone and steal money and goods. The message tells the victim to click or tap a link to what purports to be the website of a well-known bank or online company
- **Pharming**— luring people to fake websites where thieves collect personal data. Normally when we indicate a website we want to visit, our browser looks up the IP address* of the site on one of many Domain Name Servers (DNS), special computers on the Internet for this purpose. Pharming involves planting false Internet addresses in the tables on a DNS that lead the browser to a counterfeit site set up by hackers.
- **Ransomware**— malware that encrypts some or all the files on a computer or mobile device and then displays a message demanding payment for the key to decrypt the files. Often, the hacker demands payment in bitcoins, an anonymous digital currency. Victims (individuals and large businesses), especially those with no safe backups, usually pay the fee.

Hacker Tools

Hackers use different tools to gain access; we discuss some of the tools

- **Spyware**— malware that can monitor and record user activities on a computer or mobile device. This includes logging keystrokes on the keyboard to capture usernames, passwords, account numbers, and other information. Spyware can log websites visited and other network activity and send the data to a remote server monitored by the hacker. More devastating, spyware can control a webcam and record activity without the user knowing
- **Botnet**— a group of computers or other devices on the Internet that have a virus or piece of malware that communicates with a central host or server controlled by a hacker (coordinated army of compromised devices). The infected devices are referred to as bots or zombies. The hacker issues commands from the central server directing the botnet to perform tasks such as sending spam, participating in online advertising fraud, or initiating a distributed denial of service attack

  Denial of service (DoS) or *distributed denial of service* (DDoS) attack—an attack in which a botnet overwhelms websites, mail servers, or other Internet locations with so many requests for service that normal users cannot access the sites or services.

Creating most hacking tools requires technical skills. However, hacking scripts (sequences of instructions to be executed) and computer code for thousands of computer viruses are available for free or a small price on the Internet, thus easily accessible to anyone.

Group Discussion

Is “harmless” hacking harmless? *(Think in terms of the system administrator’s response when they detect an intruder)*

Applications of Hacking

Identity Theft

- Various crimes in which a criminal or large, well-organized criminal group uses the identity of an unknowing innocent person.
- Criminals use stolen credit and debit card numbers to buy expensive items, or they sell the numbers to others who use them.
- The identity thieves take out loans, raid the victim’s bank account or use the victim’s identity in various other ways for financial gain.
- Collecting information useful for identity theft is the goal of a significant amount of hacking, and hacking is a significant step in some of the monetary thefts that result, for example, accessing someone’s bank account and stealing the money.
- Identity thieves love the millions of résumés that people post on job-hunting sites. Thieves collect addresses, ID numbers, birth dates, work histories, and all the other details that help them convincingly adopt the identity of the job seeker. Some pose as employers and post fake job announcements; others respond to job hunters and ask for more information, perhaps saying they need it for a background check. Because identity thieves misuse such sites, job seekers must adapt and be more cautious by omitting sensitive data from a posted résumé, not providing sensitive information until they have an actual interview, or finding other ways to determine that the potential employer is authentic.

Applications of Hacking

Breaches

- A security breach is any incident that results in unauthorized access to computer data, applications, networks or devices. It results in information being accessed without authorization. Typically, it occurs when an intruder is able to bypass security mechanisms.
- Security breach vs data breach
  - A security breach is effectively a break-in, whereas a data breach is defined as the cybercriminal getting away with information.
- Confidential information has immense value. It's often sold on the dark web; for example, names and credit card numbers can be bought, and then used for the purposes of identity theft or fraud. It's not surprising that security breaches can cost companies huge amounts of money
- Types of security breaches
  - Exploit attacks a system vulnerability
  - Cracking and guessing of weak passwords
  - Malware attacks
  - Drive-by downloads: viruses or malware delivered through a compromised or spoofed website
  - Social engineering

Applications of Hacking

Hacktivism

- Hacktivism is hacking to promote a political clause or to make recognition of any kind of clause.
- People who agree with the political or social position of the hackers tend to see an act as “activism,” while those who disagree see it as ordinary crime (or worse).
- Suppose we know that a political cause motivates the hackers.
  - How do we begin to evaluate the ethics of their hacktivism?
  - Suppose a religious group, to protest homosexuality, disables a website for gay people, and suppose an environmentalist group, to protest a new housing development, disables a website of a real estate developer.
  - Many people who argue that one of these acts is justifiable hacktivism would argue that the other is not, because one takes a conservative position and the other takes a liberal position. Yet, it would be very difficult to develop a sound ethical basis for distinguishing them.
- The nations in which hacktivism is likely to have the most ethical justification are those least likely to respect acts of civil disobedience. Oppressive governments control the means of communication and prohibit open political discussion, ban some religions, and jail or kill people who express opposition views. In such countries, where openly communicating one’s views is impossible or dangerous, there might be good arguments to justify political hacking to get one’s message out to the public

Why Is the Digital World So Vulnerable?

A variety of factors contribute to security vulnerabilities and weaknesses:

- the inherent complexity of computer systems,
- the development history of the Internet and the Web,
- the software and communications systems that run phones, the Web, industrial systems, and the
- many interconnected devices we use,
- the speed at which new applications develop,
- economic, business, and political factors, and
- human nature.

Security

Tools to Help Protect the Digital World

- **The evolution of credit card fraud and protection:** the security measures have increasingly grown since inception of credit cards therefore securing it's users from digital theft
- **Encryption:** generally includes a coding scheme, or cryptographic algorithm, and specific sequences of characters (e.g., digits or letters), called *keys*, used by the algorithm to encode or decode data. Modern encryption technology is very secure and has a flexibility and variety of applications beyond protecting data. For example, it is used to create digital signatures, authentication methods, and digital cash.
- **Anti-malware software and trusted applications:** tools and software that assist nontechnical users to protect their own devices and files and to avoid being the weak link in the security chain e.g use of antivirus or anti-malware etc
- **Authenticating websites:** Sometimes fake websites, or emails that direct us to them, are easy to spot because of poor grammar and generally low quality. Web browsers, search engines, and add-on software can filter for websites considered safe or show alerts for sites known to collect and misuse personal information
- **Authenticating users:** Example of how Gmail sends a code to your phone for continual use of the email service
- **Biometrics:** Biometrics are biological characteristics that are unique to an individual. They include fingerprints, voice prints, face structure, hand geometry, eye (iris or retina) patterns, and DNA.
- **Multifactor authentication:** To protect against stolen credentials, many websites and organizations use "multifactor" or "two-factor" authentication. There are three categories of authentication technologies:

  1. something you know—a password, PIN, or secret key phrase
  2. something you are—a voiceprint, fingerprint, or retinal scan
  3. something you have—a debit or credit card, smartphone,

People Who Can Help Protect the Digital World

- *Cybersecurity professionals: Strive to achieve C.I.A*
  - protecting systems and networks
  - Testing the security of existing systems and networks
  - Investigating security breaches
- *Software designers, programmers, and system administrators*

  System administrators have a professional, ethical, and often legal obligation to take reasonable security precautions to protect their systems. They must anticipate risks, prepare for them, and stay up to date about new risks and new security measures
- *Users*

  While it is tempting to place the blame for large data breaches on software developers, system administrators, and IT staff, users bear responsibility for some breaches. Three password practices can help us protect our own data and the systems we interact with at work and on the Web:
  - Choose strong passwords.
  - Change passwords periodically.
  - Do not use the same password for multiple purposes

A look at the Law

What does the Kenyan law say of Computer fraud and Computer misuse?