Module CS5052NI Professional Issues, Ethics and Computer Law

2023

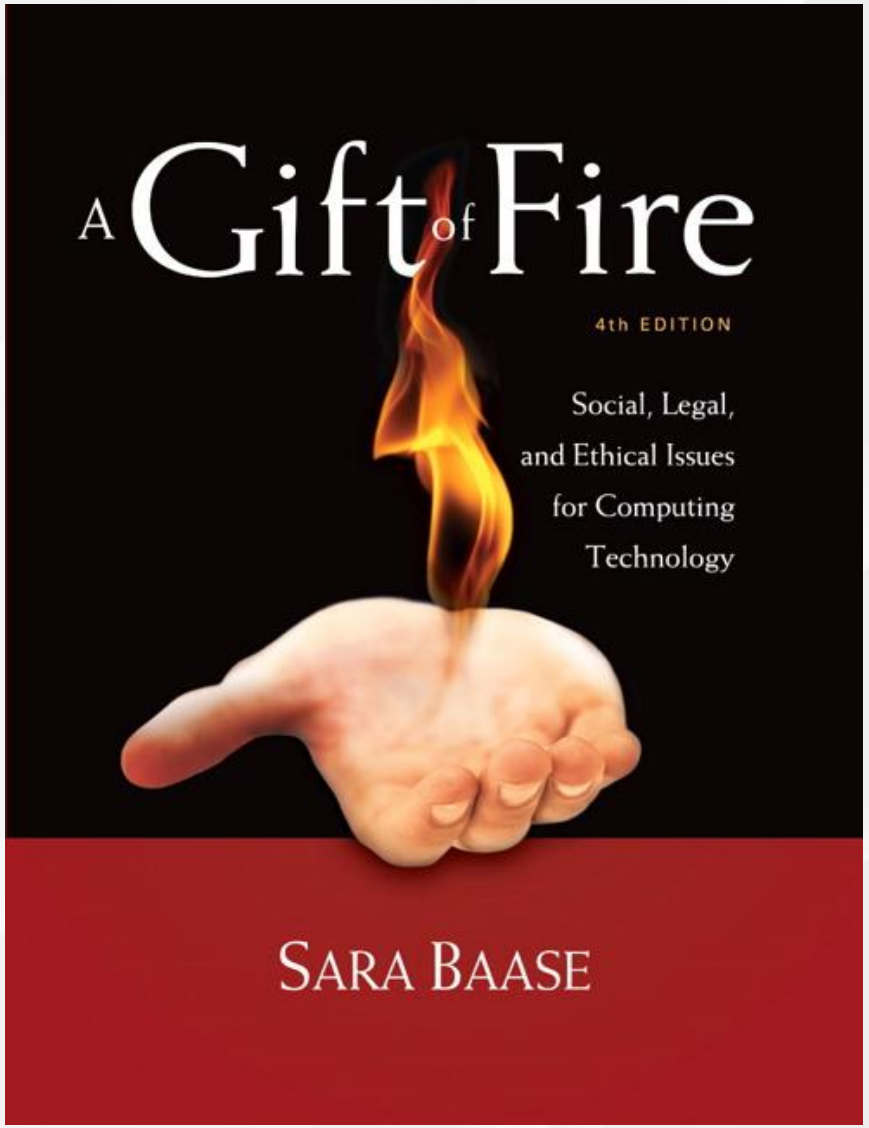
A Gift of Fire

Fifth edition

Sara Baase

Chapter 5:

Crime

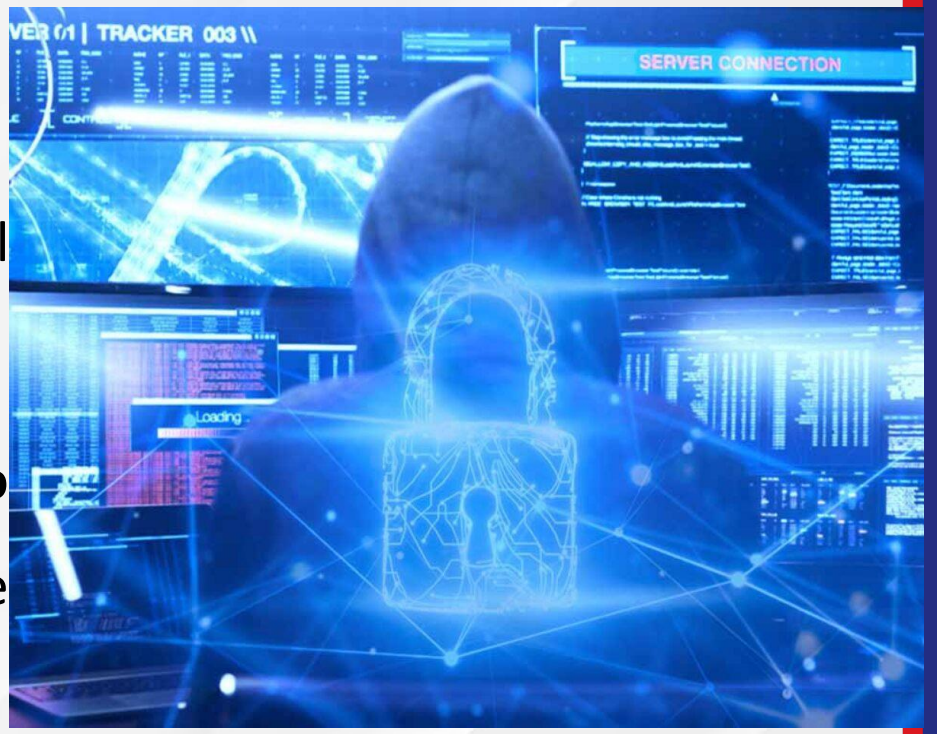


Agenda

- Crime
  - Hacking
  - Identity Theft and Credit Card Fraud
  - Whose Laws Rule the Web

What does Hacking mean?

- Intentional, unauthorized access to computer systems
- A "**hacker**" is a creative expert that uses their technical knowledge to overcome a problem.
- The hacker **may alter system or security features to accomplish a goal** that differs from the original purpose of the system.
- Corporations employ **hackers as part of them support staff**.

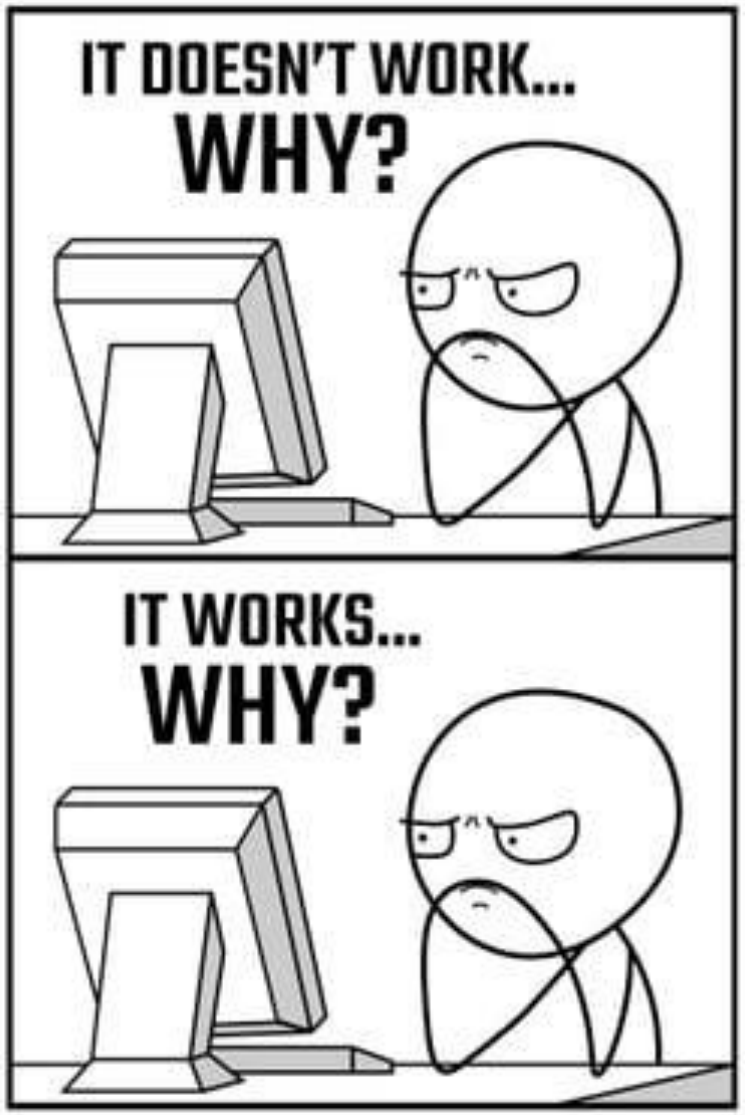


Techniques for hacking

- Social Engineering & Phishing
- Malware-Injecting Devices
- Missing Security Patches
- Cracking Passwords
- Distributed Denial-of-Service (DDoS)

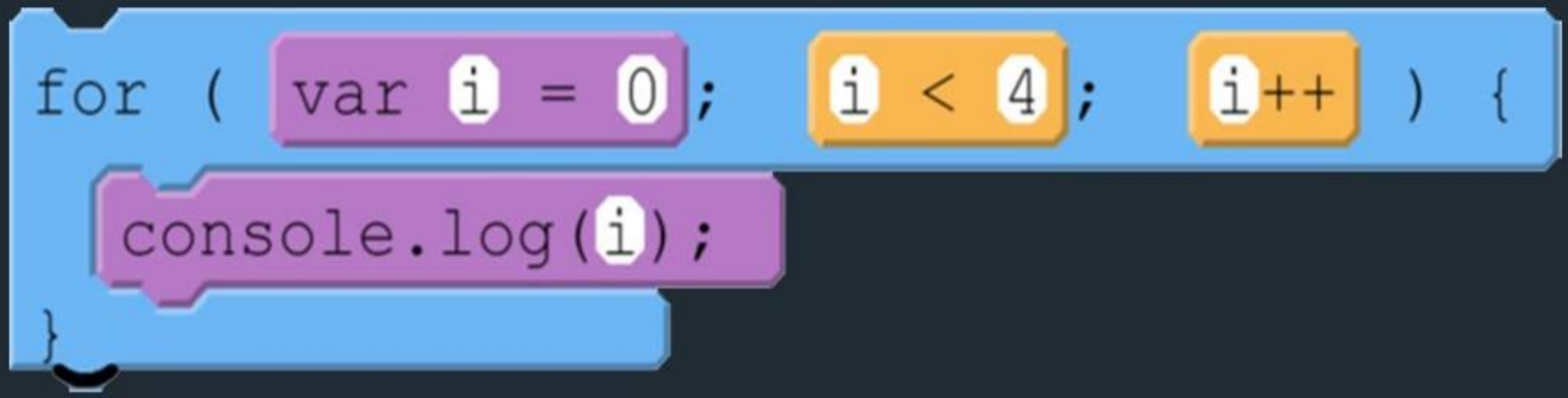
Hacking

- The term has changed over time
- Phase 1: The joy of programming
  - Early 1960s to 1970s
  - It was a positive term
  - A "**hacker**" was a creative programmer who wrote elegant or clever code
  - A "**hack**" was an especially clever piece of code



Hacking

```
for (var i = 0; i < 4; i++) {
   console.log(i);
}
```



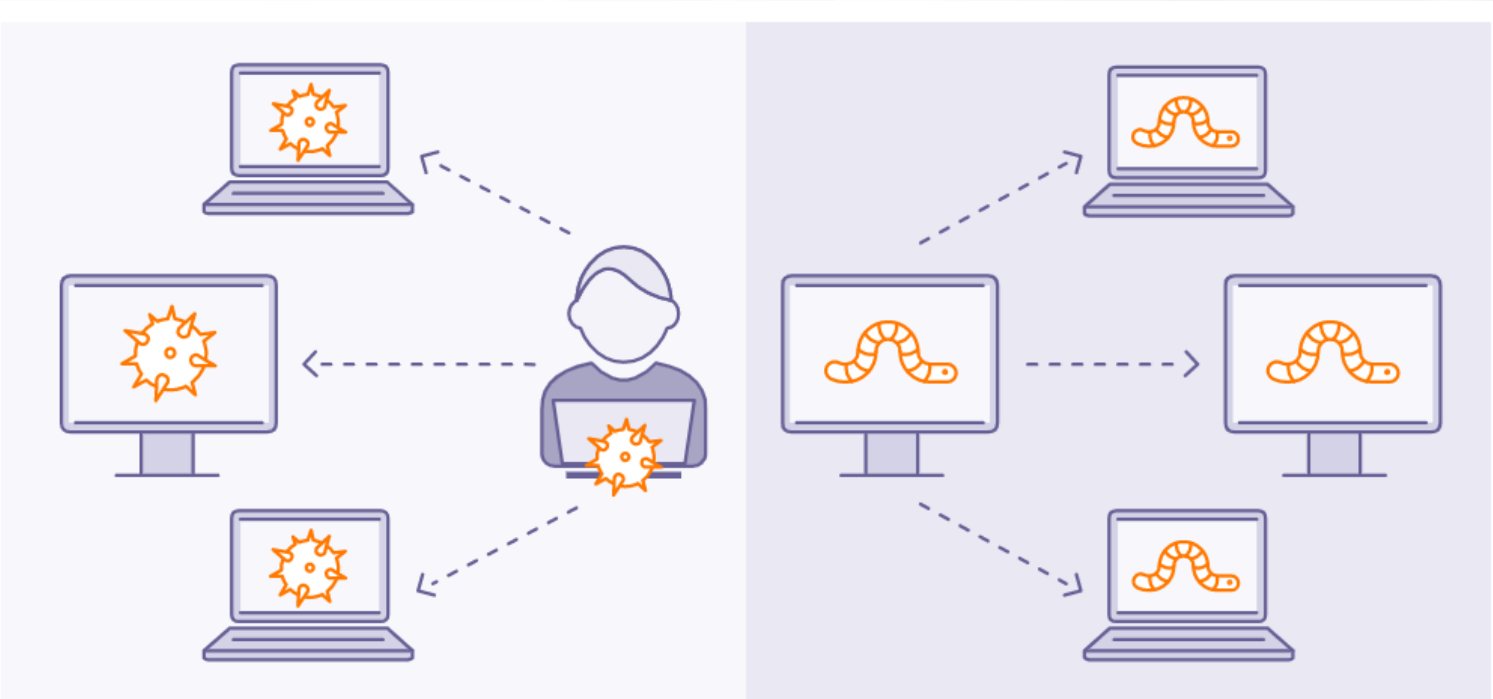
Hacking

Phase 2: 1970s to mid 1990s

- Hacking took on **negative connotations**
- Breaking into computers for which the hacker does not have authorized access
- Still primarily individuals
- Includes the spreading of computer worms and viruses and ‘phone phreaking’
- Companies began using hackers to analyze and improve security

Hacking

Phase 2: 1970s to mid 1990s

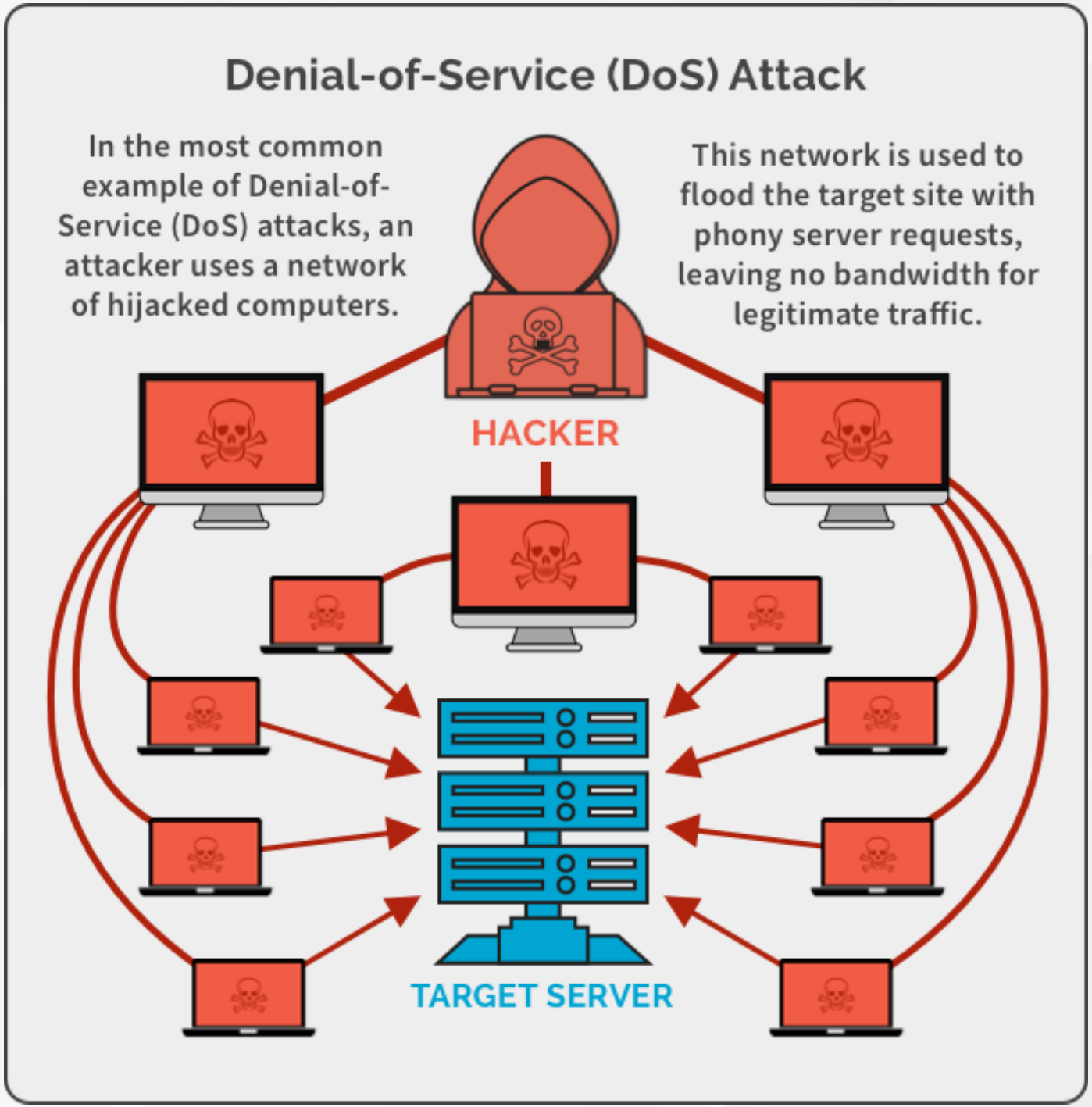


Hacking

Phase 3: The growth of the Web and mobile devices

- **Beginning in mid 1990s**
- The growth of the Web changed hacking; **viruses and worms could be spread rapidly**
- Political hacking (Hacktivism) surfaced
- Denial-of-service (DoS) attacks used to shut down Web sites
- Large scale theft of personal and financial information

Hacking



Arlington college (इरिलङटन कलेज)
informatics college · pokhara
ITAHARI INTERNATIONAL COLLEGE

Hacking

Is “harmless hacking” harmless?

- Responding to non malicious or prank hacking uses resources.
- Hackers could accidentally do significant damage.
- Almost all hacking is a form of **trespass**.

Hacking

Hacktivism, or Political Hacking

- Use of **hacking to promote a political cause**
- Disagreement about whether it is a form of civil disobedience and how (whether) it should be punished
- Some use the appearance of hacktivism to hide other criminal activities
- How do you determine whether something is hacktivism or simple vandalism?

Hacker types

- White Hat Hackers: **Ethical Hackers**. not illegal
- Black Hat Hackers: C**rackers**, illegal
- Grey Hat Hackers : blend of both black hat and white hat hackers. act for their fun. intent to show weakness and earn
- Miscellaneous Hackers
- Red Hat Hackers: Like Grey hat. But hack government agencies and generally anything that falls under the category of sensitive information.
- Blue Hat Hackers : someone outside computer security consulting firms who is used to bug-test .
- Elite Hackers: social status among hackers, which is used to describe the most skilled
- Script Kiddie: non-expert who breaks into computer systems by using pre-packaged automated tools written by others
- Neophyte": "newbie" or "Green Hat Hacker". New to hacking and has almost no knowledge
- Hacktivist: Activist using technology to announce social message

Hackers as Security Researchers

Hackers as Security Researchers

- "White hat hackers" use their skills to demonstrate system vulnerabilities and improve security

Ethical dilemmas:

- **Is it ethical to break into a system without permission, even with good intentions?**
- **How can people responsibly inform potential victims of security vulnerabilities without informing malicious hackers who would exploit them?**

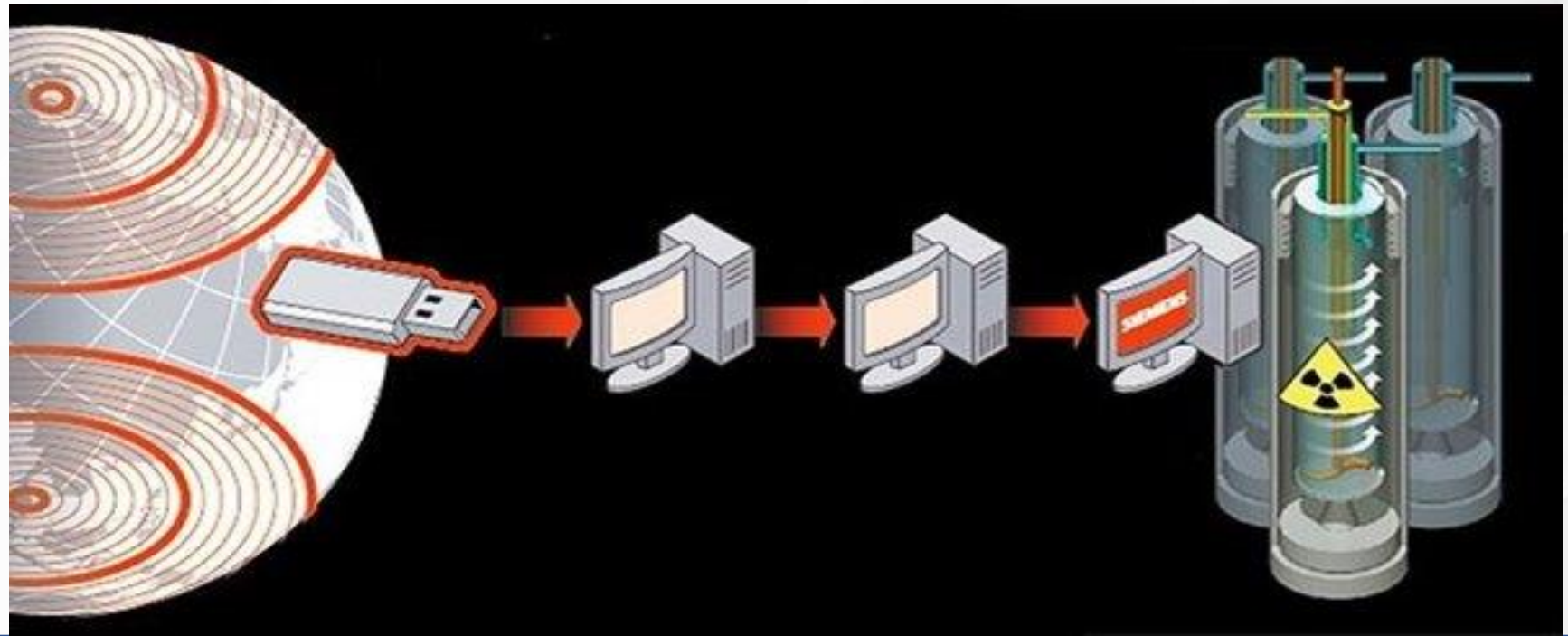
Many security researcher hackers are scornful of big software companies because of the large number of security flaws in their products and because they are slow to plug leaks even when they know of them.

Hacking as Foreign Policy

- **Hacking by governments has increased**
- Pentagon has announced it would consider and treat some cyber attacks **as acts of war, and the U.S. might respond with military force.**
- How can we make critical systems safer from attacks?

Stuxnet

- An extremely **sophisticated worm,** first uncovered in 2010 by **Kaspersky Lab**
- Targets a particular type of control system, which **allow the automation of electromechanical processes** like factory assembly lines, amusement rides, etc



Stuxnet

- Beginning in 2008, stuxnet reportedly compromised Iranian PLCs, collecting information on industrial systems and causing the fast-spinning centrifuges to tear themselves apart.
- Stuxnet reportedly ruined almost one fifth of Iran's nuclear centrifuges. Targeting industrial control systems, the worm infected over 200,000 computers and caused 1,000 machines to physically degrade.

Security

- **Hacking is a problem, but so is poor security.**
- Variety of factors contribute to security weaknesses:
  - History of the Internet and the Web
  - Inherent complexity of computer systems
  - Speed at which new applications develop
  - Economic and business factors
  - Human nature

Hacking

- Internet started with open access as a means of **sharing information for research**
- **Attitudes about security** were **slow** to catch up with the risks.
- **Firewalls** are used to monitor and filter out communication from untrusted sites or that fit a profile of suspicious activity.
- Security is often playing **catch-up to hackers** as new vulnerabilities are discovered and exploited.

Responsibility for Security

- Developers have a responsibility to develop with security as a goal.
- Businesses have a responsibility to use security tools and monitor their systems to prevent attacks from succeeding.
- Home users have a responsibility to ask questions and educate themselves on the tools to maintain security (personal firewalls, anti-virus and anti-spyware).

The Law: Catching and Punishing Hackers

- **1984 Congress passed the Computer Fraud and Abuse Act (CFAA)**
  - Covers government computers, financial and medical systems, and activities that involve computers in more than one state, including computers connected to the Internet
  - Under CFAA, it is **illegal to access a computer without authorization**
  - **USA PATRIOT Act** expanded definition of loss to include cost of responding to an attack, assessing damage and restoring systems

The Law: Catching and Punishing Hackers

- **Penalties for young hackers**
  - Many young hackers have matured and gone on to productive and responsible careers
  - Temptation to over or under punish
  - Sentencing depends on intent and damage done
  - Most young hackers receive probation, community service, and/or fines
  - Not until 2000 did a young hacker receive time in juvenile detention

Identity Theft and Credit Card Fraud

Stealing Identities

- Identity Theft – various crimes in which criminals use the identity of an unknowing, innocent person
  - Use credit/debit card numbers, personal information, and social security numbers
  - 18–29-year-olds are the most common victims because they use the Web most and are unaware of risks
  - E-commerce has made it easier to steal and use card numbers without having the physical card

Identity Theft and Credit Card Fraud

Stealing Identities

- Techniques used to steal personal and financial information
  - Requests for personal and financial information disguised as legitimate business communication
    - Phishing – e-mail
    - Smishing
    - Vishing – voice phishing

Stealing Identities

- Pharming – false Web sites that fish for personal and financial information by planting false URLs in Domain Name Servers
- Online resumés and job-hunting sites may reveal SSNs, work history, birth dates and other information that can be used in identity theft

Responses to Identity Theft

- Authentication of email and Web sites
- Use of encryption to securely store data, so it is useless if stolen
- Authenticating customers to prevent use of stolen numbers, may trade convenience for security
- In the event information is stolen, a fraud alert can flag your credit report; some businesses will cover the cost of a credit report if your information has been stolen

Responses to Identity Theft

- **Biological characteristics unique to an individual**
- No external item (card, keys, etc.) to be stolen
- Used in areas where security needs to be high, such as identifying airport personnel
- **Biometrics can be fooled,** but more difficult to do so, especially as more sophisticated systems are developed

Whose Laws Rule the Web

When Digital Actions Cross Borders

- Laws vary from country to country.
- Corporations that do business in multiple countries must comply with the laws of all the countries involved.
- Someone whose actions are legal in their own country may face prosecution in another country where their actions are illegal.

Whose Laws Rule the Web

Libel, Speech and Commercial Law

- Where a trial is held is important not just for differences in law, but also costs associated with travel between countries; cases can take some time to come to trial and may require numerous trips.
- Freedom of speech suffers if businesses follow laws of the most restrictive countries.
- Some countries have strict regulations on commercial speech and advertising.

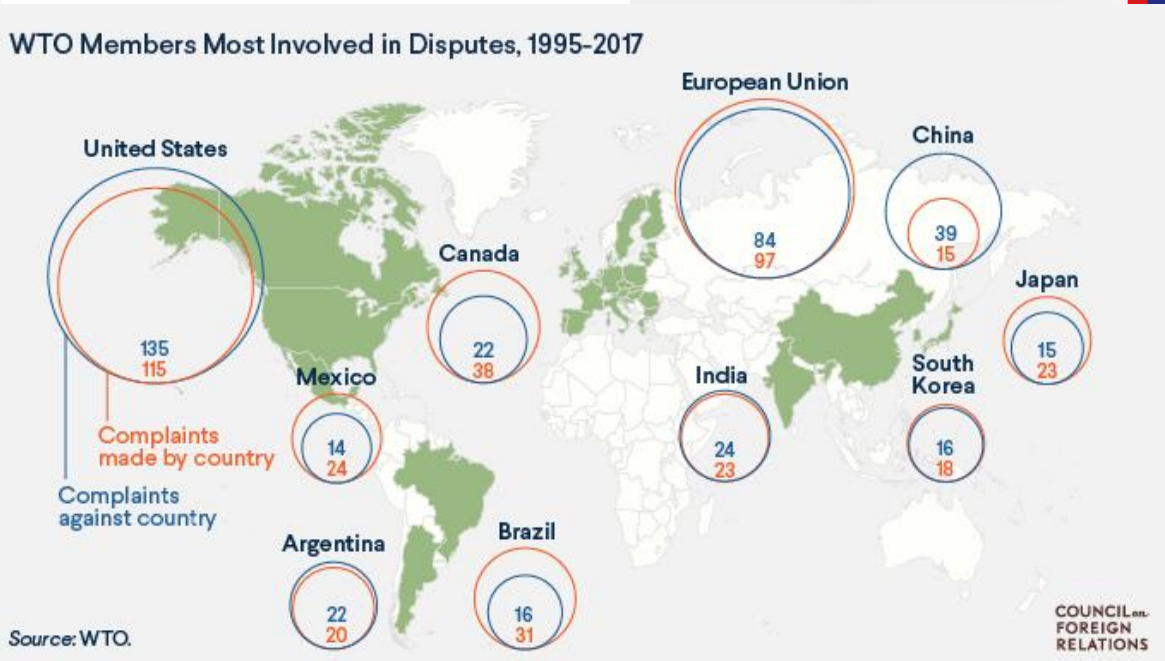
Culture, Law, and Ethics

- Respecting cultural differences is not the same as respecting laws
- Where a large majority of people in a country support prohibitions on certain content, is it ethically proper to abandon the basic human rights of free expression and freedom of religion for minorities?

Potential Solutions

International Agreements

- Countries of World Trade Organization (WTO) agree not to prevent their citizens from **buying certain services from other countries** if those services are legal in their own.
- WTO agreement does not help when a product, service, or information is legal in one country and not another.



Potential Solutions

Alternative principles

- Responsibility-to-prevent-access
  - Publishers must prevent material or services from being accessed in countries where they are illegal.
- Authority-to-prevent entry
  - Government of Country A can act within Country A to try to block the entrance of material that is illegal there but may not apply its laws to the people who create and publish the material, or provide a service, in Country B if it is legal there.

Any questions?