Instituto Politécnico Nacional
"La Técnica al Servicio de la Patria"

CIC
Centro de Investigación en Computación

Laboratorio de Ciberseguridad

Centro de Investigación en Computación(CIC)
Instituto Politécnico Nacional - México.

Cyber security A-15

Dr. Ponciano Jorge Escamilla Ambrosio
pescamilla@cic.ipn.mx
http://www.cic.ipn.mx/~pescamilla/

Cyber security course

2.8. Cybercrime

2.9. Cyberwarfare

Cybercrime: antecedents

- The Internet and its network protocols were never intended to protect against cybercriminals.
  - Was designed to accommodate computer-based communications in a trusted community.
  - Was designed for maximum efficiency without regard for security.
- The Internet is now a global place for communication, search, and trading.
- Despite improvements, **the Internet is still fundamentally insecure.**

Cybercrime

Cybercrime is crime that requires a computer, a network, and a human interface.

- Most computer-based crime exploits users' ignorance and their inability to deal with flourishing technology and security mechanisms.

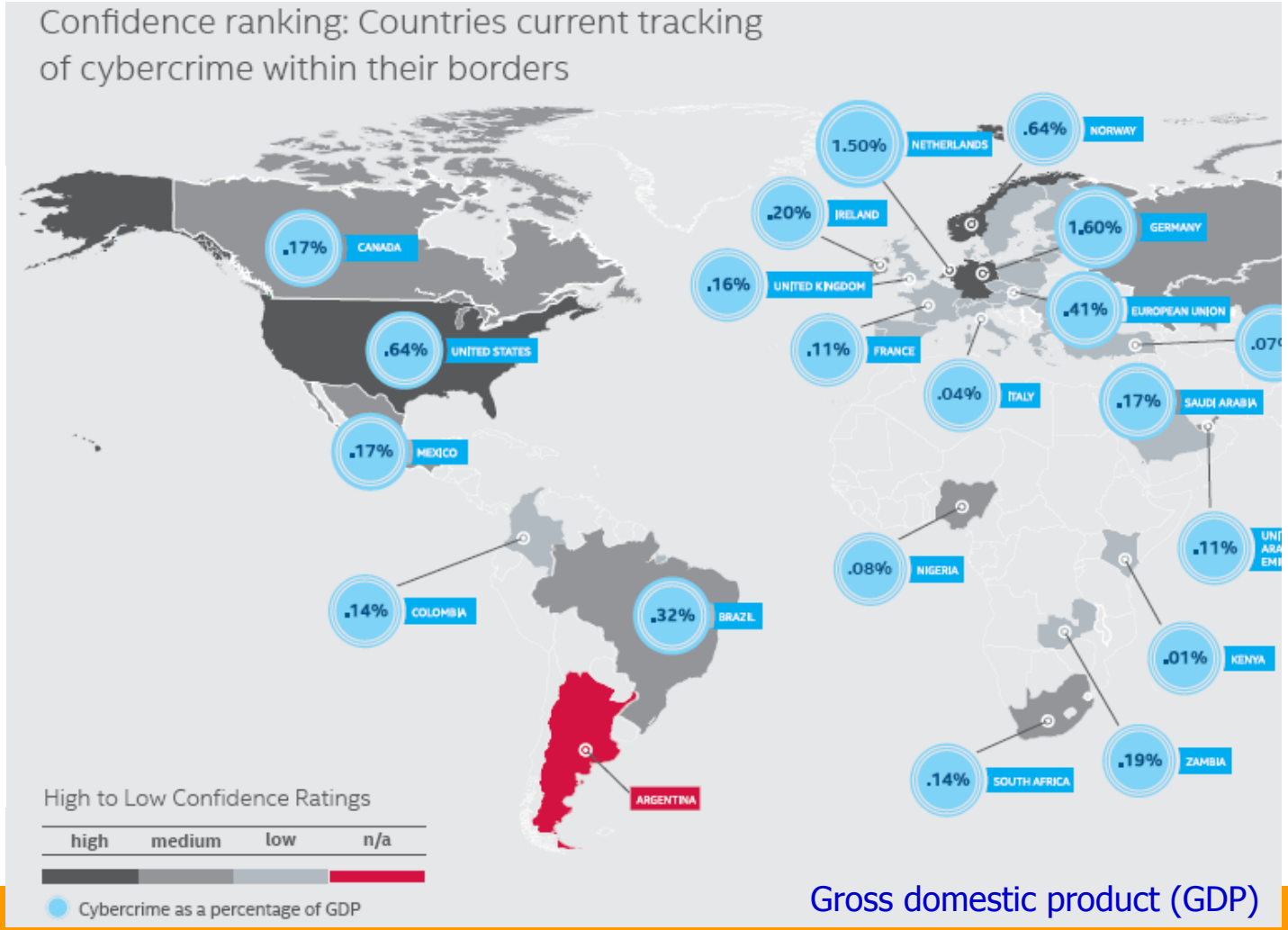
Cybercrime

- Cybercrime categories
  - Modus operandi
    - Crimes against the machine (hacking etc.)
    - Crimes using the machine (frauds etc.)
    - Crimes in the machine (pornography, hate speech, social networking originated offences)
  - Mediated by technology
  - Security concern (victim group)
    - Personal security
    - Corporate security
    - National security

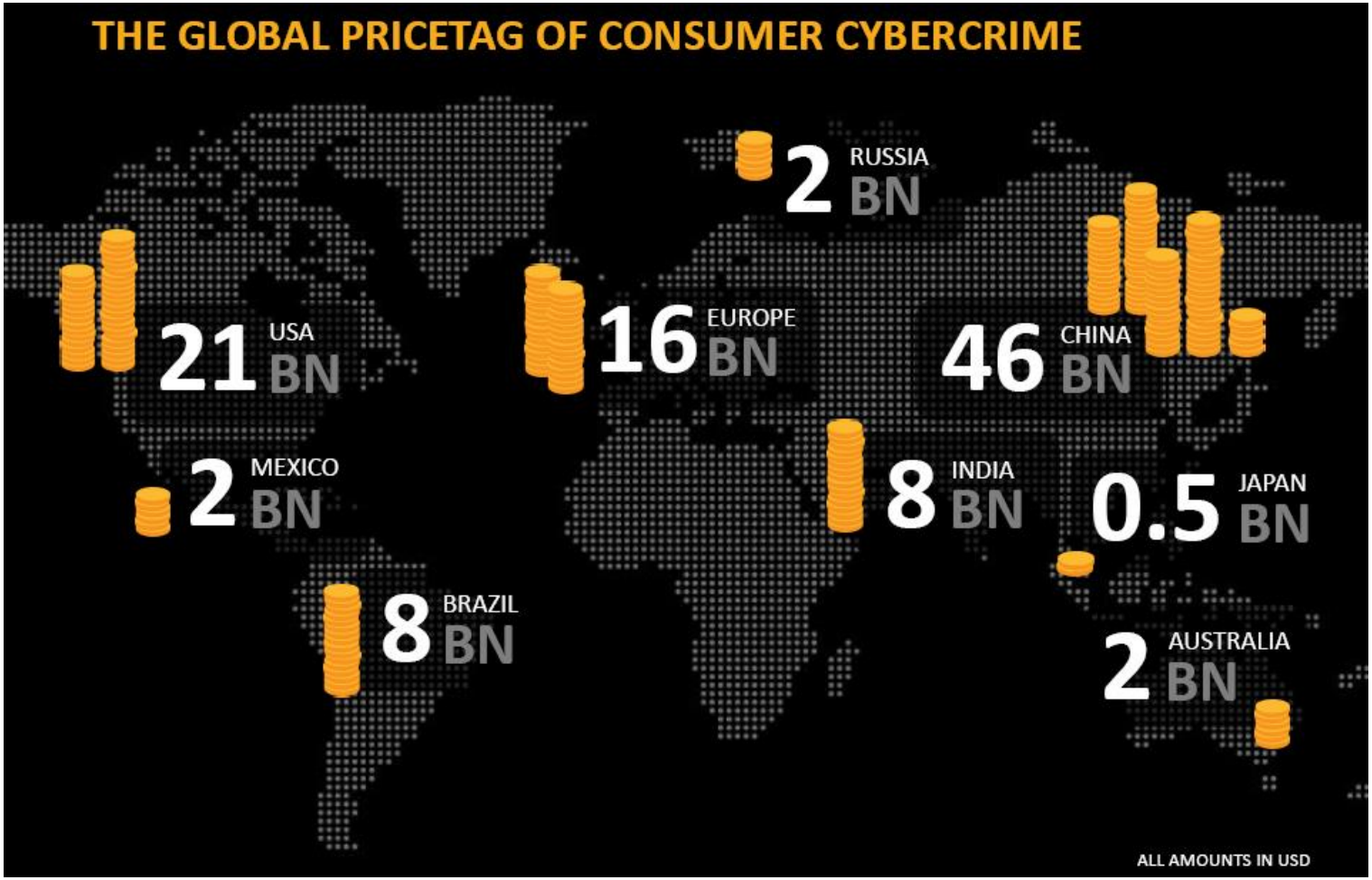
Cybercrime

G20 Countries

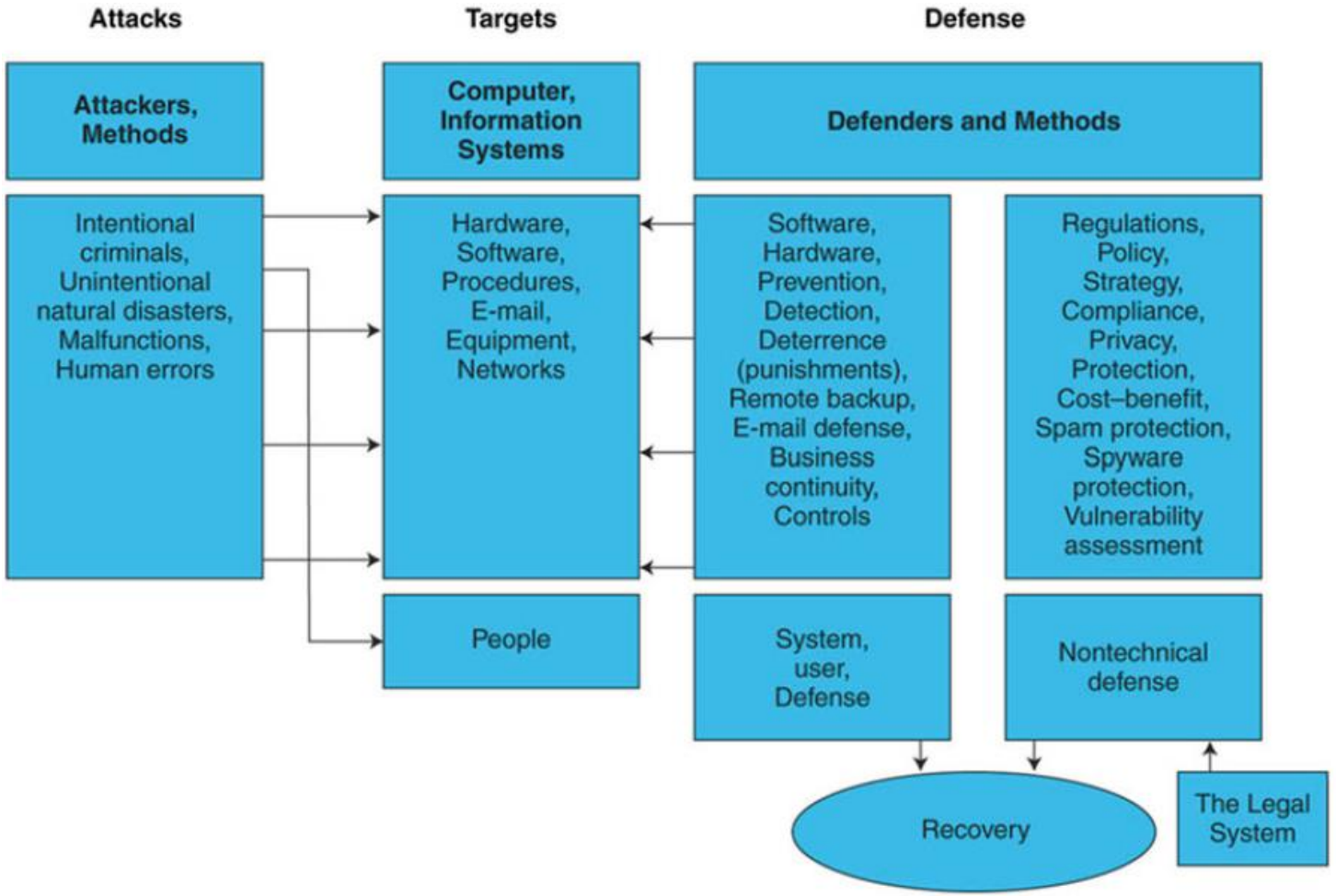
Australia (.08%)
Brazil (.32%)
Canada (.17%)
China (.63%)
European Union (.41%)
France (.11%)
Germany (1.60%)
India (.21%)
Japan (.02%)
Mexico (.17%
Russia (.10%)
Saudi Arabia (.17%)
Turkey (.07%)
United Kingdom (.16%)
United States (.64%)



Cybercrime

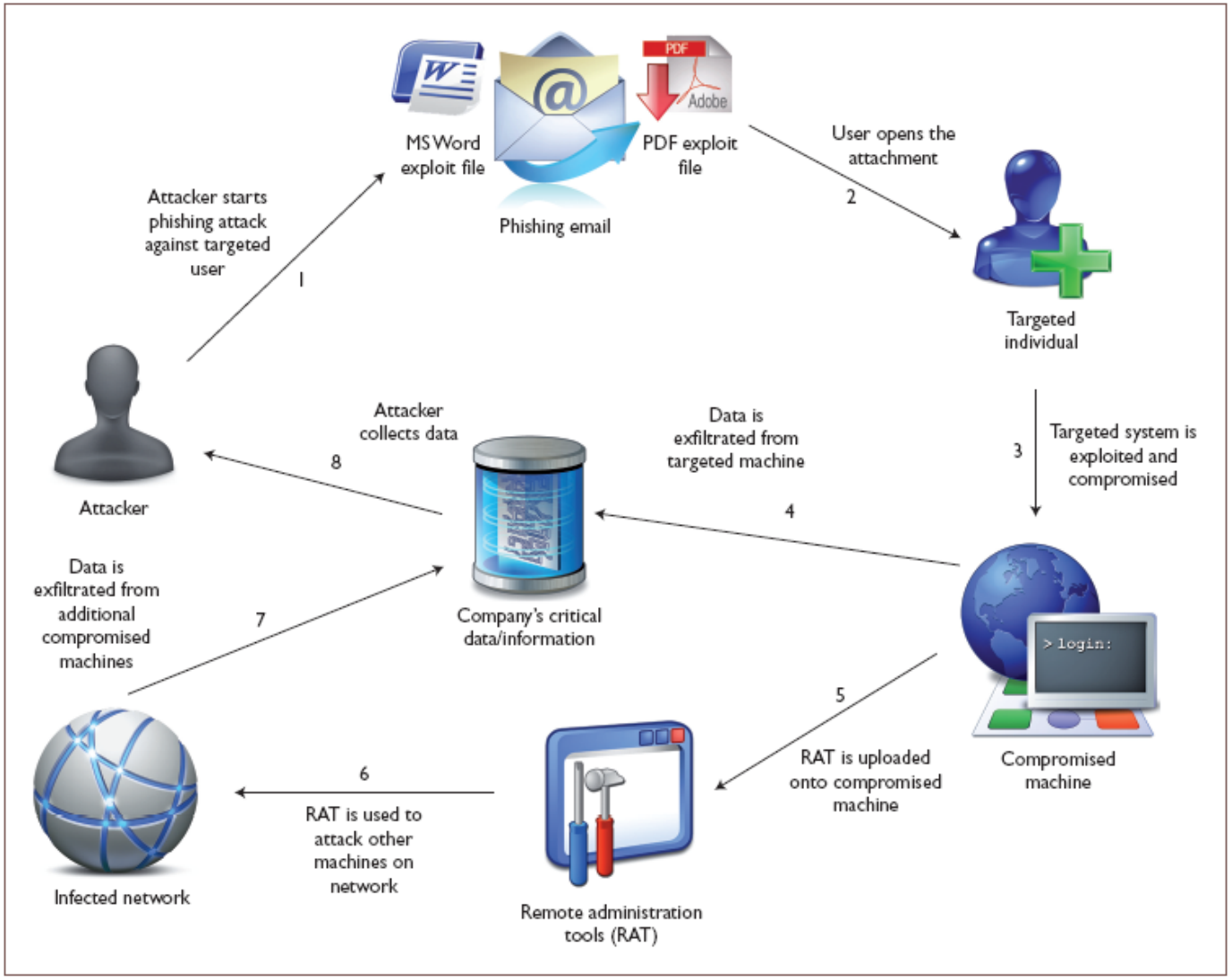

THE GLOBAL PRICETAG OF CONSUMER CYBERCRIME
2 BN RUSSIA
21 BN USA
16 BN EUROPE
46 BN CHINA
2 BN MEXICO
8 BN INDIA
0.5 BN JAPAN
8 BN BRAZIL
2 BN AUSTRALIA
ALL AMOUNTS IN USD

Cybercrime: Security Battleground



Life cycle of a generic targeted attack

The life cycle of a generic targeted attack. A targeted attack is directed toward a specific individual, group, business, or government body.



Attacks

- Software and systems knowledge are used to perpetrate ***technical attacks***.
- ***Organizational attacks*** are those where the security of a network or the computer is compromised (e.g., lack of proper security awareness training).

Technical security attack methods

- Malware (Virus, Worm, Trojan)
- Unauthorized Access
- Denial-of-Service Attacks
- Spam and Spyware
- Hijacking (Servers, Pages)
- Botnets

Technical security attack methods

- ***Malware*** (or malicious software) is software code, that when spread, is designed to infect, alter, damage, delete, or replace data or an information system without the owner's knowledge or consent.
  - Malware is a comprehensive term that describes any malicious code or software (e.g., a virus is a "subset" of malware).
  - Malware attacks are the most frequent security breaches, affecting 22% of companies[1].

[1]Lawinski, J. "Companies Spend on Security Amid Mobile and Social Threats." Baseline , September 14, 2011.

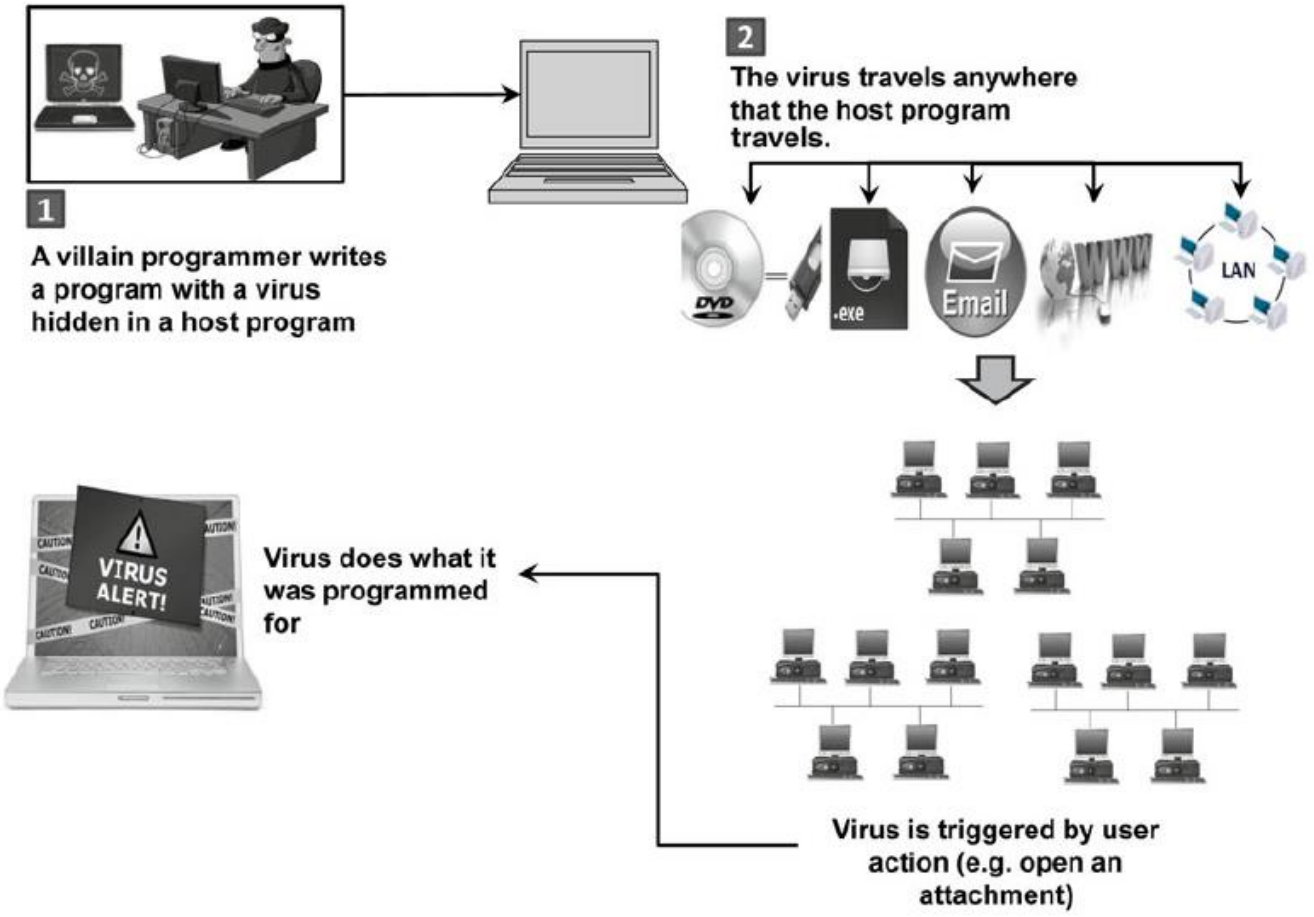
Technical security attack methods

- Malware includes computer viruses, worms, botnets, Trojan horses, phishing tools, spyware tools, and other malicious and unwanted software.

Virus

- A ***virus*** is programmed software inserted by criminals into a computer to damage the system; running the infected host program activates the virus.
- A virus has two basic capabilities:
  - First, it has a mechanism by which it spreads.
  - Second, it can carry out damaging activities once it is activated.
  - Sometimes a particular event triggers the virus's execution.

Computer virus spreading



Worms

- Unlike a virus, a worm can replicate itself automatically (as a “standalone” – without any host or human activation).
- Worms use networks to propagate and infect a computer or handheld device and can even spread via instant messages or e-mail.
- A worm can infect many devices in a network as well as degrade the network’s performance.
- Worms either exploit a vulnerability on the target system or use some kind of social engineering to trick users into executing them.

Macro viruses and Macro worms

- A macro virus (macro worm) is a malware code that is attached to a data fi le rather than to an executable program (e.g., a Word file).
- Macro viruses can attack Word files as well as any other application that uses a programming language.
  - When the document is opened or closed, the virus can spread to other documents on the computer's system.

Trojan Horse

- A Trojan horse is a program that seems to be harmless or even looks useful but actually contains a hidden malicious code.
- Users are tricked into executing an infected fi le, where it attacks the host, anywhere from inserting pop-up windows to damaging the host by deleting files, spreading malware, and so forth.
  - The name is derived from the Trojan horse in Greek mythology.
- Trojans spread only by user interaction

Trojan Horse

- Cryptolocker
  - Discovered in September 2013, Cryptolocker is a ransomware Trojan bug. This malware can come from many sources including e-mail attachments, can encrypt files on your computer, so that you cannot read these files. The malware owner then offers to decrypt the data in exchange for a Bitcoin or similar untraceable payment system.

Denial of Service (DoS)

- A ***denial-of-service (DoS)*** attack is a malicious attempt to make a server or network resource unavailable to users, usually by temporarily interrupting or suspending the services of a host connected to the Internet.
- A DoS attack causes the system to crash or become unable to respond in time, so the site becomes unavailable.

Denial of Service (DoS)

- One of the most popular types of DoS attacks occurs when a hacker “floods” the system by overloading the system with “useless traffic” so a user is prevented from accessing their e-mail, websites, etc.
- A attack Dos is a malicious attack caused by one computer and one Internet connection as opposed to a ***Distributed DoS (DDoS)*** attack, which involves many devices and multiple Internet connections.

Botnets

- A ***botnet*** (also known as ***"zombie army"***), is malicious software that criminals distribute to infect a large number of hijacked Internet connected computers controlled by hackers.
- The infected computers then form a "botnet," causing the personal computer to "perform unauthorized attacks over the Internet" without the user's knowledge.

Botnets

- Unauthorized tasks include sending spam and e-mail messages, attacking computers and servers, and committing other kinds of fraud, causing the user's computer to slow down.
- Each attacking computer is considered computer robot.

Home Appliance "Botnet"

- The Internet of Things (IoT) can also be hacked. Since participating home appliances have a connection to the Internet, they can become computers that can be hacked and controlled.
  - The first home attack, which involved television sets and at least one refrigerator, occurred between December 2013 and January 2014, and was referred to as "the fi rst home appliance 'botnet' and the fi rst cyberattack from the Internet of Things." Hackers broke into more than 100,000 home appliances and used them to send over 750,000 malicious e-mails to enterprises and individuals worldwide.

Malversting

- ***Malvertising*** is a malicious form of Internet advertising used to spread malware.
- Malvertising is accomplished by hiding malicious code within relatively safe online advertisements.

Attacks

If you get an e-mail that congratulates you on winning a large amount of money and asks you to “Please view the attachment,” don’t!

Security strategy

- Three necessary attributes are related to the ***Information Assurance (IA) model***:
  - Confidentiality
  - Integrity
  - Availability.
- Three concepts are related to the IA model:
  - Authentication
  - Authorization
  - Nonrepudiation.

The phases of security defense

1. Prevention and deterrence (preparation). Good controls may prevent criminal activities as well as human error from occurring.
   - Controls can also deter criminals from attacking computerized systems and deny access to unauthorized human intruders. Also, necessary tools need to be acquired.

The phases of security defense

1. **Prevention and deterrence (preparation).** Good controls may prevent criminal activities as well as human error from occurring.

- Controls can also deter criminals from attacking computerized systems and deny access to unauthorized human intruders. Also, necessary tools need to be acquired.

The phases of security defense

2. **Initial Response** . The first thing to do is to verify if there is an attack. If so, determine how the intruder gained access to the system and which systems and data are infected or corrupted.

3. **Detection.** The earlier an attack is detected, the easier it is to fi x the problem, and the smaller amount of damage is done. Detection can be executed by using inexpensive or free intrusion detecting software.

The phases of security defense

4. **Containment (contain the damage).** This objective is to minimize or limit losses once a malfunction has occurred. It is also called *damage control* . Damage control can be done, for example, by using *fault-tolerant* hardware and software that enable operation in a satisfactory, but not optimal, mode until full recovery is made.

The phases of security defense

5. **Eradication .** Remove the malware from infected hosts.

6. **Recovery.** Recovery needs to be planned for to assure quick return to normal operations at a reasonable cost. One option is to replace parts rather than to repair them. Functionality of data should also be restored.

The phases of security defense

7. **Correction.** Finding the causes of damaged systems and fixing them will prevent future occurrences.

6. **Awareness and compliance.** All organization members must be educated about possible hazards and must comply with the security rules and regulations.

The Defense

- **Access control** determines who (person, program, or machine) can legitimately use the organization's computing resources (which resources, when, and how).
  - A resource refers to hardware, software, Web pages, text fi les, databases, applications, servers, printers, or any other information source or network component.
  - Typically, access control defines the rights that specific users with access may have with respect to those resources (i.e., read, view, write, print, copy, delete, execute, modify, or move).

The Defense

- Access control involves authorization (having the right to access) and authentication , which is also called user identification (user ID), i.e., proving that the user is who he or she claims to be. Each user has a distinctive identification that differentiates it from other users. Typically, user identification is used together with a password.

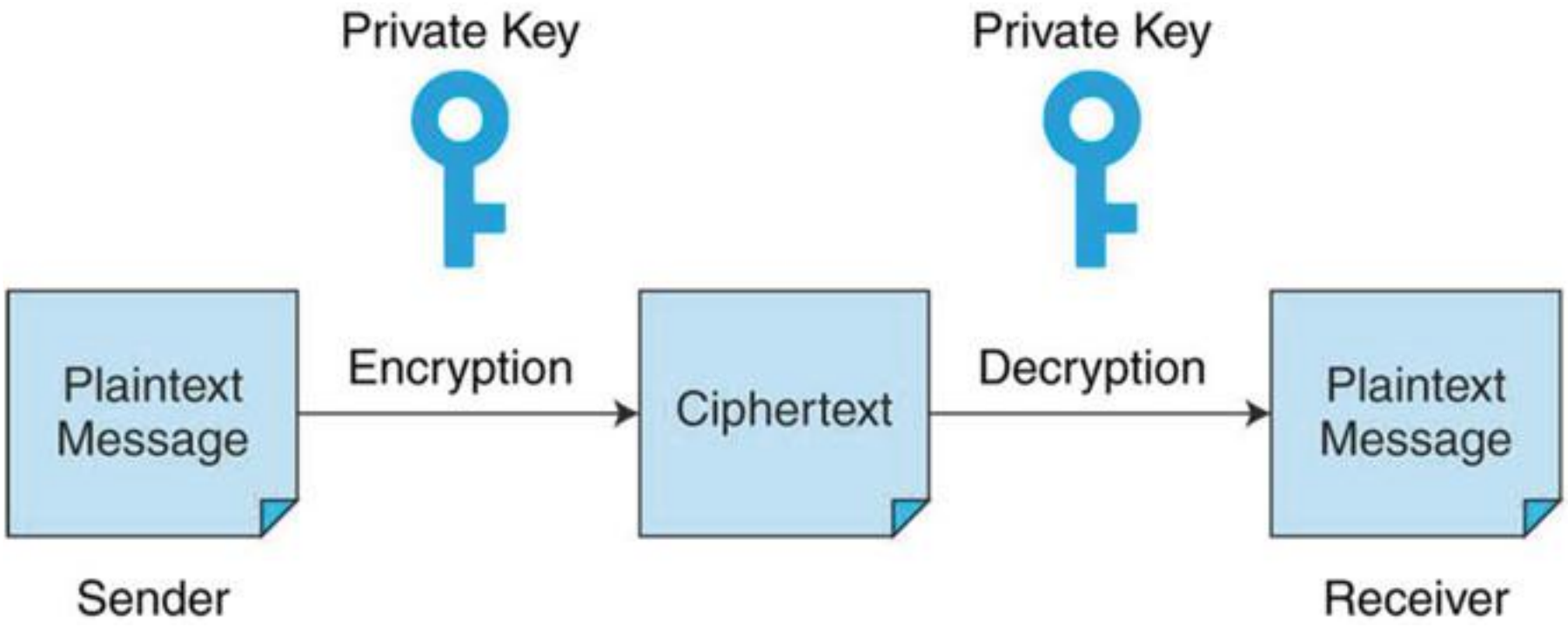
The Defense

- After a user has been identified , the user must be authenticated. Authentication is the process of verifying the user's identity and access rights. Verification of the user's identity usually is based on one or more characteristics that distinguish one individual from another.
  - Password
  - Biometric system: Thumbprint or fingerprint, Retinal scan, Voice ID, Facial recognition, Signature recognition.

The Defense

- **Encryption** is the process of encoding data into a form (called a ciphertext) that will be difficult, expensive, or time-consuming for an unauthorized person to understand. All encryption methods have five basic components: plaintext, ciphertext , an encryption algorithm , the key, and key space.

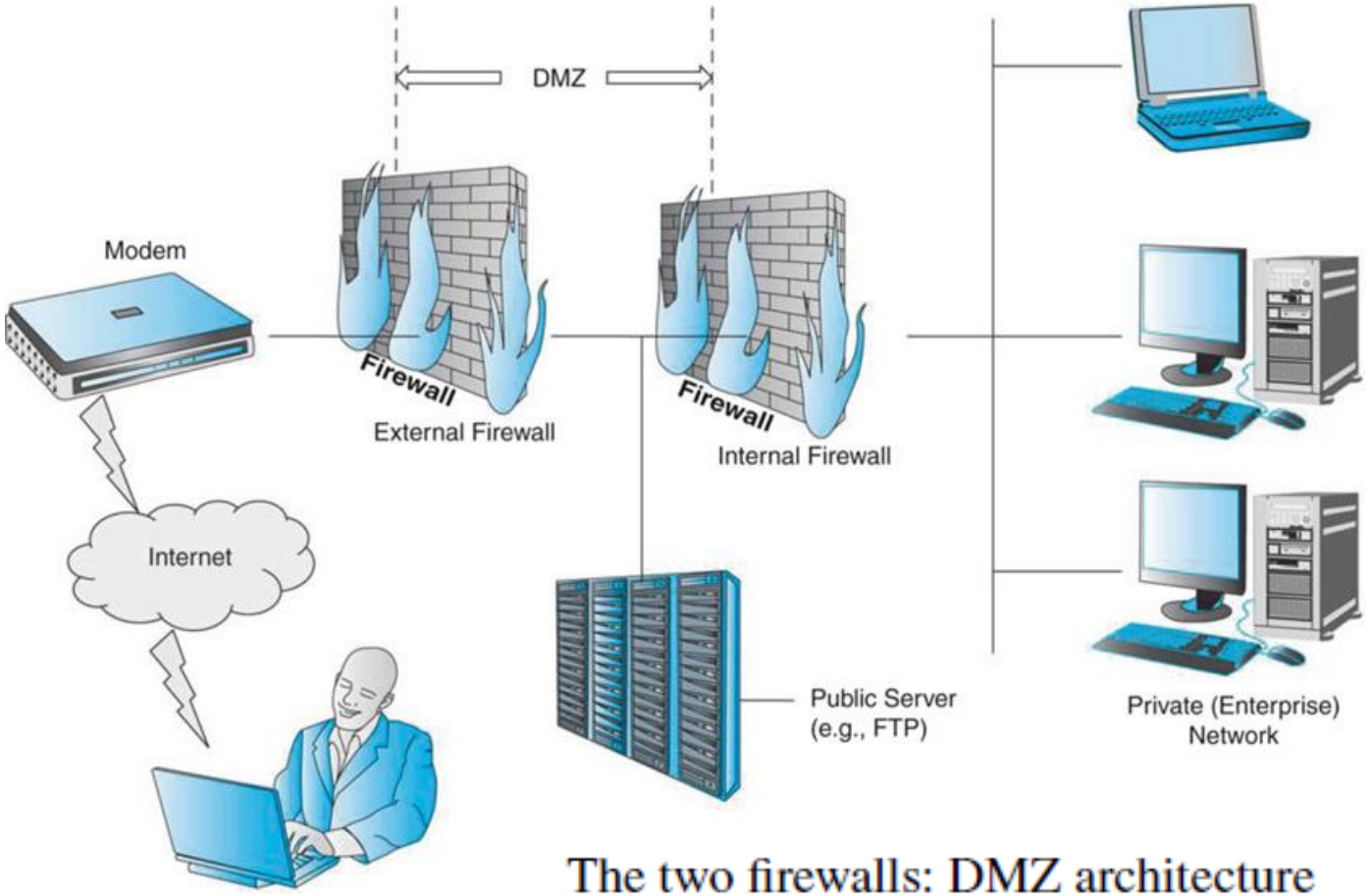
Symmetric encryption



Firewall

- Firewalls are barriers between an internal trusted network (or a PC) and the untrustworthy Internet.
- A firewall is designed to prevent unauthorized access to and from private networks, such as intranets.
- Technically, a firewall is composed of hardware and a software package that separates a private computer network (e.g., your LAN) from a public network (the Internet).

Firewall



The two firewalls: DMZ architecture

Cyberwarfare

- Cyberwarfare or (Cyberwar) refers to any action by a nation-state or international organization to penetrate another nation's computer networks for the purpose of causing damage or disruption.
- Cyberwarfare also includes acts of 'cyberhooliganism,' cybervandalism or cyberterrorism. The attack usually is done through viruses, DoS, or botnets.

Cyberwarfare major threats

- Online acts of espionage (cyberspionage) and security breaches
  - are done to obtain national material and information of a sensitive or classified nature through the exploitation of the Internet.
- Sabotage
  - the use of the Internet to disrupt online communications with the intent to cause damage.
- Attacks on SCADA (Supervisory Control and Data Acquisition) network and NCIs (National Computational Infrastructure).

Cyberwarfare example 1

- Stuxnet
  - In December 2010, the Iranian nuclear program was attacked via sophisticated computer worm (rumored to have been created by the United States and Israel). The attack was successful, causing major physical damage to the nuclear program, delaying it by months or possibly even years.

Cyberwarfare example 2

- Turla
  - One of the most complex cyberespionage incidents that has ever occurred (2014) is the suspected Russian spyware Turla, which was used to attack hundreds of government computers in the U.S. and Western Europe.