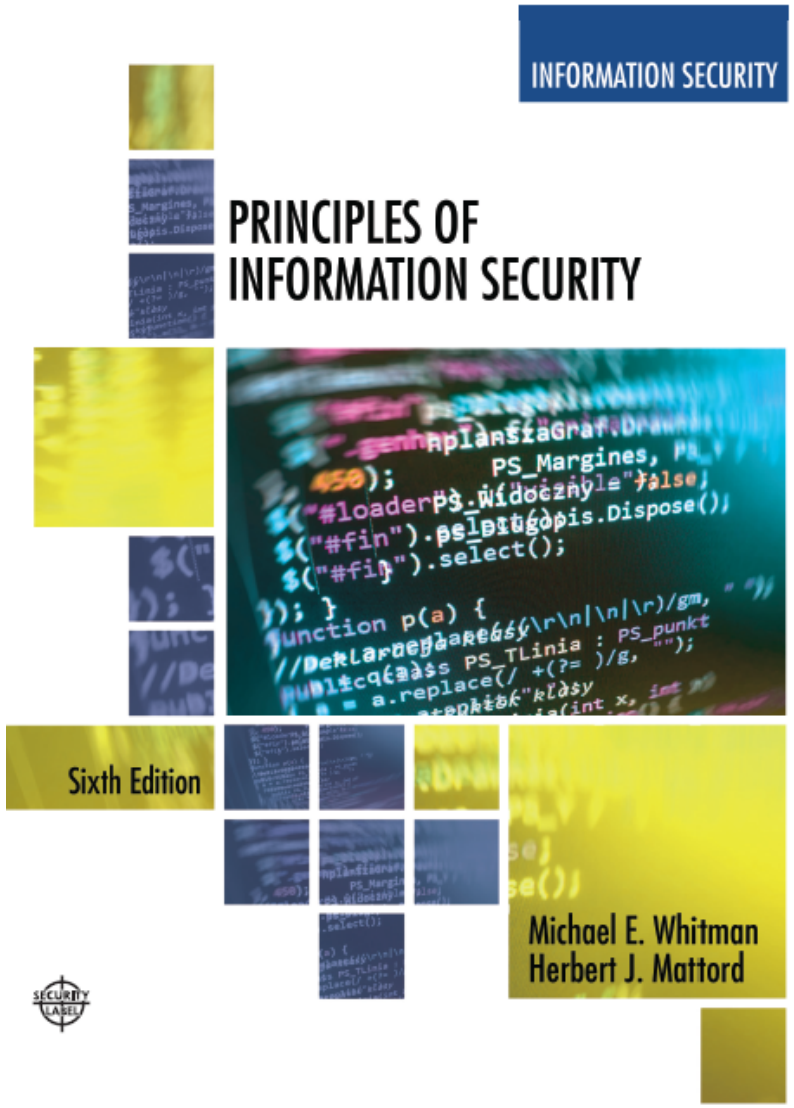


Source: Principles of Information Security

Chapter 2

The Need for Security

Dr. Ibrahim Waziri Jr.

Learning Objectives

Upon completion of this material, you should be able to:

- Discuss the organizational need for information security
- List and describe the threats posed to information security and common attacks associated with those threats
- List the common development failures and errors that result from poor software and system security efforts

Introduction

- The primary mission of an information security program is to ensure information assets—information and the systems that house them—remain safe and useful.
- If no threats existed, resources could be used exclusively to improve systems that contain, use, and transmit information.
- Threat of attacks on information systems is a constant concern.

Business Needs First

Information security performs four important functions for an organization:

- Protecting the organization's ability to function
- Protecting the data and information the organization collects and uses
- Enabling the safe operation of applications running on the organization's IT systems
- Safeguarding the organization's technology assets

Threats and Attacks

Management must be informed about the various threats to an organization's people, applications, data, and information systems.

- **Threat:** a potential risk to an asset's loss of value.
- **Attack:** An intentional or unintentional act that can damage or otherwise compromise information and the systems that support it.
- **Exploit:** A technique used to compromise a system.
- **Vulnerability:** A potential weakness in an asset or its defensive control system(s).

Overall security is improving, but so is the number of potential hackers.

Categories of Threats to Information Security

#	Category of Threat	Attack Examples
1	Compromises to intellectual property (IP)	Piracy, copyright infringement
2	Deviations in quality of service	Internet service provider, power, etc.
3	Espionage or trespass	Unauthorized access and/or data collection
4	Forces of nature	Fire, floods, earthquakes. lightning
5	Human error or failure	Accidents, employee mistakes
6	Information extortion	Blackmail, information disclosure
7	Sabotage or vandalism	Destruction of systems or information
8	Software attacks	Viruses, worms, macros, denial of service
9	Technical hardware failures or errors	Equipment failure
10	Technical software failures or errors	Bugs, code problems, unknown loopholes
11	Technological obsolescence	Antiquated or outdated technologies
12	Theft	Illegal confiscation of equipment/ information

1 - Compromises to IP

Intellectual property (IP): creation, ownership, and control of original ideas as well as the representation of those ideas.

- The most common IP breaches involve software piracy.
- Enforcement of copyright law has been attempted with technical security mechanisms (DRM)
- Organizations:
  - Software & Information Industry Association (SIIA)
  - Business Software Alliance (BSA)
  - US Patent and Trademark Office (USPTO)
  - World Intellectual Property Organization (WIPO)

2 - Deviations in Quality of Service

Information systems depends on the successful operation of many interdependent support systems.

- **Internet service issues**
  - Internet service provider (ISP) failures can considerably undermine the availability of information.
  - Outsourced Web hosting provider assumes responsibility for all Internet services as well as for the hardware and Web site operating system software.

- **Communications and other service provider issues**
  - Other utility services affect organizations: telephone, water, wastewater, trash pickup.
  - Loss of these services can affect an organization's ability to function.

- **Power irregularities**
  - Lead to fluctuations such as power excesses, power shortages, and power losses
  - Sensitive electronic equipment vulnerable to and easily damaged/destroyed by fluctuations
  - Controls can be applied to manage power quality

3 - Espionage or Trespass

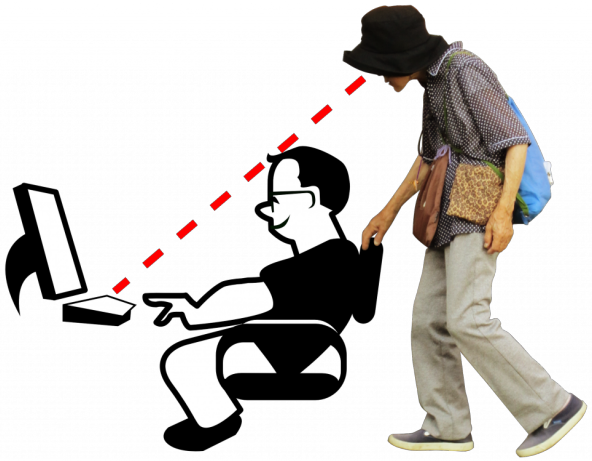
Access of protected information by unauthorized individuals.

Hackers: use skill, guile, or fraud to bypass controls protecting others' information

- Expert hackers: Develop software scripts and program exploits
- Unskilled hackers: Use expertly written software to exploit a system
- Cracker: "cracks" or removes software protection designed to prevent unauthorized duplication
- Phreaker: hacks the public telephone system to make free calls or disrupt services

Password attacks: includes Cracking, Brute force, Dictionary Attacks, Rainbow tables, Social engineering etc.

Shoulder Surfing



Password Attacks (Alpha)

Case-Insensitive Passwords Using a Standards Alphabet Set (No Numbers or Special Characters)		
Password Length	**Odd of cracking: 1 in (Based on Numbers of Characters ^ Password length):**	**Estimated Time to Crack***
8	208,827,064,576	1.01 seconds
9	5,429,503,678,976	26.2 seconds
10	141,167,095,653,376	11.4 minutes
11	3,670,344,486,987,780	4.9 hours
12	95,428,956,661,682,200	5.3 days
13	2,481,152,873,203,740,000	138.6 days
14	64,509,974,703,297,200,000	9.9years
15	1,677,259,342,285,730,000,000	256.6 years
16	43,608,742,899,428,900,000,000	6,672.9 years

*Estimated Time to crack is based on a 2015-era PC with an intel i7-6700K Quad Core CPU performing 207.23 Dhrystone GIPS (giga/ billion instructions per second) at 4.0 GHz.

Password Attacks (Alphanumeric)

Case-Sensitive Passwords Using a Standards Alphabet Set (with Numbers and Special Characters)		
Password Length	**Odd of cracking: 1 in (Based on Numbers of Characters ^ Password length):**	**Estimated Time to Crack***
8	2,044,140,858,654,980	2.7 hours
9	167,619,550,409,708,000	9.4 days
10	13,744,803,133,596,100,000	2.1 years
11	1,127,073,856,954,880,000,000	172.5 years
12	92,420,056,270,299,900,000,000	14,141.9 years
13	7,578,444,614,164,590,000,000,000	1,159,633.8 years
14	621,432,458,361,496,000,000,000,000	95,089,967.6 years
15	50,957,461,585,642,700,000,000,000,000	7,797,377,343.5 years
16	4,178,511,850,022,700,000,000,000,000,000	639,384,942,170.1 years

*Estimated Time to crack is based on a 2015-era PC with an intel i7-6700K Quad Core CPU performing 207.23 Dhrystone GIPS (giga/ billion instructions per second) at 4.0 GHz.

4 - Forces of Nature

Forces of nature can present some of the most dangerous threats.

- Such as: Fire, Flood, Hurricane etc.

- They disrupt not only individual lives but also storage, transmission, and use of information.

- Organizations must implement controls to limit damage and prepare contingency plans for continued operations.
  - Alternate recovery sites etc.

5 - Human Error or Failure

These are acts performed without malicious intent or in ignorance due to Inexperience, Improper training, Incorrect assumptions, social engineering etc. Employees are among the greatest threats to an organization's data.

- Employee mistakes can easily lead to:
  - Revelation of classified data
  - Entry of erroneous data
  - Accidental data deletion or modification
  - Data storage in unprotected areas
  - Failure to protect information

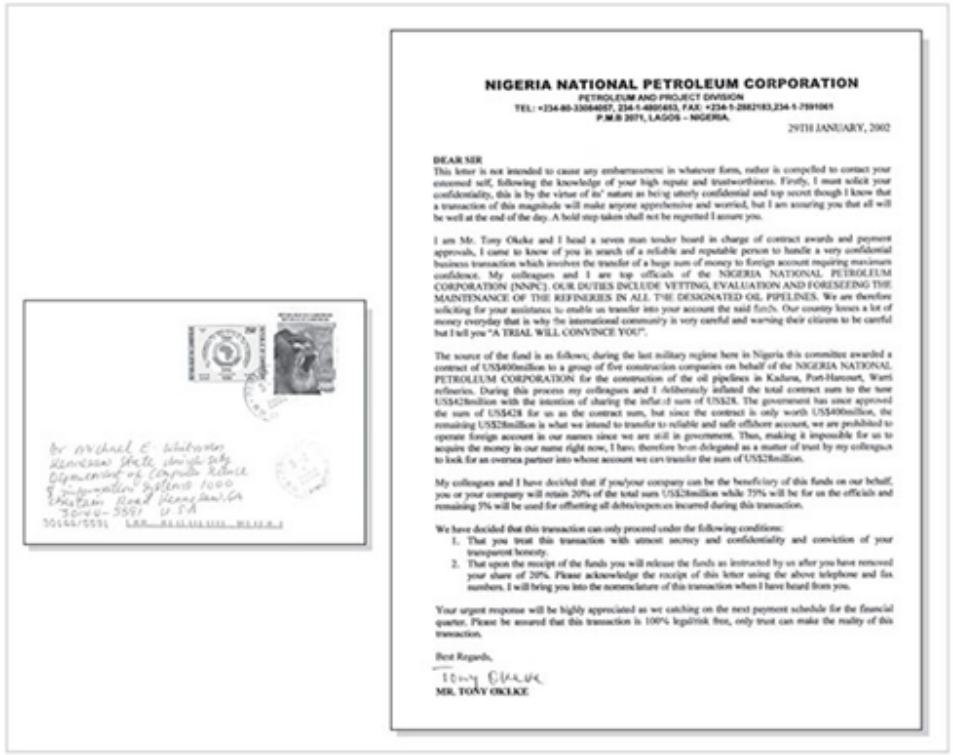
Tommy Twostory,
convicted burglar

Harriett Allthumbs,
confused the copier with the shredder
when preparing the annual sales report

Elite Skillz,
wannabe hacker

- Many of these threats can be prevented with training, ongoing awareness activities, and controls.

Social Engineering



NIGERIA NATIONAL PETROLEUM CORPORATION
PETROLEUM AND PROJECT DIVISION
TEL: +234-80-33084057, 234-1-4605653, FAX: +234-1-2692183,234-1-7591061
P.M.B 2071, LAGOS – NIGERIA.

29TH JANUARY, 2002

DEAR SIR

This letter is not intended to cause any embarrassment in whatever form, rather is compelled to contact your esteemed self, following the knowledge of your high repute and trustworthiness. Firstly, I must solicit your confidentiality, this is by the virtue of its' nature as being utterly confidential and top secret though I know that a transaction of this magnitude will make anyone apprehensive and worried, but I am assuring you that all will be well at the end of the day. A bold step taken shall not be regretted I assure you.

I am Mr. Tony Okeke and I head a seven man tender board in charge of contract awards and payment approvals, I came to know of you in search of a reliable and reputable person to handle a very confidential business transaction which involves the transfer of a huge sum of money to foreign account requiring maximum confidence. My colleagues and I are top officials of the NIGERIA NATIONAL PETROLEUM CORPORATION [NNPC]. OUR DUTIES INCLUDE VETTING, EVALUATION AND FORESEEING THE MAINTENANCE OF THE REFINERIES IN ALL T^IE DESIGNATED OIL PIPELINES. We are therefore soliciting for your assistance to enable us transfer into your account the said funds. Our country knows a lot of money everyday that is why the international community is very careful and warning their citizens to be careful but I tell you "A TRIAL WILL CONVINCE YOU".

The source of the fund is as follows; during the last military regime here in Nigeria this committee awarded a contract of US$400million to a group of five construction companies on behalf of the NIGERIA NATIONAL PETROLEUM CORPORATION for the construction of the oil pipelines in Kaduna, Port-Harcourt, Warri refineries. During this process my colleagues and I deliberately inflated the total contract sum to the tune US$428million with the intention of sharing the inflated sum of US$28. The government has since approved the sum of US$428 for us as the contract sum, but since the contract is only worth US$400million, the remaining US$28million is what we intend to transfer to reliable and safe offshore account, we are prohibited to operate foreign account in our names since we are still in government. Thus, making it impossible for us to acquire the money in our name right now, I have therefore been delegated as a matter of trust by my colleagues to look for an oversea partner into whose account we can transfer the sum of US$28million.

My colleagues and I have decided that if you/your company can be the beneficiary of this funds on our behalf, you or your company will retain 20% of the total sum US$28million while 75% will be for us the officials and remaining 5% will be used for offsetting all debts/expenses incurred during this transaction.

We have decided that this transaction can only proceed under the following conditions:

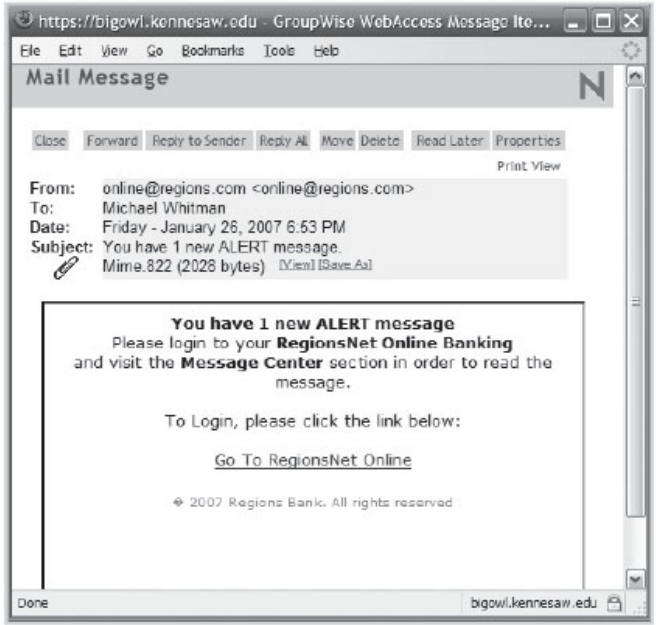
1. That you treat this transaction with utmost secrecy and confidentiality and conviction of your transparent honesty.
2. That upon the receipt of the funds you will release the funds as instructed by us after you have removed your share of 20%. Please acknowledge the receipt of this letter using the above telephone and fax numbers. I will bring you into the nomenclature of this transaction when I have heard from you.

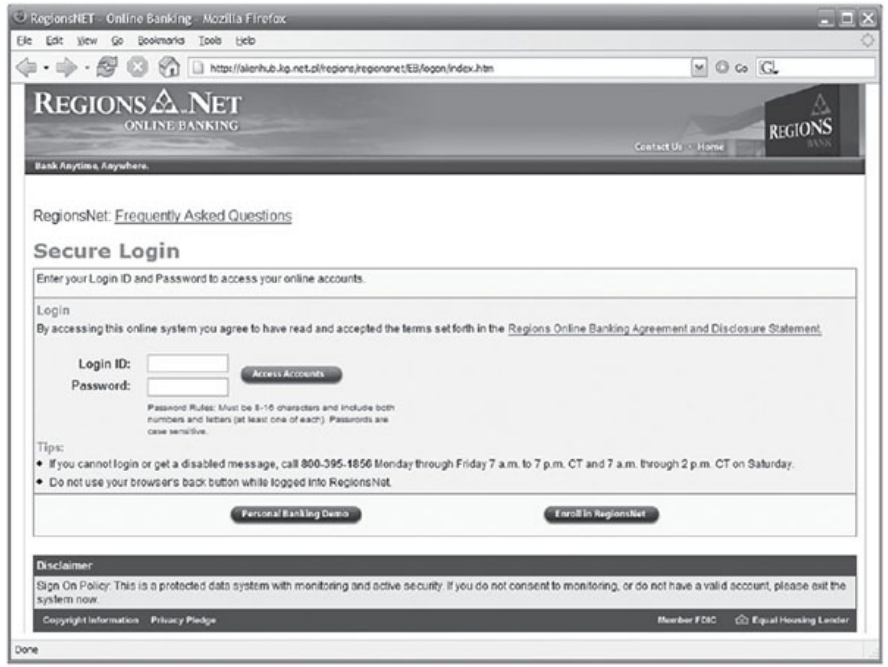
Your urgent response will be highly appreciated as we catching on the next payment schedule for the financial quarter. Please be assured that this transaction is 100% legal/risk free, only trust can make the reality of this transaction.

Best Regards,

MR. TONY OKEKE

Advance-fee fraud: indicates recipient is due money and small advance fee/personal banking information required to facilitate transfer.





Phishing: attempt to gain personal/confidential information; apparent legitimate communication hides embedded code that redirects user to third-party site.

6 - Information Extortion

Attacker steals information from a computer system and demands compensation for its return or nondisclosure.

Types of Information Extortion (or Cyberextortion) attacks includes:

Cyber blackmail – sextortion, GoT blackmail, Sony Hack

Ransomware - WannaCry & NotPetya

7 - Sabotage or Vandalism

- Threats can range from petty vandalism to organized sabotage.
- Web site defacing can erode consumer confidence, diminishing organization's sales, net worth, and reputation.
- Threat of hacktivist or cyberactivist operations is rising. – Anonymous, LulzSec
- Cyberterrorism/Cyberwarfare: a much more sinister form of hacking.

Anonymous Group Logo

8 - Software Attacks

Malware (malicious code): It includes the execution of viruses, worms, Trojan horses, and active Web scripts with the intent to destroy or steal information.

- **Virus:** It consists of code segments that attach to existing program and take control of access to the targeted computer.
- **Worms:** They replicate themselves until they completely fill available resources such as memory and hard drive space.
- **Trojan horses:** malware disguised as helpful, interesting, or necessary pieces of software.
- **Polymorphic threat:** evolves to elude detection

Well-known Malware Attacks

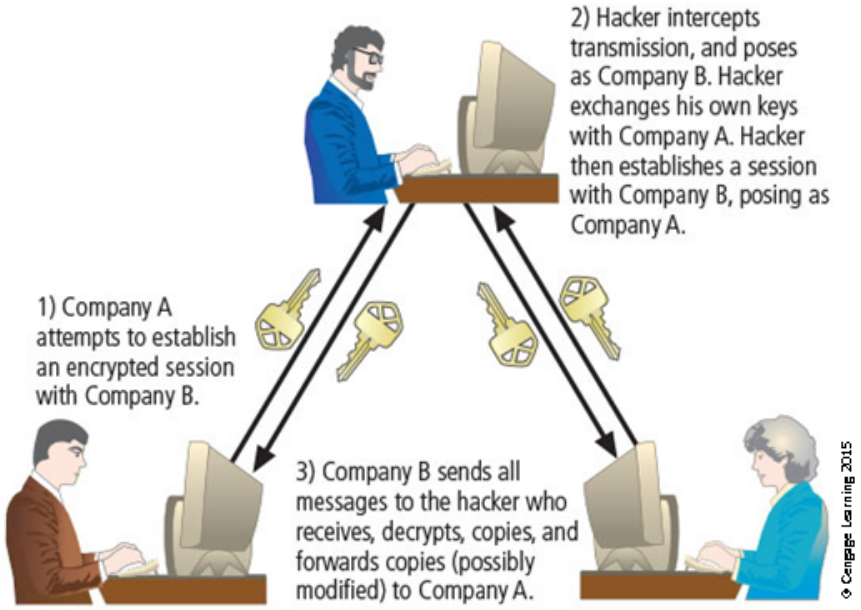
Malware	Type	Year	Estimated Number of Systems Infected	Estimated Financial Damage
Stuxnet	Worm	2010	200,000	Iran's Nuclear Program
MyDoom	Worm	2004	2 million	$ 38 billion
Klez (and variants)	Virus	2001	7.2% of Internet	$19.8 billion
ILOVEYOU	Virus	2000	10% of Internet	$ 5.5 billion
Sobig F	Worm	2003	1 million	$ 3 billion
Code Red (and CR II)	Worm	2001	400,000 servers	$ 2.6 billion
SQL slammer, a.k.a. Sapphire	Worm	2003	75,000	$ 950 million to $ 1.2 billion
Melissa	Macro virus	1999	Unknown	$ 300 million to $ 600 million
CIH, a.k.a. Chernobyl	Memory-resident virus	1998	Unknown	$ 250 million
Storm Worm	Trojan horse virus	2006	10 million	Unknown
Conficker	Worm	2009	15 million	Unknown
Nimda	Multivector worm	2001	Unknown	Unknown
Sasser	Worm	2004	500,000 to 700,000	Unknown
Nesky	Virus	2004	Under 100,000	Unknown
Leap-A/Oompa-A	Virus	2006	Unknown (Apple)	Unknown

8 - Software Attacks

Back door: gaining access to system or network using known or previously unknown/newly discovered access mechanism. Apple-FBI encryption backdoor dispute.

Pharming: It attacks a browser's address bar to redirect users to an illegitimate site for the purpose of obtaining private information.

Man-in-the-middle (MiTM) or Middle Person: An attacker monitors the network packets, modifies them, and inserts them back into the network.

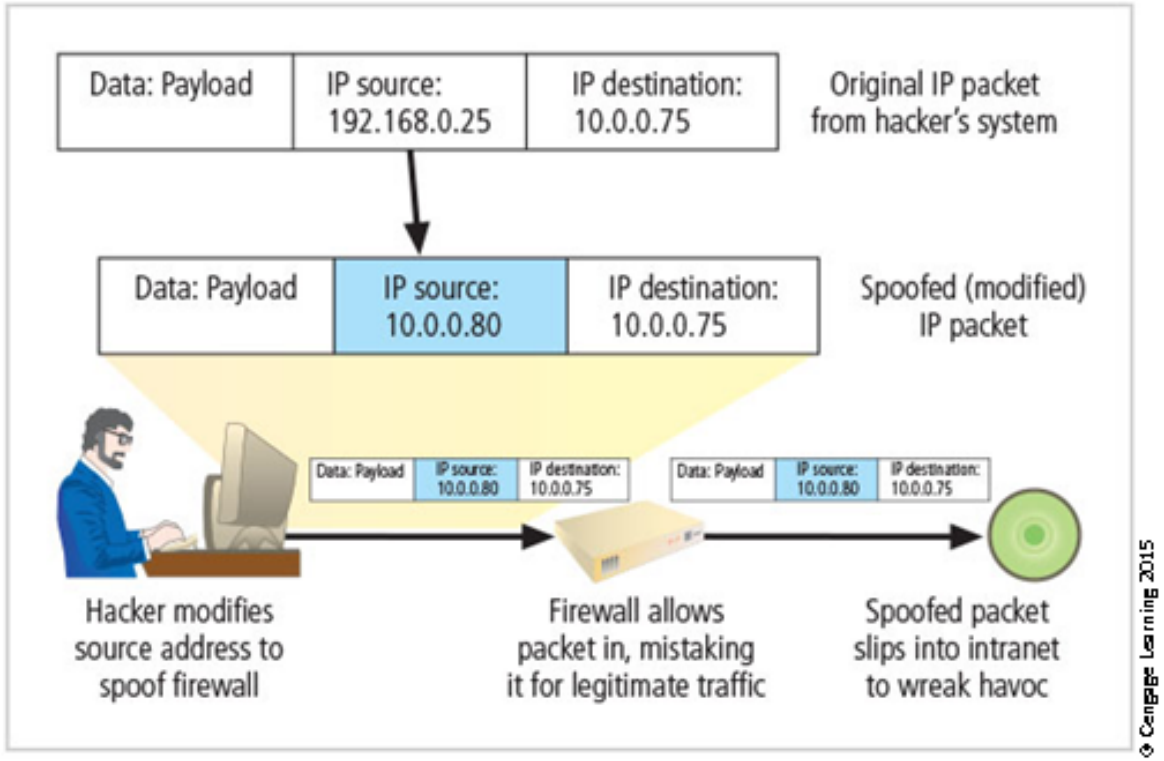


Man-in-the-middle

8 - Software Attacks

Packet sniffing: Monitoring data traveling over network; it can be used both for legitimate management purposes and for stealing information from a network.

IP Spoofing: A technique used to gain unauthorized access; intruder assumes a trusted IP address.



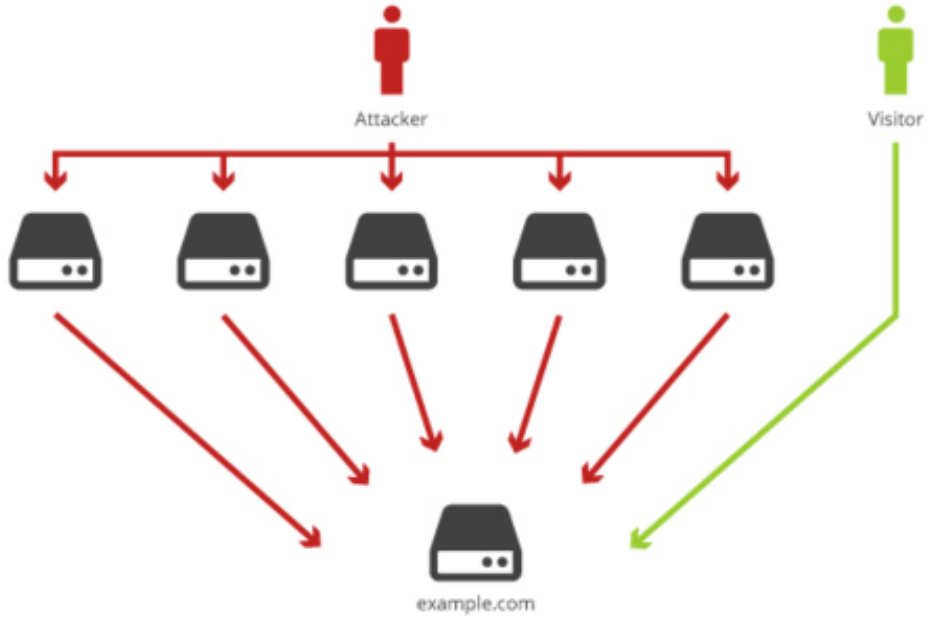
IP Spoofing

8 - Software Attacks

Denial-of-service (DoS) & Distributed DoS: An attacker sends a large number of connection or information requests to a target. - GitHub attack in 2018 (1.35Tbps)

- **Mail bombing (also a DoS):** An attacker routes large quantities of e-mail to target to overwhelm the receiver.

- **Spam** (unsolicited e-mail)**:** It is considered more a nuisance than an attack, though is emerging as a vector for some attacks.



DDoS Attack

9 - Technical Hardware Failures/Errors

- They occur when a manufacturer distributes equipment containing a known or unknown flaw.
- They can cause the system to perform outside of expected parameters, resulting in unreliable service or lack of availability.
- Some errors are terminal and some are intermittent.
  - Intel Pentium CPU failure.
  - Mean time between failure (MTBF) measures the amount of time between hardware failures.

Samsung Fold and Samsung Exploding Battery

10 - Technical Software Failures/Errors

Large quantities of computer code are written, debugged, published, and sold before all bugs are detected and resolved.

- Combinations of certain software and hardware can reveal new software bugs.
- Entire Web sites are dedicated to documenting bugs.
- Open Web Application Security Project (OWASP) is dedicated to helping organizations create/operate trustworthy software and publishes a list of top security risks.

The Deadly Sins in Software Security

Common failures in software development:

- Buffer overruns
- Catching exceptions
- Command injection
- Cross-site scripting (XSS)
- Failure to handle errors
- Failure to protect network traffic
- Failure to store and protect data securely
- Failure to use cryptographically strong random numbers
- Format string problems
- Neglecting change control
- Improper file access
- Improper use of Secure Sockets Layer (SSL)
- Information leakage
- Integer bugs (overflows/underflows)
- Race conditions
- SQL injection

Problem areas in software development

- Trusting network address resolution
- Unauthenticated key exchange
- Use of magic URLs and hidden forms
- Use of weak password-based systems
- Poor usability

11 - Technological Obsolescence

- Antiquated/outdated infrastructure can lead to unreliable, untrustworthy systems.
- Proper managerial planning should prevent technology obsolescence.
- IT plays a large role.

12 - Theft

- Illegal taking of another's physical, electronic, or intellectual property.
- Physical theft is controlled relatively easily.
- Electronic theft is a more complex problem; the evidence of crime is not readily apparent.

Summary

- Information security performs four important functions:
  - Protecting organization's ability to function
  - Enabling safe operation of applications implemented on organization's IT systems
  - Protecting data an organization collects and uses
  - Safeguarding the technology assets in use at the organization

- Threats or dangers facing an organization's people, information, and systems fall into the following categories:
  - Compromises to intellectual property, Deviations in quality of service, Espionage or trespass, Forces of nature, Human error or failure, Information extortion, Sabotage or vandalism, Software attacks, Technical hardware failures or errors, Technical software failures or errors, Technological obsolescence, and Theft