Chapter 2
Managing Security

Reading:

[1] Dieter Gollmann **"Computer Security"**. Wiley (published 2011), pages 13-29, chap2.

[2] Chuck Easttom, **"Computer Security Fundamentals"**, Third Edition, 2016.

Objectives

- Introduce security policies.
- Give a brief introduction to security management.
- Cover the basics of risk and threat analysis.

Outline

2.1 Attacks and Attackers

2.2 Security Management

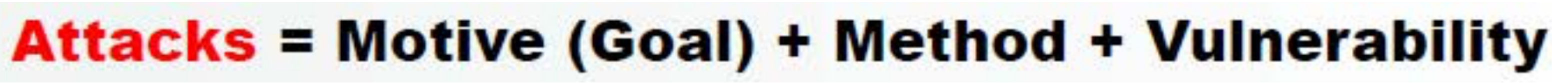
2.3 Risk and Threat Analysis

2.1 Attacks and Attackers

- **Credit card payments**: the traffic between customer and merchant should be protected.
- **The basic Internet protocols:** no confidentiality, easy to capture card numbers and use them later for fraudulent purchases.
- SSL was developed by Netscape in the mid 1990s

2.1 Attacks and Attackers

- ***Attacks**:* is any attempt to expose, alter, disable, destroy, steal or gain unauthorized access to or make unauthorized use of an asset.



Attacks = Motive (Goal) + Method + Vulnerability

- ***Attackers (Hackers):*** Any person who are able to destroy, change, or delete data on systems and performs illegal activities on the Internet for his benefits like financial account hijacking for stealing money, etc.

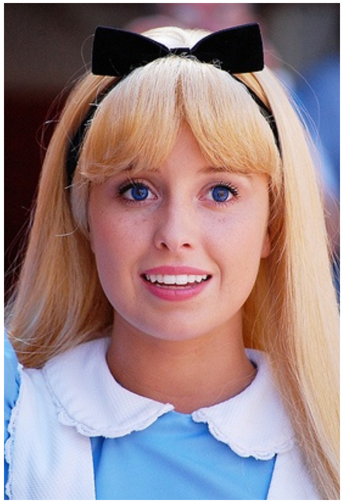
Types of Attacks on a System

- Operating system attacks
- Application level attacks
- Shrink wrap code attacks
- Misconfiguration attacks

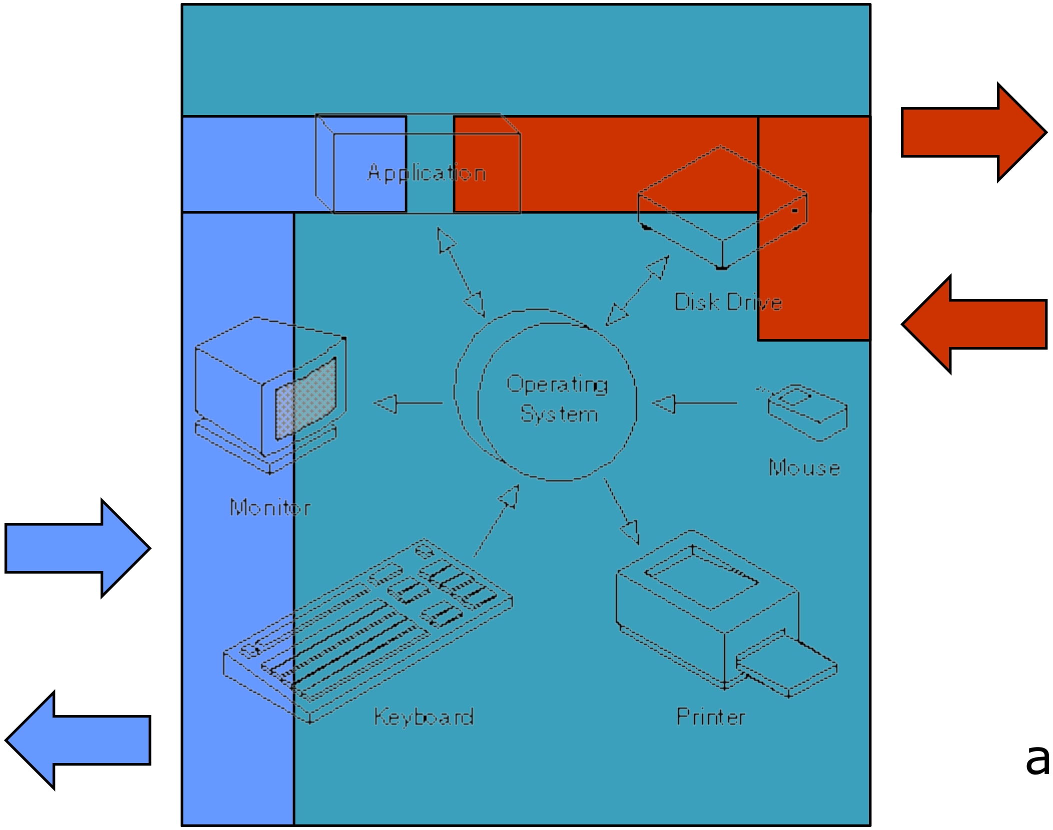
Operating System Attacks

- Attackers search for OS vulnerabilities and exploit them to gain access to a network system.
- Some of vulnerabilities:
  - Buffer overflow vulnerabilities
  - Bugs in operating system
  - Unpatched operating system

Operating System Attacks



Alice



OS Attacker

Controls malicious files and applications

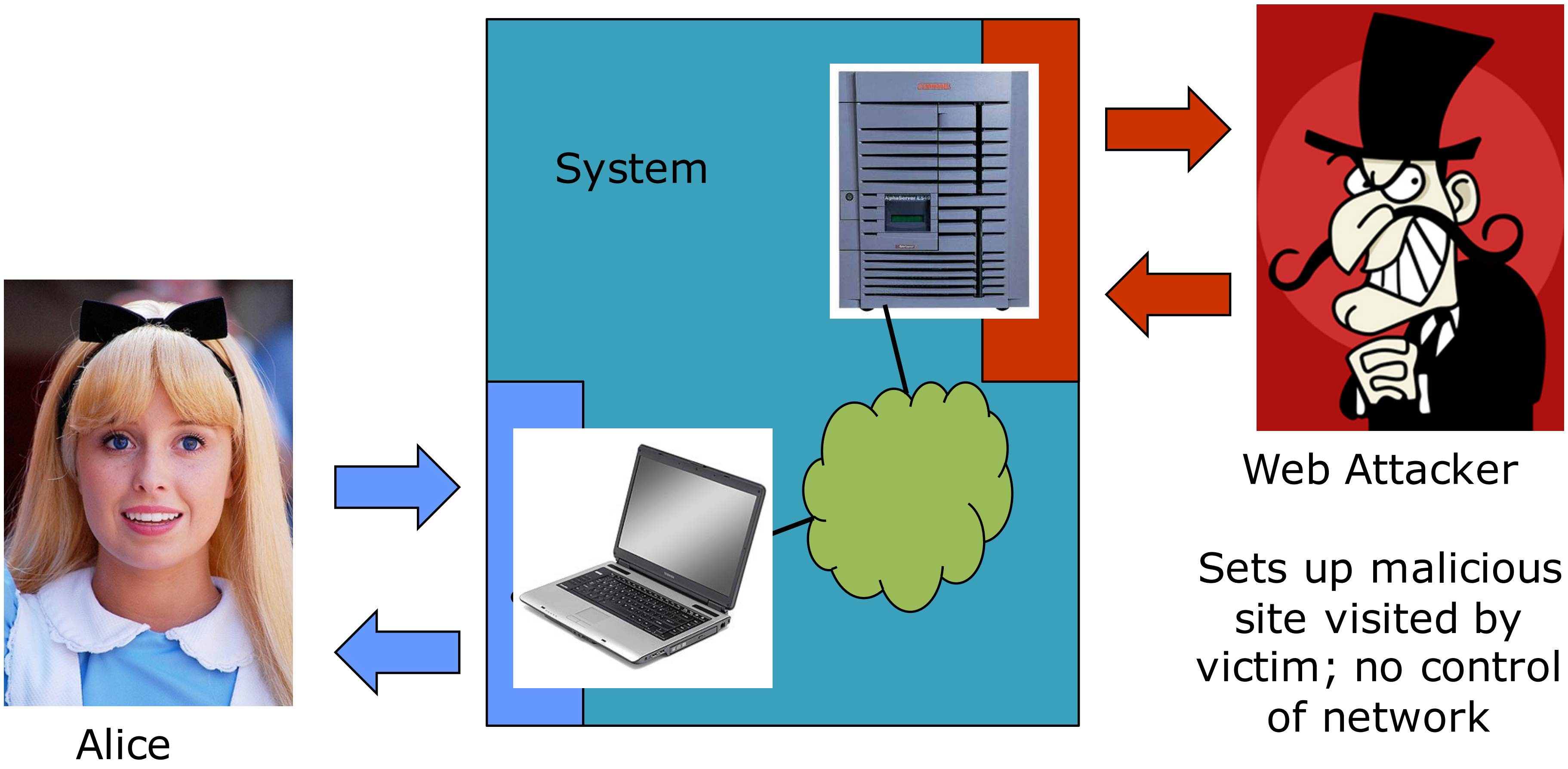
Application-Level Attacks

- Software applications come with tons of functionalities and features
- There is a dearth of time to perform complete testing before releasing products
- Poor or nonexistent error checking in applications
  - Buffer overflow attacks
  - Cross-site scripting

Application-Level Attacks

  - Denial of service and SYN attacks
  - SQL injection attacks
  - Malicious bots
- **Other application-level attacks include:**
  - Phishing
  - Session hijacking
  - Man-in-the-middle attacks
  - Parameter/Form tampering

Application-Level Attacks

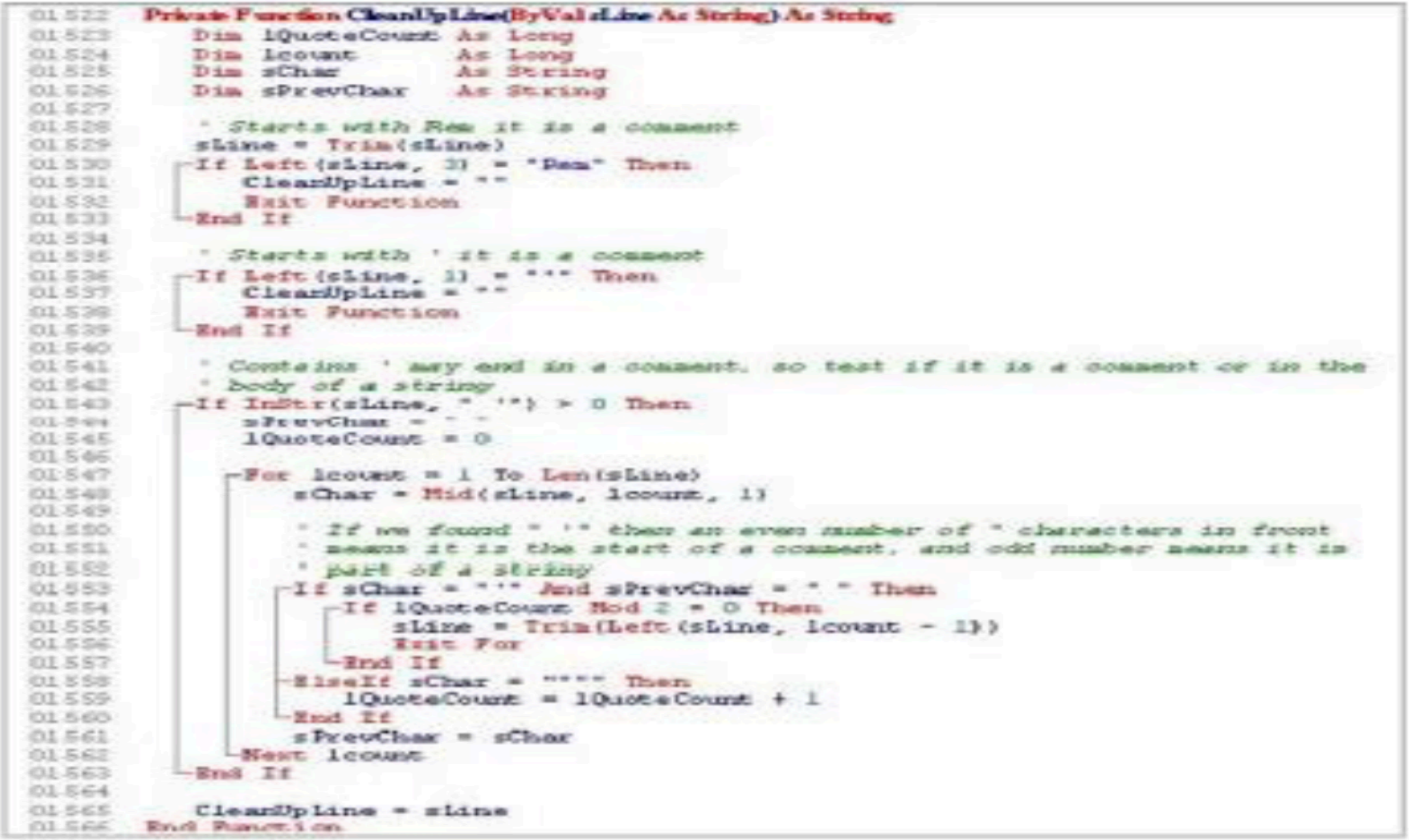


Sets up malicious site visited by victim; no control of network

Shrink Wrap Code Attacks

- When you install an OS/Application, it comes with tons of sample scripts to make the life of an administrator easy
- The problem is “not fine tuning” of customizing these scripts
- This will lead to default code or shrink wrap code attacks

Shrink Wrap Code Attacks

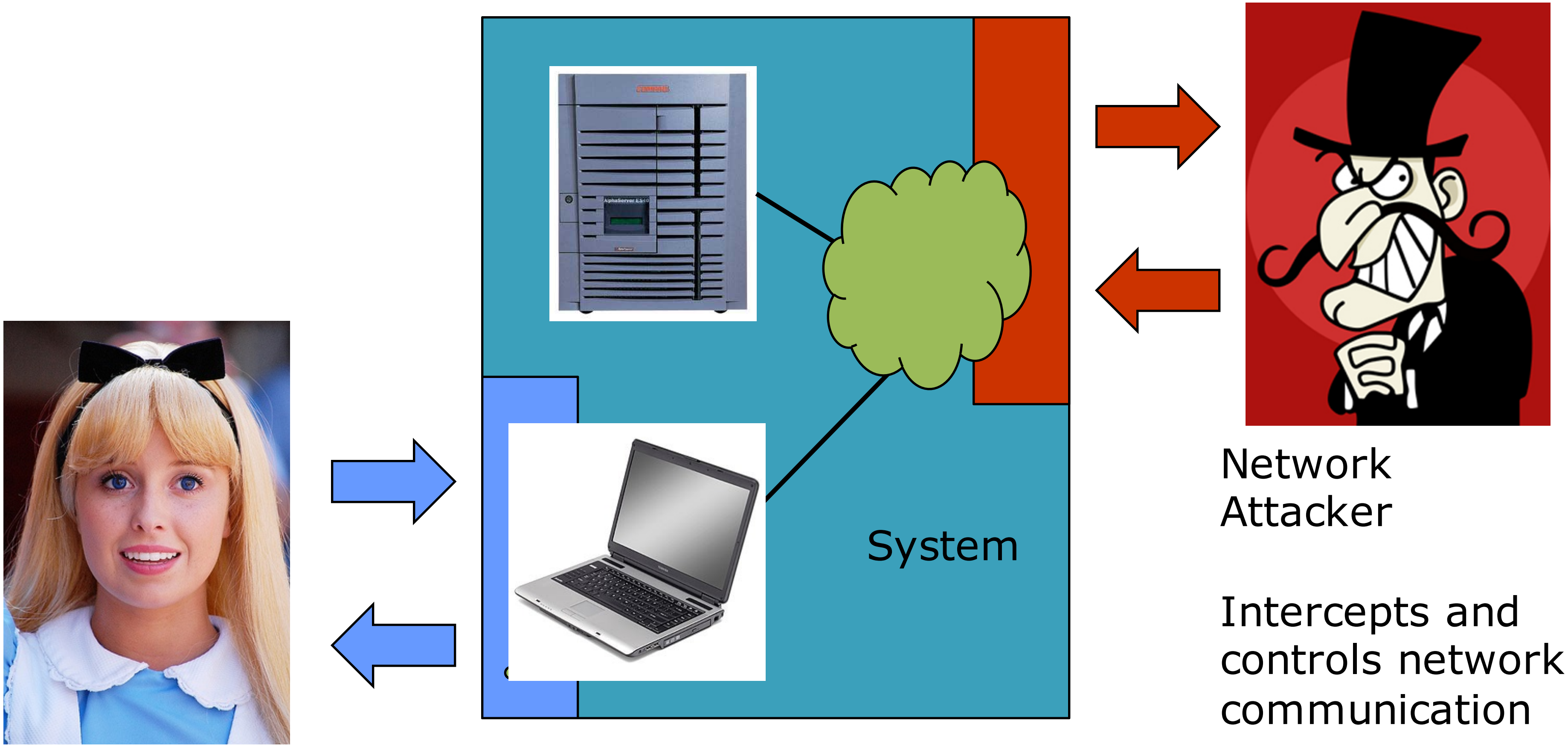


```
Private Function CleanUpLine(ByVal sLine As String) As String
    Dim lQuoteCount As Long
    Dim lcount      As Long
    Dim sChar       As String
    Dim sPrevChar   As String

    ' Starts with Rem it is a comment
    sLine = Trim(sLine)
    If Left(sLine, 3) = "Rem" Then
        CleanUpLine = ""
        Exit Function
    End If

    ' Starts with ' it is a comment
    If Left(sLine, 1) = "'" Then
        CleanUpLine = ""
        Exit Function
    End If

    ' Contains ' may end in a comment, so test if it is a comment or in the
    ' body of a string
    If InStr(sLine, " '") > 0 Then
        sPrevChar = " "
        lQuoteCount = 0

        For lcount = 1 To Len(sLine)
            sChar = Mid(sLine, lcount, 1)

            ' If we found " '" then an even number of " characters in front
            ' means it is the start of a comment, and odd number means it is
            ' part of a string
            If sChar = "'" And sPrevChar = " " Then
                If lQuoteCount Mod 2 = 0 Then
                    sLine = Trim(Left(sLine, lcount - 1))
                    Exit For
                End If
            ElseIf sChar = """" Then
                lQuoteCount = lQuoteCount + 1
            End If
            sPrevChar = sChar
        Next lcount
    End If

    CleanUpLine = sLine
End Function
```

Misconfiguration Attacks

- If a system is misconfigured, such as change is made in the file permission, it can no longer be considered as secure
- The administrators are expected to change the configuration of the devices before they are deployed in the network. Failure to do this allows the default settings to be used to attack the system
- In order to optimize the configuration of the machine, remove any redundant services or software

Misconfiguration Attacks



System

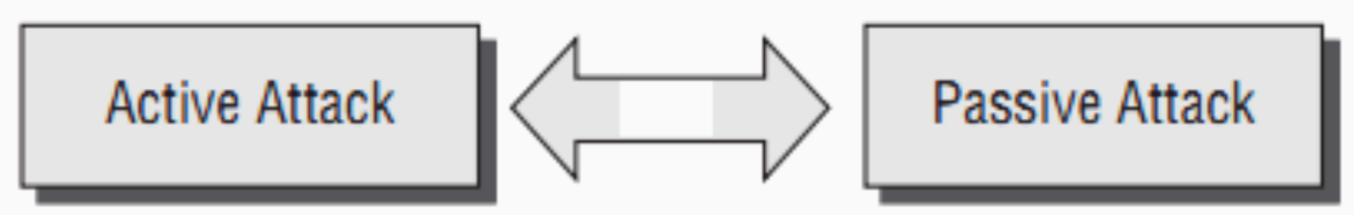
Network Attacker

Intercepts and controls network communication

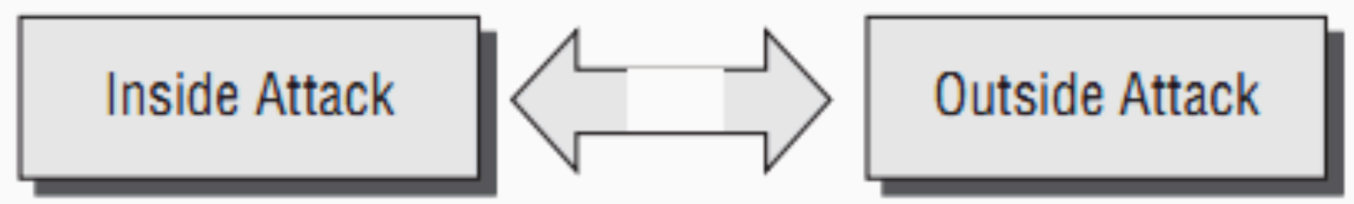
Alice

Types of Attacks

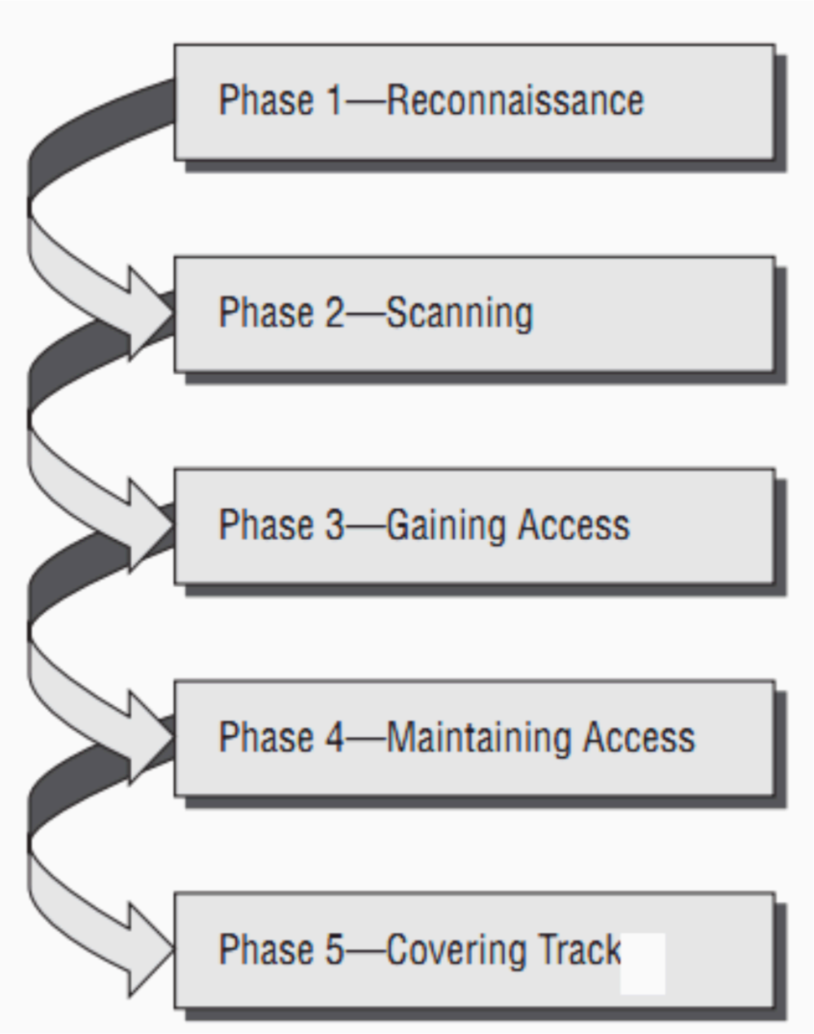
- Passive: Sniffer, ...
- Active: DDoS, Scan port, ...



- Inside
- Outside



Attacking Phases



Phase 1
Passive and Active Reconnaissance

- **Reconnaissance:** attacker seeks to gather information. Have two types of Reconnaissance:
  - *Passive Reconnaissance*: involves acquiring information without directly interacting with the target.

  For example: Sniffing to gather IPs, domains, servers, services,…

  - *Active Reconnaissance*: involves interacting with the target directly by any means

  For example: Supperscan, Nessus, …

Phase 2
Scanning

Scanning:

- It is a Pre-Attack phase
- Use Port Scanners, Nmap, Acunetix Web Vulnerability Scanner, Angry Ip Scan, etc.
- Extract Information: such as Computer name, IP address, user account, etc. to launch attack

Phase 3
Gaining Access

- **Gaining Access** refers to the point where the attacker obtains access to the operating system or applications on the computer or network.
- The attacker can gain access at the operating system level, application level, or network level.
- The attacker can escalate privileges to obtain complete control of the system. Example include password cracking, buffer overflows, denial of service, session hijacking, etc.

Phase 4
Maintaining Access

- **Maintaining Access** refers to the phase when the attacker tries to retain his/her ownership of the system.
- Attacker use compromised system to launch further attacks.
- Attacker may prevent the system from being owned by other attackers by securing their exclusive access with Backdoor, RootKits, or Trojans.
- Attackers can upload, download, or manipulate data, application, and configurations on the owned system.

Phase 5
Covering Track

- Covering track refers to the activities carried out by an attacker to hide malicious acts.
- The attacker's intentions include: Continuing access to the victim's system, remaining unnoticed and uncaught, deleting evidence that might lead to his prosecution.
- The attacker overwrite the server, system, and application logs to avoid suspicion.

➔ **Attackers always cover tracks to hide their identify**

Hacker Classes

1. **Black Hats:** Individuals with extraordinalry computing skills, resorting to malicious or destructive activities and are also known as crackers.
2. **White Hats:** Individuals professing hacker skills and using them for defensive purposes and are also known as security analysts.
3. **Gray Hats**: Individuals who work both offensively and defensively at various times.

Hacker Classes

4. **Suicide Hackers:** Individuals who aim to bring down critical infrastructure for a “cause” and are not worried about facing jail term or any other kind of punishment.
5. **Script Kiddies:** An unskilled hacker who compromised system by running scripts, tools, and software developed by real hackers.
6. **Cyber Terrorists**: Individuals with wide range of skills, motivated by religious or political beliefs to create fear by large-scale disruption of computer network

Hacker Classes

7. **State Sponsored Hackers:** Individuals employed by the government to penetrate and gain top secret information and to damage information systems of other governments.

What is Ethical Hacking?

- Ethical hacking involves the use of hacking tools, tricks, and techniques to **identify vulnerabilities** so as to ensure system security.
- It focuses on simulating techniques used by attackers to **verify the existence of exploitable vulnerabilities** in the system security.
- Ethical hackers performs security assessment of their organization **with the permission of concerned authorities.**

Why Ethical Hacking is Necessary

“To beat a hacker, you need to think like one”

- Ethical hacking is necessary as it **allows to counter attacks from malicious hackers** by anticipating methods used by them to break into a system.

❑ **Reasons why organizations recruit ethical hackers:**

- To **prevent hackers** from gaining access to organization's information systems.
- To **uncover vulnerabilities** in system and explore their potential risks.
- To analyze and **strengthen an organization's security** including policies, network protection infrastructure, and end-user practices

Why Ethical Hacking is Necessary

❑ **Ethical Hackers try to answer the following questions**

- What can the intruder see on the **target system**? (Reconnaissance and Scanning phases)
- What can an **intruder do** with that information? (Gaining Access and Maintaining Access phases)
- Does anyone at the target **notice the intruders' attempt** or successes? (Reconnaissance and Covering tracks phases)
- If all the **components of information system** are protected, updated, and patched.

Why Ethical Hacking is Necessary

- How much effort, time, and money is required to obtain **complete protection**?
- Are the **information security measures** in the compliance to industry and legal standards?

Skills of an Ethical Hacker

1. Technical Skills

- Has in-depth **knowledge of major operating environments**, such as Windows, Unix, Linux, and Macintosh.
- Has in-depth **knowledge of networking concepts**, technologies and related hardware and software.
- Should be a **computer expert** adept at technical domains.
- Has **knowledge of security areas** and related issues.
- Has **"high technical" knowledge** to launch the sophisticated attacks.

Skills of an Ethical Hacker

2. Non-Technical skills:

Some of the non-technical characteristics of an ethical hacker include:

- *Ability to learn and adapt new technologies quickly.*
- *Strong work ethics, and good problem solving and communication skills.*
- *Committed to organization's security policies.*
- *Awareness of local standards and laws*

2.2 Information Security Policies

- Security policies are the foundation of the **security infrastructure.**
- Information security policy defines the basic security requirements and rules to be implemented in order to **protect** and **secure organization's information systems.**

Goals of security policies

- Maintain an outline for the management and administration of network security.
- Protect an organization's computing resources.
- Prevent waste of company's computing resources.
- Prevent unauthorized modifications of the data.

Goals of security policies

- Reduce risk caused by illegal use of the system resource.
- Differentiate the user's access rights.
- Protect confidential, information from theft, misuse, unauthorized disclosure

Types of Security Policies

Promiscuous Policy

No restrictions on usage of system resources

Permissive Policy

- Policy begins wide open and only known dangerous services/ attacks or behaviors are blocked
- It should be updated regularly to be effective

Types of Security Policies

Prudent Policy (Thận trọng)

- It provides **maximum security**.
- It **blocks all services** and only safe/necessary services are enabled individually; everything is logged

Paranoid Policy (Hoang tưởng)

- It **forbids (cấm) everything**, no Internet connection, or limited Internet usage.

Examples of Security Policies

❑ **Access Control policy**

- It defines the resources being protected and the rules that control access to them.

❑ **User-Account Policy**

- It defines the account creation process, and authority, rights and responsibilities of user accounts.

❑ **Remote-Access Policy**

- It defines who can have remote access, and defines access medium and remote access security controls.

Examples of Security Policies

❑ Information-Protection Policy

- It defines the sensitivity levels of information, who may have access, how is it stored and transmitted, and how should it be deleted from storage media.

❑ Firewall-Management Policy

- It defines access, management, and monitoring of firewalls in the organization

❑ Special-Access Policy

- This policy defines the terms and conditions of granting special access to system resources

Examples of Security Policies

❑ **Network-Connection Policy**

- It defines who can install new resources on the network, approve the installation of new devices, document network changes, etc.

❑ **Email Security Policy**

- It is created to govern the proper usage of corporate email

❑ **Passwords Policy**

- It provides guidelines for using password protection on organization's resources

❑ **Acceptable-Use Policy**

- It defines the acceptable use of system resources

Measuring Security

The Goal of Measuring security:

- To convince (thuyết phục) managers (or customers) of the benefits of a new security mechanism.
- To look at potential security of system
- To ensure that the security features provided are properly used.
- To measure the cost of attacks:
  - the time an attacker has to invest in the attack, e.g. analyzing software products
  - the expenses (chi phí) the attacker has to incur, e.g. computing cycles or special equipment,
  - the knowledge necessary to conduct the attack.

Security Management Standards

What security management standards have to be taken in an organization.

➔These standards is **ISO 27002**

The major topics in ISO 27002 are as follows:

- *Security policy*
- *Organization of information security*
- *Asset management*

Security Management Standards

- Human resources security.
- Physical and environmental security
- Communications and operations management.
- Access control
- Information security incident management

2.3 Risk and Threat Analysis

- **Risk:** is the possibility that some incidents or attacks can cause damage to your enterprise.

- **It can be conducted in the following phases:**
  – The design phase of a system,
  – during the implementation phase,
  – and during operations

Assets

- ❑ **Hardware:** laptops, servers, routers, mobile phones, netbooks, smart cards, etc.;
- ❑ **Software:** applications, operating systems, database management systems, source code, object code, etc.;
- ❑ **Data and information:** essential data for running and planning your business, design documents, digital content, data about your customers, etc.;
- ❑ **Reputation**.

Threats

- ❑ **Spoofing identities**: an agent pretends (giả vờ) to be somebody else; this can be done to avoid responsibility or to misuse authority given to someone else.
- ❑ **Tampering with data:** violates (vi phạm) the integrity of an asset; e.g. security settings are changed to give the attacker more privileges.
- ❑ **Repudiation**: an agent denies having performed an action to escape responsibility.

Threats

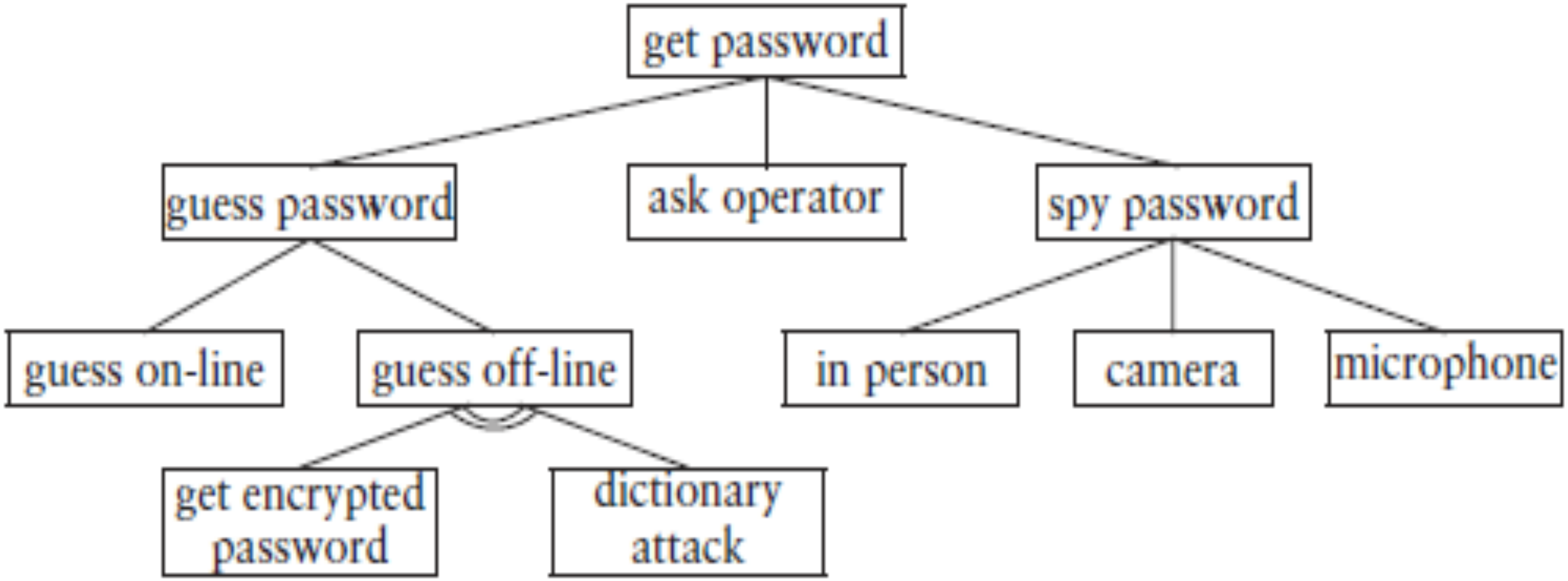
- ❑ **Information disclosure** – violates (vipham) the confidentiality of an asset; information disclosed to the wrong parties may lose its value (e.g. trade secrets); your organization may face penalties if it does not properly protect information (e.g. personal information about individuals).
- ❑ **Denial of service** – violates the availability of an asset; denial-of-service attacks can make websites temporarily unavailable; the media have reported that such attacks have been used for blackmail.
- ❑ **Elevation of privilege** – an agent gains more privileges.

Vulnerabilities

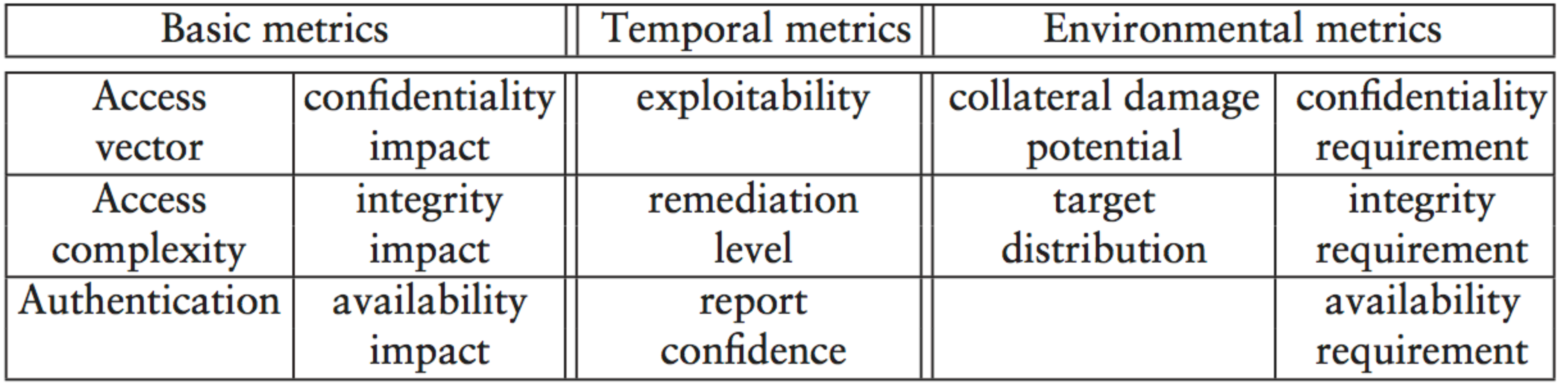
Typical vulnerabilities of a IT system are:

- Accounts with system privileges where the default password, such as ‘MANAGER’ has not been changed;
- programs with unnecessary privileges;
- programs with known flaws;
- weak access control settings on resources
- weak firewall configurations that allow access to vulnerable services.

Attacks


get password
guess password
ask operator
spy password
guess on-line
guess off-line
in person
camera
microphone
get encrypted password
dictionary attack

Common Vulnerability Scoring System

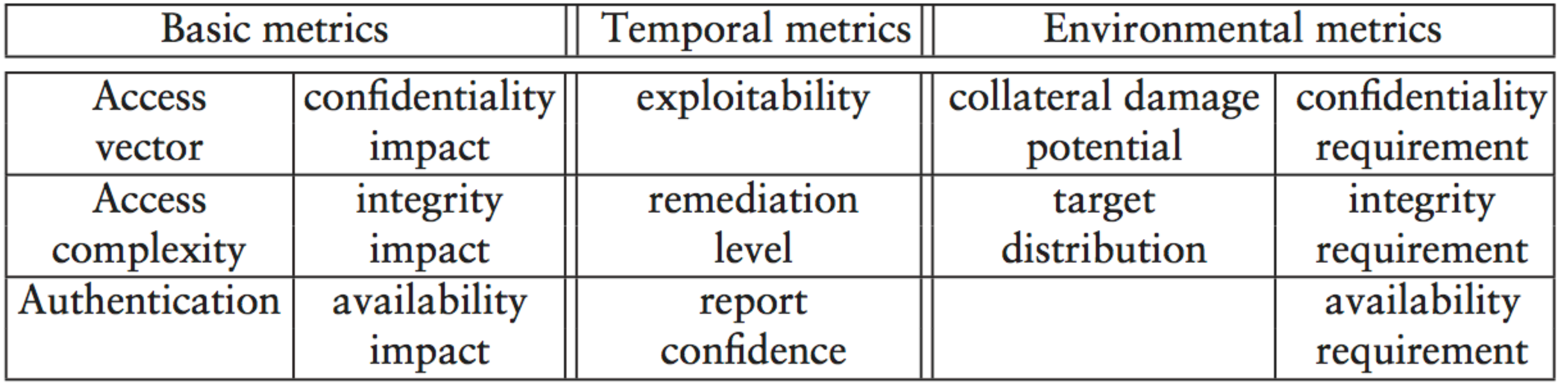


Basic metrics		Temporal metrics	Environmental metrics	
Access vector	confidentiality impact	exploitability	collateral damage potential	confidentiality requirement
Access complexity	integrity impact	remediation level	target distribution	integrity requirement
Authentication	availability impact	report confidence		availability requirement

❑ The **basic metric** group collects generic aspects of a vulnerability.

- Where the vulnerability can be exploited (local or remote attacker?)
- How complex an exploit would have to be?
- How many times an attacker would have to be authenticated during an attack?

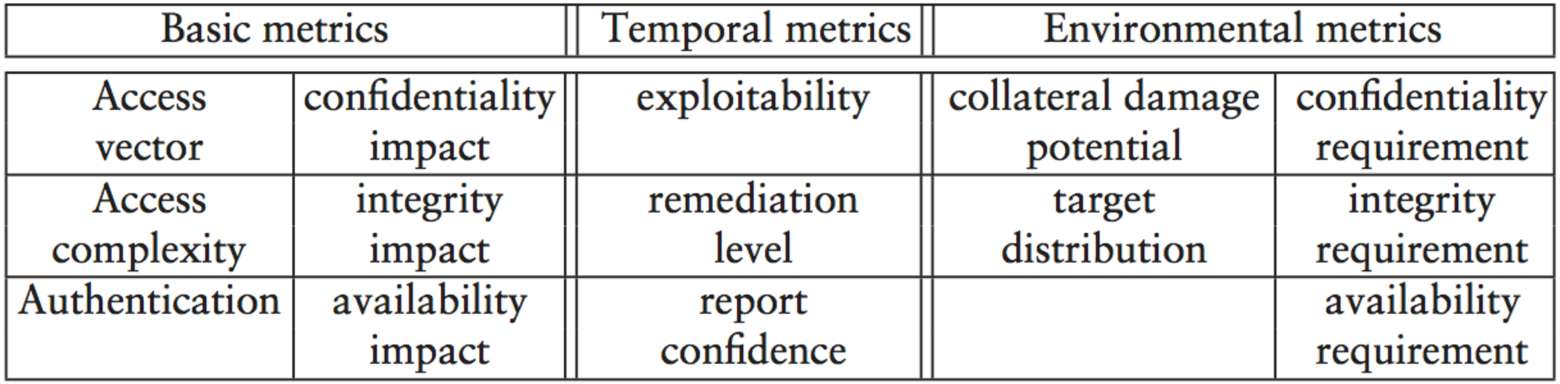
Common Vulnerability Scoring System



Basic metrics		Temporal metrics	Environmental metrics	
Access vector	confidentiality impact	exploitability	collateral damage potential	confidentiality requirement
Access complexity	integrity impact	remediation level	target distribution	integrity requirement
Authentication	availability impact	report confidence		availability requirement

- ❑ The **temporal metrics group** captures the current state of exploits and countermeasures.
  - *Exploitability* is related to reproducibility and captures the state of exploits available.
  - *The remediation level* notes to what extent fixes addressing the vulnerability are available.
  - *Report confidence rates* the quality of the source announcing the vulnerability.

Common Vulnerability Scoring System



Basic metrics		Temporal metrics	Environmental metrics	
Access vector	confidentiality impact	exploitability	collateral damage potential	confidentiality requirement
Access complexity	integrity impact	remediation level	target distribution	integrity requirement
Authentication	availability impact	report confidence		availability requirement

- The **environmental metrics group** rates the impact on the assets of a given organization.
    - *Collateral damage potential* covers damage outside the IT system, such as loss of life, loss of productivity, or loss of physical assets.
    - *Target distribution* measures the number of potential targets within the organization.
    - Environmental metrics rate IT assets according to the *standard security requirements* of confidentiality, integrity, and availability.

Quantitative and Qualitative Risk Analysis

$$Risk = Assets \times Threats \times Vulnerabilities.$$

- ❑ ***Quantitative*** risk analysis takes ratings from a mathematical domain such as a probability space.
- ❑ ***Qualitative*** risk analysis takes values from domains that do not have an underlying mathematical structure.
- **Assets** could be rated on a scale of

  A. Critical *B. Very important*

  C. Important *D. Not important.*
- **Vulnerabilities** could be rated on a scale of:

  A. Has to be fixed immediately *B. Has to be fixed soon*

  C. Should be fixed *D. Fix if convenient.*
- **Threats** could be rated on a scale of:

  A. very likely *B. Likely*

  C. Unlikely *D.Very unlikely.*

Countermeasures – Risk Mitigation
Các biện pháp đối phó - giảm nhẹ rủi ro

- ❑ The result of a risk analysis is a **prioritized list of threats**, and **recommended countermeasures** to mitigate risk.
- ❑ However:
  - *Risk analysis for a larger organization will take time.*
  - *IT system in the organization and the world outside will keep changing.*
  - *The costs of a full risk analysis may be difficult to justify to management.*
- ❑ Organizations may opt for ***baseline protection*** as an alternative
  - *Analyzes the security requirements for typical cases.*
  - *Recommends appropriate security measures*

References

Tham khảo chính

[1] Dieter Gollmann **“Computer Security”**. Wiley (published 2011), pages 13-29.

[2] Chuck Easttom, **“Computer Security Fundamentals”**, Third Edition, 2016.