School of Computing Science and Engineering

Program:B.Tech(BA+BD)

Course Code:CSBD4070

Course Name:Big Data Security

Course Outcomes :

CO NUMBER	TITLE
CO1	Understand and apply the models of Information Security
CO2	Apply and critique strategies for personal privacy protection and Understand and build security frameworks for big data
CO3	Build security in Hadoop environment
CO4	To use big-data analytics principles to build security applications
CO5	To detect security threats and vulnerabilities using security analytic
CO6	Ability to independently carry out research / Investigations, identify problems and develop solutions to solve practical problems in **Big Data Security**. (Create)

Course Prerequisites

- **Knowledge on Big Data**

Syllabus

Unit I: Introduction to Information System Security

Information System Security: Critical characteristics of Information - NSTISSC Security Model- Components of information System SDLC Information assurance - Security Threats and vulnerabilities - Overview of Security threats- Security Standards

UNIT II: Privacy and Security of Big Data

Privacy in Big Data: Privacy need for Data Sharing Anonymization design principles Data Anonymization in multidimensional data- Data Anonymization in time series data Threats to anonymized data- Privacy preserving data mining Dynamic data Protection - Security, Compliance, Auditing and Protecting: Steps to secure big data Classifying Data Protecting Big Data Compliance

Intellectual Property Rights and challenges

UNIT III: Security Design

Security Design: Kerberos Default Hadoop Model without security - Hadoop Kerberos Security- Open source authentication in Hadoop-Log monitoring Encryption for Hadoop.

UNIT IV: INTRODUCTION TO SECURITY ANALYTICS

Introduction to Security Analytics – Techniques in Analytics – Analysis in everyday life – Challenges in Intrusion and Incident Identification – Simulation and Security Process, Analytical Softwares and tools, Malware Analysis – static and dynamic analysis - Security Intelligence –Security Breaches.

UNIT V: APPLICATIONS OF SECURITY ANALYTICS

Access Analytics – Analysis of Log file -Security analysis with text mining –Machine Learning and data mining applications for security: Intrusion detection and network anomaly detection. Big data analytics for security: Analyzing DDOS – Distributed Denial of Service attack: counter based method, and access pattern based method – Machine learning for Ransom ware detection and prevention.

Unit VI: Advances and the Latest Trends

The advances and the latest trends in the course as well as the latest applications of the areas covered in the course.

The latest research conducted in the areas covered in the course.

Discussion of some latest papers published in IEEE transactions and ACM transactions, Web of Science and SCOPUS indexed journals as well as high impact factor conferences as well as symposiums.

Discussion on some of the latest products available in the market based on the areas covered in the course and patents filed in the areas covered in the course

Text Books

1. Michael E. Whitman, Herbert J Mattord, Principles of Information Security, Sixth edition, Vikas Publishing House, 2017
2. Nataraj Venkataramanan, Ashwin Shriram, Data Privacy: Principles and Practice, First edition, Chapman and Hall/CRC, 2016
3. Mark Talabis, Robert McPherson, I Miyamoto and Jason Martin, “Information Security Analytics: Finding Security Insights, Patterns, and Anomalies in Big Data”, Syngress Media,U.S., 2014

Reference Books

1. Ben Spivey, Joey Echeverria, Hadoop Security Protecting Your Big Data Problem, OReilly Media, 2015
2. Mark Van Rijmenam, Think Bigger: Developing a Successful Big Data Strategy for Your Business, First edition, Amazon, 2014
3. Behrouz A. Forouzan, “Cryptography and Network Security”, Tata McGraw Hill Education, 2nd Edition, 2010.
4. Douglas R. Stinson ,“Cryptography Theory and Practice ”, Chapman & Hall/CRC, 3rd Edition, 2006.
5. William Stallings, “Crpyptography and Network security: Principles and Practices”, Pearson/PHI, 5th Edition, 2010.

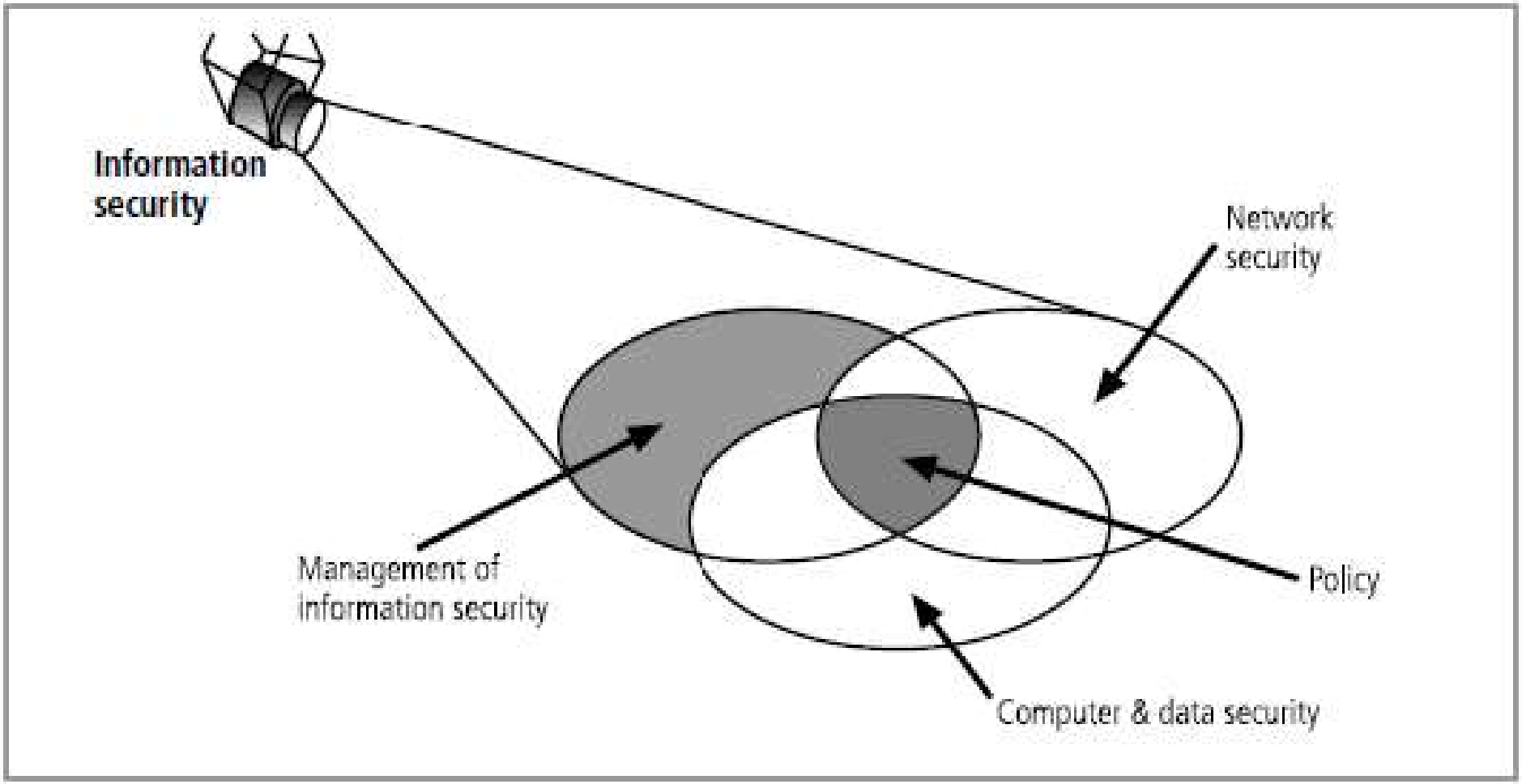
What is Security?

- **Security** is "the quality or state of being secure—to be free from danger."
- In other words, protection against adversaries—from those who would do harm, intentionally or otherwise—is the objective

Multiple layers of security

- **Physical security**, to protect physical items, objects, or areas from unauthorized access and misuse
- **Personnel security**, to protect the individual or group of individuals who are authorized to access the organization and its operations
- **Operations security**, to protect the details of a particular operation or series of activities
- **Communications security**, to protect communications media, technology, and content
- **Network security**, to protect networking components, connections, and contents
- **Information security**, to protect the confidentiality, integrity and availability of information assets, whether in storage, processing, or transmission. It is achieved via the application of policy, education, training and awareness, and technology

Components of Information Security



Key Information Security Concepts

- **Access:** A subject or object's ability to use, manipulate, modify, or affect another subject or object.
- **Asset:** The organizational resource that is being protected. An asset can be logical, such as a Web site, information, or data; or an asset can be physical, such as a person, computer system, or other tangible object

Key Information Security Concepts

- **Attack:** An intentional or unintentional act that can cause damage to or otherwise compromise information and/or the systems that support it. Attacks can be active or passive, intentional or unintentional, and direct or indirect.
- **Control, safeguard,** or **countermeasure:** Security mechanisms, policies, or procedures that can successfully counter attacks, reduce risk, resolve vulnerabilities, and otherwise improve the security within an organization.

Key Information Security Concepts

- **Exploit:** A technique used to compromise a system. This term can be a verb or a noun. Threat agents may attempt to exploit a system or other information asset by using it illegally for their personal gain.
- **Exposure:** A condition or state of being exposed. In information security, exposure exists when a vulnerability known to an attacker is present.

Key Information Security Concepts

- **Loss:** A single instance of an information asset suffering damage or unintended or unauthorized modification or disclosure. When an organization's information is stolen, it has suffered a loss..
- **Protection profile** or **security posture:** The entire set of controls and safeguards, including policy, education, training and awareness, and technology, that the organization implements (or fails to implement) to protect the asset.

Key Information Security Concepts

- **Risk:** The probability that something unwanted will happen. Organizations must minimize risk to match their **risk appetite** —the quantity and nature of risk the organization is willing to accept.
- **Subjects** and **objects:** A computer can be either the **subject** of an attack—an agentnentity used to conduct the attack—or the **object** of an attack—the target entity

Key Information Security Concepts

- **Threat:** A category of objects, persons, or other entities that presents a danger to an asset. Threats are always present and can be purposeful or undirected.
- **Threat agent:** The specific instance or a component of a threat
- **Vulnerability:** A weaknesses or fault in a system or protection mechanism that opens it to attack or damage.

Key Information Security Concepts

Threat: Theft
Threat agent: Ima Hacker

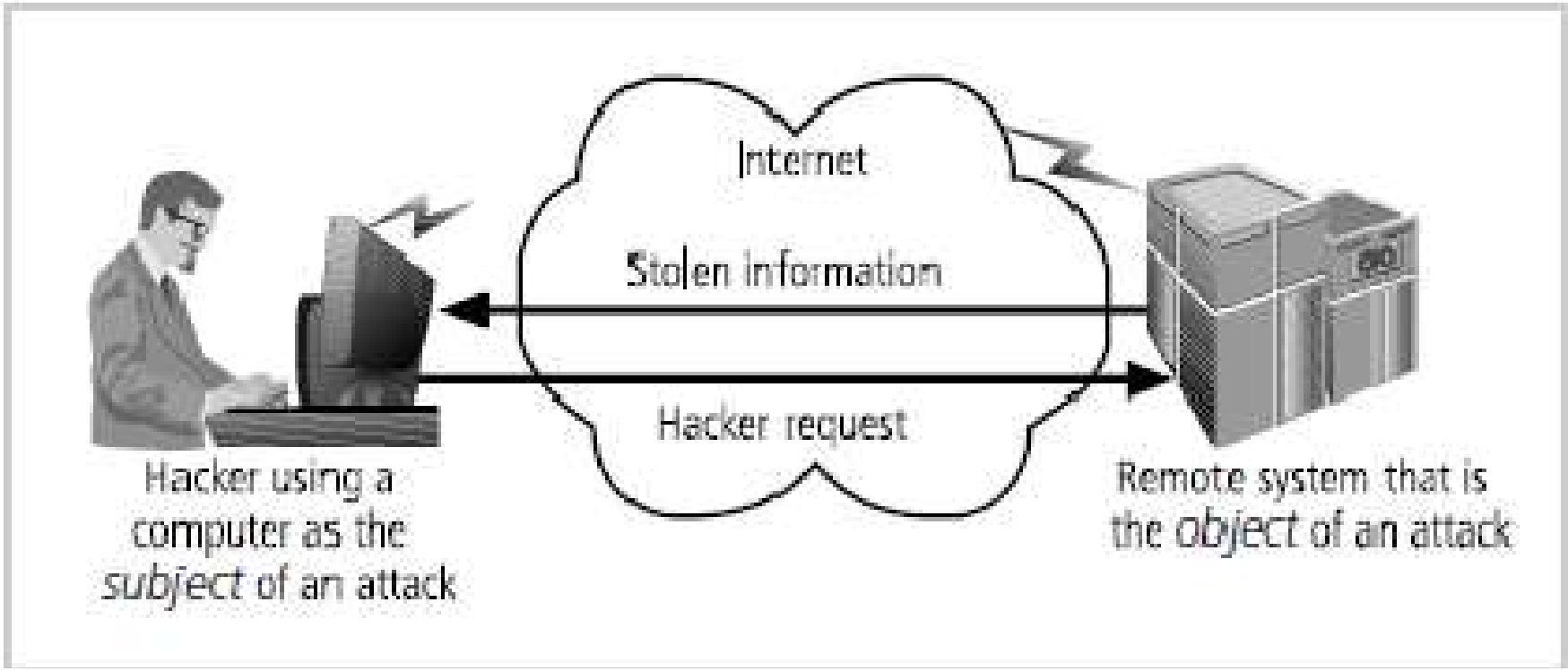
Vulnerability: Buffer overflow in online database Web interface

Exploit: Script from MadHackz Web site

Attack: Ima Hacker downloads an exploit from MadHackz web site and then accesses buybay's Web site. Ima then applies the script which runs and compromises buybay's security controls and steals customer data. These actions cause buybay to experience a loss.

Asset: buybay's customer database

Key Information Security Concepts



Critical Characteristics of Information

- The value of information comes from the characteristics it possesses.
- When a characteristic of information changes, the value of that information either increases, or, more commonly, decreases. Some characteristics affect information's value to users more than others do. This can depend on circumstances

Critical Characteristics of Information

- **Availability: Availability** enables authorized users—persons or computer systems—to access information without interference or obstruction and to receive it in the required format.
- **Accuracy** Information has **accuracy** when it is free from mistakes or errors and it has the value that the end user expects. If information has been intentionally or unintentionally modified, it is no longer accurate.

Critical Characteristics of Information

- **Authenticity Authenticity** of information is the quality or state of being genuine or original, rather than a reproduction or fabrication. Information is authentic when it is in the same state in which it was created, placed, stored, or transferred.
- **Integrity** Information has **integrity** when it is whole, complete, and uncorrupted. The integrity of information is threatened when the information is exposed to corruption, damage, destruction, or other disruption of its authentic state. Corruption can occur while information is being stored or transmitted.

Critical Characteristics of Information

- **Confidentiality** Information has **confidentiality** when it is protected from disclosure or exposure to unauthorized individuals or systems.
- Confidentiality ensures that *only* those with the rights and privileges to access information are able to do so. When unauthorized individuals or systems can view information, confidentiality is breached.
- To protect the confidentiality of information, you can use a number of measures, including the following:
  - Information classification
  - Secure document storage
  - Application of general security policies
  - Education of information custodians and end users

Critical Characteristics of Information

- **Utility** The **utility** of information is the quality or state of having value for some purpose or end. Information has value when it can serve a purpose. If information is available, but is not in a format meaningful to the end user, it is not useful.
- **Possession** The **possession** of information is the quality or state of ownership or control. Information is said to be in one's possession if one obtains it, independent of format or other characteristics. While a breach of confidentiality always results in a breach of possession,a breach of possession does not always result in a breach of confidentiality


Thank You