Information Security – Attacks and Prevention

A basic overview

Objective

Purpose of the program

To understand various information security vulnerabilities and the threats that can exploit them. Further, to understand solutions to mitigate these threats in the context of our organization's security policies and business objectives.

Agenda

- Information Security – The basics
- Security policies and International Standards
- Top IT Vulnerabilities
- Attacks & Attackers
- Defence in Depth
  - Security basics
  - System security
  - Network security
  - Application security
- Quiz
- Summary & Acknowledgments

Confidentiality

Making sure only those people who are authorized to view or access the information can do so.

My bank account details are “Confidential”

So, is the information stored in your business computer

Personal perspective

Business perspective

Integrity

Making sure only those people who are authorized to edit or change the information can do so.

Personal perspective

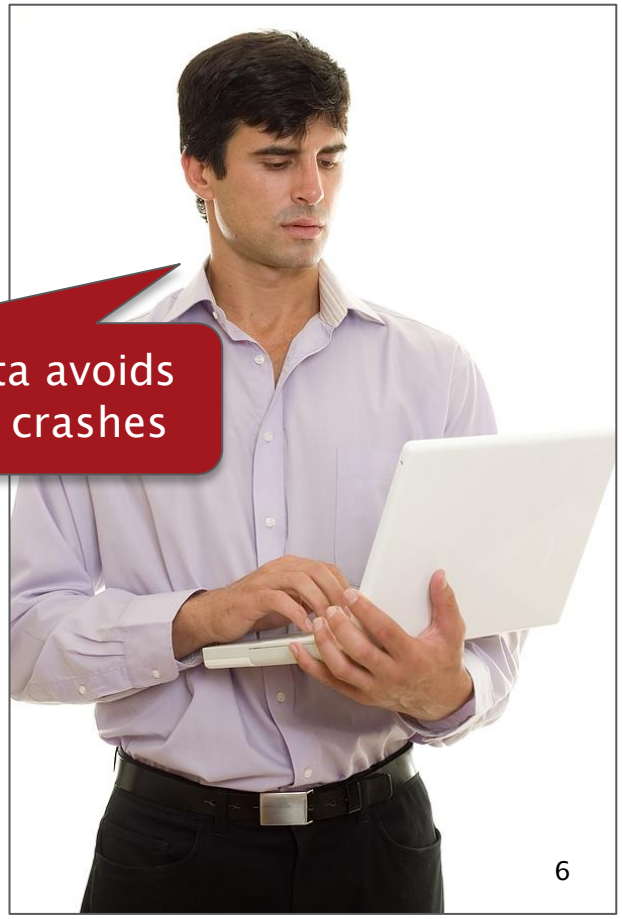
Business perspective

Availability

Making sure that information is available to authorized people when they need it.

I keep backups of my bank statements in case disputes arise

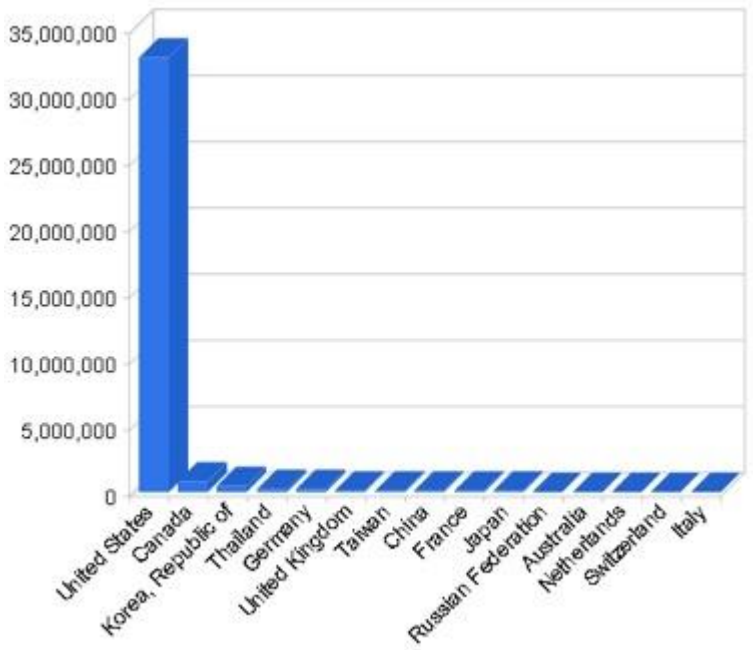
Backups of business data avoids panic in case of system crashes



Personal perspective

Business perspective

Hackers / Cybercriminals



Courtesy – SANS Top Cyber Security Risks

Motivations

- Political
- Financial
- Fun/ Personal pride

Primary targets (country-wise)

- USA
- Canada
- Republic of Korea
- Thailand

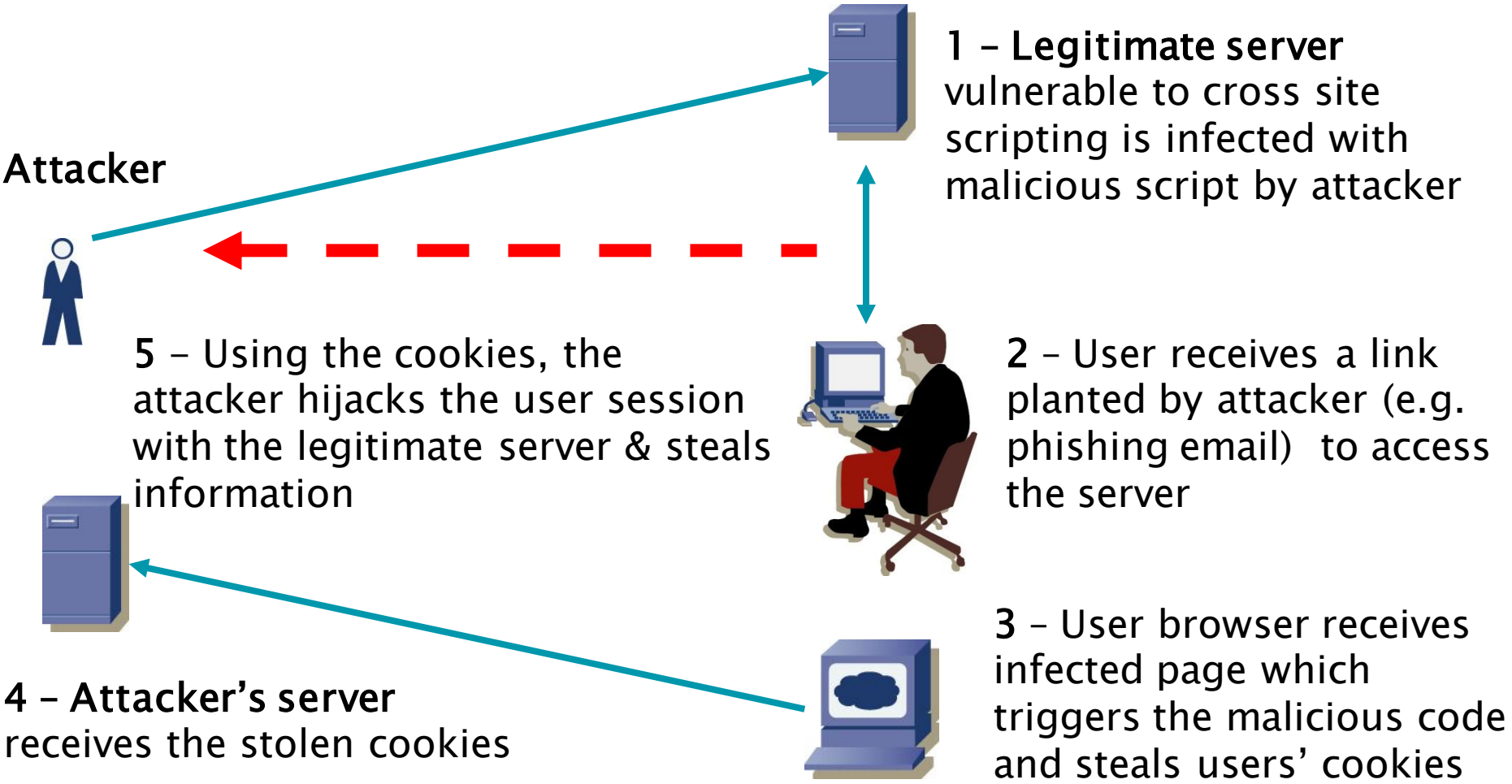
Common attacks

- SQL Injection
- Cross Site Scripting
- PHP File Include

Cross Site Scripting

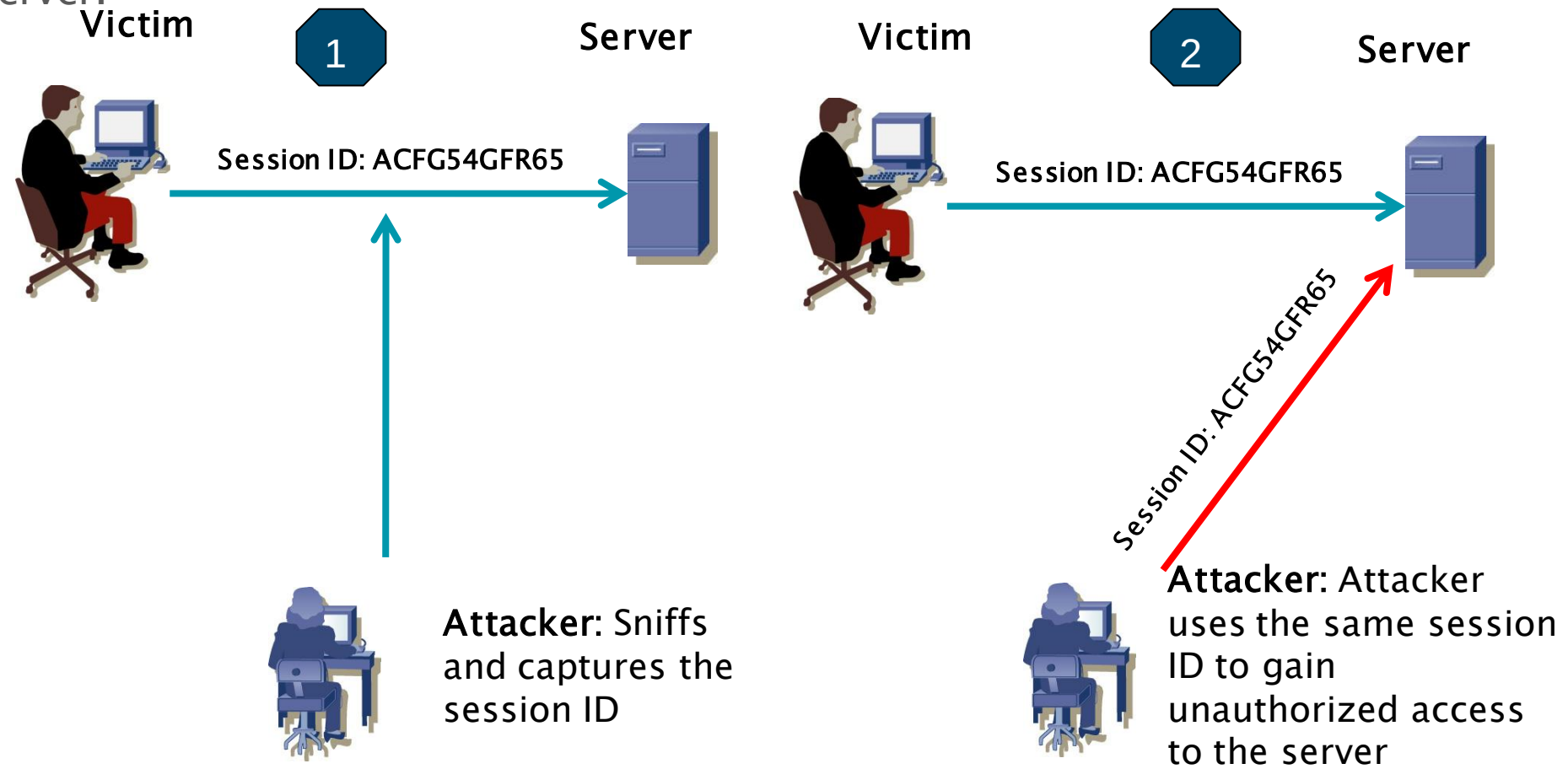
- Dynamic web-pages (using JavaScript etc.) add to the end-user experience
- Web sites with static pages have full control over how the browser interprets the pages
- Dynamic websites do not have full control over how the browsers interpret the pages
- An attacker can introduce malicious content via dynamic web-pages
- These malicious content when executed by the client's browser can help the attacker achieve one or more of the following goals
    - Make the user execute malicious scripts by connecting a malicious server under the attacker's control
    - Take over the user session before the user's session cookie expires
    - Make the user connect to a malicious server of the attacker's choice

Attack example: Cross site scripting



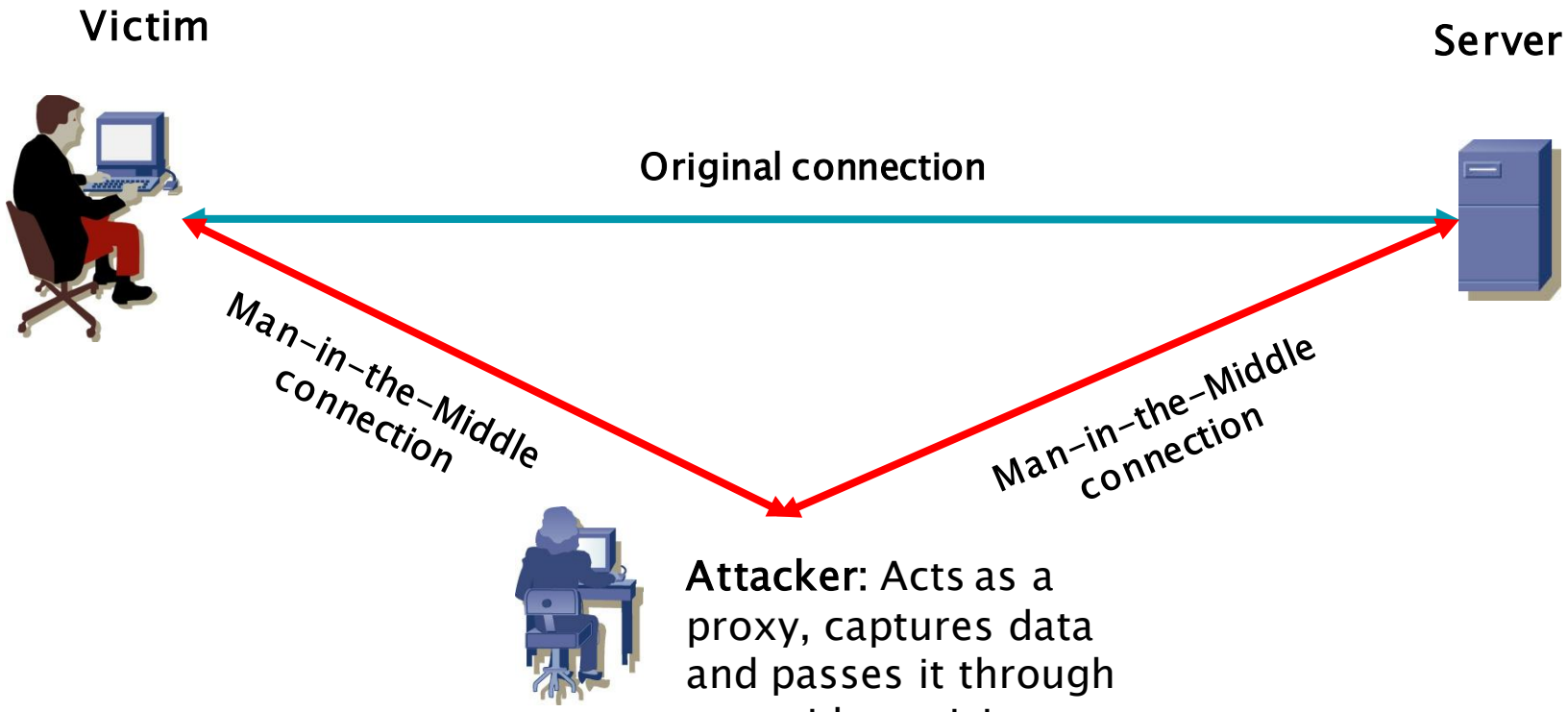
Session sniffing

The attacker uses a sniffer to capture a valid token session called “Session ID”, then he uses the valid token session to gain unauthorized access to the Web Server.



Man in the middle attack

Attacker intercepts a communication between two systems and splits it using different techniques, one between the client and the attacker and the other between the attacker and the server. The victim and the server think that they are communicating with each other, unaware that the attacker is in between acting as a proxy.



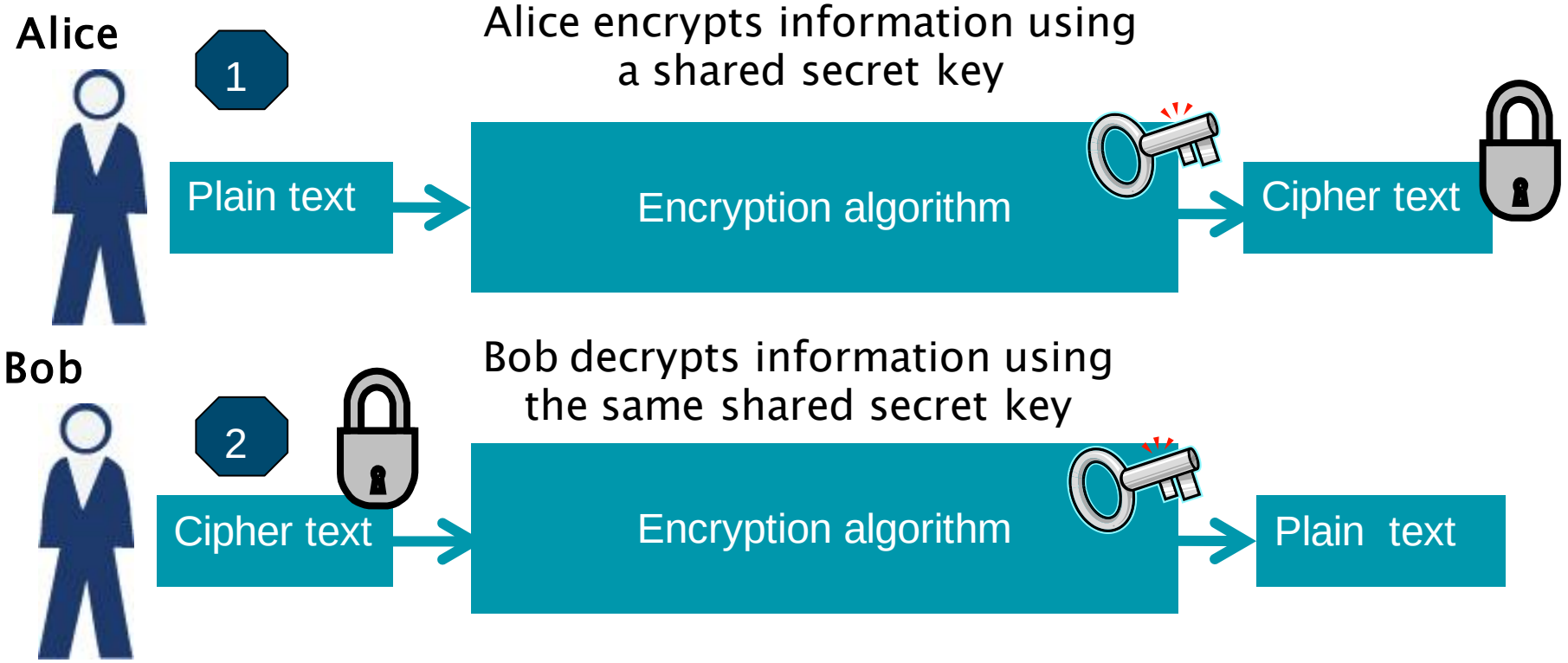
Implementing Defence in Depth

Defence in depth is achieved by deploying layers of security controls. Defence-in-depth can be split into 4 verticals.

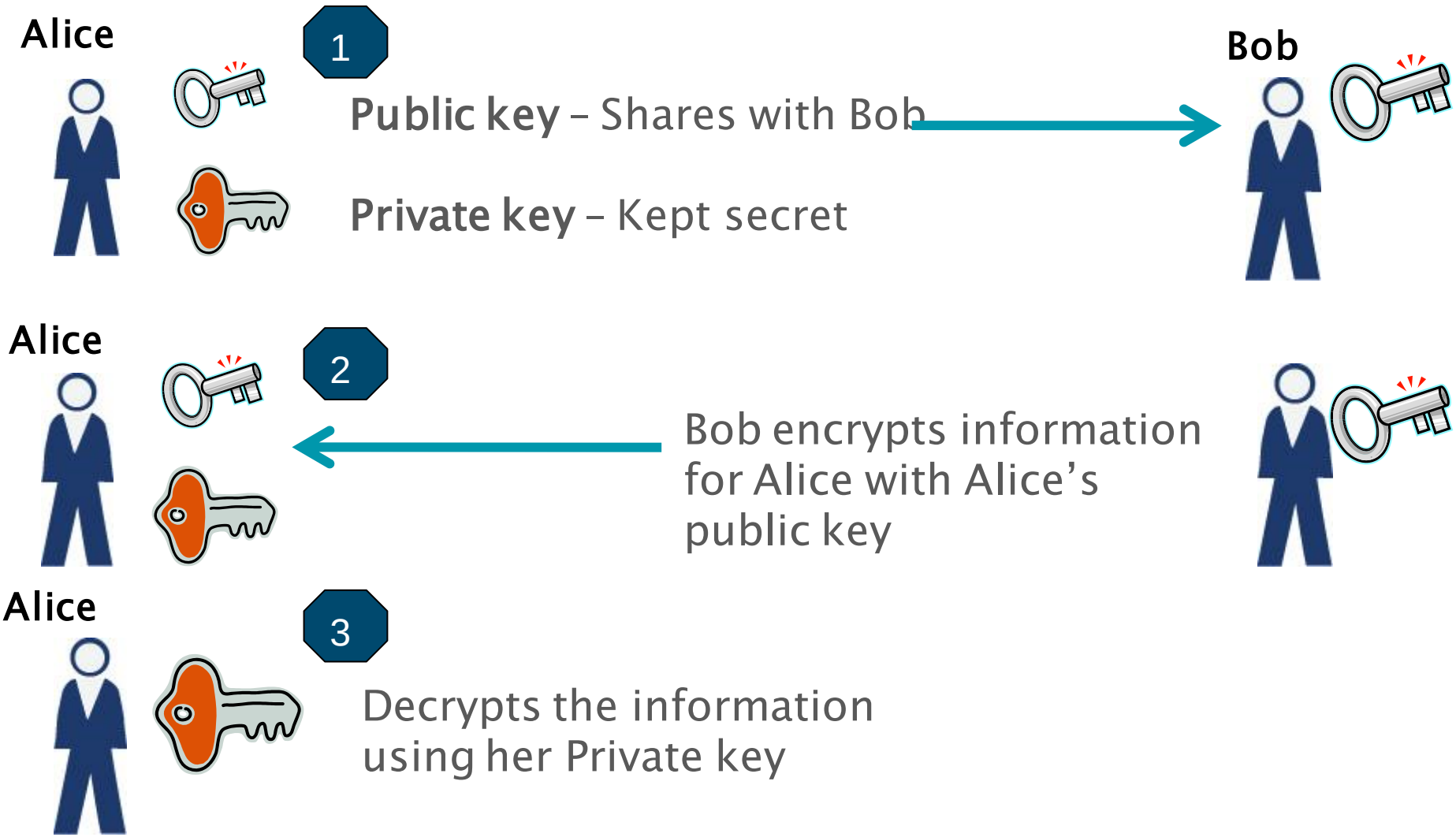
- Security basics
- System Security
- Network Security
- Application Security

Symmetric key encryption

Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key.



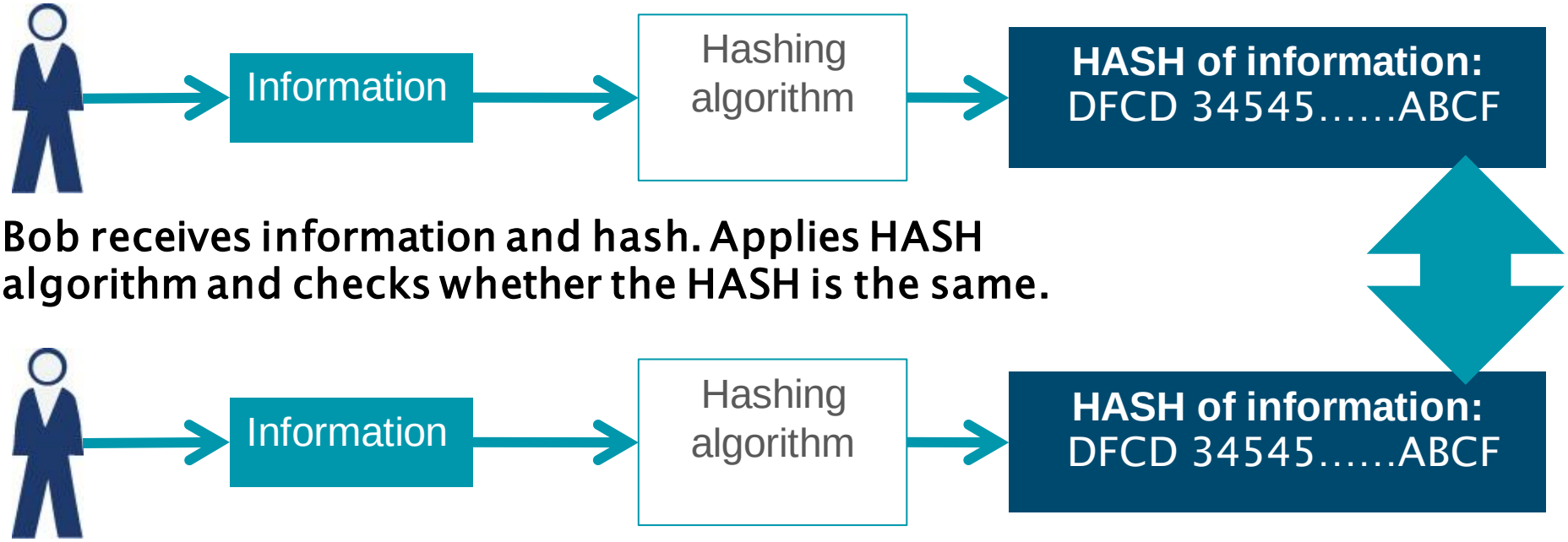
Public key encryption – In action



Hashing vs. Encryption

- Hashing is used only to verify data and not to hide it or protect it
- Hashing verifies whether the data sent is the data received
- The popular hashing algorithms are MD5 and SHA-1

Alice send information to Bob with the HASH



Bob receives information and hash. Applies HASH algorithm and checks whether the HASH is the same.

6. **Is the statement true or false – PHP File Include is a type of cross site scripting vulnerability**

a. True
b. False

7. **Which of the following statements are correct**

a. An application layer firewall performs packet inspection
b. A network layer firewall performs source verification
c. Firewalls can perform NAT (Network Address Translation)
d. All of the above

8. **A program should be able to access only the absolute minimal information and information resources that is required for executing the intended task and nothing more – This is an example of …**

a. Segregation of duties
b. Access control
c. Least privilege
d. User segregation

9. **Strict control of software changes and having multiple people approve and perform the tasks associated with the change is an example of…**

a. Principle of least privilege
b. Segregation of duties
c. Access control
d. None of the above

10. **The IPS detection method based on signatures and attack patterns is called**

a. Stateful inspection detection method
b. Signature based detection method
c. Statistical anomaly based detection method
d. Stateful protocol analysis detection method

11. **The advantage of Client-to-Site VPN is that…**

a. It is very fast
b. It works on all computing devices
c. User can connect while traveling (while out of office)
d. It works better on laptops