Cloud Security

Module 6 Part 1

What is cloud security and why it is essential?

Cloud Security

- Cloud Security is security principles/measures applied to protect data, applications and infrastructure associated within the Cloud Computing technology.
- These security measures are configured to protect cloud data, support regulatory compliance and protect customers' privacy as well as setting authentication rules for individual users and devices.
- From authenticating access to filtering traffic, cloud security can be configured to the exact needs of the business.

Authentication

Authentication is the process of *verifying who a user is.*

Operating System usually authenticates user using:

- **What you know?**
  - ✔ Username/Password
- **What you have?**
  - ✔ User Card/key
- **What you possess?**
  - ✔ User Attribute - fingerprint/eye retina

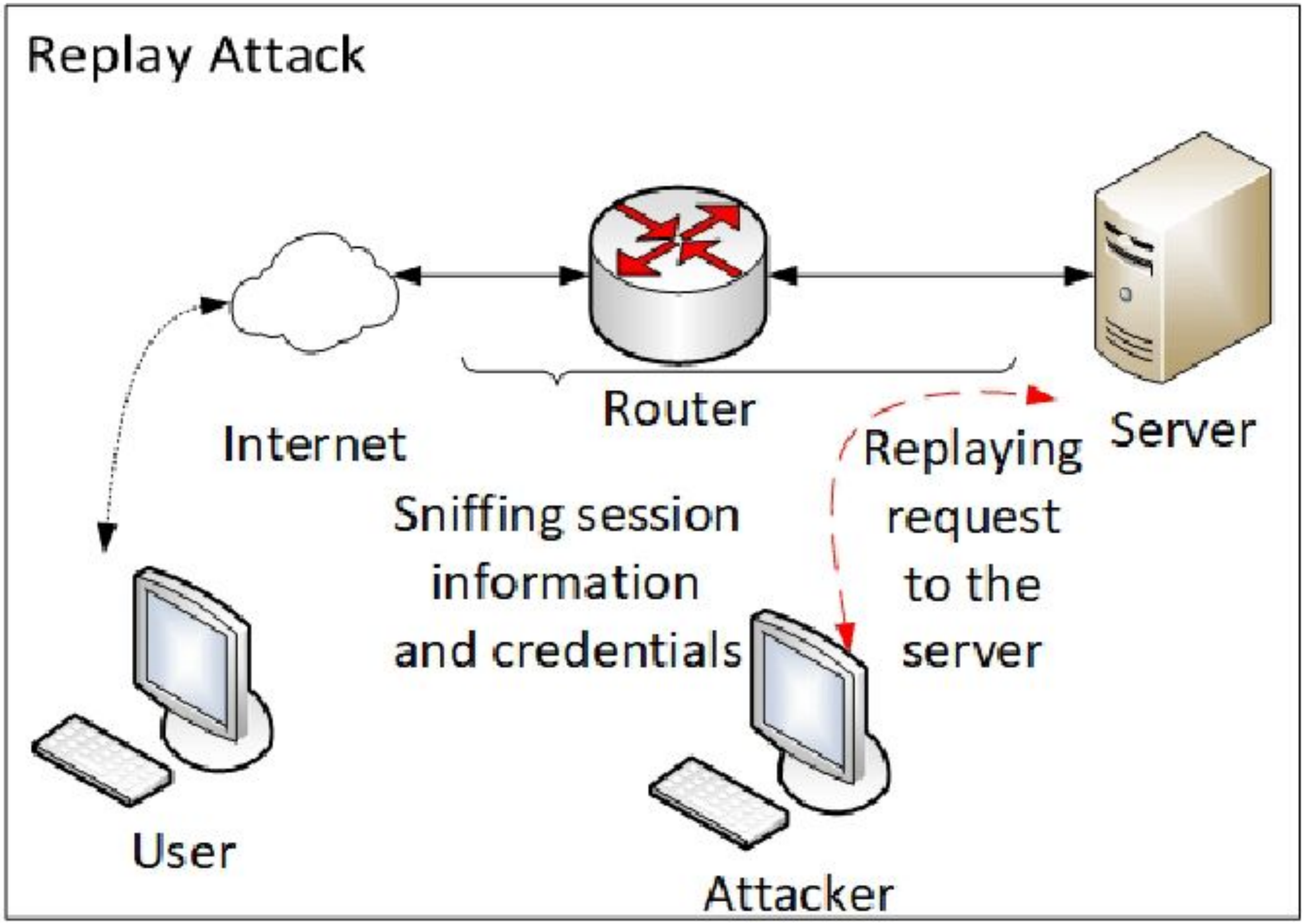
One Time Password (OTP)

a. Random Numbers
b. Secret key
c. Network Password

Advantages of OTP over static password?

Replay Attack

- OTP is not vulnerable to Replay Attack.


Replay Attack
Internet
Router
Server
Replaying request to the server
Sniffing session information and credentials
User
Attacker

Program Threat

Vulnerability vs Threat vs Risk ???

Threat is an action, potential action, or inaction, likely to cause damage, harm or loss.

Program Threat is the process invoked by the program to do malicious tasks.

- Trojan Horse
- Trap Door
- Logic Bomb
- Virus

Security Concerns

- Where the user data exists?
- Data Backup.
- Data center follows security measures or not.
- Data residency - Legal issues.

Security Framework

- An information security framework is a series of documented processes that are used to define the policies and procedures around the implementation and ongoing management of information security controls in an enterprise environment.

- These frameworks are basically a "blueprint" for building an information security program to manage risk and reduce vulnerabilities.

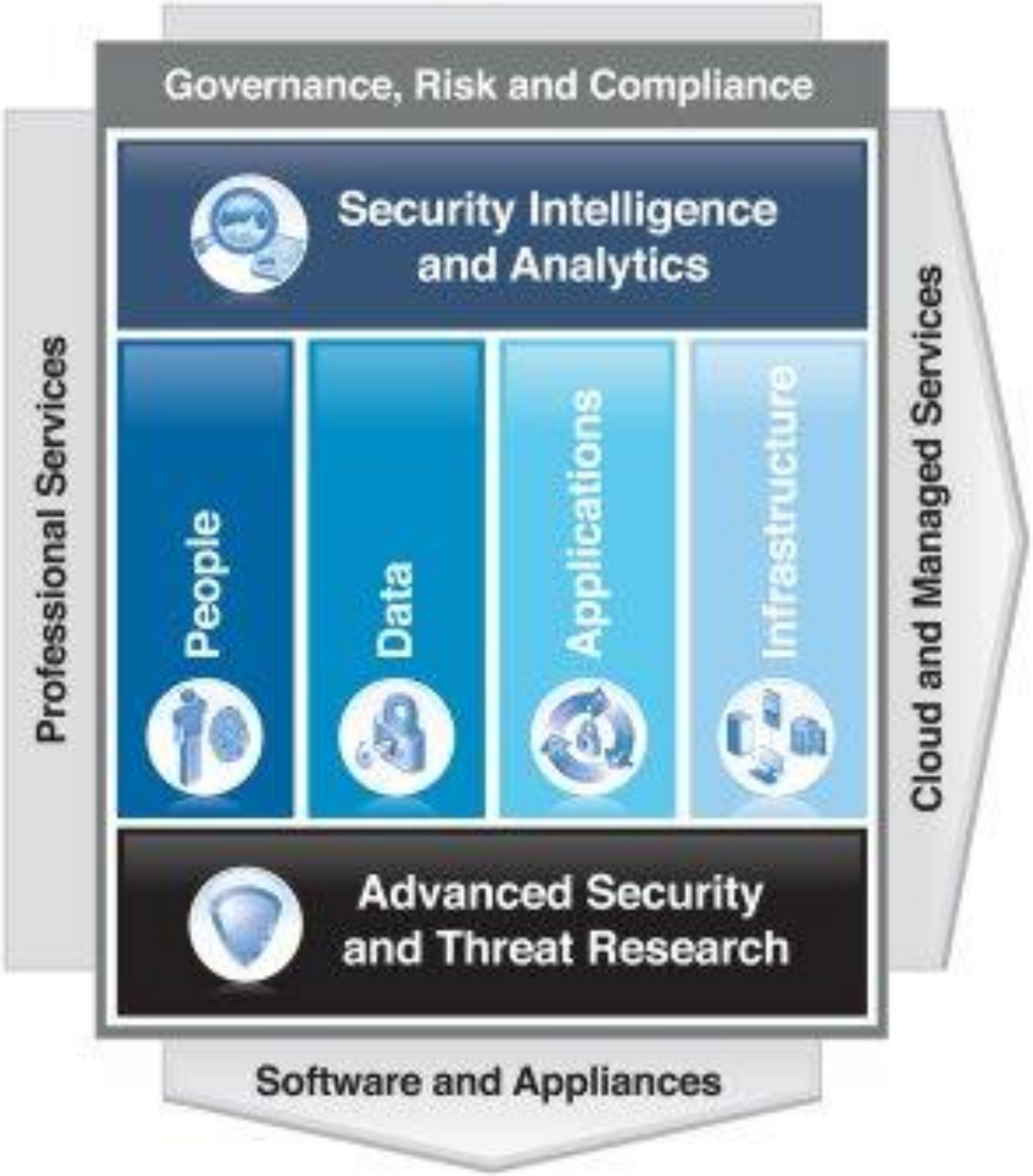
- Information security can utilize these frameworks to define and prioritize the tasks required to build security into an organization.

- Frameworks are often customized to solve specific information security problems, just like building blueprints are customized to meet their required specifications and use.

- There are frameworks that were developed for specific industries as well as different regulatory compliance goals.

- They also come in varying degrees of complexity and scale. However, you will find that there is a large amount of overlap in general security concepts as each one evolves.

IBM Security Framework



Governance, Risk and Compliance

Security Intelligence and Analytics

People

Data

Applications

Infrastructure

Advanced Security and Threat Research

Professional Services

Cloud and Managed Services

Software and Appliances

Architecture Principles

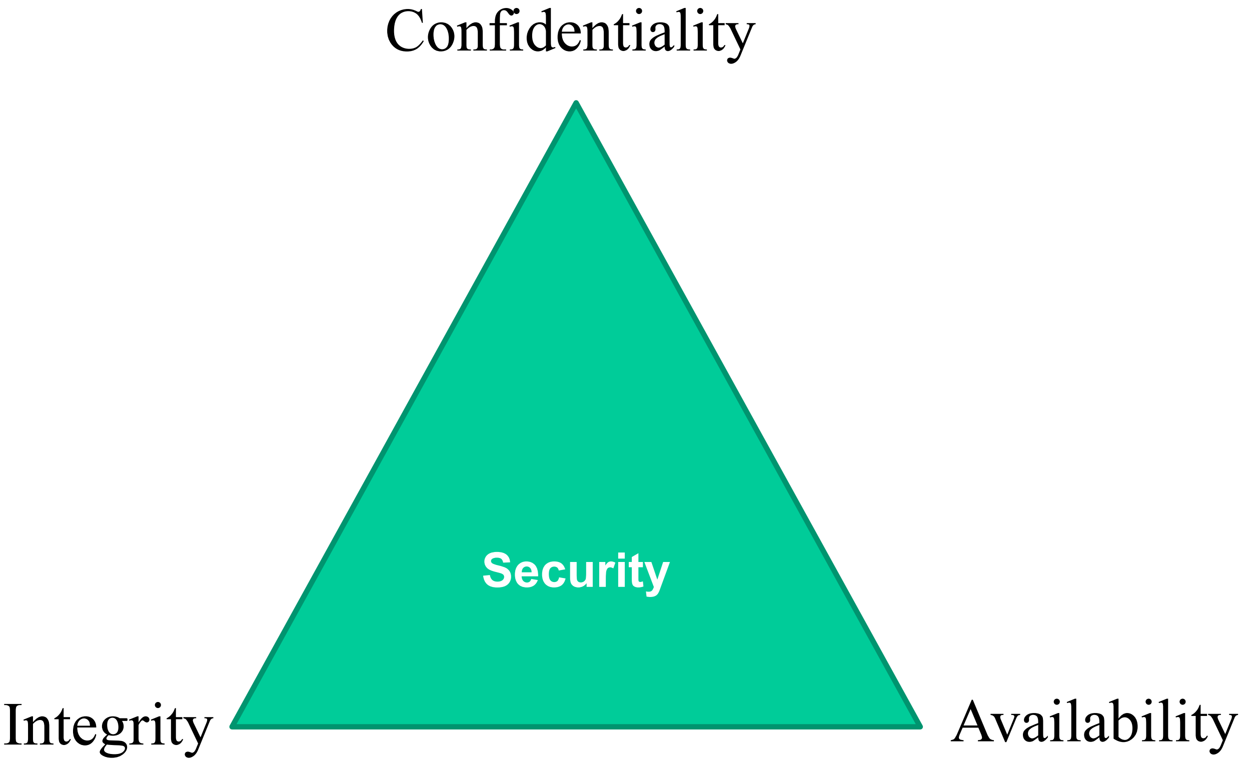
- **Support Open Standards and embrace transparency**
  - Avoid security by obscurity
  - Document trust and threat models
  - Support all chief platforms, languages and run time settings
- **Provide security by default**
  - Ship security policies “out of the box” with security enabled
- **Design for accountability**
  - Audit Structure
- **Design for regulatory reporting**
- **Design for Privacy**
  - Decrease the use of individually recognizable data
  - Track the use of individually recognizable data

Contd...

- **Design for consumability**
  - Security services must be operable by programmers
  - Security services must be operable by IT management systems
- **Provide multiple level of protections**
  - Least privileges
  - Zoning
  - Multiple layers of enforcement and detection
- **Separation of security duties**
  - Roles & responsibilities
- **Design for context awareness**
- **Use security models to create consistency**

Understanding Security Risks

CIA Triad



Top Security Risks

- **LOSS OF GOVERNANCE:** in using cloud infrastructures, the client necessarily cedes control to the Cloud Provider (CP) on a number of issues which may affect security. At the same time, SLAs may not offer a commitment to provide such services on the part of the cloud provider, thus leaving a gap in security defenses.

- **LOCK-IN:** there is currently little on offer in the way of tools, procedures or standard data formats or services interfaces that could guarantee data, application and service portability. This can make it difficult for the customer to migrate from one provider to another or migrate data and services back to an in-house IT environment. This introduces a dependency on a particular CP for service provision, especially if data portability, as the most fundamental aspect, is not enabled.

- **ISOLATION FAILURE:** multi-tenancy and shared resources are defining characteristics of cloud computing. This risk category covers the failure of mechanisms separating storage, memory, routing and even reputation between different tenants (e.g., so-called guest-hopping attacks).

- **COMPLIANCE RISKS:** investment in achieving certification (e.g., industry standard or regulatory requirements) may be put at risk by migration to the cloud:

  - if the CP cannot provide evidence of their own compliance with the relevant requirements

  - if the CP does not permit audit by the cloud customer (CC).

In certain cases, it also means that using a public cloud infrastructure implies that certain kinds of compliance cannot be achieved (e.g., PCI DSS).

Contd...

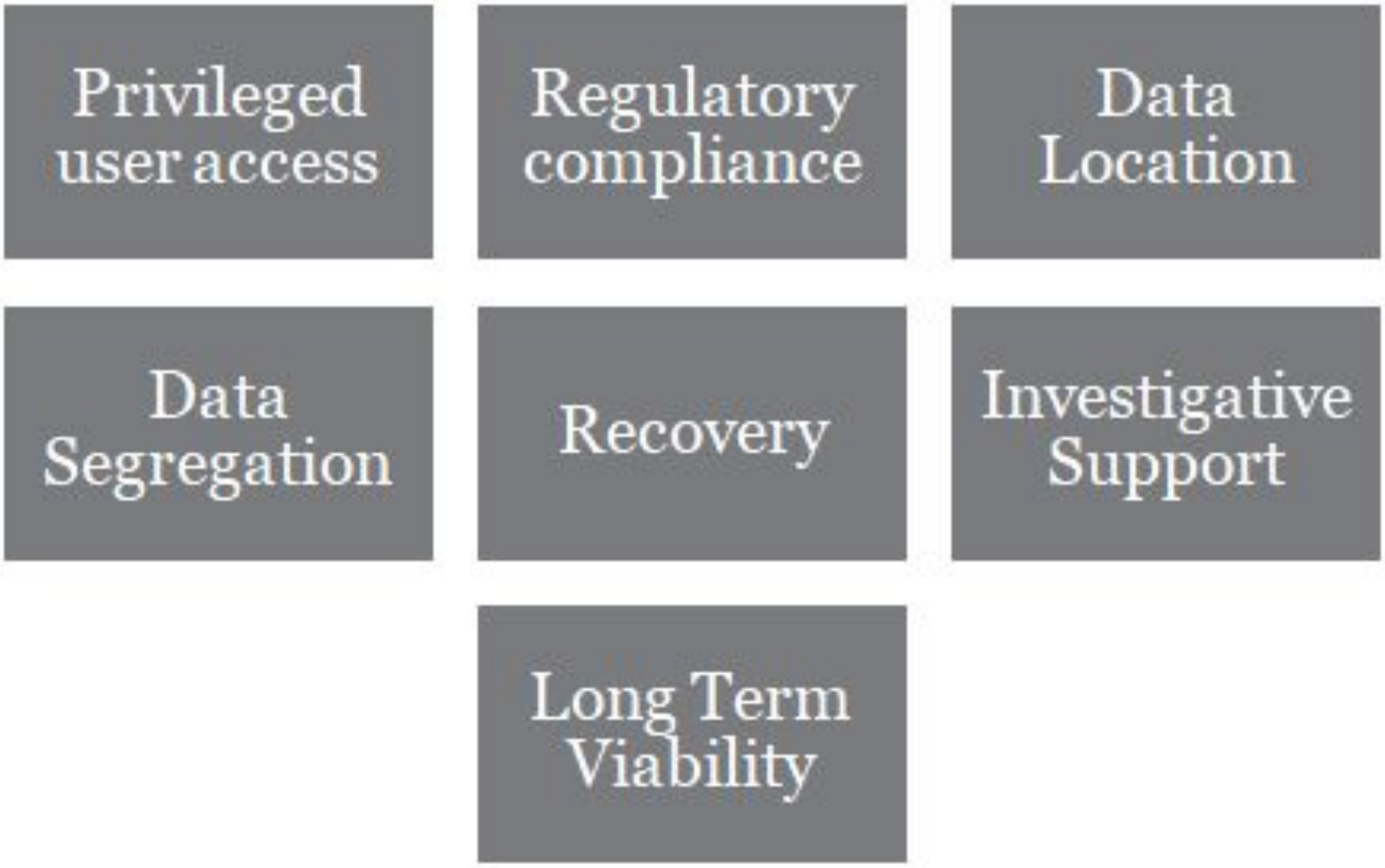
- **MANAGEMENT INTERFACE COMPROMISE:** customer management interfaces of a public cloud provider are accessible through the Internet and mediate access to larger sets of resources (than traditional hosting providers) and therefore pose an increased risk, especially when combined with remote access and web browser vulnerabilities.

- **DATA PROTECTION:** cloud computing poses several data protection risks for cloud customers and providers. In some cases, it may be difficult for the cloud customer (in its role as data controller) to effectively check the data handling practices of the cloud provider and thus to be sure that the data is handled in a lawful way..

- **INSECURE OR INCOMPLETE DATA DELETION:** when a request to delete a cloud resource is made, as with most operating systems, this may not result in true wiping of the data. Adequate or timely data deletion may also be impossible (or undesirable from a customer perspective), either because extra copies of data are stored but are not available, or because the disk to be destroyed also stores data from other clients.

- **MALICIOUS INSIDER:** while usually less likely, the damage which may be caused by malicious insiders is often far greater. Cloud architectures necessitate certain roles which are extremely high-risk. Examples include CP system administrators and managed security service providers.

Gartner's Seven Cloud Computing Security Risks



Privileged user access

Regulatory compliance

Data Location

Data Segregation

Recovery

Investigative Support

Long Term Viability

Securing Multi-Tenant Environment

- Every tenant’s workload must be completely isolated from every other tenant’s workloads and administrators.
- For organizations to effectively isolate their workloads they need to:
  - Prevent unauthorized communication between one cloud tenant’s VMs and virtual networks and any other tenant’s resources.
  - Prevent a privileged user from either exposing their workloads to others (accidentally or intentionally) or gaining unauthorized access to another tenant’s workloads.
  - Log all virtual administrator activity per tenant to ensure compliance.

Effective Isolation and Workload Security in Multi-tenant Cloud

Goals:

1. **Cloud Protection**

   HyTrust Cloud Control provides advanced privileged user access control, policy enforcement, forensic and automated compliance for private clouds.

2. **Data Encryption**

   HyTrust Data Control provides powerful data-at-rest encryption and integrated key management for workloads running in any cloud environment.

3. **Key Management**

   Encrypting workloads helps enterprises to ensure their data is protected. One of the challenges of workload encryption is scaling the management of encryption keys.

Contd...

- The **HyTrust** Cloud Security Policy Framework makes secure multi tenancy possible by enforcing

  - *access controls and encryption policies for virtual and cloud infrastructure.*

- Effectively segmenting cloud deployments and securely isolating each tenant’s critical applications and data.
- detailed logging and analysis of privileged admin account actions.

Vulnerability

- **Vulnerability** is a weakness which can be exploited by an attacker, to perform unauthorized actions within a computer **system**.
- Vulnerability is the intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw.
- To exploit a vulnerability, an attacker must have at least one applicable tool or technique that can connect to a system weakness.

Vulnerability Scanning Tools:

- ❖ *Nessus*
- ❖ *Nikto2*
- ❖ *Netsparker, and many more...*

Vulnerabilities In Cloud Computing

➢Vulnerabilities in Virtual Machines

- Possible covert channels in the collocation of VMs.
- Unrestricted allocation and deallocation of resources with VMs.
- Uncontrolled Migration - VMs can be migrated from one server to another server due to fault tolerance, load balance, or hardware maintenance.
- Uncontrolled snapshots – VMs can be copied in order to provide flexibility, which may lead to data leakage.
- Uncontrolled rollback could lead to reset vulnerabilities - VMs can be backed up to a previous state for restoration, but patches applied after the previous state disappear.
- VMs have IP addresses that are visible to anyone within the cloud - attackers can map where the target VM is located within the cloud (Cloud cartography).

Vulnerabilities In Cloud Computing

Vulnerabilities in Virtual Machine Images

- Uncontrolled placement of VM images in public repositories.
- VM images are not able to be patched since they are dormant artifacts.

Vulnerabilities in Virtual Networks

- The cloud characteristic ubiquitous network access means that cloud services are accessed via network using standard protocols. In most cases, this network is the Internet, which must be considered untrusted. Internet protocol vulnerabilities - such as vulnerabilities that allow man-in-the-middle attacks - are therefore relevant for cloud computing.
- Sharing of virtual bridges by several virtual machines.

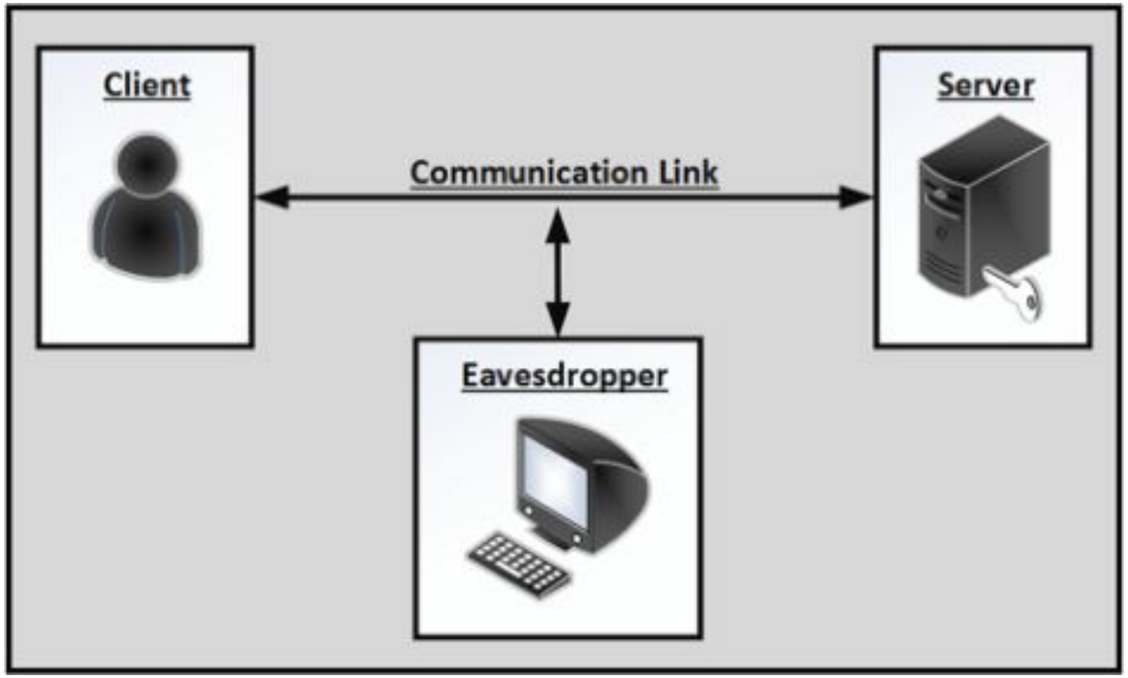
Hypervisor Vulnerabilities

- A typical scenario enabled by exploiting a hypervisor’s vulnerability is called *‘guest to host escape’,*
  allowing the guest to execute code on the host.

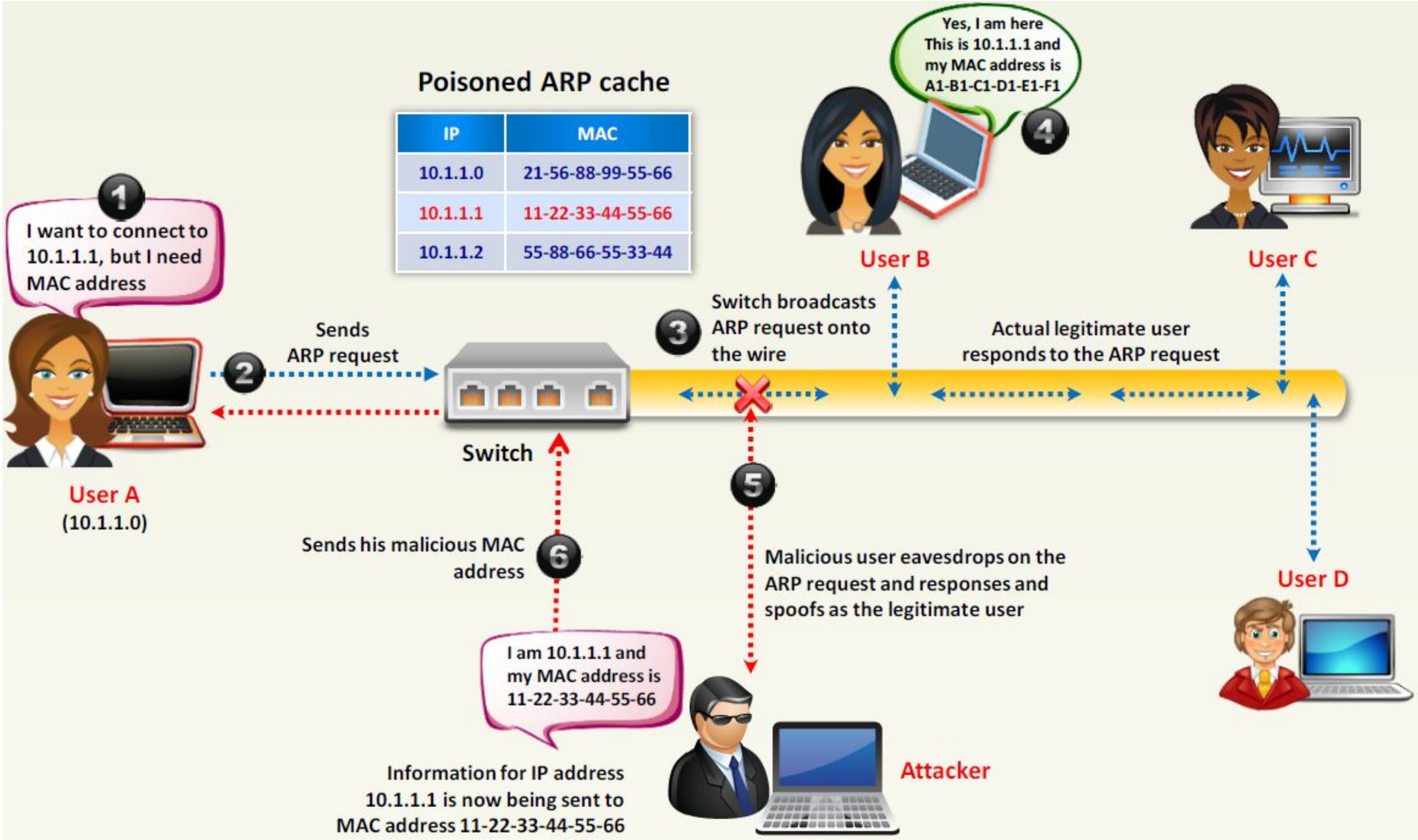
- Another scenario is ‘*VM hopping*’: in which an attacker hacks a VM using some standard method and then – exploiting some hypervisor vulnerability – takes control of other VMs running on the same hypervisor.

Cloud Account/Server Hijacking

- **Cloud account hijacking** is a common tactic in identity theft schemes in which the attacker uses stolen account information to conduct malicious or unauthorized activity.
- When **cloud account hijacking** occurs, an attacker typically uses a compromised email **account** or other credentials to impersonate the **account** owner.



ARP Spoofing



Poisoned ARP cache

IP	MAC
10.1.1.0	21-56-88-99-55-66
10.1.1.1	11-22-33-44-55-66
10.1.1.2	55-88-66-55-33-44

1 I want to connect to 10.1.1.1, but I need MAC address

2 Sends ARP request

3 Switch broadcasts ARP request onto the wire

4 Yes, I am here This is 10.1.1.1 and my MAC address is A1-B1-C1-D1-E1-F1

Actual legitimate user responds to the ARP request

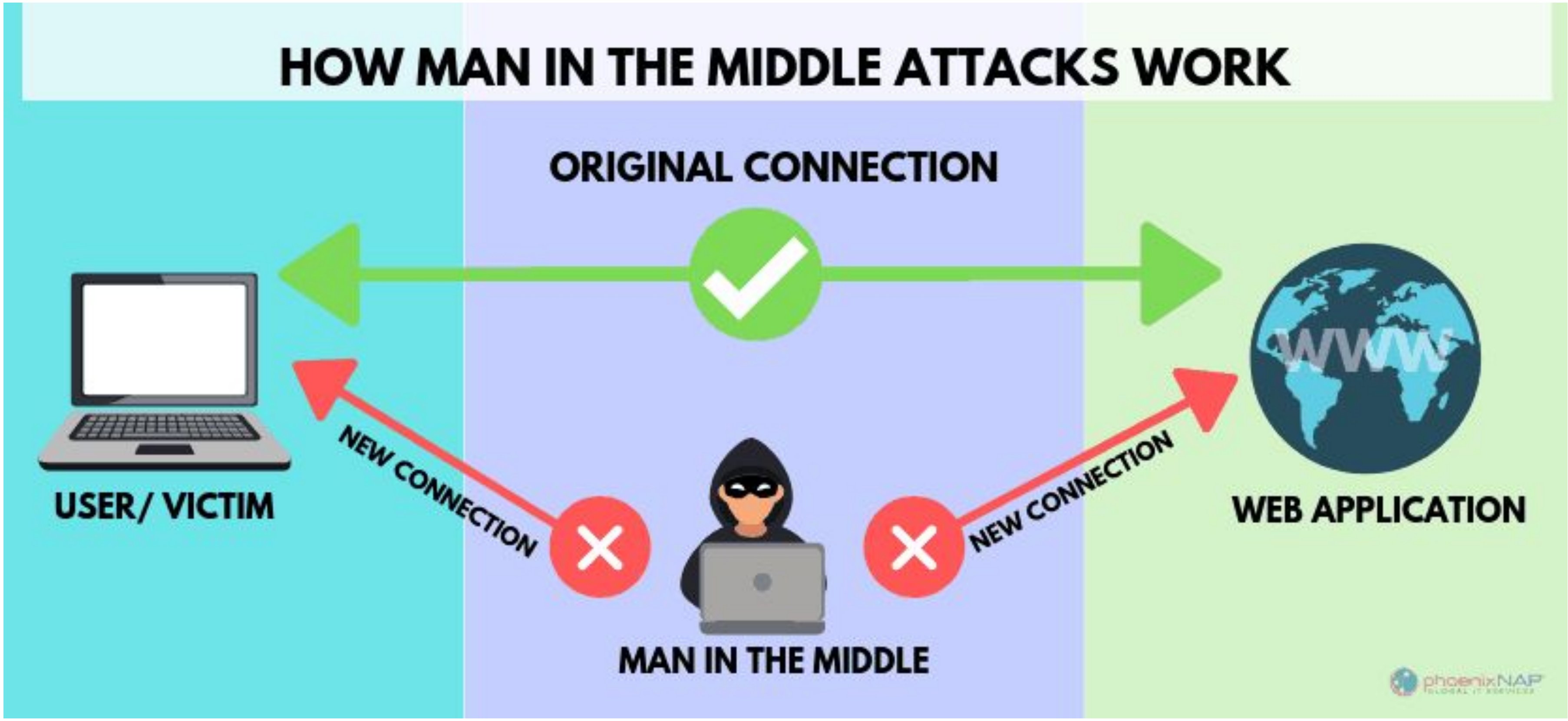
5 Malicious user eavesdrops on the ARP request and responses and spoofs as the legitimate user

6 Sends his malicious MAC address

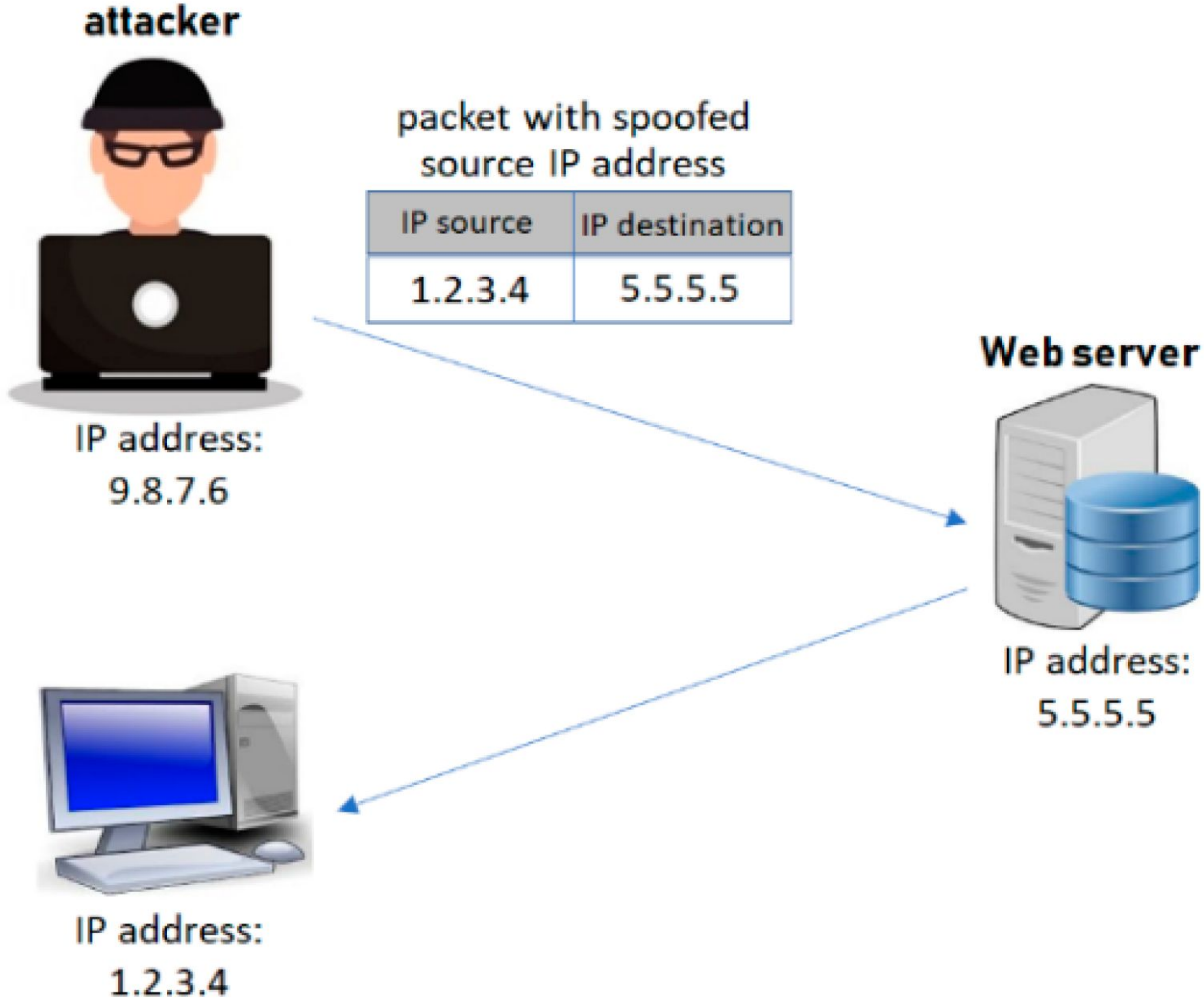
I am 10.1.1.1 and my MAC address is 11-22-33-44-55-66

Information for IP address 10.1.1.1 is now being sent to MAC address 11-22-33-44-55-66

Man-in-the-Middle (MITM) Attack



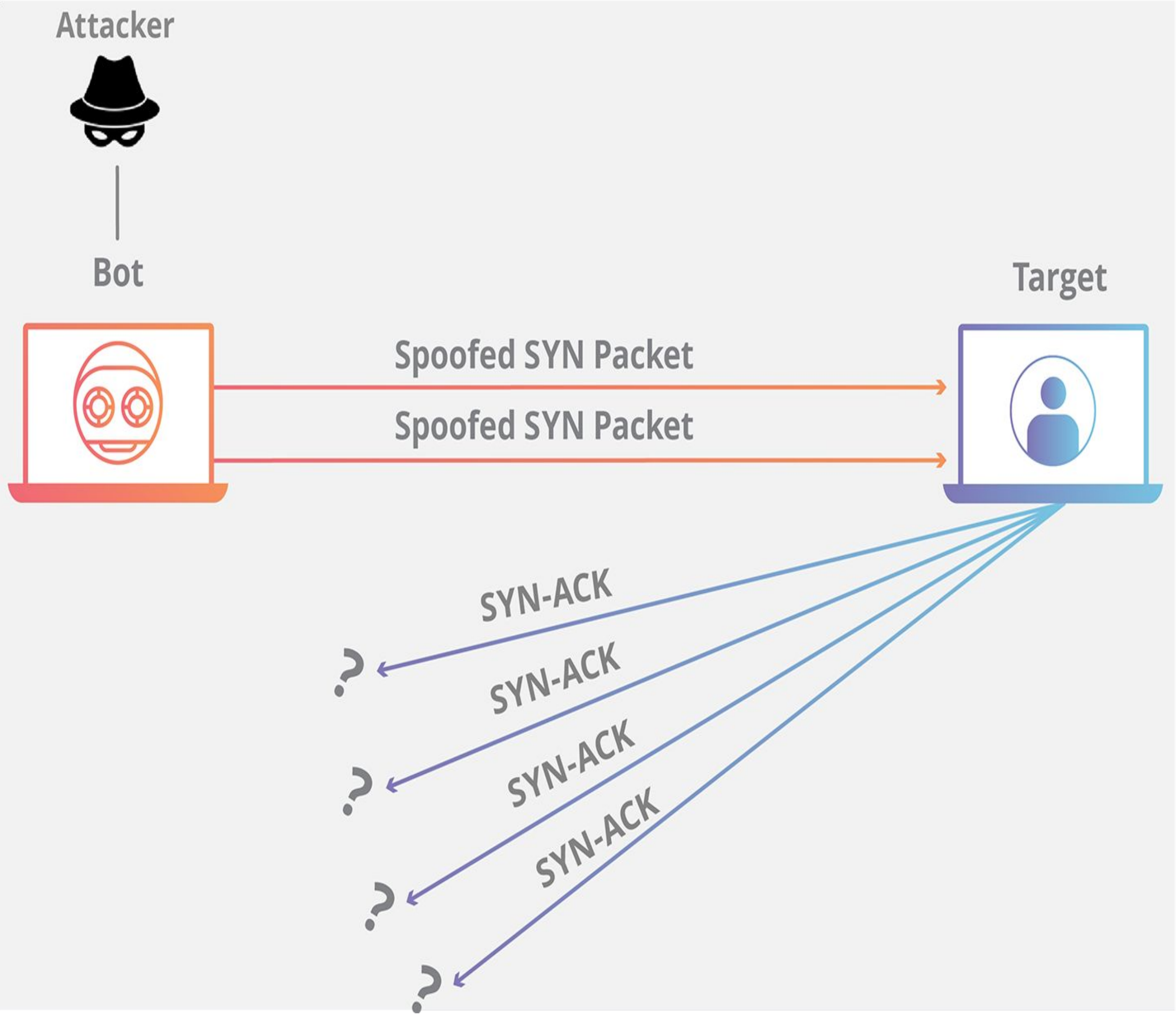
IP Spoofing



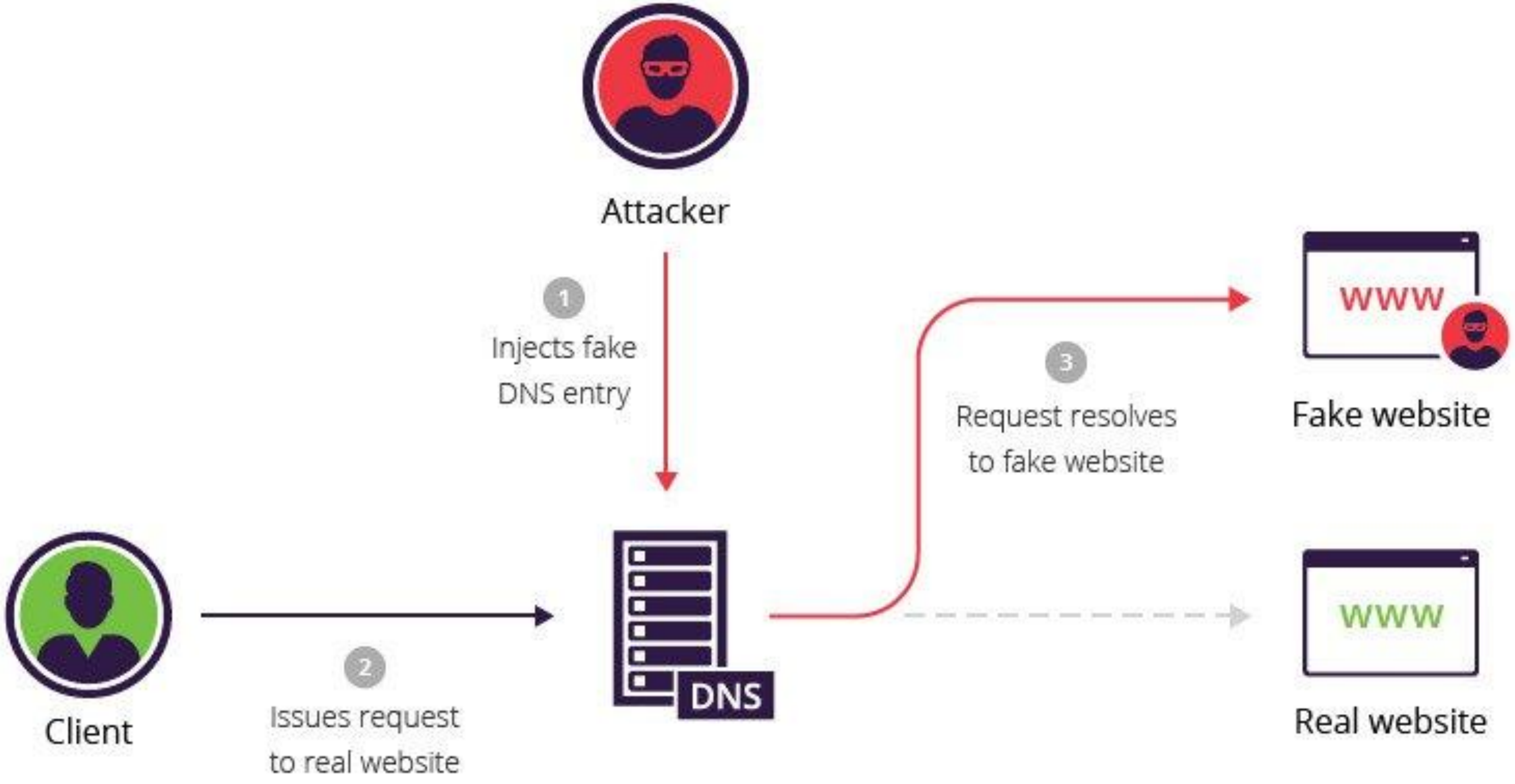
packet with spoofed source IP address

IP source	IP destination
1.2.3.4	5.5.5.5

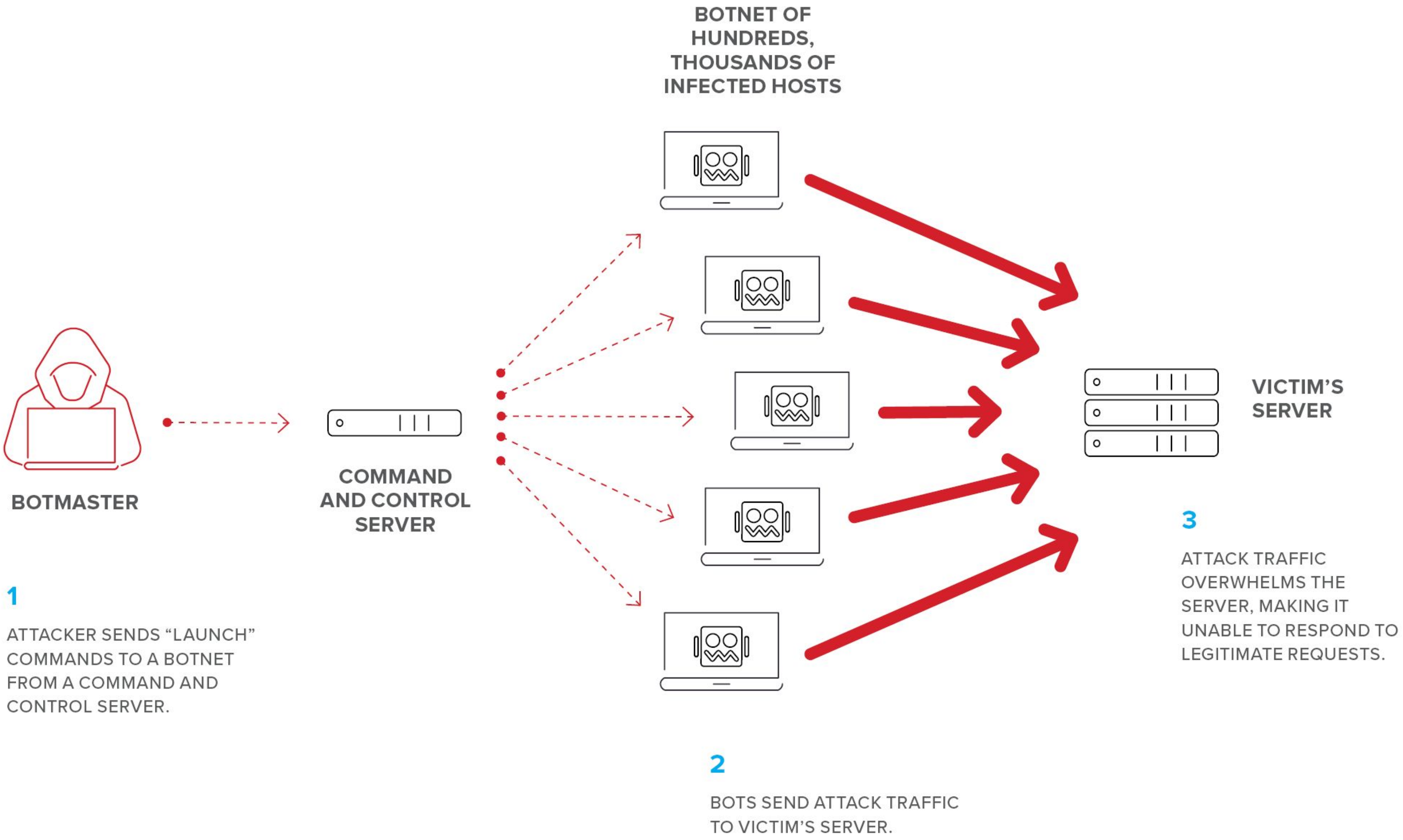
TCP Handshaking in IP Spoofing



DNS Spoofing



DDoS Attack



BOTNET OF HUNDREDS, THOUSANDS OF INFECTED HOSTS

BOTMASTER

COMMAND AND CONTROL SERVER

VICTIM'S SERVER

1

ATTACKER SENDS "LAUNCH" COMMANDS TO A BOTNET FROM A COMMAND AND CONTROL SERVER.

2

BOTS SEND ATTACK TRAFFIC TO VICTIM'S SERVER.

3

ATTACK TRAFFIC OVERWHELMS THE SERVER, MAKING IT UNABLE TO RESPOND TO LEGITIMATE REQUESTS.

Secure Your Cloud

- Ensure local backup
- Avoid storing sensitive information
- Use encryption
- Apply reliable password
- Log everything
- Do not forget the firewall