Infrastructure Security

The network, host, and application levels

Infrastructure Security: The Network Level

- When looking at the network level of infrastructure security, it is important to distinguish between **public clouds** and **private clouds**.
- With **private clouds**, there are **no new attacks**, **vulnerabilities, or changes in risk specific** to this topology that information security personnel need to consider.
- However, if you choose to use public cloud services, there are four significant risk factors.

Risk factors in case of public cloud services

- Ensuring the **confidentiality and integrity** of your organization's data-in-transit to and from your public cloud provider
- **Ensuring proper access control** (authentication, authorization, and auditing) to whatever resources you are using at your public cloud provider
- **Ensuring the availability** of the Internet-facing resources in a public cloud that are being used by your organization, or have been assigned to your organization by your public cloud providers
- **Replacing the established model of network zones and tiers with domains**

Ensuring Data Confidentiality and Integrity

- Some resources and data previously confined to a private network are now **exposed to the Internet**, and to a shared public network belonging to a **third-party cloud** provider.

Ensuring Proper Access Control

- Since some subset of these resources (or maybe even all of them) is now exposed to the Internet, an organization using a public cloud faces a significant increase in risk to its data.
- The ability to audit the operations of your cloud provider's network (let alone to conduct any realtime monitoring, such as on your own network), even after the fact, is probably non-existent.
- You will have **decreased access to relevant network-level logs and data, and a limited ability to thoroughly conduct investigations and gather forensic data**

Ensuring the Availability of Internet-Facing Resources

- Reliance on network security has increased because an increased amount of data or an increased number of organizational personnel now depend on externally hosted devices to ensure the availability of cloud-provided resources.
- Examples are,
- BGP prefix hijacking
- DNS cache poisoning
- DDoS attack

BGP prefix hijacking

- Prefix hijack in autonomous system address space that belongs to someone else without her permission.
- Such announcements often occur because of a configuration mistake, but that misconfiguration may still affect the availability of your cloud-based resources.
- According to a study presented to the North American Network Operators Group (NANOG) in February 2006, several hundred such misconfigurations occur per month.
- Probably the best known example of such a misconfiguration mistake occurred in February 2008 when Pakistan Telecom made an error by announcing a dummy route for YouTube to its own telecommunications partner, PCCW, based in Hong Kong.
- The intent was to block YouTube within Pakistan because of some supposedly blasphemous videos hosted on the site. The result was that YouTube was globally unavailable for two hours

DNS attacks

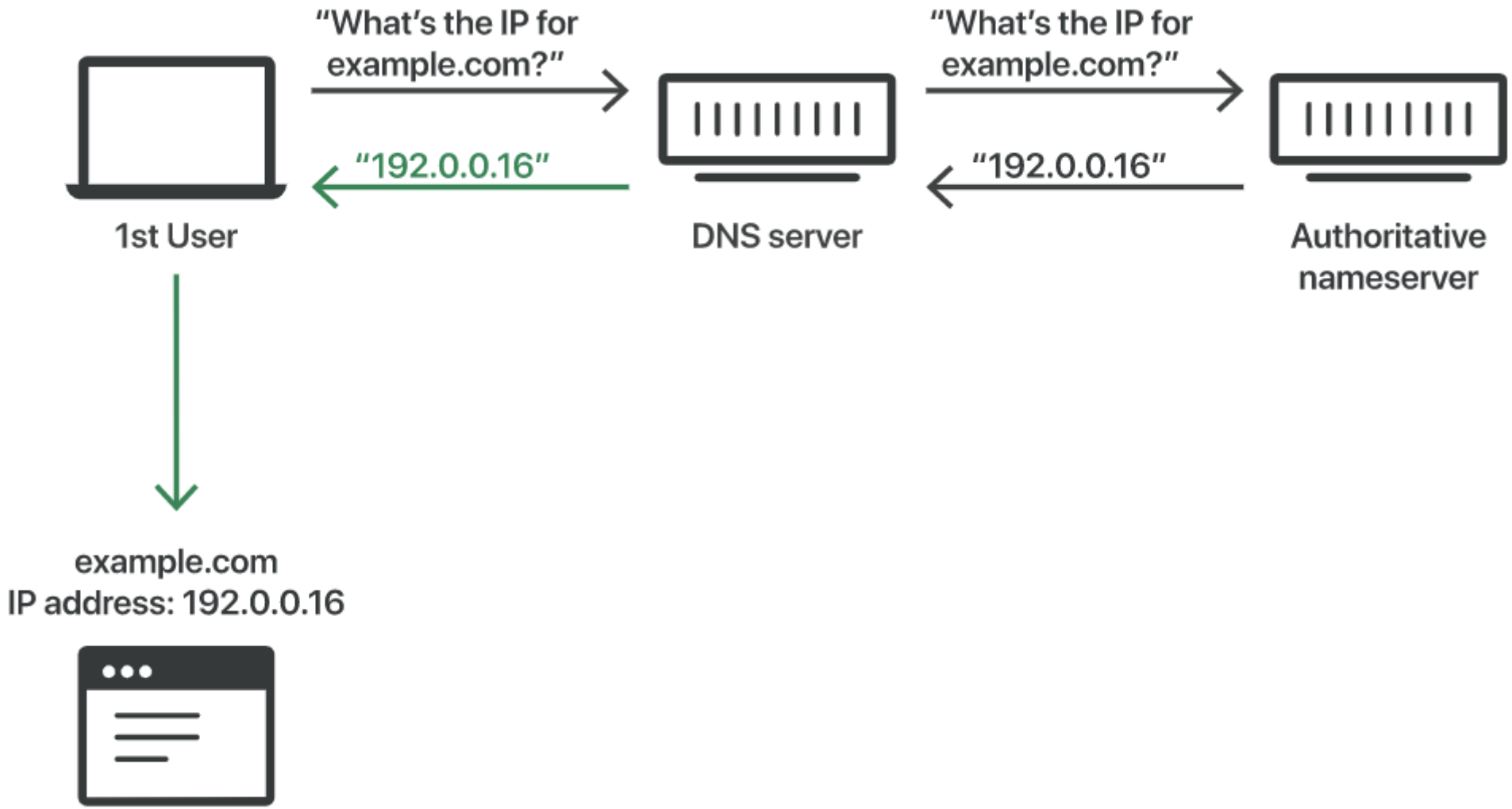
- DNS attacks are another example of problems associated with this third risk factor.
- In fact, there are several forms of DNS attacks to worry about with regard to cloud computing.
- DNS cache poisoning is one of such attack.

DNS cache poisoning

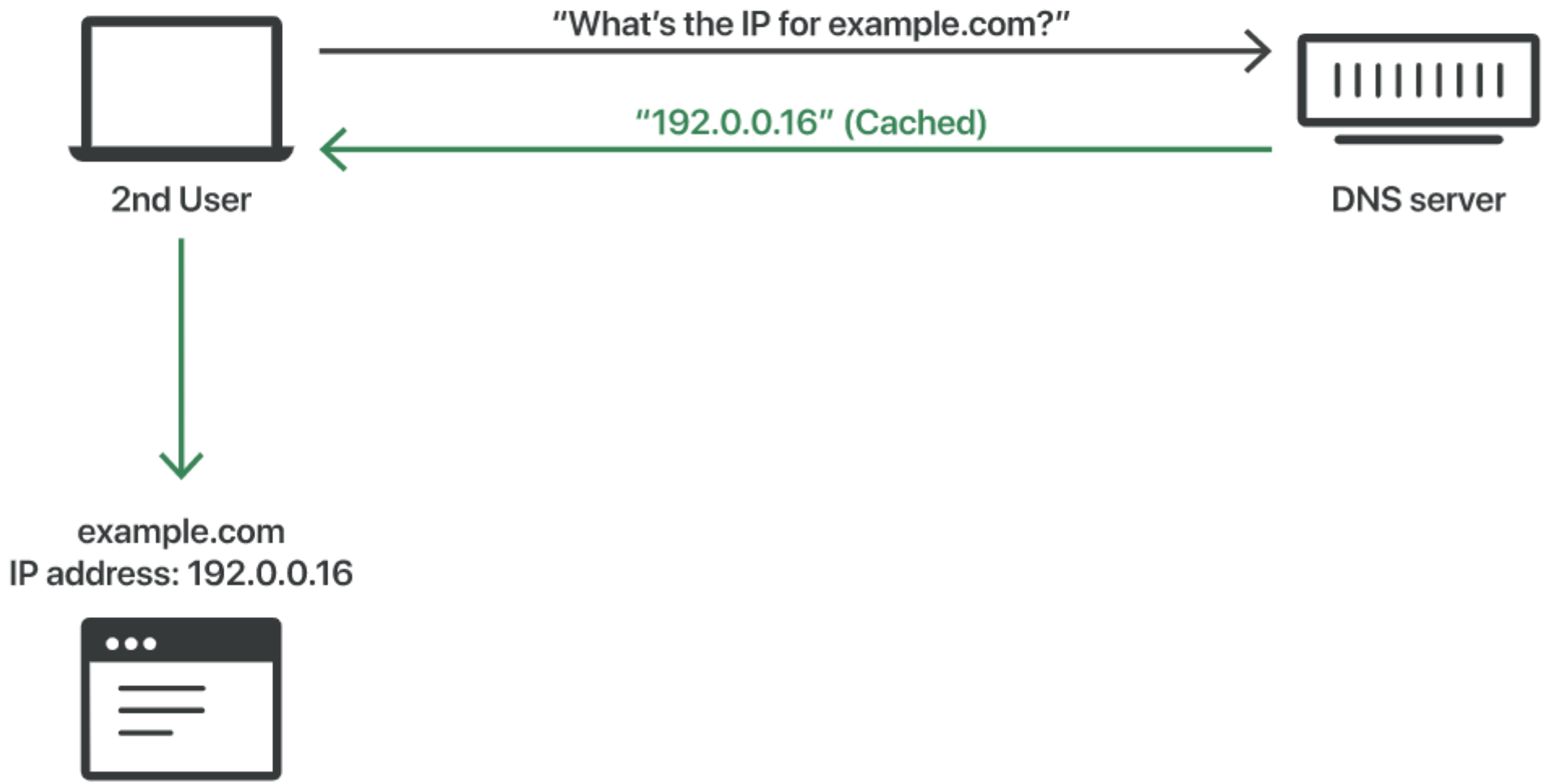
- Imagine that, as a senior-year prank, high school seniors change out all the room numbers on their high school campus, so that the new students who don't know the campus layout yet will spend the next day getting lost and showing up in the wrong classrooms.
- Now imagine that the mismatched room numbers get recorded in a campus directory, and students keep heading to the wrong rooms until someone finally notices and corrects the directory.
- DNS cache poisoning is the act of entering false information into a DNS cache, so that DNS queries return an incorrect response and users are directed to the wrong websites. DNS cache poisoning is also known as 'DNS spoofing.'
- IP addresses are the 'room numbers' of the Internet, enabling web traffic to arrive in the right places. DNS resolver caches are the 'campus directory,' and when they store faulty information, traffic goes to the wrong places until the cached information is corrected.
- Because there is typically no way for DNS resolvers to verify the data in their caches, incorrect DNS information remains in the cache until the time to live (TTL) expires, or until it is removed manually.

DNS resolvers

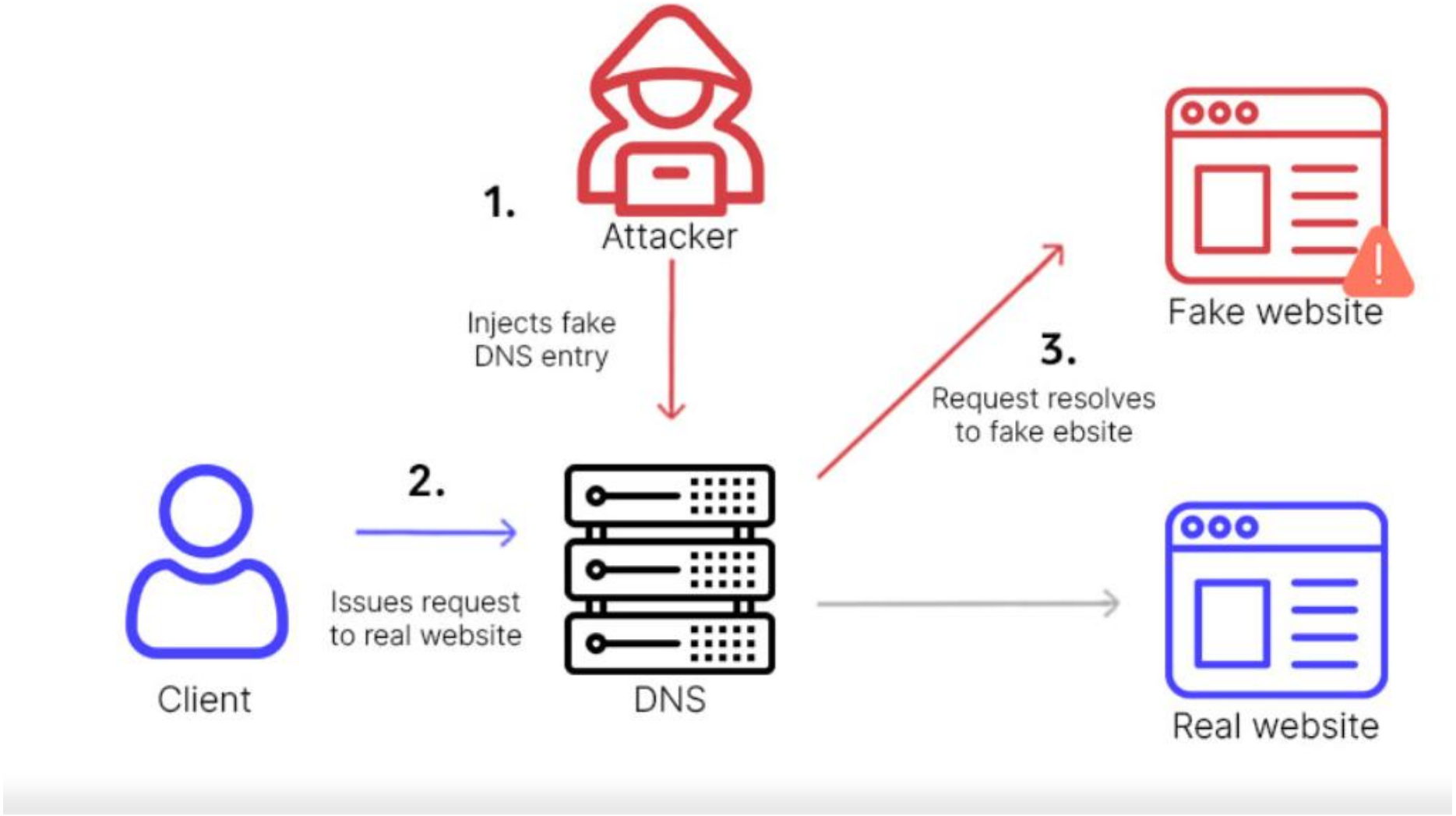
- DNS resolvers provide clients with the IP address that is associated with a domain name. In other words, they take human-readable website addresses like 'cloudflare.com' and translate them into machine-readable IP addresses. When a user attempts to navigate to a website, their operating system sends a request to a DNS resolver. The DNS resolver responds with the IP address, and the web browser takes this address and initiates loading the website.
- A DNS resolver will save responses to IP address queries for a certain amount of time. In this way, the resolver can respond to future queries much more quickly, without needing to communicate with the many servers involved in the typical DNS resolution process.

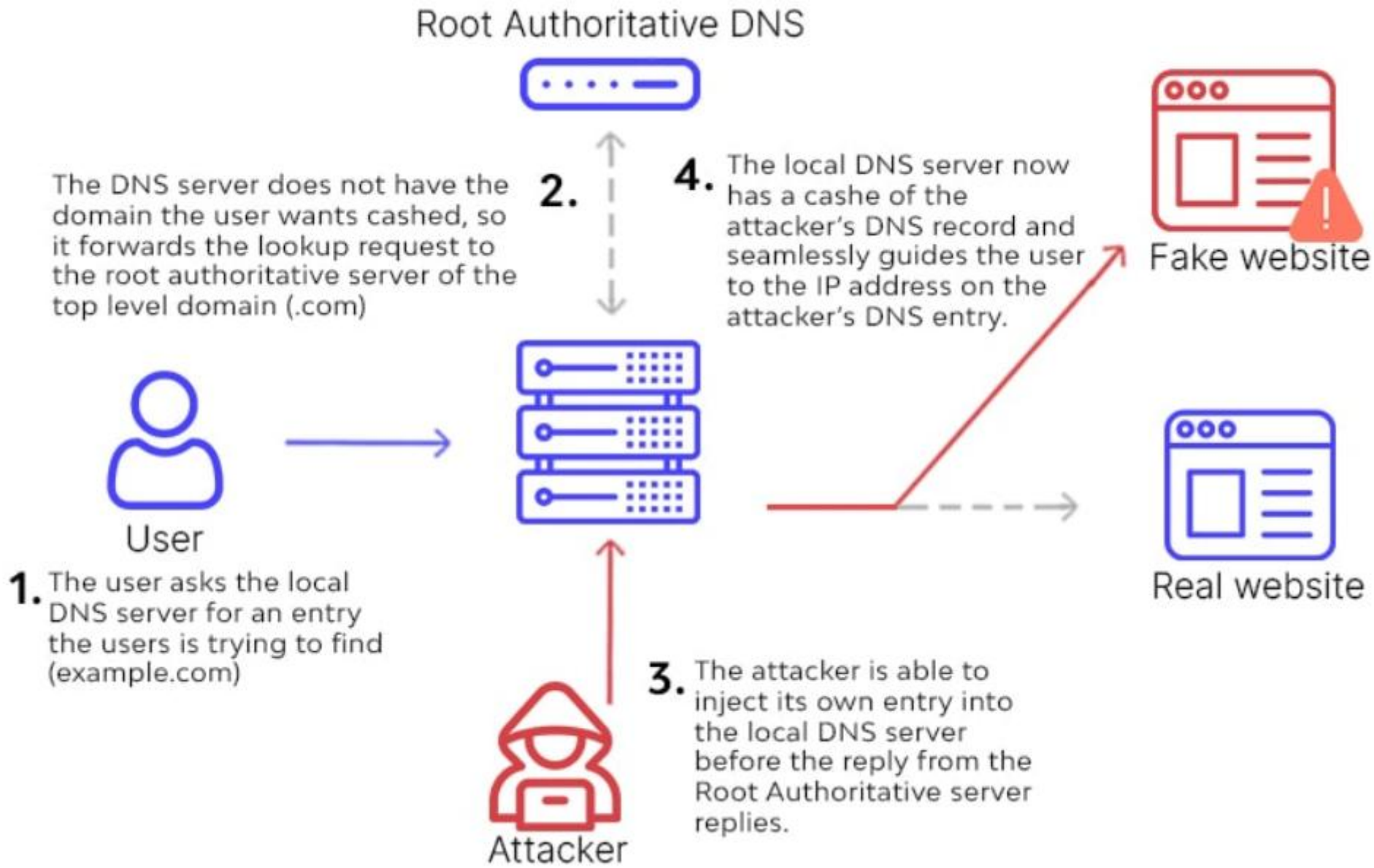

"What's the IP for example.com?"
"What's the IP for example.com?"
"192.0.0.16"
"192.0.0.16"
1st User
DNS server
Authoritative nameserver
example.com
IP address: 192.0.0.16

DNS Cached Response:



Poison DNS caches




Root Authoritative DNS
The DNS server does not have the domain the user wants cashed, so it forwards the lookup request to the root authoritative server of the top level domain (.com)
2.
4. The local DNS server now has a cashe of the attacker's DNS record and seamlessly guides the user to the IP address on the attacker's DNS entry.
Fake website
User
1. The user asks the local DNS server for an entry the users is trying to find (example.com)
Real website
3. The attacker is able to inject its own entry into the local DNS server before the reply from the Root Authoritative server replies.
Attacker

DoS and DDoS

- A final example of problems associated with this third risk factor is denial of service (DoS) and distributed denial of service (DDoS) attacks.
- Again, although DoS/DDoS attacks are not new and are not directly related to the use of cloud computing, the issue with these attacks and cloud computing is an increase in an organization's risk at the network level because of some increased use of resources external to your organization's network.
- For example, there continue to be rumors of continued DDoS attacks on AWS, making the services unavailable for hours at a time to AWS users.

Replacing the Established Model of Network Zones and Tiers with Domains

- For years, network security has relied on zones, such as intranet versus extranet and development versus production, to segregate network traffic for improved security. This model was based on exclusion—only individuals and systems in specific roles have access to specific zones.
- The traditional model of **network zones and tiers has been replaced in public cloud computing with "security groups," "security domains," or "virtual data centers" that have logical separation between tiers but are less precise and afford less protection than the formerly established model.**
- In the established model of network zones and tiers, not only were development systems logically separated from production systems at the network level, but these two groups of systems were also physically separated at the host level. The cloud computing model of separation by domains provides logical separation for addressing purposes only. There is no longer any "required" physical separation, as a test domain and a production domain may very well be on the same physical server.

Network-Level Mitigation

- Note that network-level risks exist regardless of what aspects of “cloud computing” services are being used (e.g., software-as-a-service, platform-as-a-service, or infrastructure-as-a-service).
- The **primary determination of risk level is therefore not which *aaS is being used, but rather whether your organization intends to use or is using a public, private, or hybrid cloud.**
- If your organization is large enough to afford the resources of a private cloud, your risks will decrease—assuming you have a true private cloud that is internal to your network.
- In some cases, a private cloud located at a cloud provider’s facility can help meet your security requirements but will depend on the provider capabilities and maturity.

- You can reduce your confidentiality risks by using **encryption**; specifically by using validated implementations of cryptography for data-in-transit.
- Secure **digital signatures** make it much more difficult, if not impossible, for someone to tamper with your data, and this ensures data integrity.
- Availability problems at the network level are far more difficult to mitigate with cloud computing—unless your organization is using a private cloud that is internal to your network topology. Even if your private cloud is a private (i.e., non-shared) external network at a cloud provider's facility, you will face increased risk at the network level.

Infrastructure Security: The Host Level

- When reviewing host security and assessing risks, you should consider the context of **cloud services delivery models (SaaS, PaaS, and IaaS) and deployment models (public, private, and hybrid).**
- The dynamic nature (elasticity) of cloud computing can bring new operational challenges from a security management perspective.
- The operational model motivates rapid provisioning and fleeting instances of VMs. Managing vulnerabilities and patches is therefore much harder than just running a scan, as **the rate of change is much higher than in a traditional data center.**
- In addition, the fact that the clouds harness the power of thousands of compute nodes, **combined with the homogeneity of the operating system employed by hosts, means the threats can be amplified quickly and easily—call it the "velocity of attack"** factor in the cloud.

SaaS and PaaS Host Security

- In general, CSPs do not publicly share information related to their **host platforms, host operating systems, and the processes that are in place to secure the hosts,** since hackers can exploit that information when they are trying to intrude into the cloud service.
- Hence, in the context of SaaS (e.g., Salesforce.com, Workday.com) or PaaS (e.g., Google App Engine, Salesforce.com's Force.com) cloud services, host security is opaque to customers and the responsibility of securing the hosts is relegated to the CSP.

- To get assurance from the CSP on the security hygiene of its hosts, you should ask the vendor to share information under a **nondisclosure agreement (NDA)** or simply demand that the CSP share the information via a controls assessment framework such as **SysTrust or ISO 27002**.
- From a controls assurance perspective, the CSP has to ensure that appropriate preventive and detective controls are in place and will have to ensure the same via a third-party assessment or ISO 27002 type assessment framework
- However, as a customer, you still **own the risk of managing information hosted in the cloud services**. It's your responsibility to get the appropriate level of assurance regarding how the CSP manages host security hygiene.

IaaS Host Security

- Unlike PaaS and SaaS, IaaS **customers are primarily responsible for securing the hosts provisioned** in the cloud.
- Given that almost all IaaS services available today employ virtualization at the host layer, host security in IaaS should be categorized as follows:
- Virtualization software security
- Customer guest OS or virtual server security

- Virtualization software security:
- The software layer that sits on top of bare metal and provides customers the ability to create and destroy virtual instances.
- Virtualization at the host level can be accomplished using any of the virtualization models, including OS-level virtualization (Solaris containers, BSD jails, Linux-VServer), paravirtualization (a combination of the hardware version and versions of Xen and VMware), or hardware-based virtualization (Xen, VMware, Microsoft Hyper-V).
- It is important to secure this layer of software that sits between the hardware and the virtual servers. In a public IaaS service, customers do not **have access to this software layer; it is managed by the CSP only.**

- Customer guest OS or virtual server security The virtual instance of an operating system that is provisioned on top of the virtualization layer and is visible to customers from the Internet; e.g., various flavors of Linux, Microsoft, and Solaris. Customers have full access to virtual servers.

Virtualization Software Security

- Since the **CSP manages** the virtualization software that sits on top of the hardware, customers will have neither visibility nor access to this software.
- CSPs should institute the necessary security controls, including restricting physical and logical access to hypervisor and other forms of employed virtualization layers
- IaaS customers should **understand the technology and security** process controls instituted by the CSP to protect the hypervisor.
- This will help you to understand the compliance and gaps with reference to your host security standard, policies, and regulatory compliances

Threats to the hypervisor

- Threats to the hypervisor The integrity and availability of the hypervisor are of utmost importance and are key to guaranteeing the integrity and availability of a public cloud built on a virtualized environment.
- A vulnerable hypervisor could **expose all user domains to malicious insiders**. Furthermore, hypervisors are potentially susceptible to subversion attacks

Virtual Server Security

- customers are responsible for securing and ongoing security management of the guest VM
- Some of the new host security threats in the public IaaS include:
  - **Stealing keys** used to access and manage hosts (e.g., SSH private keys)
  - Attacking **unpatched, vulnerable services** listening on standard ports (e.g., FTP, NetBIOS, SSH)
  - **Hijacking accounts** that are not properly secured (i.e., weak or no passwords for standard accounts)
  - Attacking systems that are not properly secured by **host firewalls**
  - **Deploying Trojans embedded in the software** component in the VM or within the VM image (the OS) itself

Securing virtual servers

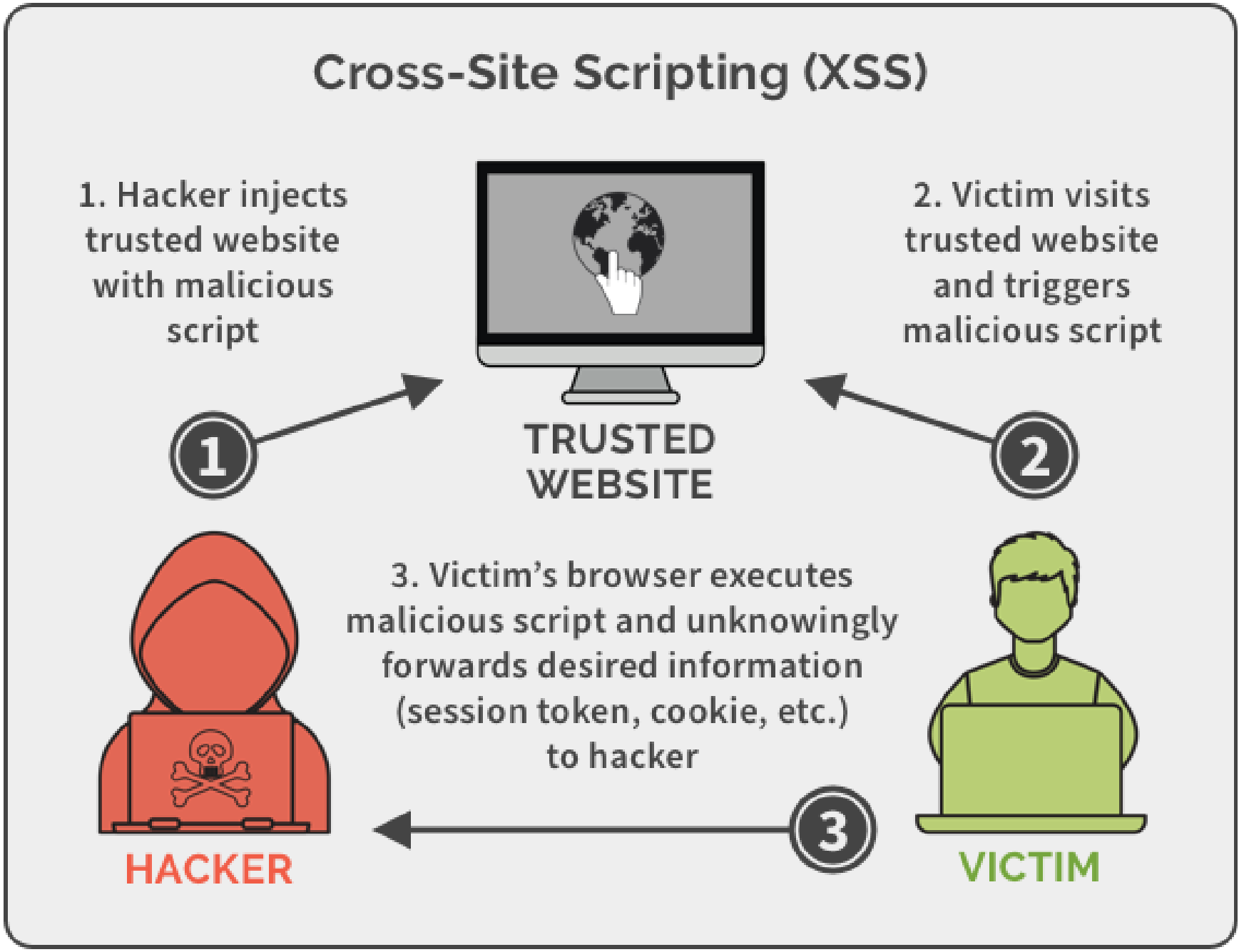
- Harden the image
- unauthorized access.
- VM images and OS versions
- Safeguard the private keys
- decryption keys
- the minimum ports
- unused services
- auditing and event logging-forensics and periodic review

Infrastructure Security: The Application Level

- **Application or software security** should be a critical element of your security program.
- Most enterprises with information security programs have **yet** to institute an application security program **to address this realm**.
- Designing and implementing applications targeted for deployment on a cloud platform will require that **existing application security programs reevaluate current practices and standards**.
- The application security spectrum ranges from standalone **single-user applications** to **sophisticated multiuser e-commerce** applications used by millions of users.
- **Web applications** such as content management systems (CMSs), wikis, **portals**, bulletin boards, and **discussion forums** are used by **small and large organizations.**
- A **large number of organizations** also **develop and maintain custom-built web applications** for their businesses using various web frameworks.

Application-Level Security Threats

- According to SANS, web application vulnerabilities in open source as well as custom-built applications accounted for almost **half the total number of vulnerabilities discovered between November 2006 and October 2007.**
- Advances in cross-site scripting (XSS) and other attacks have demonstrated that criminals looking for financial gain can exploit **vulnerabilities resulting from web programming error**s as new ways to penetrate important organizations.
- The existing threats exploit well-known application vulnerabilities includes cross-site scripting (XSS), SQL injection, malicious file execution, and other vulnerabilities resulting from programming errors and design flaws.


Cross-Site Scripting (XSS)
1. Hacker injects trusted website with malicious script
2. Victim visits trusted website and triggers malicious script
TRUSTED WEBSITE
1
2
3
3. Victim's browser executes malicious script and unknowingly forwards desired information (session token, cookie, etc.) to hacker
HACKER
VICTIM

FUNCTIONING OF AN SQL INJECTION

1. Hacker identifies vulnerable, SQL-driven website & injects malicious SQL query via input data.

WEBSITE INPUT FIELDS

2. Malicious SQL query is validated & command is executed by database.

01

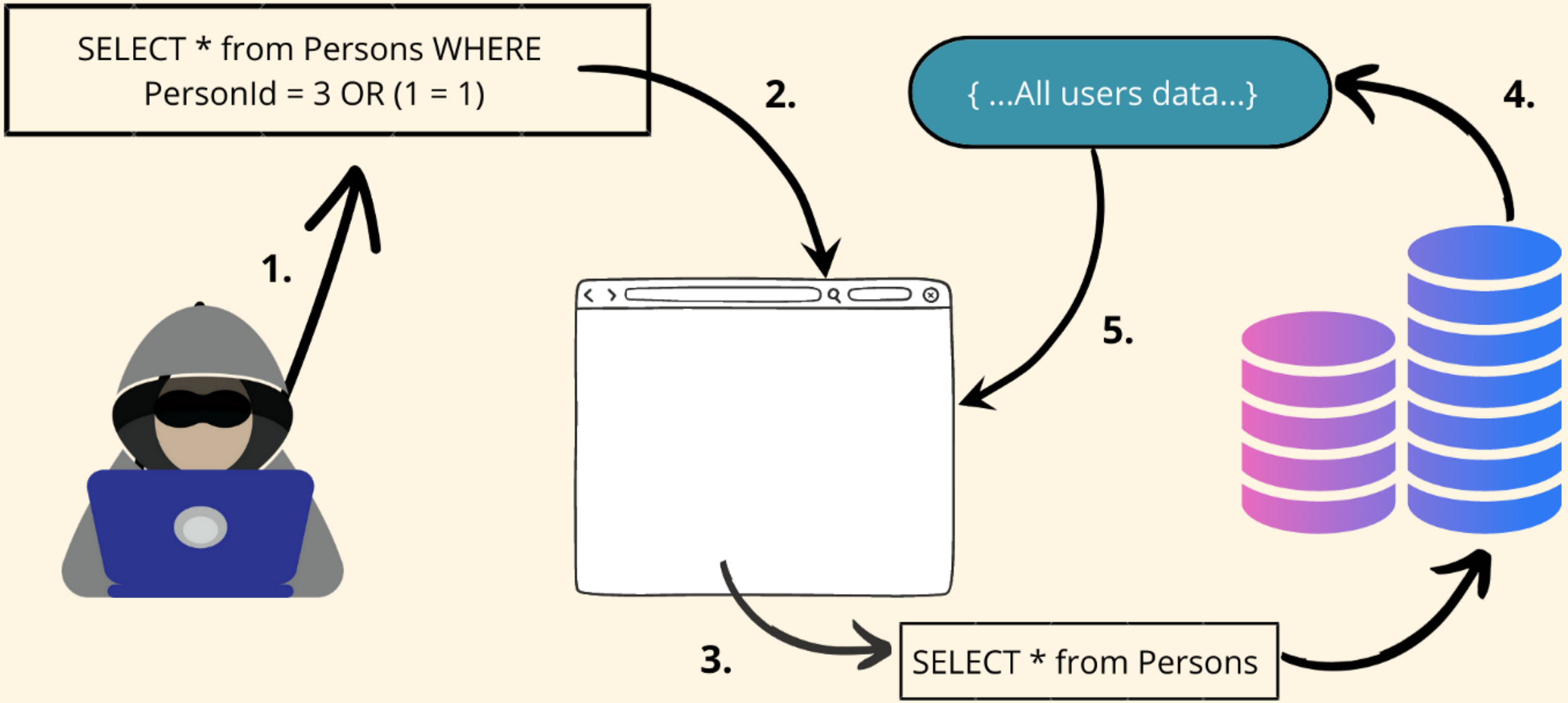
02

03

HACKER

3. Hacker is granted access to view and alter records or potentially act as database administrator

DATABASE



The addition of 1=1 in the SQL query by the hacker modifies the actual query and all the user data is fetched as 1=1 always holds true

malicious file execution

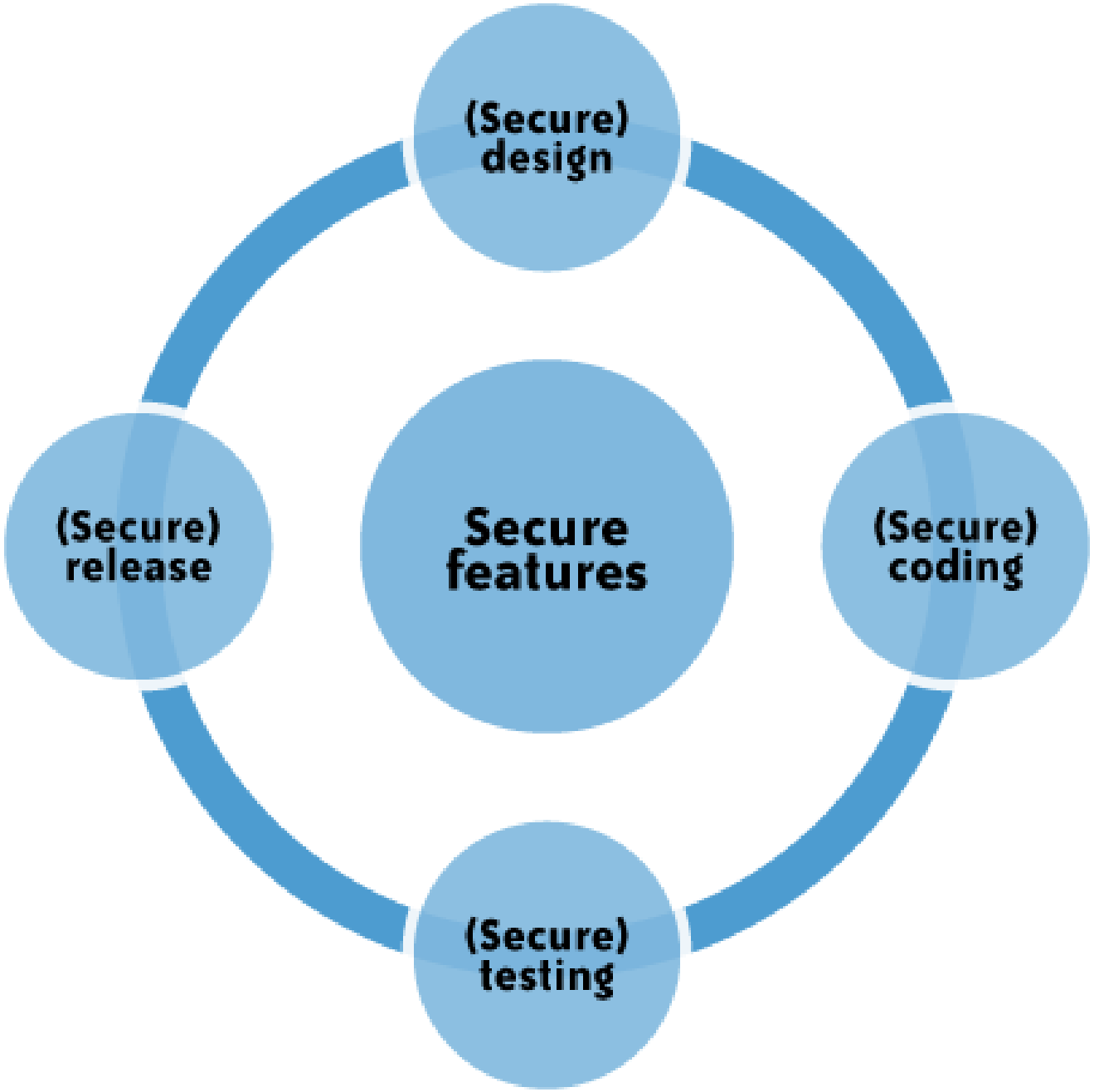
- **Malicious file execution** attacks are the attacks associated with users uploading harmful **malicious code on the internet-facing website and the execution of the malicious code causing harm to the computer network system.**
- Malicious file execution attacks are based on the principle that websites and web applications become more dangerous because they have **granted access to users to upload files on them**.
- Accepting files from the user makes the websites vulnerable to the execution of malicious files within them.

Application-Level Security Threats

- Armed with knowledge and tools, hackers are constantly scanning web applications (accessible from the Internet) for application vulnerabilities.
- They are then exploiting the vulnerabilities they discover for various illegal activities including **financial fraud, intellectual property theft, converting trusted websites into malicious servers** serving client-side exploits**, and phishing scams**.
- All web frameworks and all types of web applications are at risk of web application security defects, ranging from insufficient validation to application logic errors.

Application-Level Security Threats

- It has been **a common practice** to use a **combination of perimeter security controls and network- and host-based access controls** to protect web applications deployed in **a tightly controlled environment**, including **corporate intranets and private clouds**, from external hackers.
- Web applications built and deployed in a **public cloud** platform will be subjected to a **high threat level**, attacked, and potentially exploited by hackers to support fraudulent and illegal activities.
- In that threat model, web applications deployed in a **public cloud must be designed** for an Internet threat model, and **security must be embedded** into the **Software Development Life Cycle (SDLC**);


(Secure) design
(Secure) coding
(Secure) testing
(Secure) release
Secure features

DoS and DDoS attacks

- Additionally, you should be cognizant of application-level **DoS and DDoS attacks** that can potentially disrupt cloud services for an extended time.
- These attacks typically originate from **compromised computer systems** attached to the Internet (routinely, **hackers hijack and control computers infected by way of viruses/worms/malware** and, in some cases, powerful unprotected servers).
- Application-level DoS attacks could manifest themselves as high-volume web **page reloads**, XML* **web services requests** (over HTTP or HTTPS), or **protocol-specific requests supported by a cloud service**.
- Since these **malicious requests blend with the legitimate traffic**, it is extremely **difficult to selectively filter** the malicious traffic without impacting the service as a whole.
- For example, a DDoS attack on Twitter on August 6, 2009, brought the service down for several hours.

Economic denial of sustainability (EDoS)

- Apart from disrupting cloud services, **resulting in poor user experience and service-level impacts**, DoS attacks can quickly drain your **company's cloud services budget.**
- DoS attacks on **pay-as-you-go cloud** applications will result in a dramatic increase in your cloud utility bill:
- you'll see increased use of network bandwidth, CPU, and storage consumption.
- This type of attack is also being characterized as *economic denial of sustainability (EDoS)*

End User Security

- You, as a customer of a cloud service, are responsible for end user security tasks—**security procedures to protect your Internet-connected PC—and** for practicing "safe surfing."
- Protection measures include use of security software, such as **anti-malware, antivirus, personal firewalls, security patches, and IPS-type software** on your Internet-connected computer.
- All Internet **browsers routinely suffer from software vulnerabilities** that make them vulnerable to end user security attacks.
- Hence, cloud customers take appropriate **steps to protect browsers from attacks**. To achieve end-to-end security in a cloud, it is essential for customers to maintain good browser hygiene.
- The means keeping the browser **patched and updated** to mitigate threats related to browser vulnerabilities.
- Currently, **although browser security add-ons are not commercially available**, users are encouraged to **frequently check their browser vendor's website for security updates, use the auto-update feature, and install patches on a timely basis to maintain end user security**

Who Is Responsible for Web Application Security in the Cloud?

- SAAS-
- Role of providers
- Role of customers- user access, authentication
  - NDA
  - Third party penetration
  - Google docs security –use case
  - Strong password policy
  - Data tags

PAAS

- Security of the PaaS platform itself (i.e., runtime engine) –csp
  - PaaS application container- multi tenant, new bugs and threats
- Security of customer applications deployed on a PaaS platform- third party service providers.
  - Customer-Deployed Application Security- NO API standard

IaaS Application Security

customers have full responsibility

basic guidance and features related to firewall policy