2022 计算思维通识教育

Computational Thinking

第5章 信息如何在互联网上传播

How Information Travels on the Internet

为什么要学习互联网的原理？互联网的设计、运行方式、管理方式、协议算法，处处都体现了计算思维是如何解决复杂问题的。

主讲人：曹轶臻

联系方式：caoyizhen@cuc.edu.cn

互联网的设计、运行方式、管理方式、协议算法，处处都体现着计算思维是如何解决复杂问题的

CONTENTS

The Guardian's John Naughton provided a really nice definition of computational thinking :" …computer science involves a new way of thinking about problem-solving: ... about thinking recursively, being alert to the need for prevention, detection and protection against risks ..."

对风险的预防、检测和保护的需要保持警惕

计算机与网络空间安全学院
School of Computer and Cyber Sciences

计算思维通识教育
Computational Thinking

04

面对攻击的网络

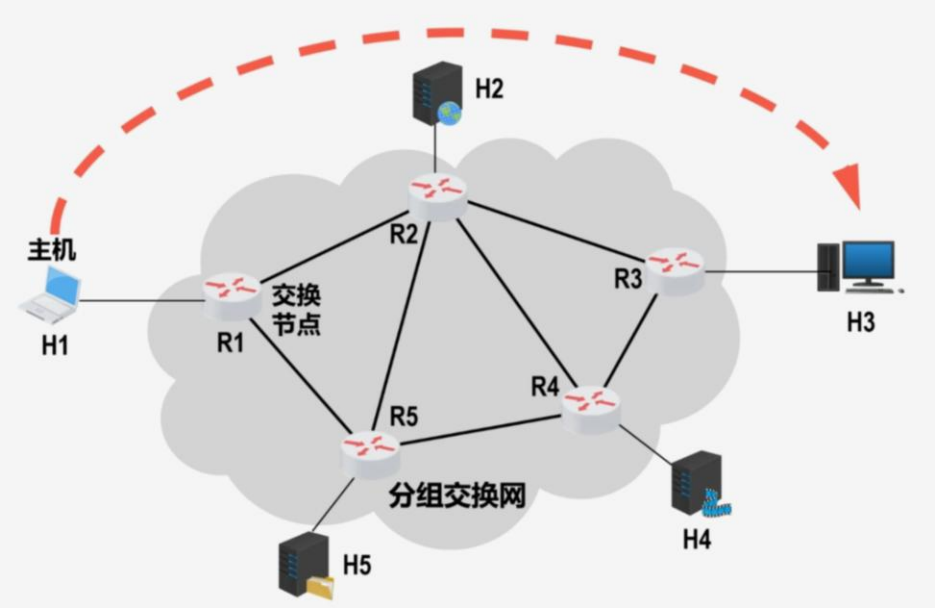
坏家伙们攻击网络的方法 4-1

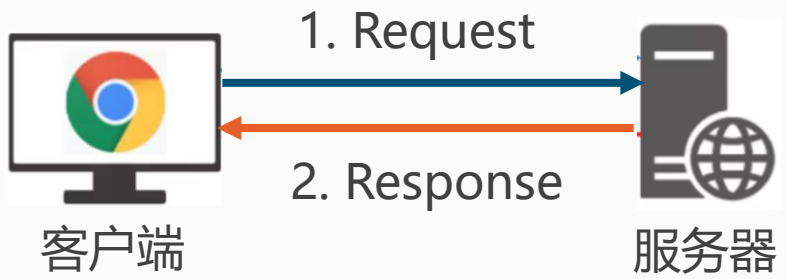
保护网络安全的方法 4-2

计算机与网络空间安全学院
School of Computer and Cyber Sciences

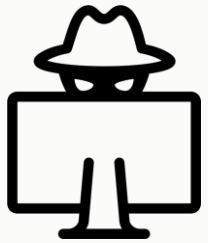
4-1 坏家伙们攻击网络的方法

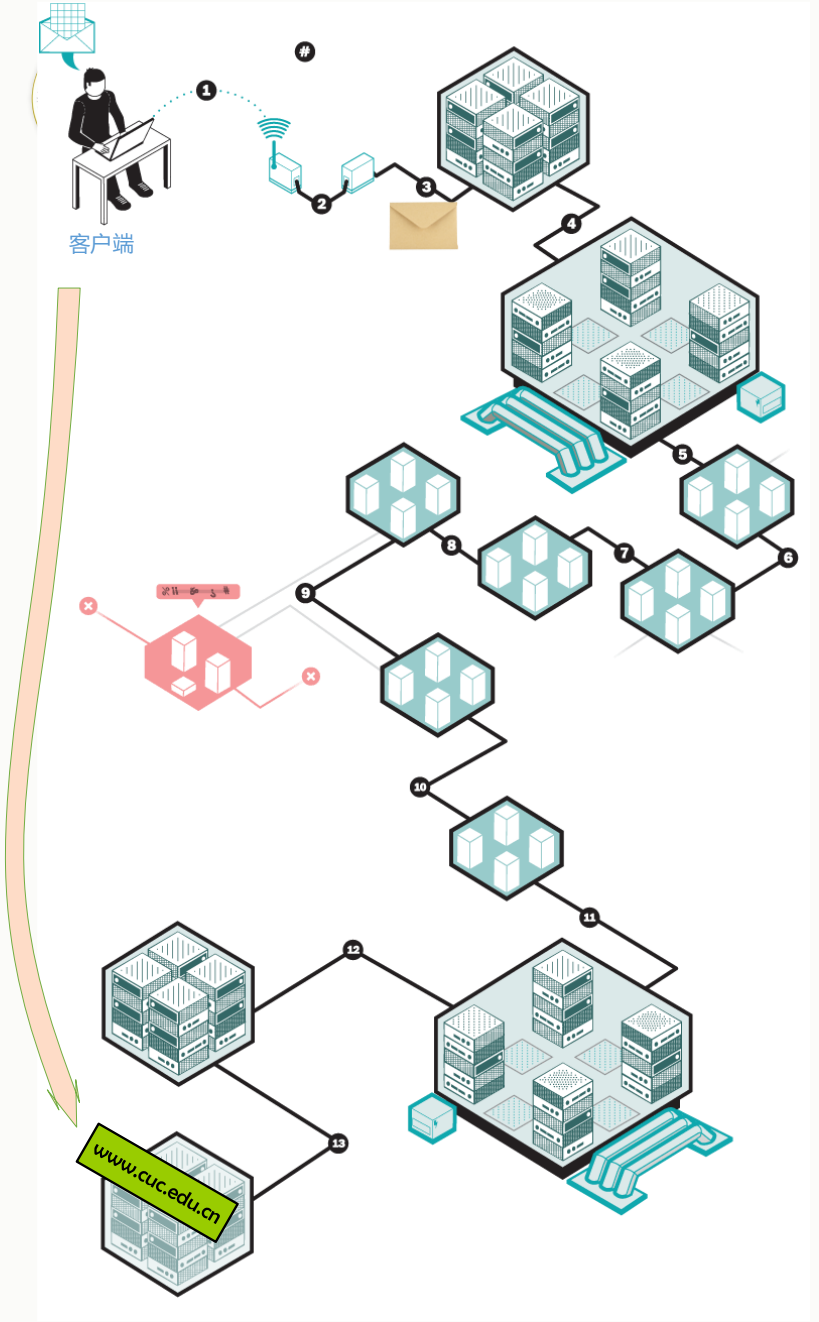
Application	HTTP、DNS...
Transport	**TCP、UDP**...
Network	IPv4/v6、ICMP...
Network Interface	No specific protocols defined





How would you attack the internet if you were a hacker ?

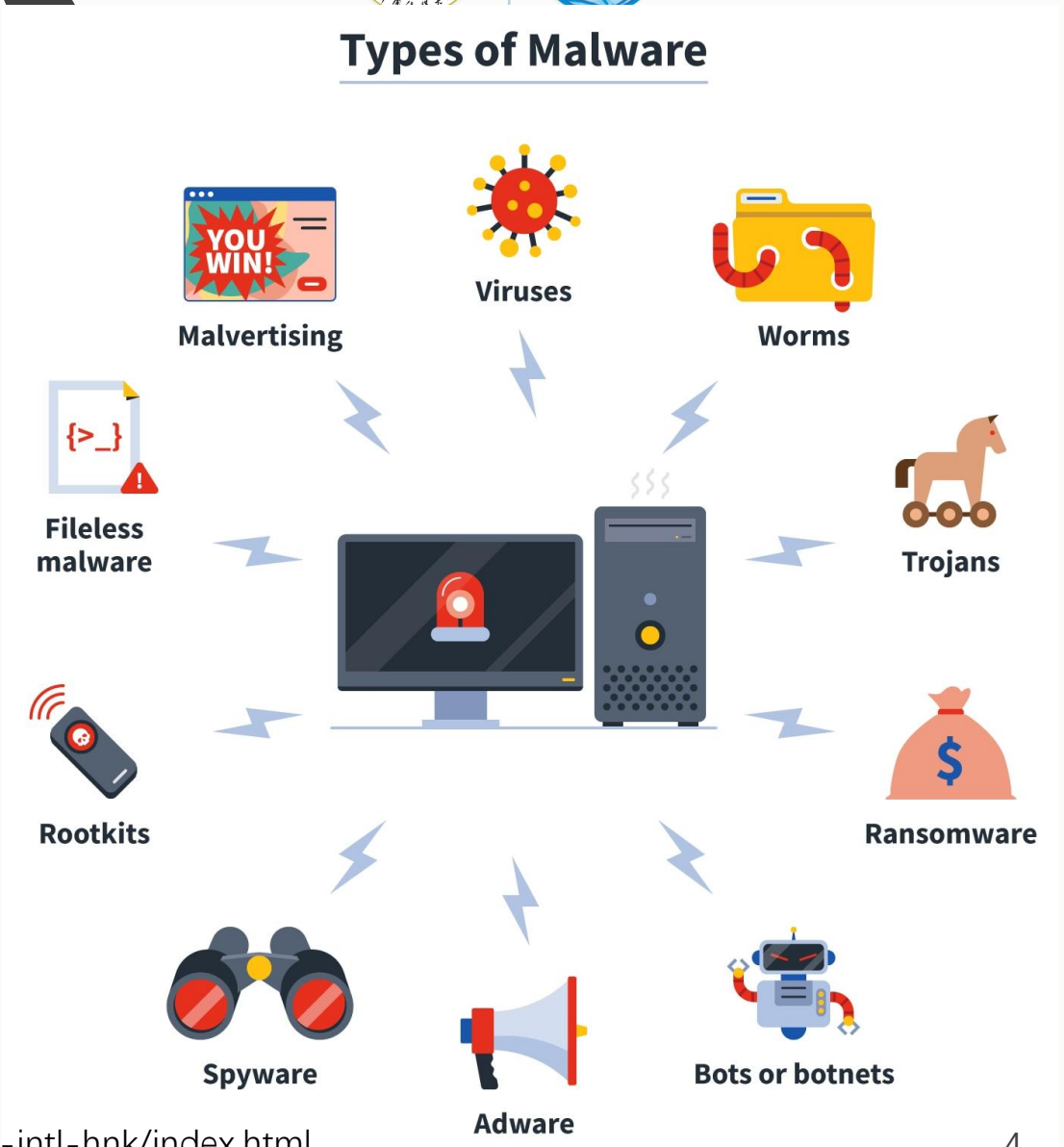




4-1 坏家伙们攻击网络的方法

1. 恶意软件（Malware）

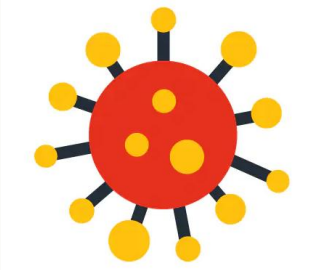
- Malware是malicious software的缩写，是网络攻击者开发的软件，通常是在受害者不知情的情况下获取访问权限或对计算机或网络造成损害。
- 恶意软件攻击的最终目标通常是相同的——获取个人信息或损坏设备，通常是为了经济利益。
- 最常见的恶意软件类型包括病毒、蠕虫、木马、勒索软件、机器人或僵尸网络、广告软件、间谍软件、无文件恶意软件和恶意广告。



图源：https://edition.cnn.com/2020/05/01/tech/iloveyou-virus-computer-security-intl-hnk/index.html

4-1 坏家伙们攻击网络的方法

1. 恶意软件（Malware）



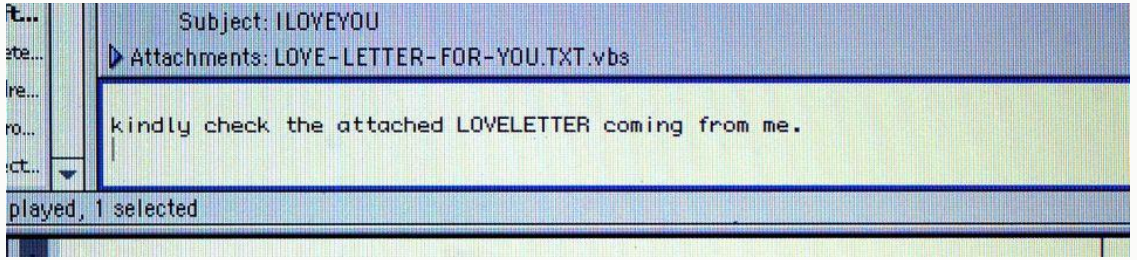
- 计算机病毒（Computer Virus）是在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机正常使用并且能够自我复制的一组计算机指令或程序代码。

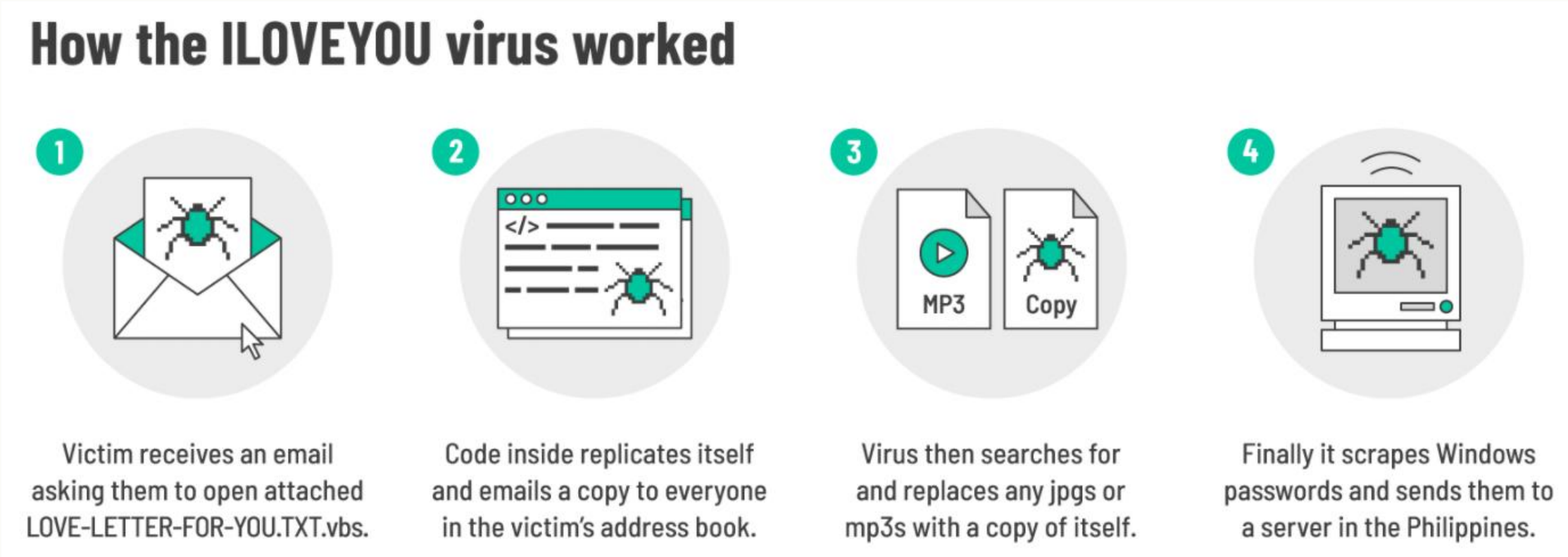
- 计算机病毒具有传染性、隐蔽性、感染性、潜伏性、可激发性、表现性或破坏性。
- 它们处于休眠状态，直到触发攻击，可能是用户下载了电子邮件附件——通常是 .exe 文件，代表“可执行”文件。
- 病毒与身体病毒相似，因为它们需要宿主（即设备）才能生存。
- 病毒从那里开始复制，将自身的副本从一台计算机传播到另一台计算机，造成最严重的破坏。

4-1 坏家伙们攻击网络的方法

1. 恶意软件（Malware）

- ILOVEYOU 病毒，2000 年

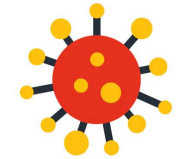




图源：https://edition.cnn.com/2020/05/01/tech/iloveyou-virus-computer-security-intl-hnk/index.html

4-1 坏家伙们攻击网络的方法

1. 恶意软件（Malware）

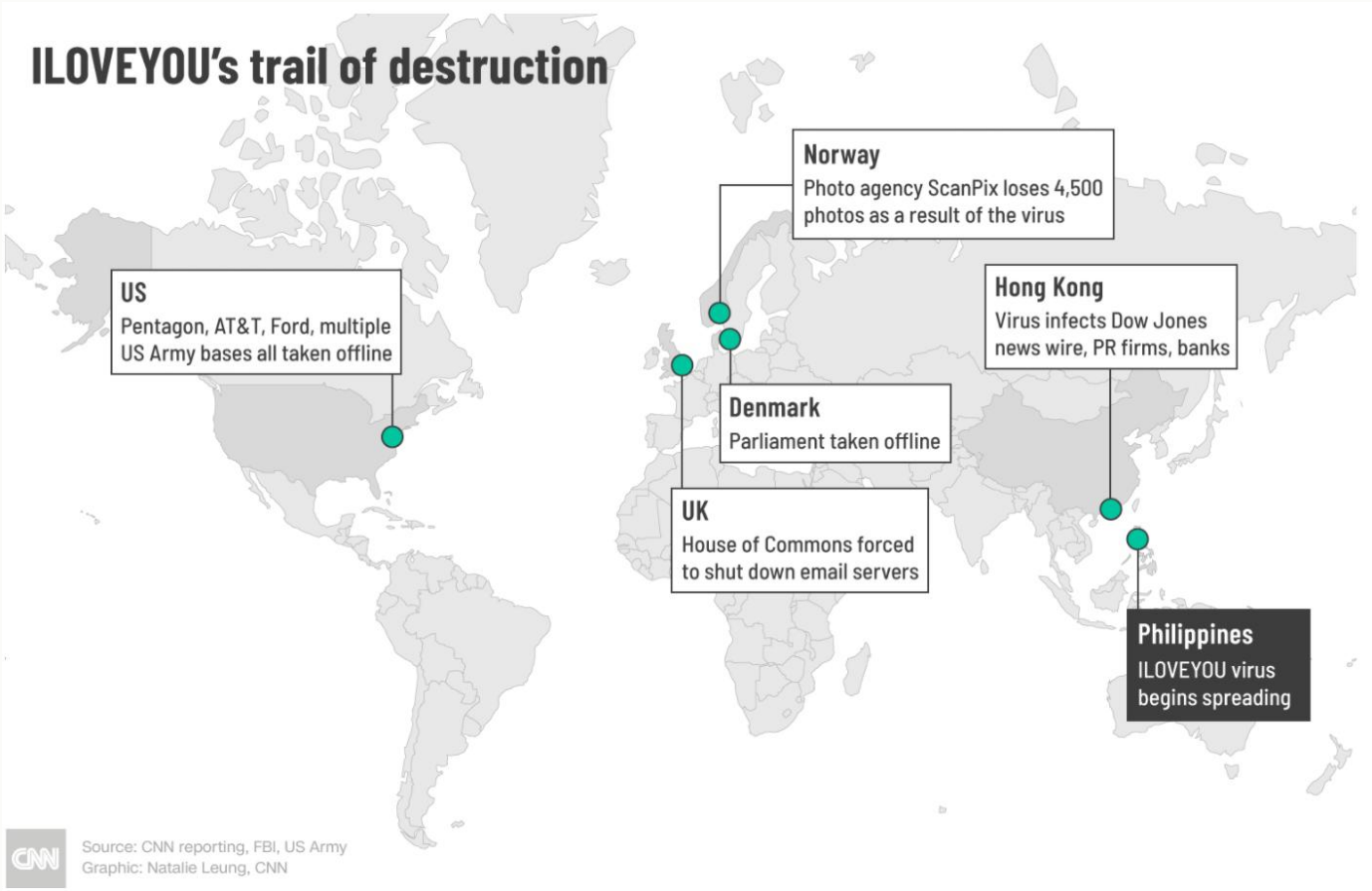


- ILOVEYOU 病毒，2000 年

导致世界各地的企业和政府机构的运营中断，从福特到美林证券再到五角大楼和英国议会无一幸免，造成了估计100亿美元的损失。

尽管计算机安全和技术在过去20年里取得了进步，但它暴露的漏洞人类至今仍在应对。

“你可以更新你的操作系统，或者你可以拥有世界上最好的电子邮件过滤器，但你无法修补人类的弱点。”



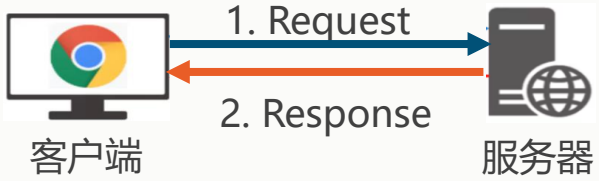
图源：https://edition.cnn.com/2020/05/01/tech/iloveyou-virus-computer-security-intl-hnk/index.html

4-1 坏家伙们攻击网络的方法

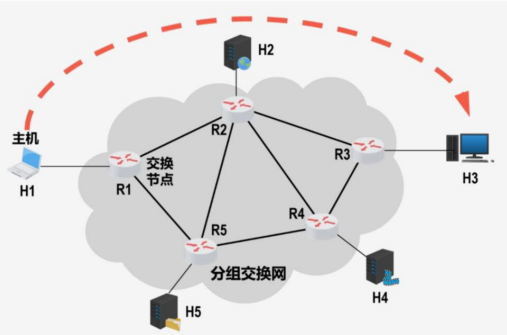
2. 拒绝服务攻击DoS/DDoS

如果说恶意软件主要针对的是个人电脑，则拒绝服务攻击(DoS, Denial of Service)则主要针对服务器，它的主要目的在于使服务器瘫痪，导致正常用户无法访问该服务器。大多数 Internet DoS 攻击属于以下三类：

① **漏洞攻击**(Vulnerability attack)：原理和恶意软件类似，都是利用软件的漏洞使目标主机系统瘫痪、崩溃，无法处理网络请求。
例如向目标主机上运行的易受攻击的应用程序或操作系统发送一些精心设计的消息，造成服务停止，或更糟，可能造成主机崩溃。



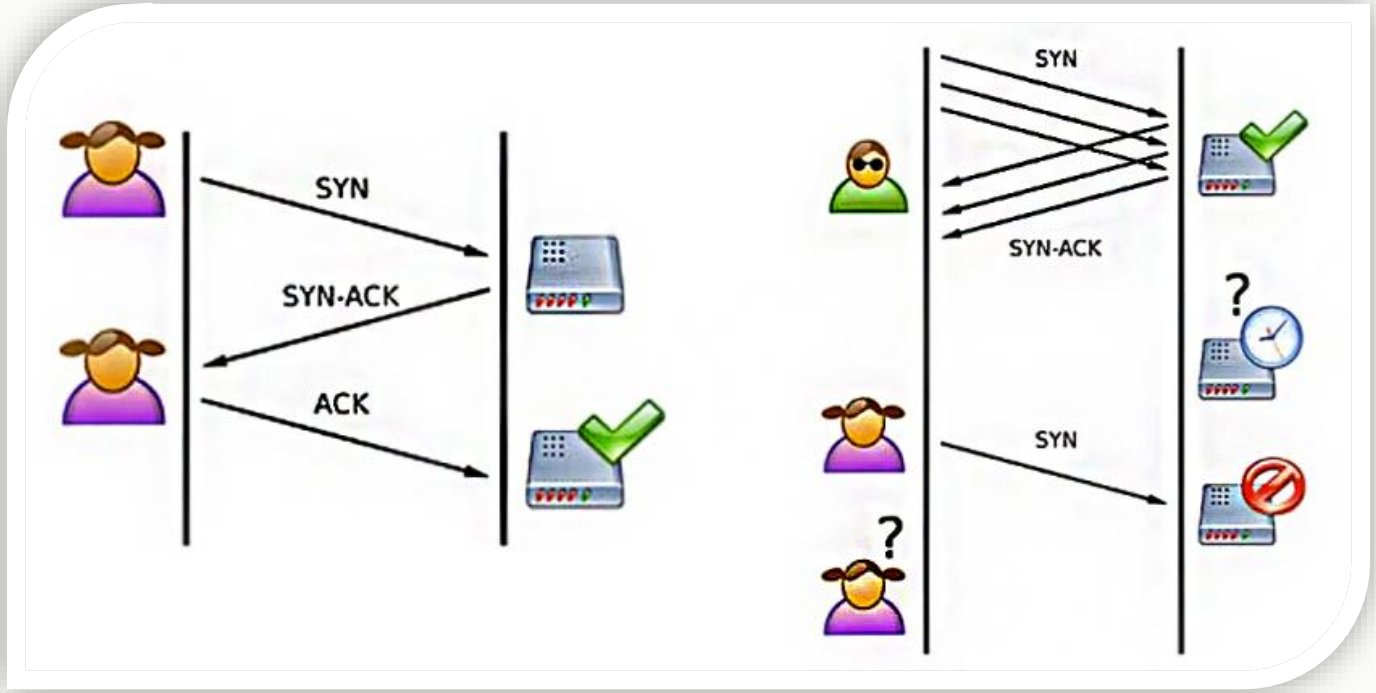
② **带宽消耗**（Bandwidth flooding）：攻击者向目标主机发送大量数据包，超过其接入网承载能力上限——导致网络拥塞，正常用户的请求无法到达服务器。



4-1 坏家伙们攻击网络的方法

2. DoS/DDoS

③ **连接消耗**(Connection flooding)，与目标服务器建立大量TCP连接，将其端口资源消耗殆尽，正常用户无法与服务器建立TCP连接。



例如： SYN Flood

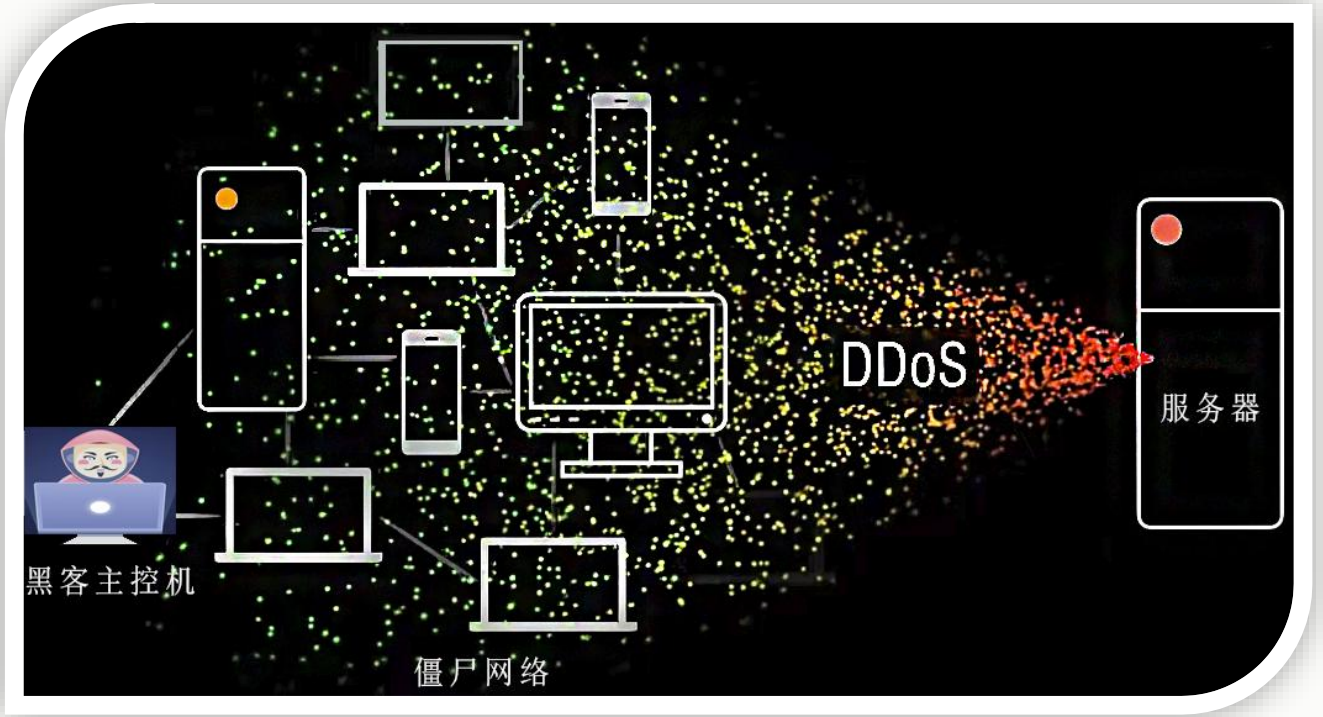
SYN Flood 攻击是黑客与服务器建立了多个半连接，致使服务器的性能受到严重限制，甚至崩溃。

4-1 坏家伙们攻击网络的方法

2. DoS/DDoS

- 如果从单一源发出所有流量，某上游路由器就能够检测出该攻击并在该流量靠近服务器之前就将其阻挡下来。

- 坏家伙想出更厉害的办法，将多台计算机联合起来作为攻击平台，通过远程连接利用恶意程序，**对一个或多个目标发起分布式拒绝服务（DDoS, Distributed DoS）攻击**，消耗目标服务器性能或网络带宽，从而造成服务器无法正常地提供服务。



DDoS攻击充分利用由数以千计的受害主机组成的僵尸网络botnets，控制僵尸网络同时对某服务器进行攻击，造成目标机器的网络堵塞，使得目标机不能正常工作，甚至瘫痪。这在今天是屡见不鲜的。相比于来自单一主机的DoS 攻击，DDoS攻击更加难以检测和防范。

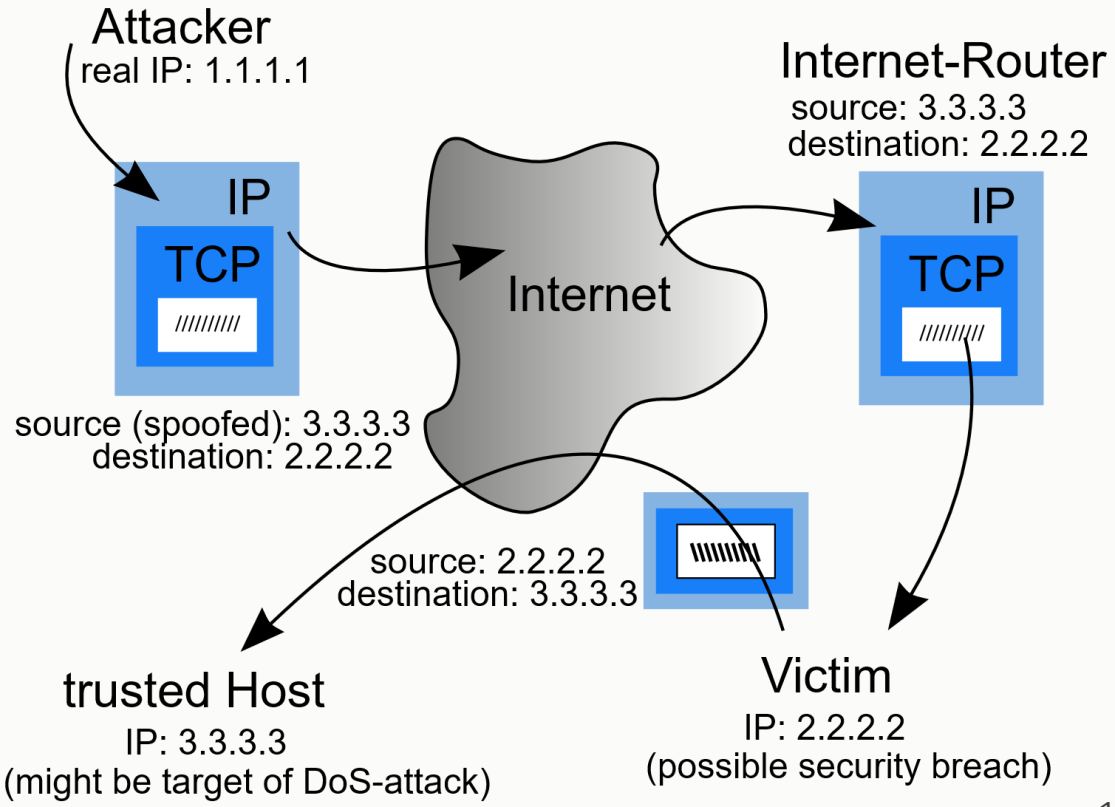
4-1 坏家伙们攻击网络的方法

3. IP欺骗

Dst IP：111.200.16.214
Src IP：111.192.102.170

- 防火墙可以帮我们把坏家伙的IP地址标记下来，防止来自该地址的分组到达目的主机，从而避免对目的主机的攻击。

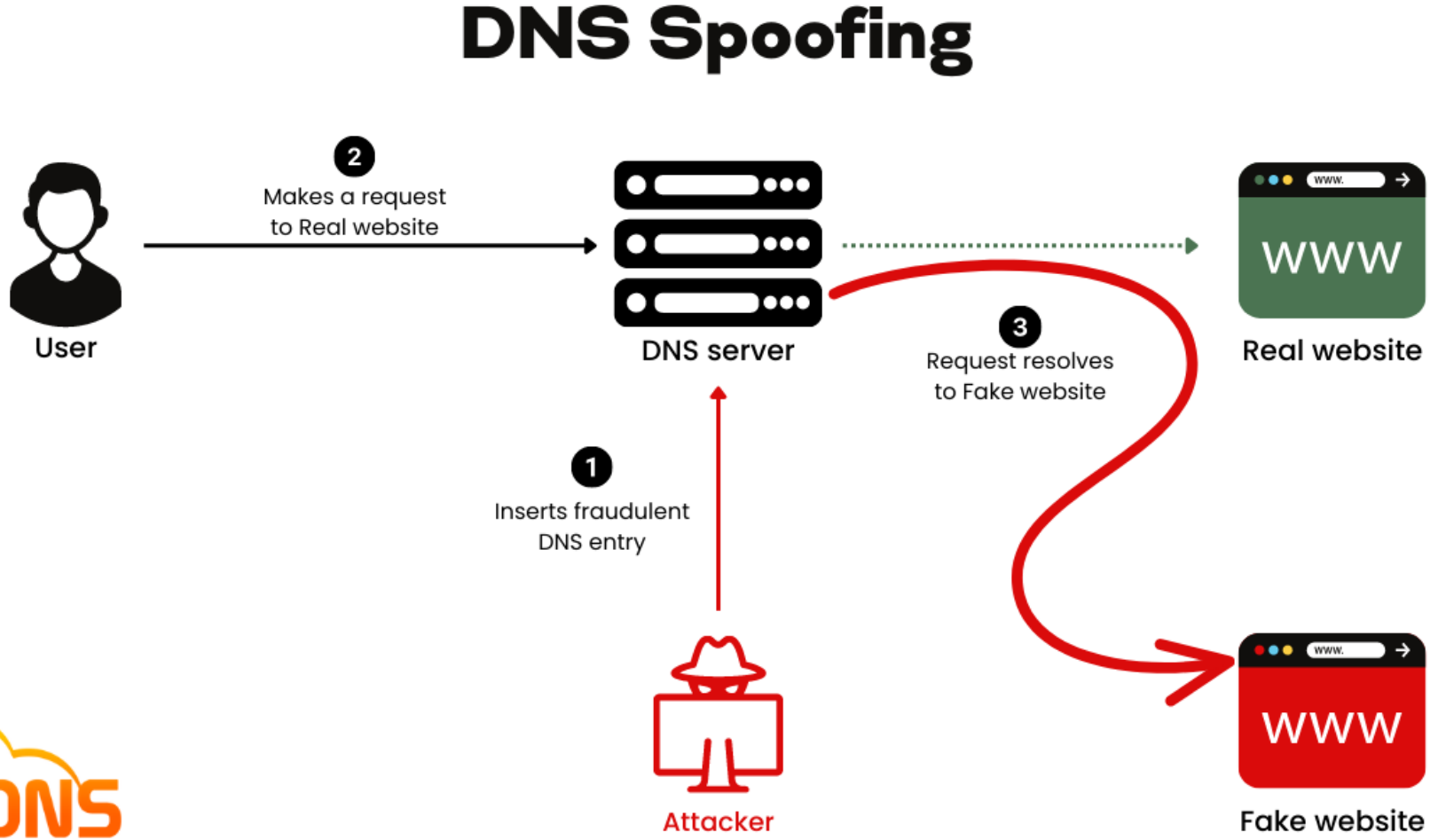
- 然而有一些坏家伙生成**具有任意源地址、分组内容和目的地址的分组**，然后将这个人工制作的分组传输到互联网中，互联网的路由器则把这些分组转发到目的地。目的节点收到这样的分组，会毫不怀疑地进行处理并执行分组中的命令。



4-1 坏家伙们攻击网络的方法

4. DNS欺骗

DNS欺骗的基本原理：如果可以冒充域名服务器，然后把查询的IP地址设为攻击者的IP地址，这样的话，用户上网就只能看到攻击者的主页，而不是用户想要取得的网站的主页了。DNS欺骗其实并不是真的“黑掉”了对方的网站，而是冒名顶替、招摇撞骗。



图源：https://www.cloudns.net/blog/dns-spoofing-dns-poisoning/

4-1 坏家伙们攻击网络的方法

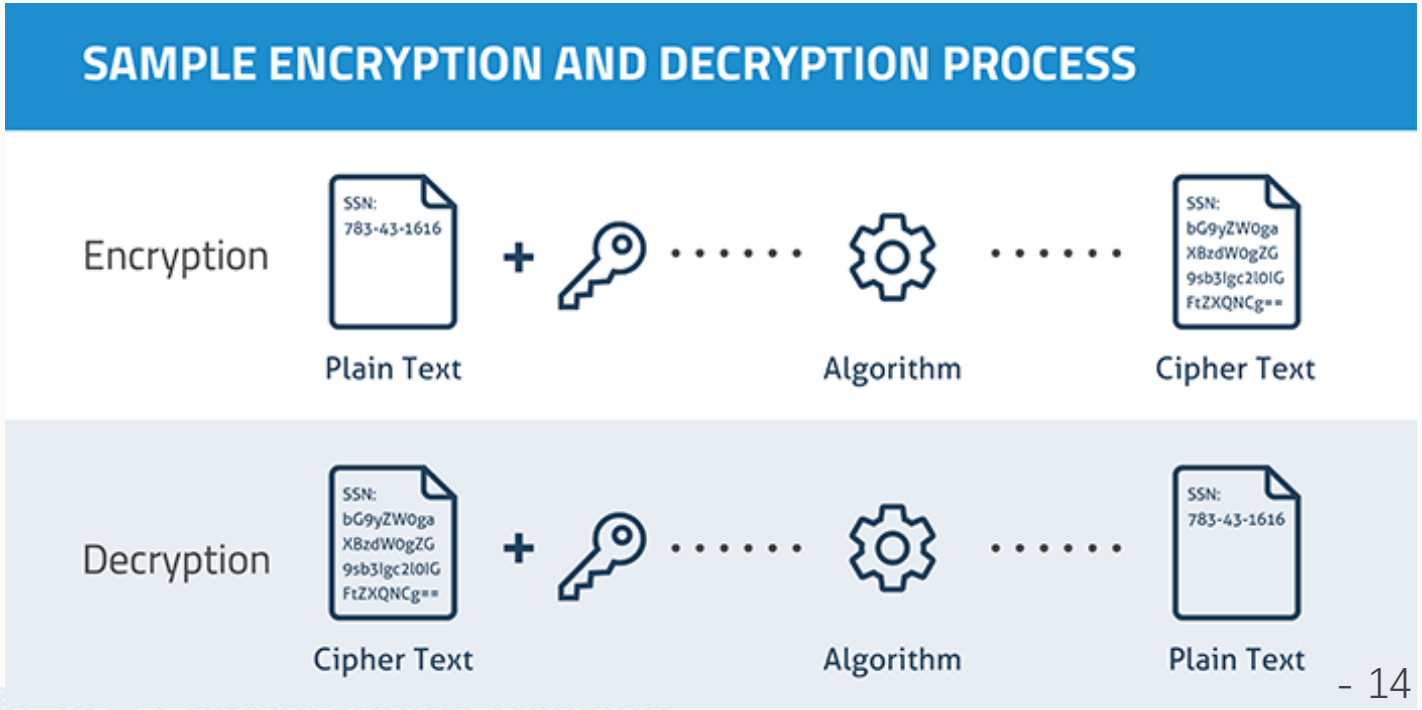
最初的计算机网络是相对封闭的环境，连接进入网络的节点都是相互信任的，之后发展为无太多限制、可以匿名的全球性互联网，才出现了IP欺骗、病毒、网络攻击等诸多问题。

4-2 保护网络安全的方法

1.加密技术与身份认证技术

- 一般情况下，网页访问、电子邮件等互联网上流动的数据不会被加密。另外，互联网中这些数据经由哪些路径传输也不是传输者可以预知的内容。
- 因此，无法避免这些信息泄露给第三方。为了防止这种信息的泄露，实现机密数据的传输，出现了各种各样的加密技术。

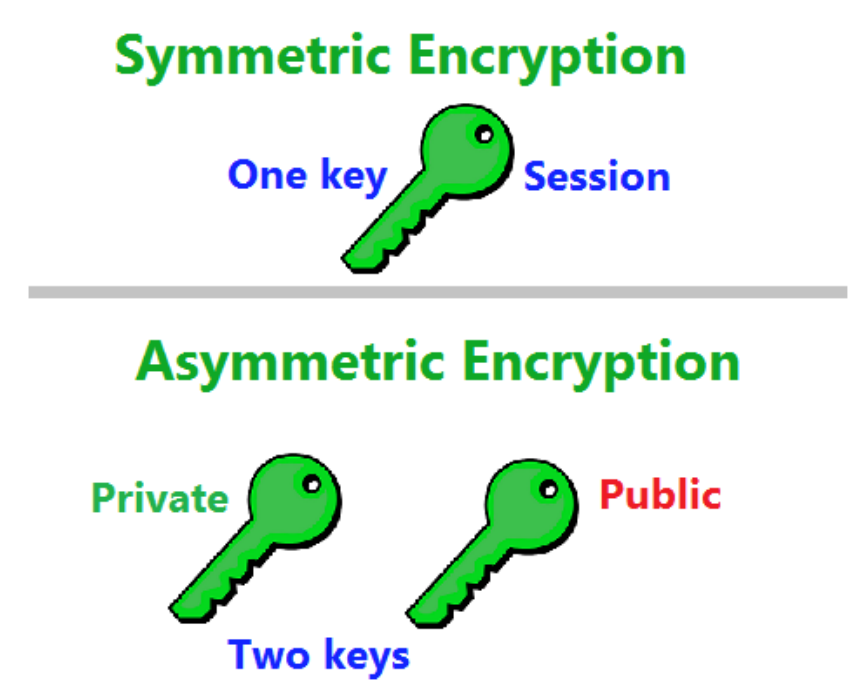
加密(Encryption)是指利用某个值（密钥）对明文(Pain Text)的数据通过一定的算法变换成加密数据（密文(Cipher Text)）的过程。它的逆过程叫做解密(Decryption)。

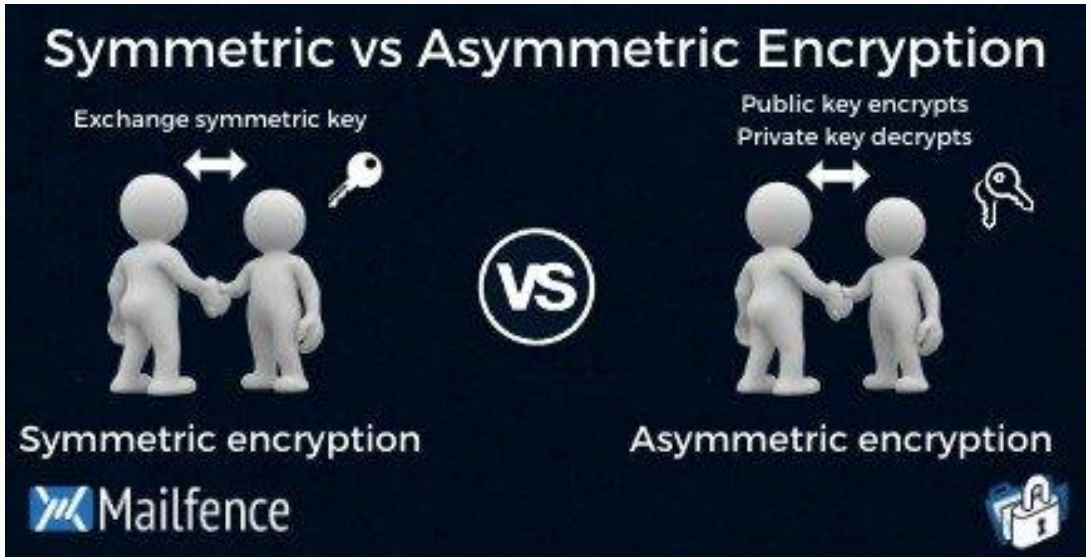


4-2-1 加密技术与身份认证技术

1. 对称加密（Symmetric Encryption） 与 非对称加密(Asymmetric Encryption)

- 加密和解密使用相同的密钥（key）叫做对称加密方式（共享密钥加密）。如果在加密和解密过程中分别使用不同的密钥（公钥public key和私钥private key）则叫做非对称加密（公钥加密）方式。

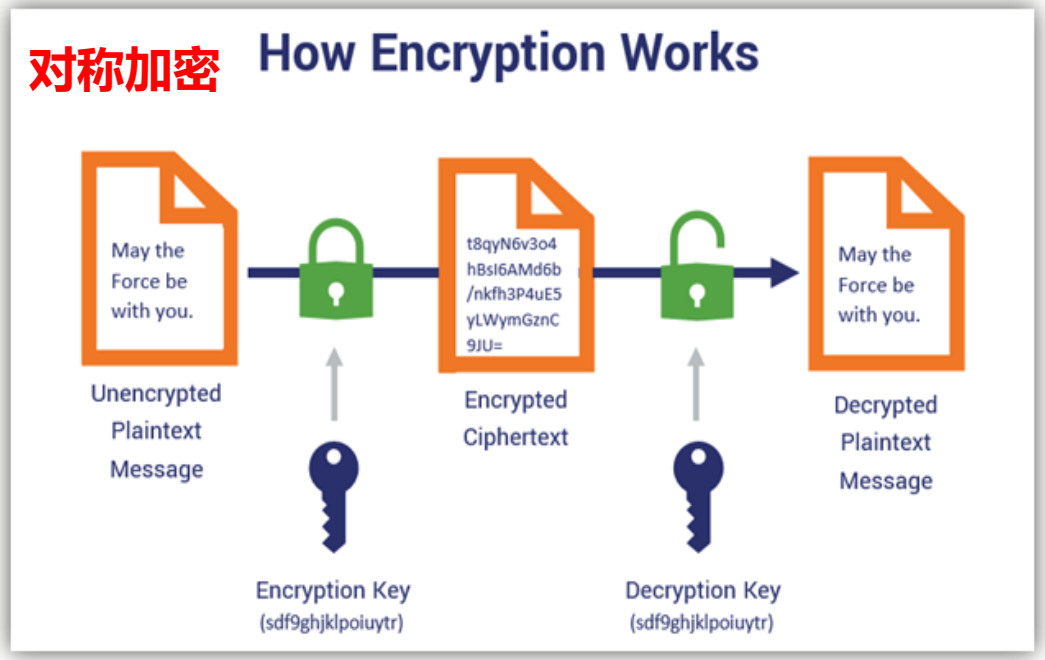




4-2-1 加密技术与身份认证技术

计算机与网络空间安全学院
School of Computer and Cyber Sciences

1. 对称加密 与 非对称加密



在对称加密方式中，最大的挑战就是如何传递安全的密钥。

```python
from cryptography.fernet import Fernet

# 待加密的数据.
message = "Hello CUCers！"

# 生成一个用于加密和解密的密钥
key = Fernet.generate_key()
fernet = Fernet(key)

# 使用上面的密钥对数据进行加密得到密文
encMessage = fernet.encrypt(message.encode())
print("original string: ", message)
print("encrypted string: ", encMessage)

# 使用相同的密钥解密密文
decMessage = fernet.decrypt(encMessage).decode()
print("decrypted string: ", decMessage)
```

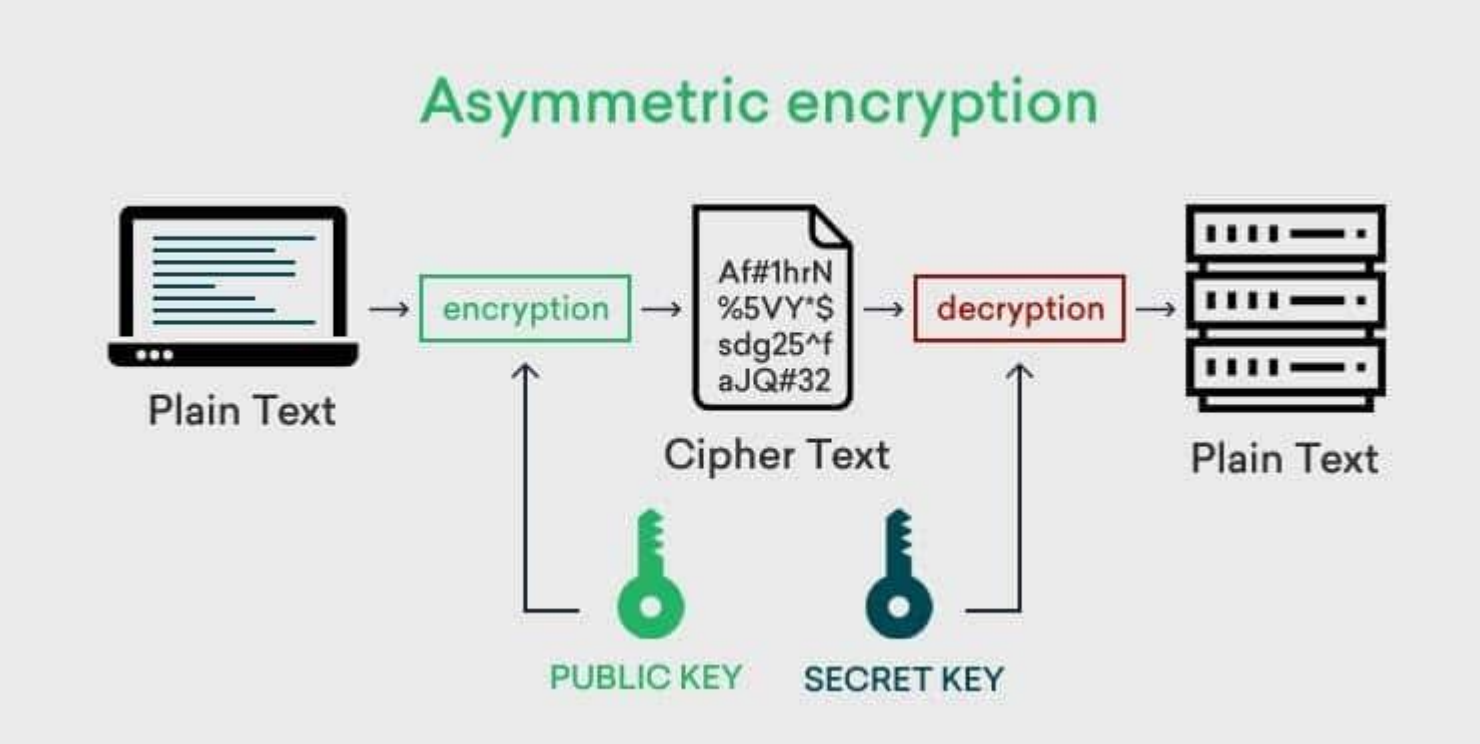
```
original string:  Hello CUCers!
encrypted string:  b'gAAAAABjnW54GjlrfTeMKyXFfszR983Q_HbgTSbJDRbFPX8m_-Mfa1IKhYFW57KSmCqIP_Pamic2H_xdMFM6vpact6klcsBpQA=='
decrypted string:  Hello CUCers!
```

4-2-1 加密技术与身份认证技术

1. 对称加密 与 非对称加密

- 如果在加密和解密过程中分别使用不同的密钥（公钥和私钥）则叫做非对称加密。

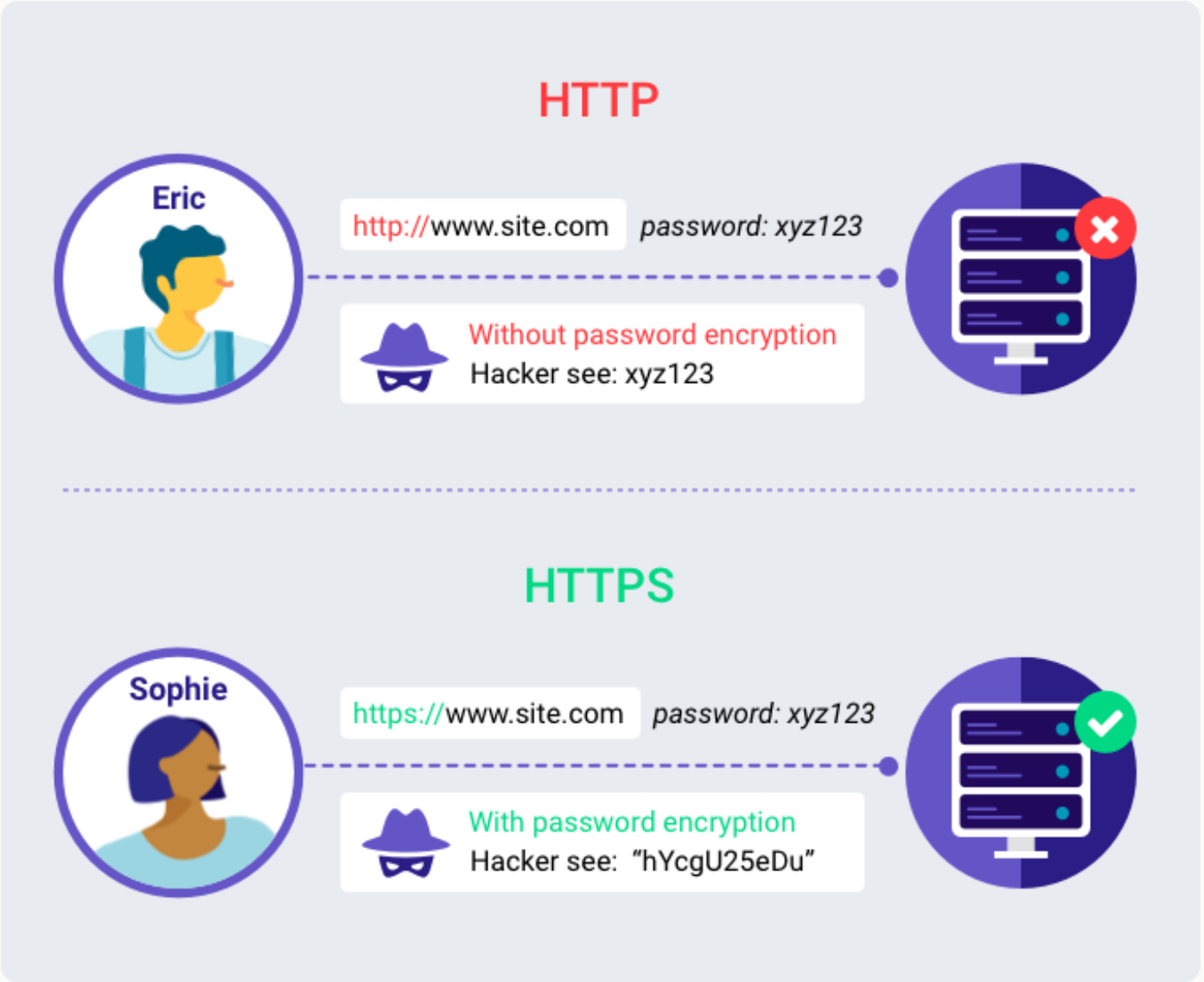
公钥可以公开，可任意向外发布；私钥不可以公开，必须由用户自行严格秘密保管，绝不透过任何途径向任何人提供，也不会透露给被信任的要通信的另一方。



4-2-1 加密技术与身份认证技术

对称加密与非对称加密的应用

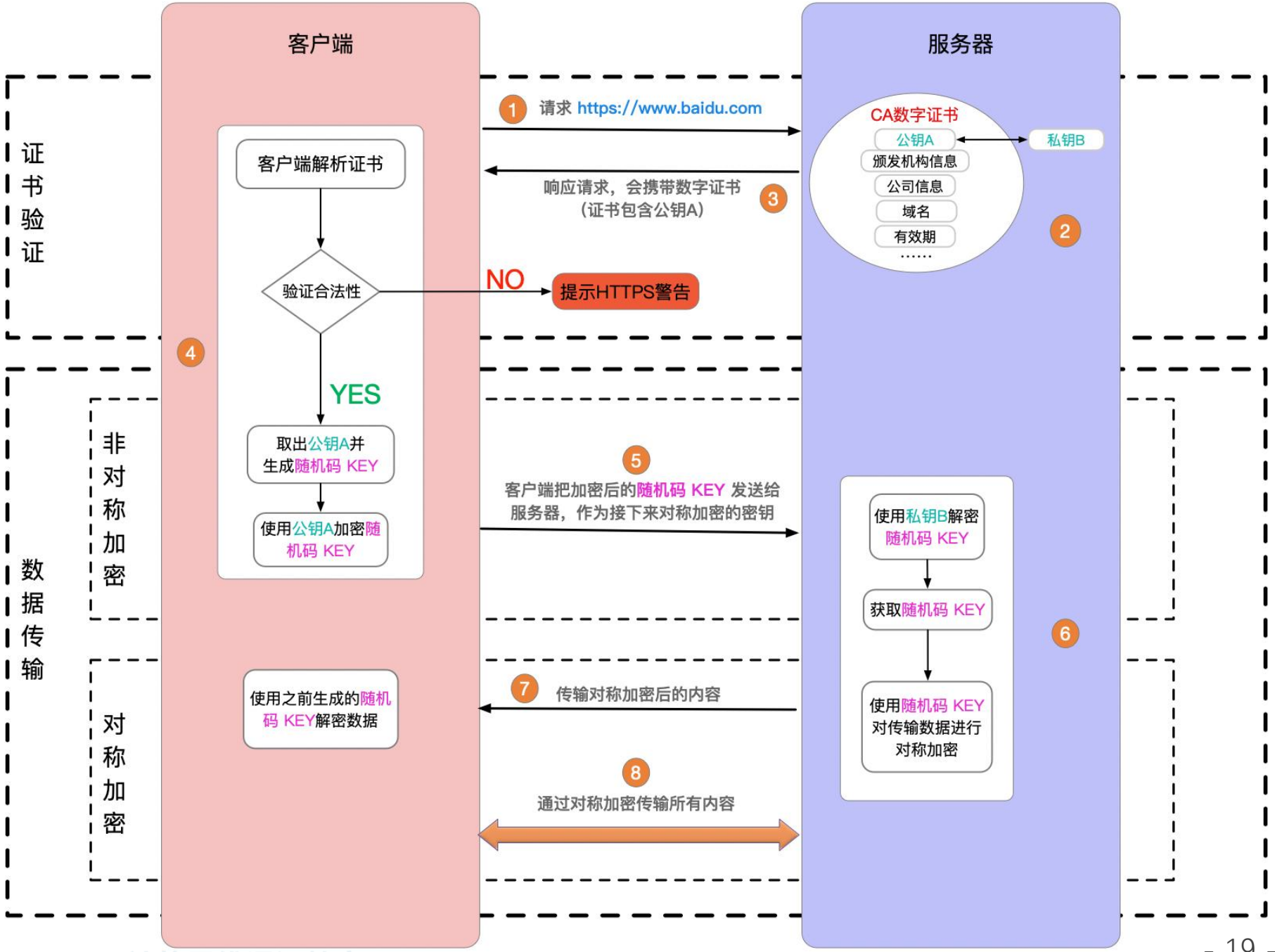
以HTTPS（HTTP over SSL）为例



4-2-1 加密技

对称加密与非对称加密的应用

以HTTPS（HTTP over SSL）为例

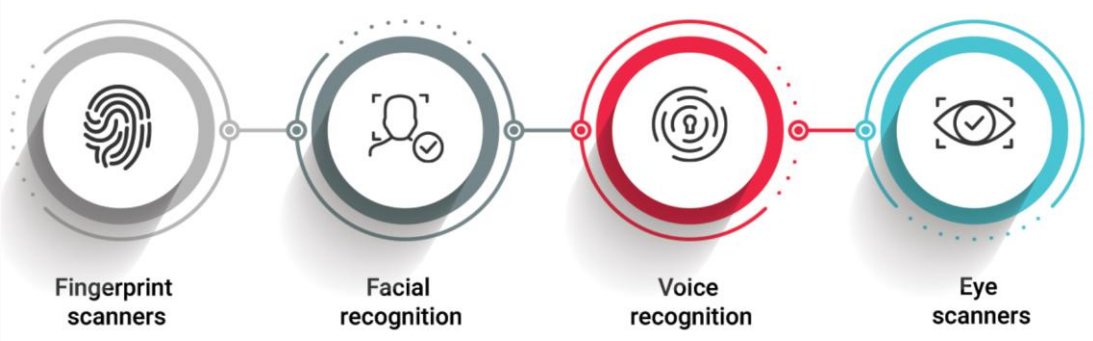


图源：https://segmentfault.com/a/1190000021494676

4-2-1 加密技术与身份认证技术

2. 身份认证技术

- 在实施系统的安全策略时，有必要验证使用者的正确性和真实性。为此，需要数据加密技术的同时，还需要身份认证（Authentication）技术。
- 可以分为以下几类：
  - **根据所知道的信息进行认证。**例如使用密码或私有代码的方式。使用公钥加密方式进行的数字认证，就需要验证是否持有私钥。
  - **根据所拥有的信息进行认证。**例如利用ID卡、密钥、电子证书、电话号码等信息的方式。在移动互联网中，可利用手机号码或终端信息进行权限认证。
  - **根据独一无二的生物特征进行认证。**

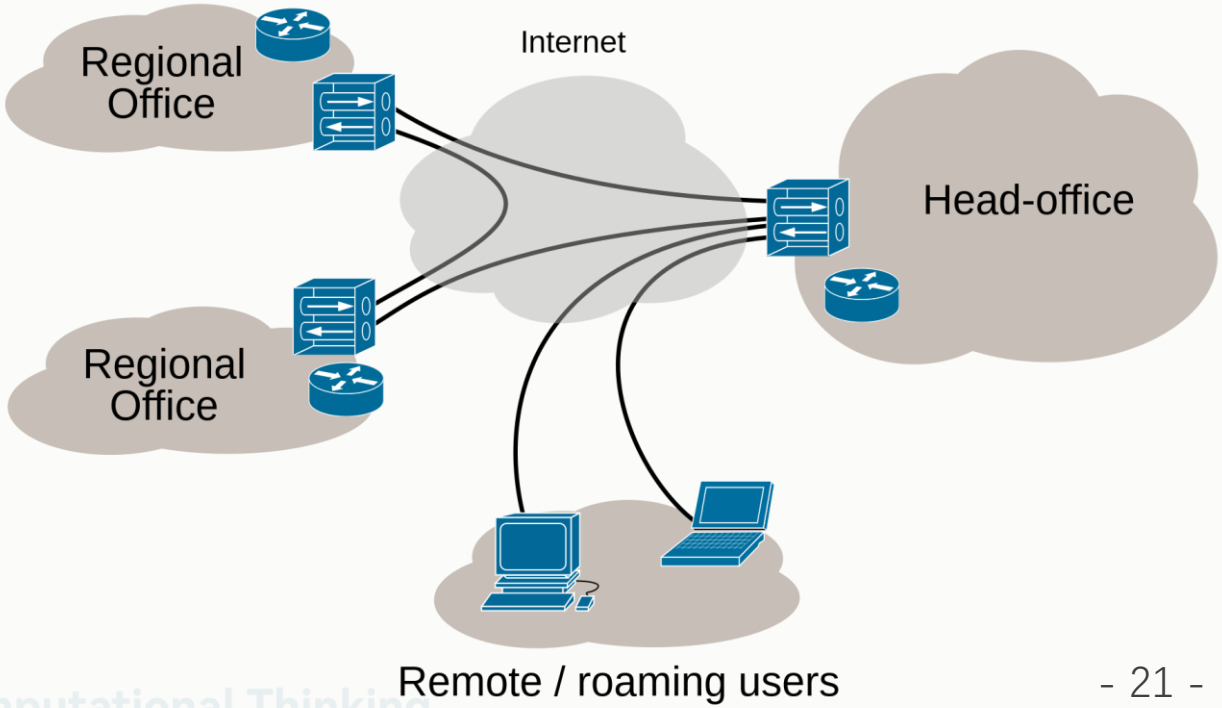


4-2-2 安全协议

1. IPsec与VPN

- 为了防止信息泄露，对机密数据的传输，一般不使用互联网等公共网络(Public Network)，而是使用**由专线连接的私有网络(Private Network)**。
  (好是好，代价太高！！)

- **VPN（Virtual Private Network，虚拟专用网）**是一种利用加密和认证技术打造的，构建在互联网这个公共网络上的私有网络。

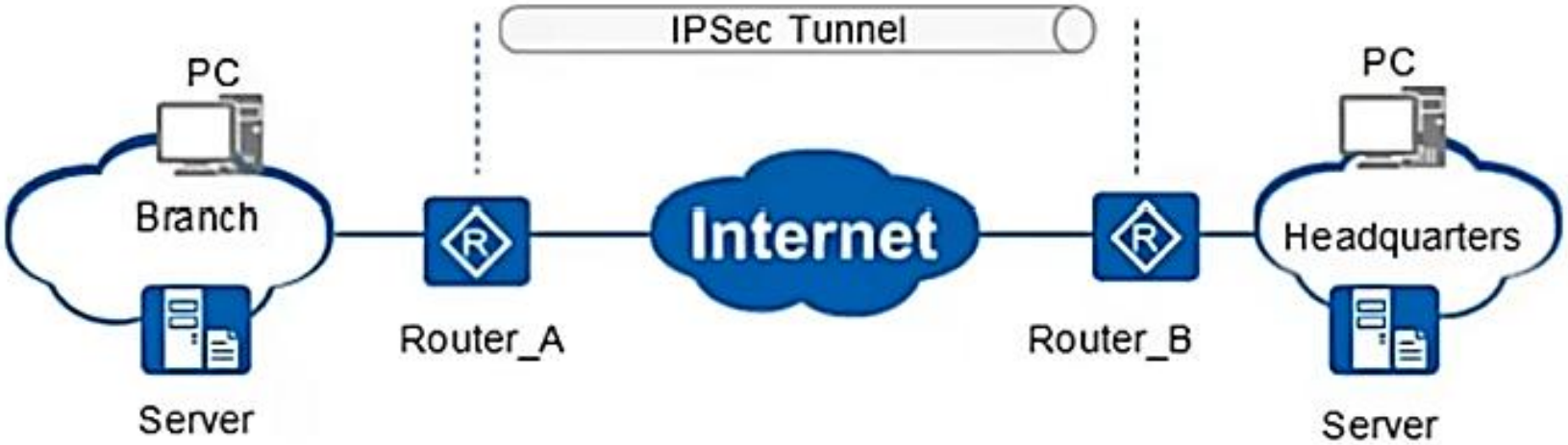


4-2-2 安全协议

1. IPsec与VPN

- 在构建VPN时，最常被使用的是**IPSec（Internet Protocol Security）协议**。它是指在IP首部的后面追加封装安全载荷和认证首部，从而对此后的数据进行加密，不被盗取者轻易解读。在发包的时候附加上述两个首部，可以在收包时根据首部对数据进行解密，恢复成原始数据。

- 基于IPsec所提供的端到端的分组通信安全功能，VPN的使用者就可以不必设防地使用一个安全的网络环境。

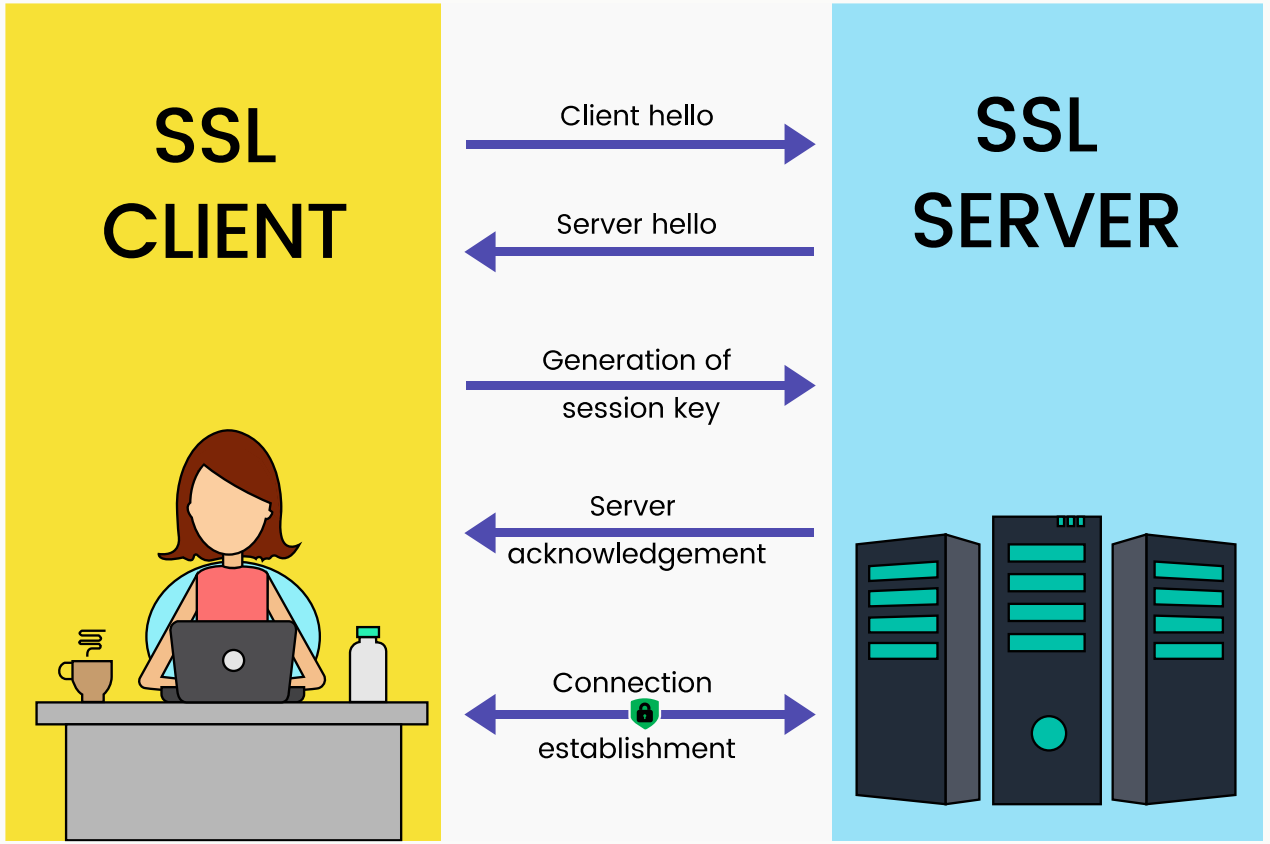


4-2-2 安全协议

2. SSL与HTTPS

- Web作为现在最主要也最重要的应用交互形式，有很多重要的信息传输，可以**通过SSL**（Secure Sockets Layer）**对HTTP通信进行加密。**

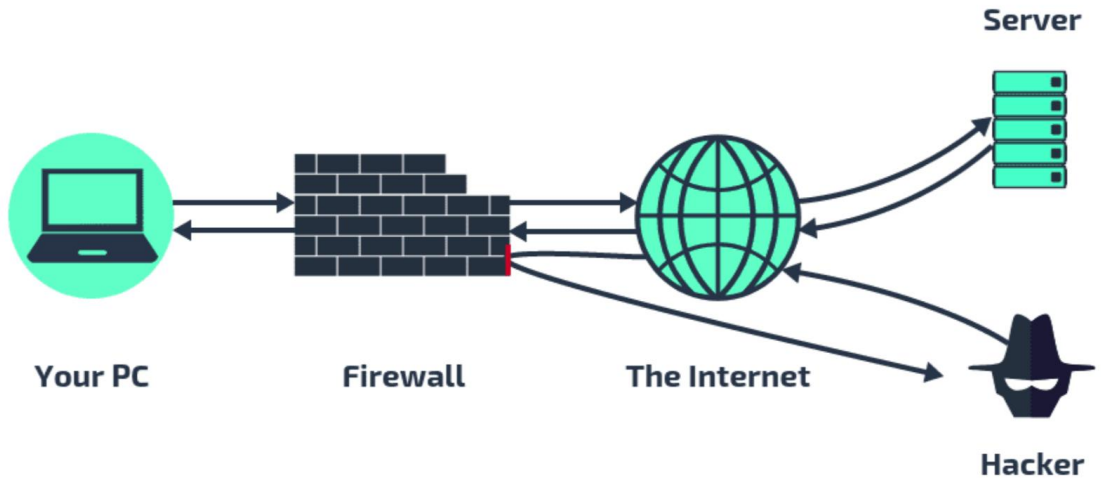
- **使用SSL的HTTP通信叫做HTTPS（超文本传输安全协议）通信**，常称为**HTTP over SSL**。HTTPS经由HTTP进行通信，但利用SSL来加密数据包。



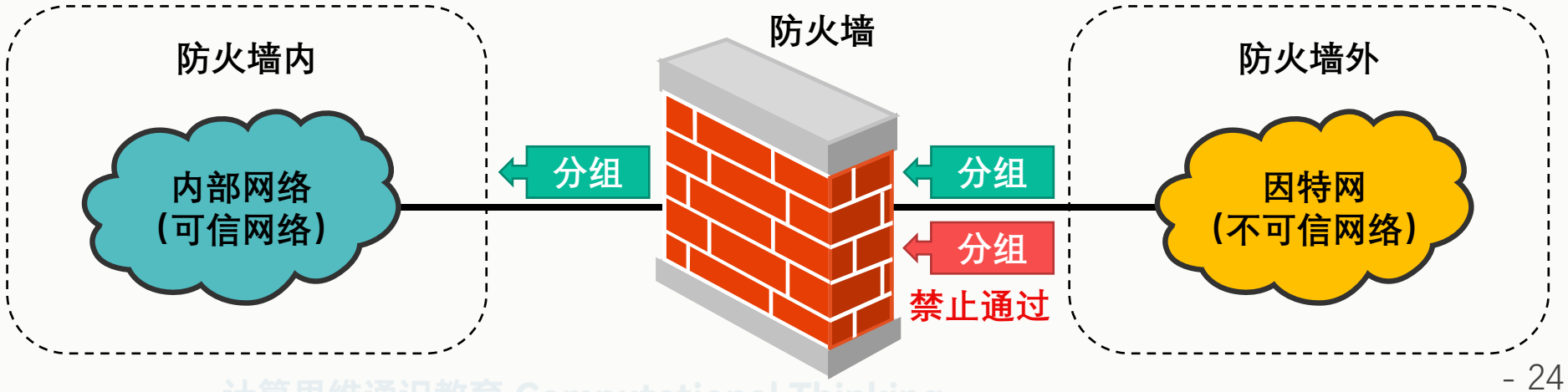
4-2-3 防火墙与入侵检测系统

1. 防火墙

一个组织机构内部的网络与互联网相连时，为了避免网络内受到非法访问的威胁，往往会设置**防火墙（Firewall）**。



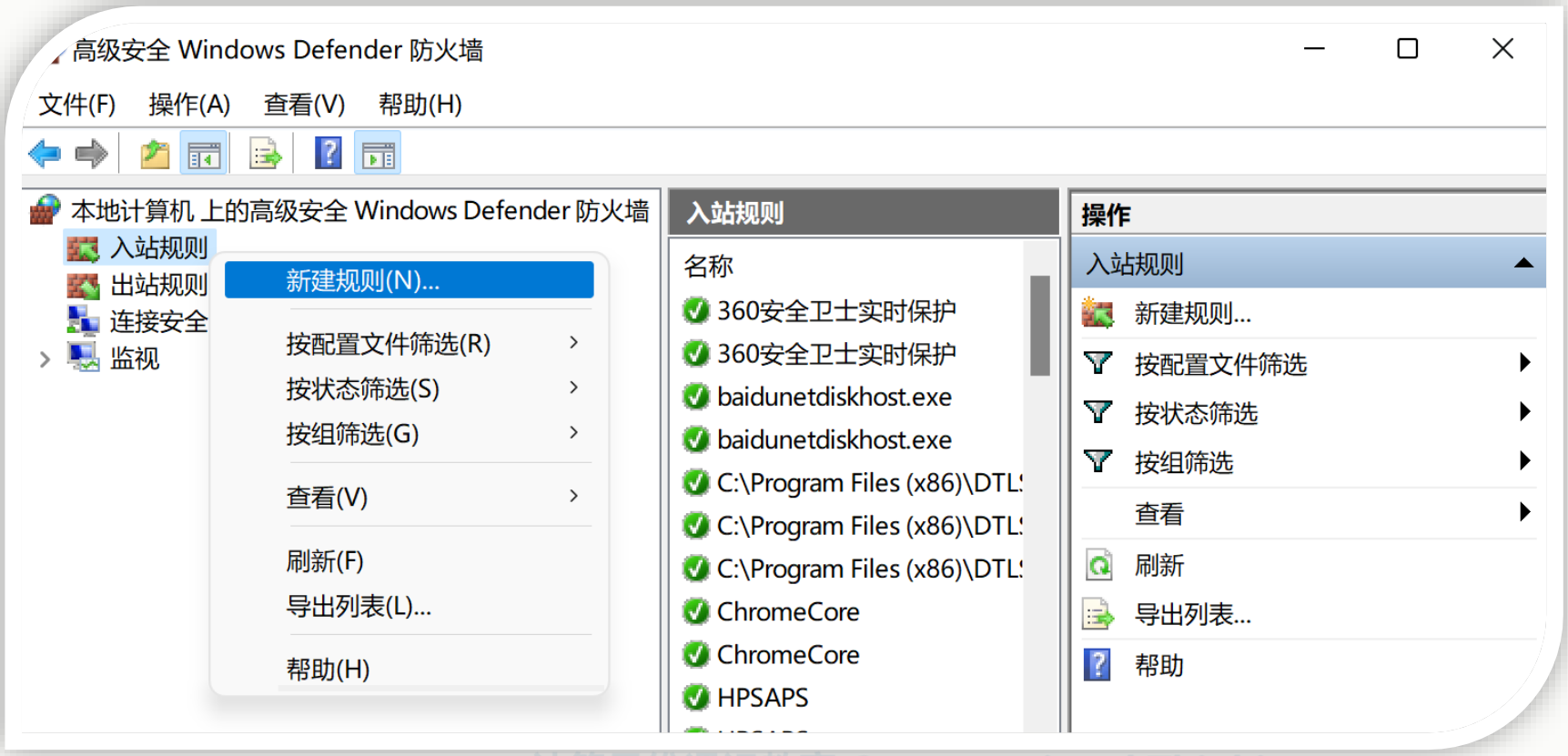
防火墙是位于两个或以上网络间，实行网络间访问或控制的硬件或软件。基本功能是隔离网络，通过将网络划分成不同的区域，制定出不同区域之间的访问控制策略来控制不同信任程度区域间传送的数据流。



4-2-3 防火墙与入侵检测系统

1. 防火墙

例如：利用Windows Defender防火墙为计算机提供网络安全。
可以创建入站或出站新规则、连接安全规则以及进行监视等操作。



4-2-3 防火墙与入侵检测系统

2. 入侵检测系统

- 防火墙并不能阻止所有的入侵行为。

- 在入侵已经开始但还未造成危害或在造成更大危害之前，及时检测到入侵并尽快阻止入侵，尽量把危害降到最小，就是非常有必要的。入侵检测系统（Intrusion Detection System，IDS）正是这样一种技术。

- IDS对出入网络的分组执行深度检查，当检查到可疑分组时，会及时向网络管理员发出警报或进行阻断。

- IDS能够检测多种网络攻击：

端口扫描 | 拒绝服务攻击 | 网络映射 | 恶意代码 | 系统漏洞

4-2-3 防火墙与入侵检测系统

2. 入侵检测系统

只能检测已知攻击，
对于未知攻击则无法防范。

基于特征的入侵检测系统

- 维护一个已知各类攻击的标志性特征的数据库。
- 检测到与某种攻击特征匹配的分组或分组序列时，就判断可能出现了某种入侵行为。
- 标志性特征必须具有很好的区分度。
- 标志性特征一般由网络安全专家提供，由单位的网络管理员定制并将其加入到数据库中。

基于异常的入侵检测系统

- 通过观察正常运行的网络流量来学习正常网络流量的统计特性和规律。
- 检测到网络流量的某种统计规律不符合正常情况时，则判断可能发生了入侵行为。
- 区分正常流量和统计异常流量是非常困难的。
- 现在很多研究致力于将机器学习方法应用于入侵检测，减少对网络安全专家的依赖。

2022

本次课程结束，请继续加油！

Computational Thinking

主讲人：曹轶臻

联系方式：caoyizhen@cuc.edu.cn

计算机与网络空间安全学院

School of Computer and Cyber Sciences