



西安电子科技大学  
XIDIAN UNIVERSITY

计算机科学与技术学院  
School of Computer Science and Technology  
国家示范性软件学院  
National Pilot School of Software Engineering

# 计算机安全导论

## 第7章 网络安全II

主讲人：张志为

二〇二四年秋季学期



协议	名称	默认端口	底层协议
HTTP	超文本传输协议	80	TCP
HTTPS	超文本传输安全协议	443	TCP
Telnet	远程登录服务的标准协议	23	TCP
FTP	文件传输协议	20传输和21连接	TCP
TFTP	简单文件传输协议	21	UDP
SMTP	简单邮件传输协议（发送用）	25	TCP
POP	邮局协议（接收用）	110	TCP
DNS	域名解析服务	53	服务器间进行域传输的时候用TCP 客户端查询DNS服务器时用 UDP



PART 1

域名系统DNS

PART 2

防火墙

PART 3

隧道

PART 4

入侵检测

PART 5

无线网



**PART 1**

**域名系统DNS**

PART 2

防火墙

PART 3

隧道

PART 4

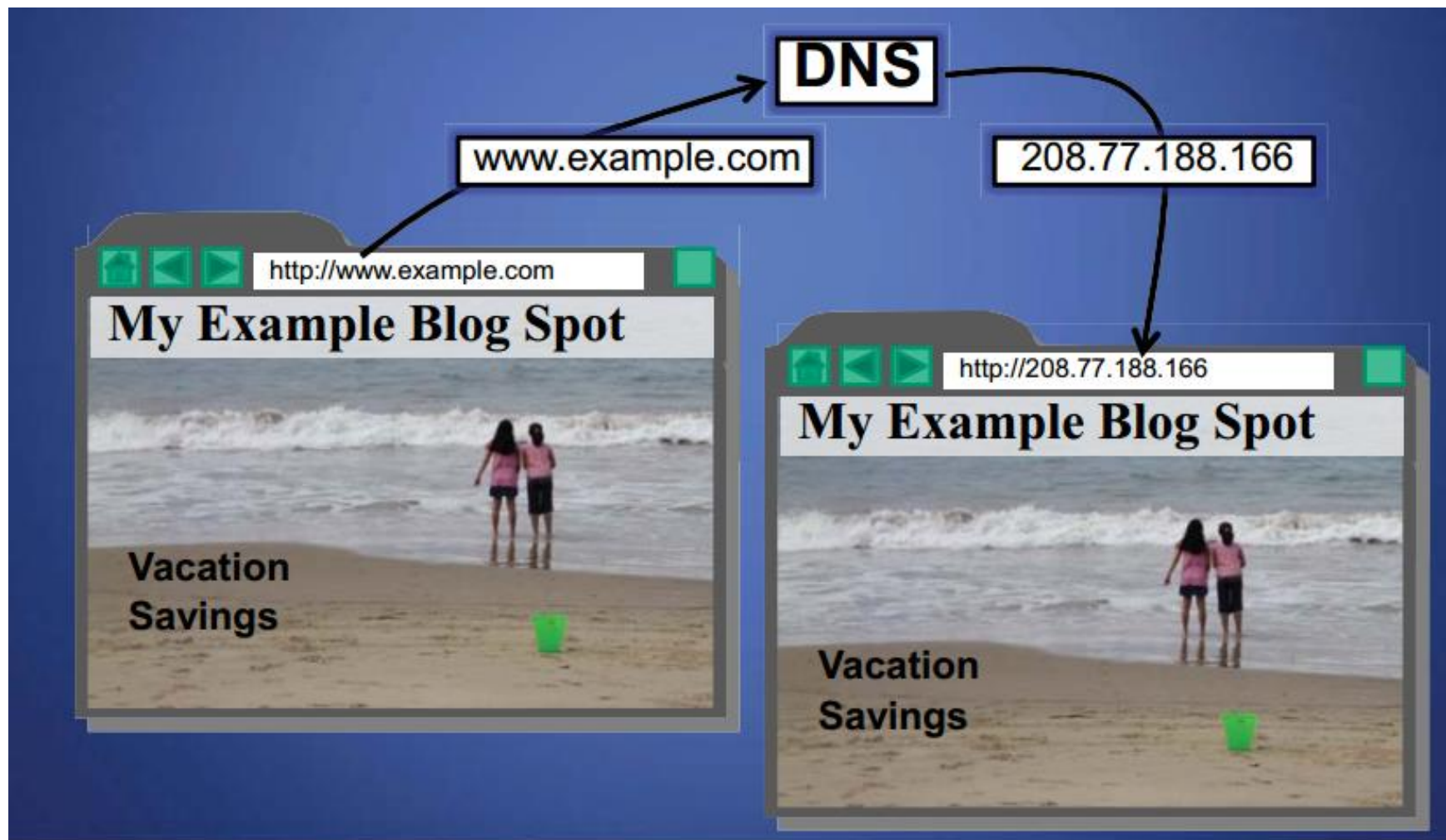
入侵检测

PART 5

无线网



域名系统（DNS）是一个基本的应用层协议，负责将域名映射到IP地址





DNS通过互联网提供存储各种资源记录的分布式数据库，包括：

- 地址（A）记录：与主机名相关联的IP地址
- 邮件交换（MX）记录：域的邮件服务器
- 名称服务器（NS）记录：域的权威服务器

For example, if example.com wishes to sub-delegate "john.example.com." to John who works at Example, inc., lines like this can be added to the example.com zone file:

```
john.example.com. NS ns1.john.example.com.  
john.example.com. NS ns2.john.example.com.  
# It's important to provide "glue"; in other words, let the world know  
# the IPs for these name servers.  
ns1.john.example.com. 10.9.8.7  
ns2.john.example.com. 10.5.77.65
```

John, who is running his own nameservers with the IPs 10.9.8.7 and 10.5.77.65 then has a zone file for john.example.com. that looks something like this:

```
# It is best if the NS records for a subzone agree with the delegation  
# records above  
john.example.com. NS ns1.john.example.com.  
john.example.com. NS ns2.john.example.com.  
  
ns1.john.example.com. 10.9.8.7  
ns2.john.example.com. 10.5.77.65  
  
# Now that that is out of the way, here is the rest of the zone  
john.example.com. 10.9.8.7  
www.john.example.com. 10.5.77.65  
john.example.com. MX 10 mail.john.example.com.  
mail.john.example.com. 10.9.8.7
```

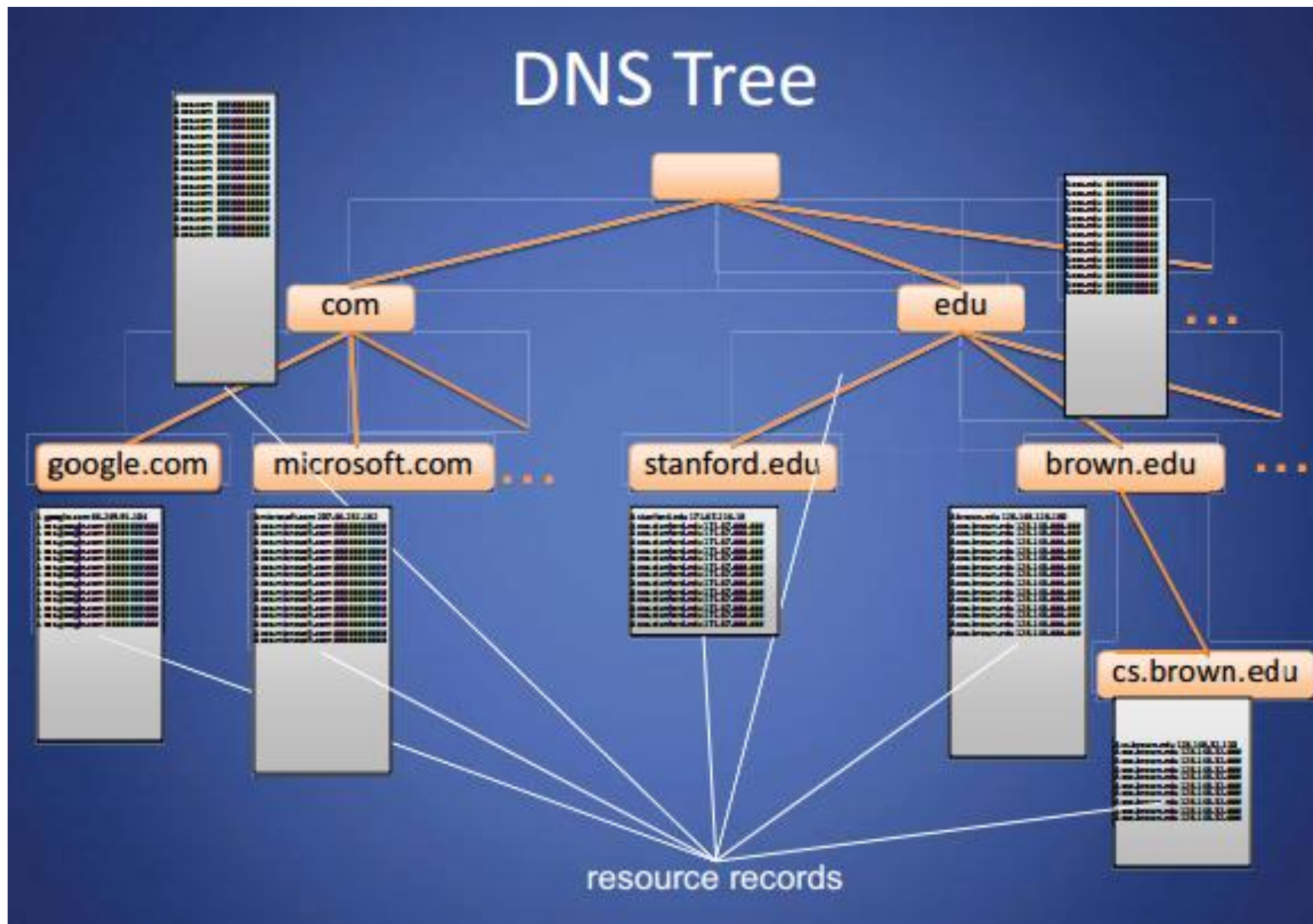
Example DNS entries from <http://www.maradns.org/tutorial/recordtypes.html>



- 域名
  - 两个或多个标记，以点分隔（例如， xidian.edu.cn）
  - 最右边的标签是顶级域名（TLD）
- 权威域名服务器的层次结构
  - 有关根域名的信息
  - 有关其子域（A记录）的信息或对其他域名服务器的引用（DNS记录）
- 权威域名服务器层次结构与域层次结构匹配：根服务器指向TLD的DNS服务器等
- 根服务器和TLD服务器不经常更改
- DNS服务器按名称而不是IP引用其他DNS服务器：有时必须通过提供IP以及名称（称为粘合记录）来引导



# DNS Tree





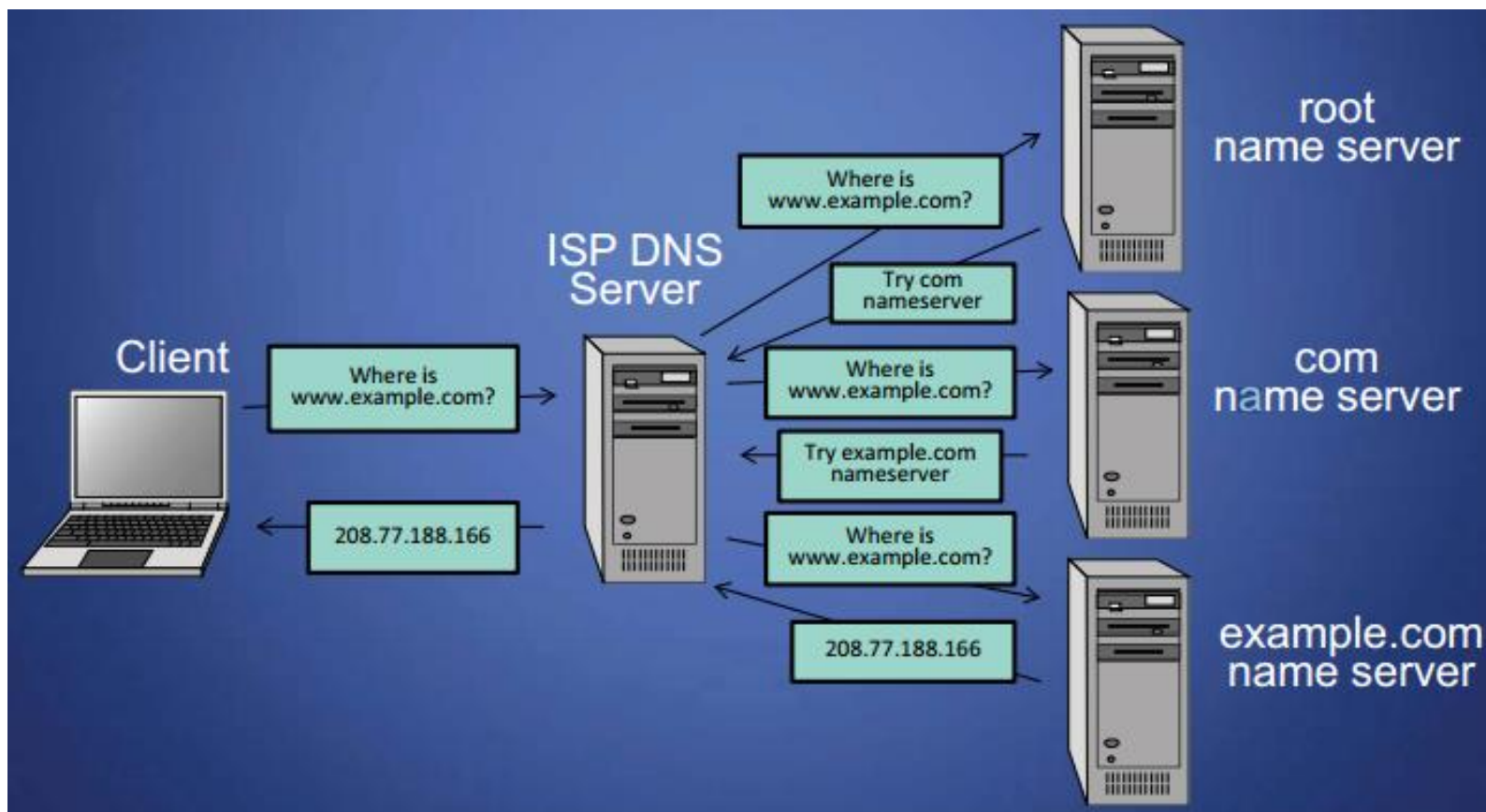


- ICANN：互联网名称与数字地址分配机构
- ICANN全面负责管理DNS。它控制根域，将对每个顶级域的控制权委托给域名注册表
- 除了一小部分通用顶级域名外，每个国家都有自己的顶级域名（cTLDS），由政府控制
- ICANN是所有通用TLD的管理机构
- 直到1999年，所有.com，.net和.org注册管理机构都由Network Solutions Incorporated处理
- 1999年11月之后，ICANN和NSI必须允许共享注册系统，目前市场上有500多个注册商
- 自1999年以来，ICANN还创建了其他gTLD，其中包括由财团或公司集团赞助的gTLD



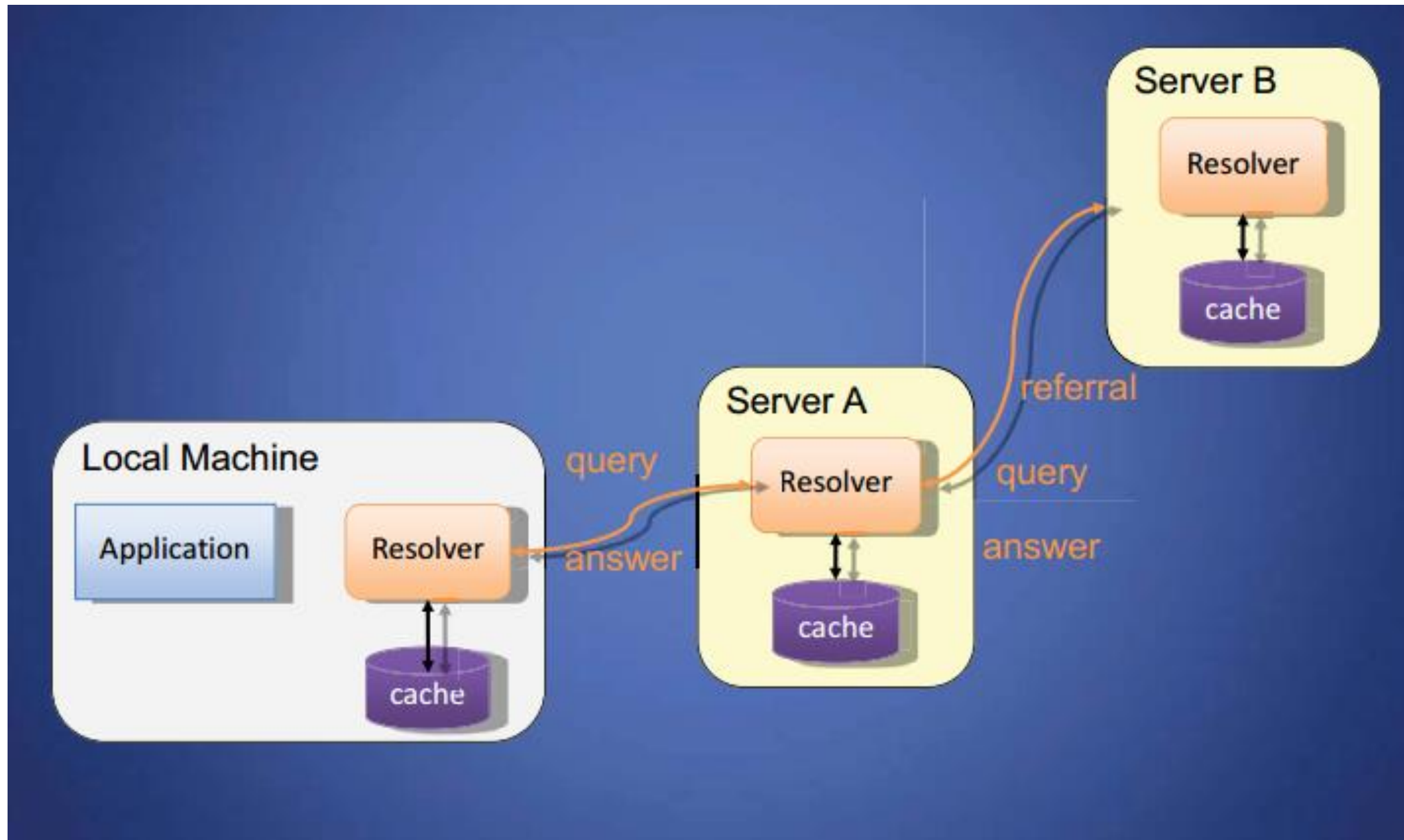
- 始于1984年
- 最初应该按功能命名
  - .com用于商业网站, .mil用于军事用途
- 最终就.com, .net, .org, .info的无限制TLD达成一致
- 1994年开始允许国家顶级域名 (如.it, .us)
- 试图在2000年创建.aero, .museum等, 回到目的层次结构

- 区域：具有相同权威DNS服务器的已连接节点的集合
- 域名不在缓存中的解决方法：



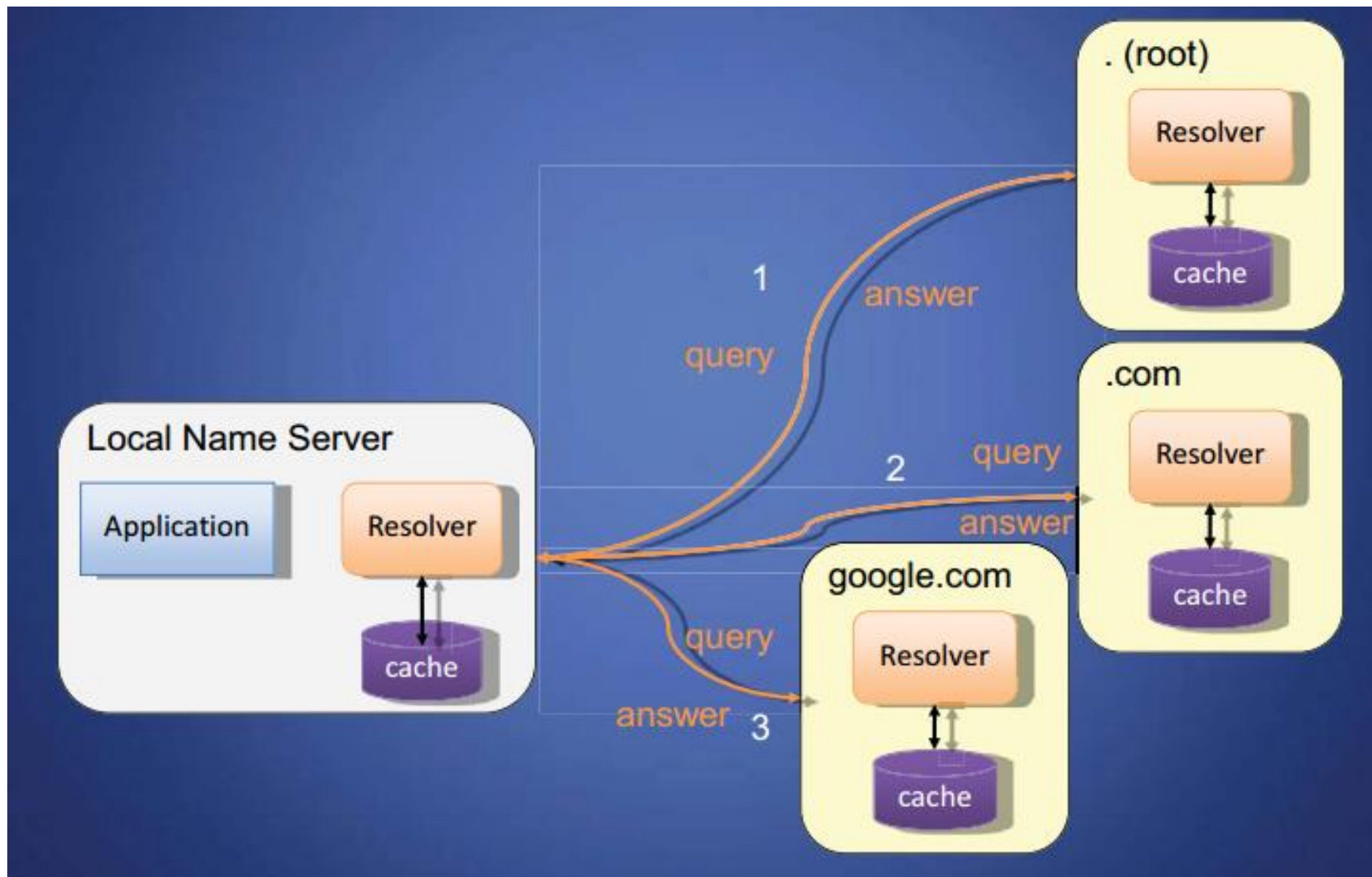


# 递归域名解析





# 迭代域名解析







- 控制在权威域名服务器（ANS）之间分配
  - 负责特定域
  - 可以为子域指定其他ANS
- ANS可以是主站或从站
  - 主站包含原始区域表
  - 从站是副本，自动更新
- 使DNS容错，自动分配负载
- ANS必须作为NS安装在父母区域中



- 许多大型提供商为域提供了多个权威域名服务器
- 问题：需要找到地理位置最接近用户的域实例
- 建议的解决方案：在递归请求中包括请求者IP的前3个八位字节，以便提供更好的服务
- 内容分发网络已经进行自适应DNS路由



- DNS查询和应答是通过UDP数据包传输的，但当请求或应答超出512B时，会用TCP替代UDP
- DNS使用的标准UDP数据包由头、查询部分、应答部分组成
- 头格式如下
  - 头包括一个16位的查询标识符，也称为事务标识符，用于标识查询和响应
- 查询部分包含如下内容
  - 查询部分是“问题序列”，每个问题由所查询域名和查询记录的类型组成，客户端选择查询ID、发送查询，并复制来自服务器的响应



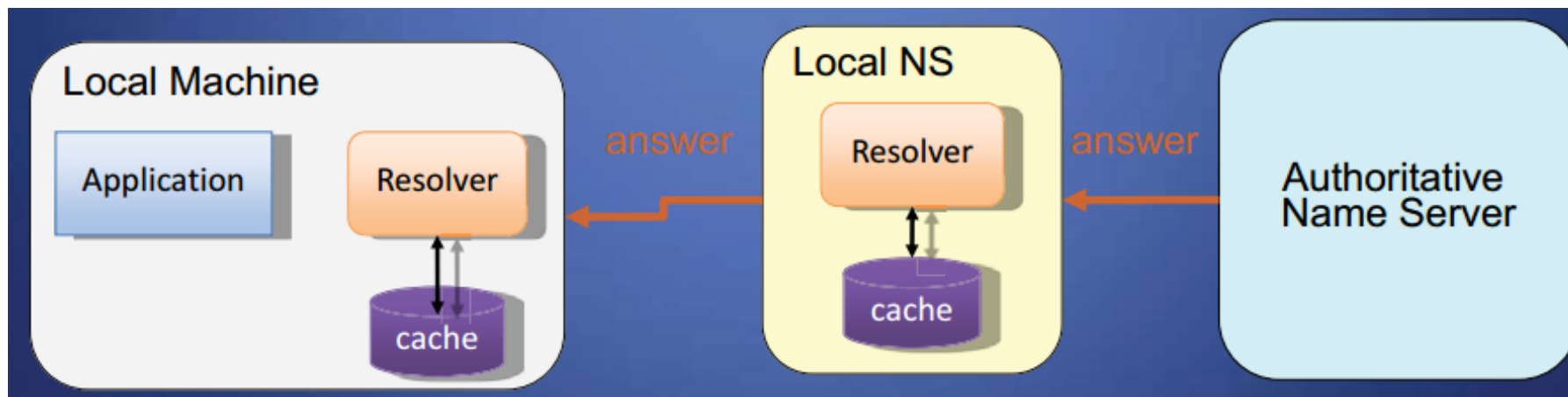
- 应答部分包括DNS记录序列，每条记录包含如下字段
  - NAME字段是变长的，包含一个全域名
  - 2个字节的TYPE字段表示DNS记录的类型
  - 2个字节的CLASS域表示记录应用的更广泛的类型，如IN用于互联网域
  - 4个字节的TTL字段指定记录存在的有效时间，以秒为单位
  - 2个字节的RDLENGTH字段表示数据段的长度，以字节为单位
  - 可变长度的RDATA段包括实际的记录数据



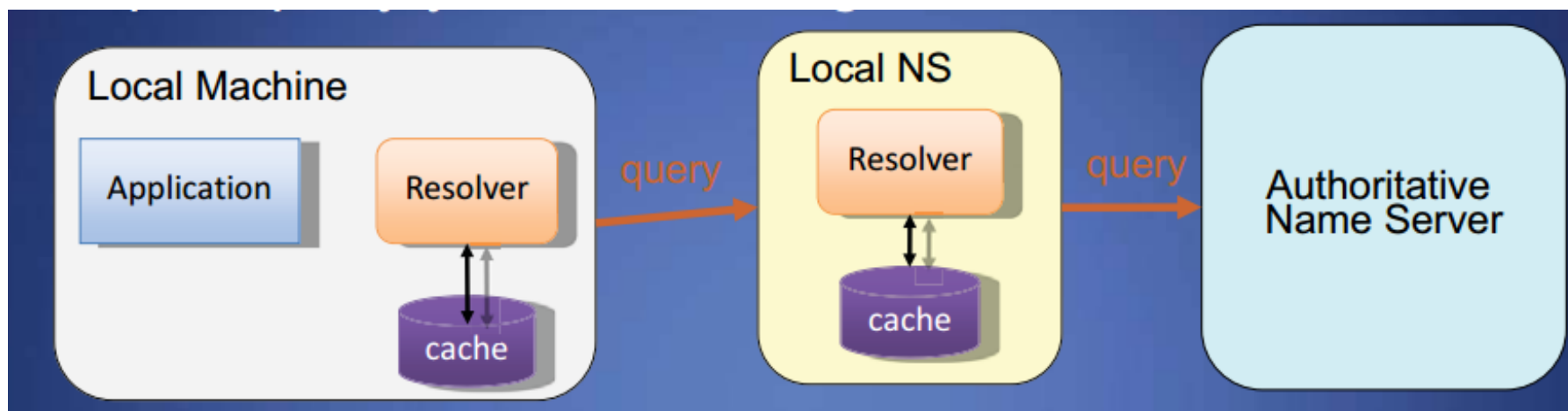
- 如果每个查询都会遍历DNS树中的路径，网络流量会过多
  - 根区域将快速过载
- DNS服务器在指定的时间内缓存结果
  - 由ANS回复的生存时间字段指定
- 操作系统和浏览器维护解析器和DNS缓存
  - 在Windows中使用命令ipconfig / displaydns查看
  - 相关的隐私问题
- DNS查询通常通过端口53上的UDP发出
  - 有效负载中的16位请求标识符



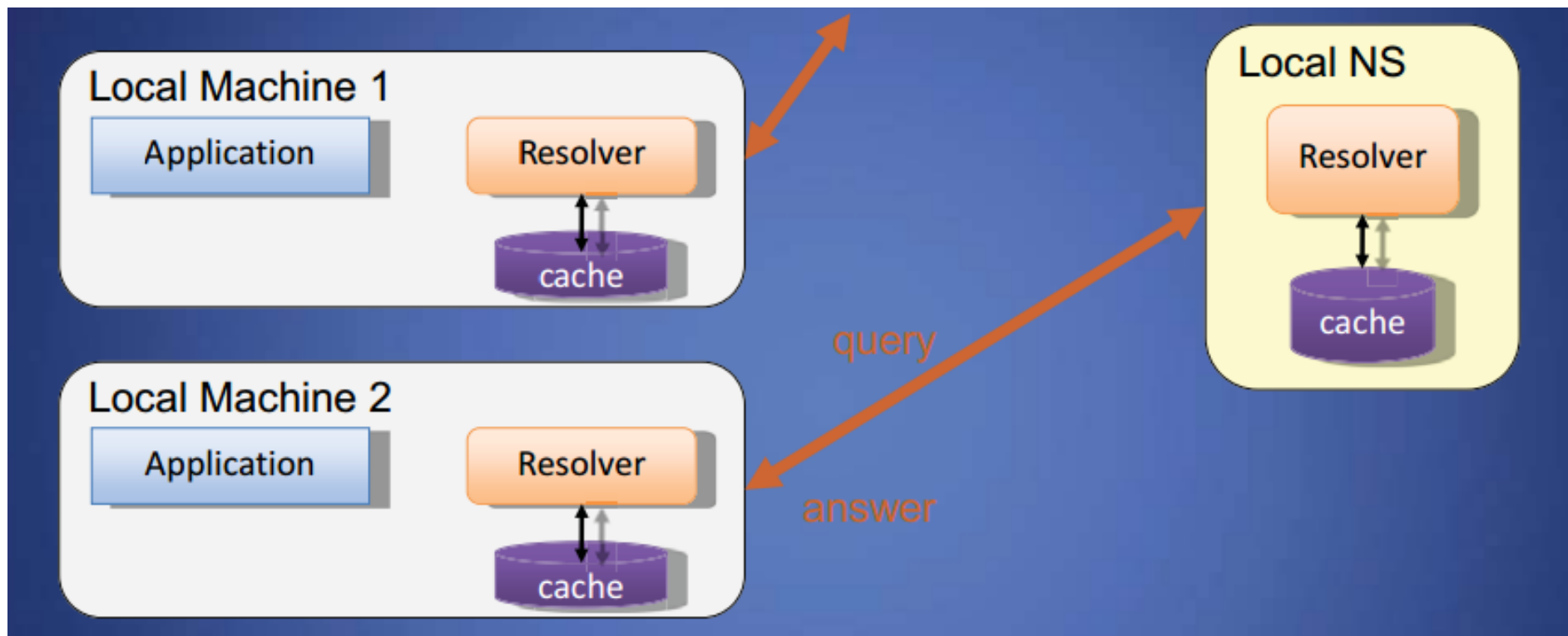
- Step1: 查询 yourdomain.org



- Step2: 在本地NS和主机上接收回复和缓存

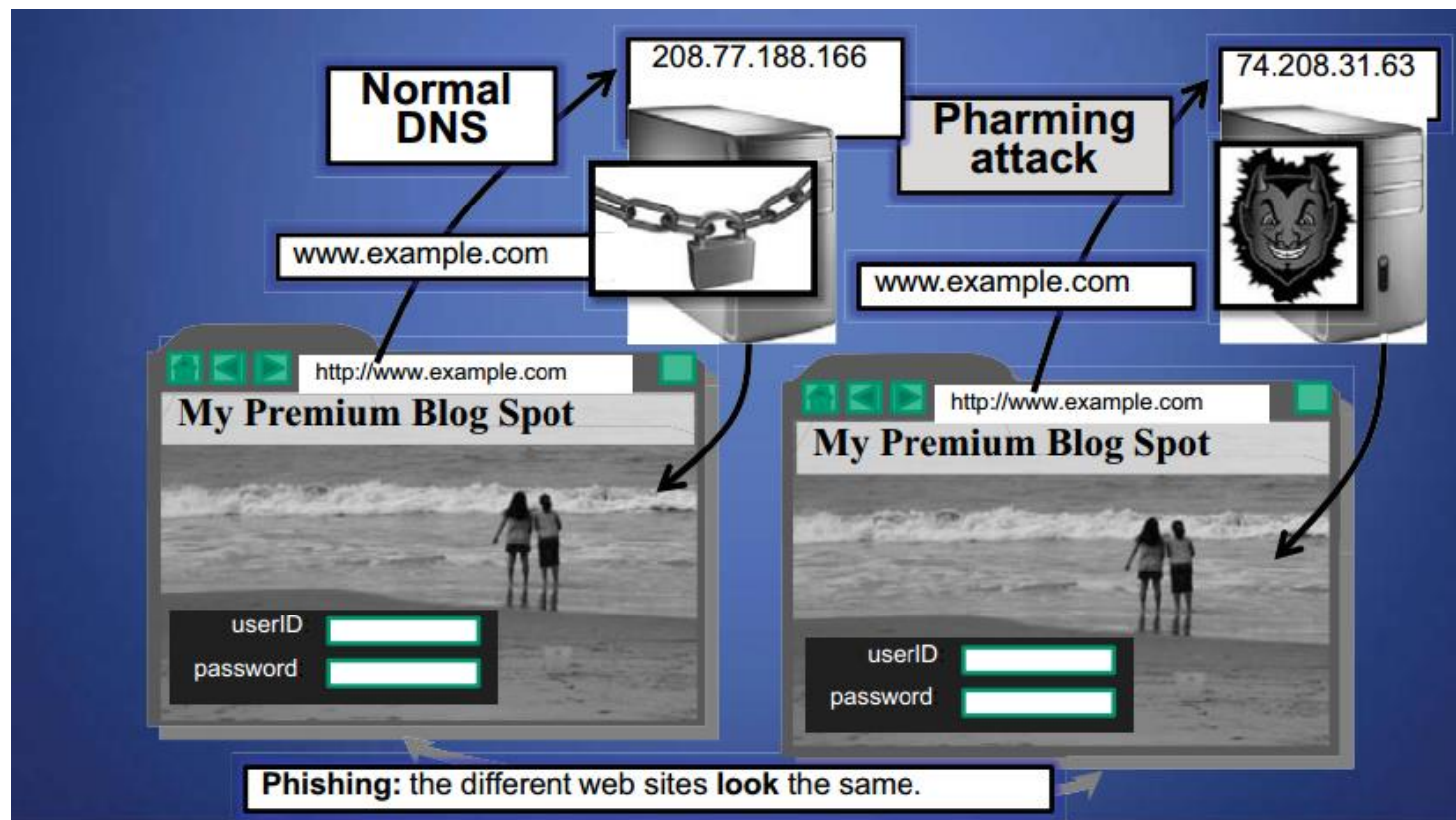


- Step3: 使用缓存结果而不是查询ANS



- Step4: 在TTL到期时退出缓存目录

- 攻击者把网站发送的请求解析成自己恶意服务器的伪装IP地址，导致受害人浏览或下载不需要的内容；网络嫁接的一个主要用途是将域名解析为一个网站，该网站表面与所请求网站相同，但实际是恶意网站，这种攻击被称为网络钓鱼





- 基本思想：攻击者欺骗DNS服务器缓存保存虚假的DNS记录
- DNS使用16位请求标识符将查询ID与响应ID配对
- 当域名服务器出现以下情况时，缓存可能会中毒
  - 忽略标识符
  - 具有可预测的ID
  - 接受未经请求的DNS记录

- 对查询使用随机标识符
- 始终检查标识符
- DNS请求的端口随机化
- 部署DNSSEC（域名系统安全扩展）

## 部署 DNSSEC 的益处



有利于保护互联网。



加强应对攻击的能力。

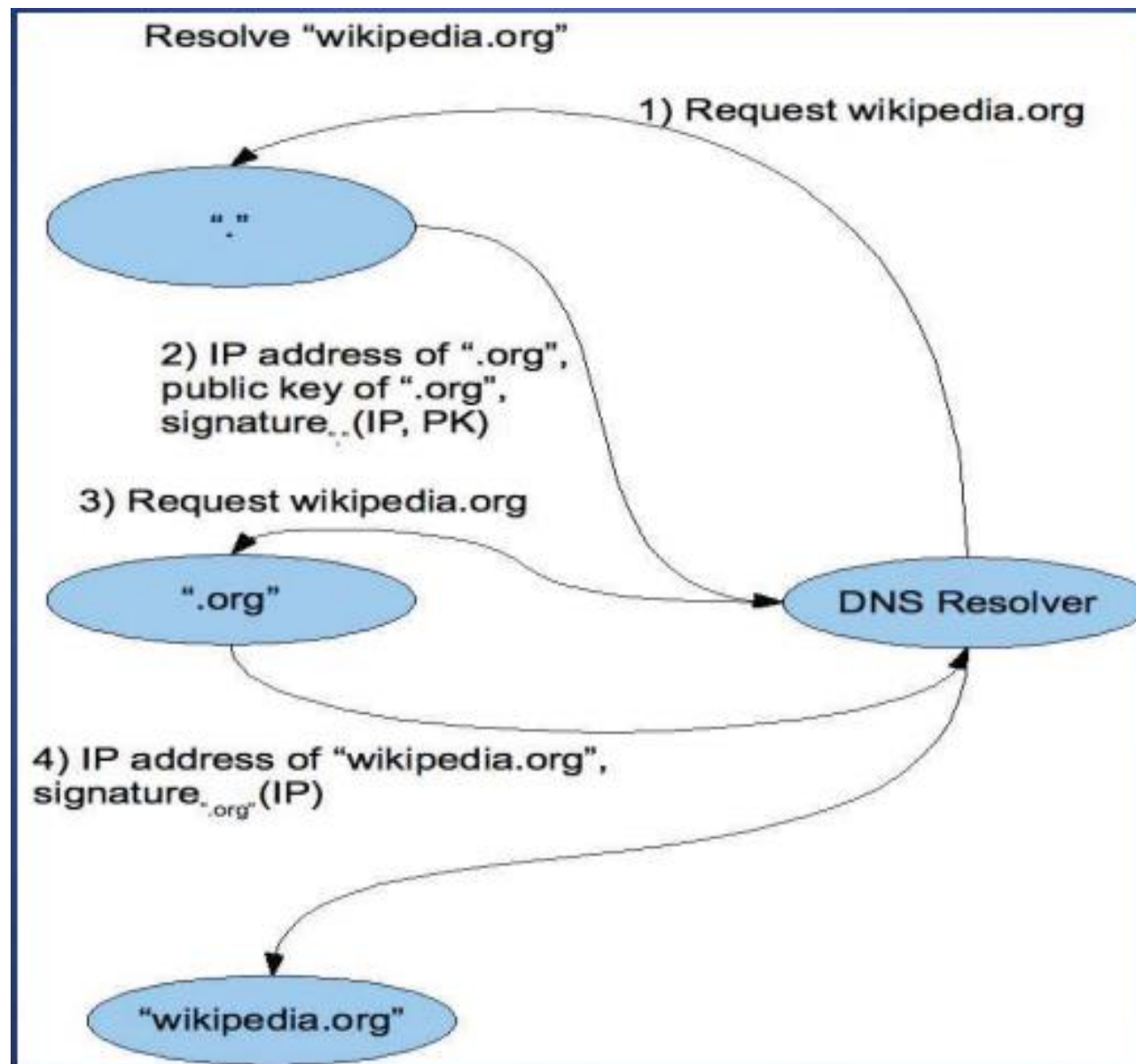


DNSSEC 验证和保护了 DNS 数据, 使得这类数据在 DNS 以外的应用程序中也值得信赖。





- 保证
  - DNS回答来源的真实性
  - 回复的完整性
  - 拒绝存在的真实性
- 通过在每一步中对DNS回复签名来实现这一点
- 使用公钥加密来签署响应
- 通常使用信任锚，操作系统中的条目来引导进程





- 随着互联网被视为关键基础设施，开始推动安全的DNS
- NIST现在正在根服务器上部署它
- 可能会给DNS服务器增加相当大的负载，因为数据包大小远大于512字节大小的UDP数据包



PART 1

域名系统DNS

**PART 2**

**防火墙**

PART 3

隧道

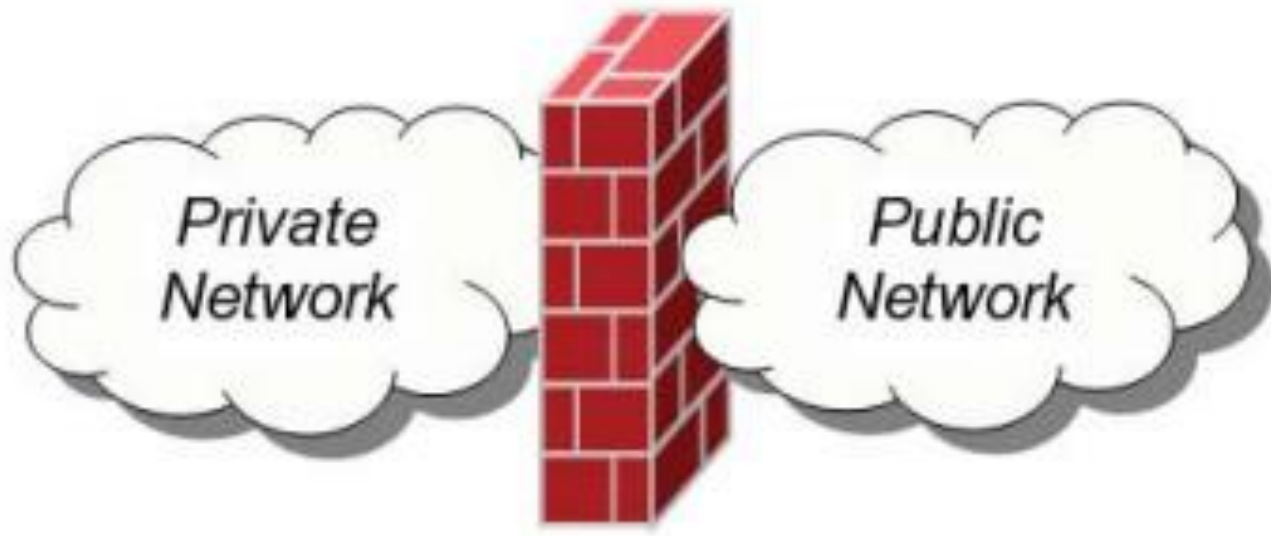
PART 4

入侵检测

PART 5

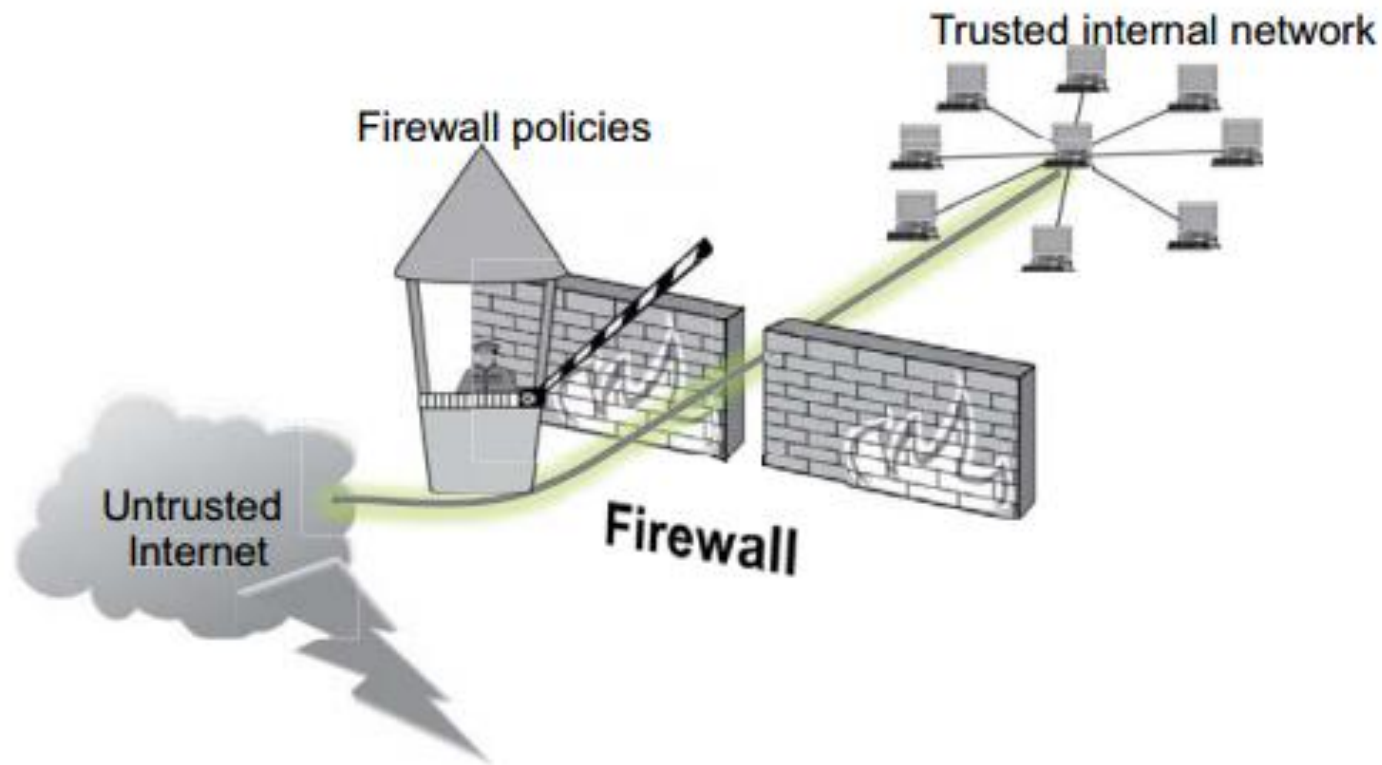
无线网

- 防火墙是一种集成的安全措施集合，旨在防止对网络计算机系统未经授权的访问
- 网络防火墙类似于建筑物中的防火墙，因为在两种情况下，它们都旨在将一个“网络”或“隔间”与另一个隔离





- 为了保护专用网络和个人计算机的安全，需要部署防火墙过滤流入或流出的流量，基于的预定义规则集称为**防火墙策略**





- 流经防火墙的数据包会有以下三种结果
  - 接受：允许通过防火墙
  - 丢弃：不允许通过防火墙，且无失败指示
  - 拒绝：不允许通过防火墙，并试着通知源端，数据包已被拒绝
- 防火墙处理数据包的策略基于被检查数据包的一些特性，包括所使用协议
  - TCP或UDP
  - 源IP地址或目的IP地址
  - 数据包应用程序级的有效载荷（如是否包含病毒）



为了有效地使对外部世界的脆弱性最小化，同时保持受信任内部网（或个人计算机）中计算机所需要的功能，有两种基本方法来创建防火墙策略（或规则集）

- 黑名单方法
  - 除了那些符合黑名单所定义的具体规则的数据包之外，其他所有的数据包都允许通过防火墙
  - 这种类型的配置更具灵活性，能确保内部网的服务不被防火墙中断，但从安全角度分析，这种方法已经假定网络管理员能列举出所有恶意流量的本质特性
- 白名单方法
  - 一种更安全的定义防火墙规则集的方法是默认拒绝策略，除非防火墙接受数据包，否则数据包会被丢弃或拒绝



## 数据包过滤器（无状态防火墙）

- 如果数据包与数据包过滤器的规则集匹配，则数据包过滤器将丢弃或接受它

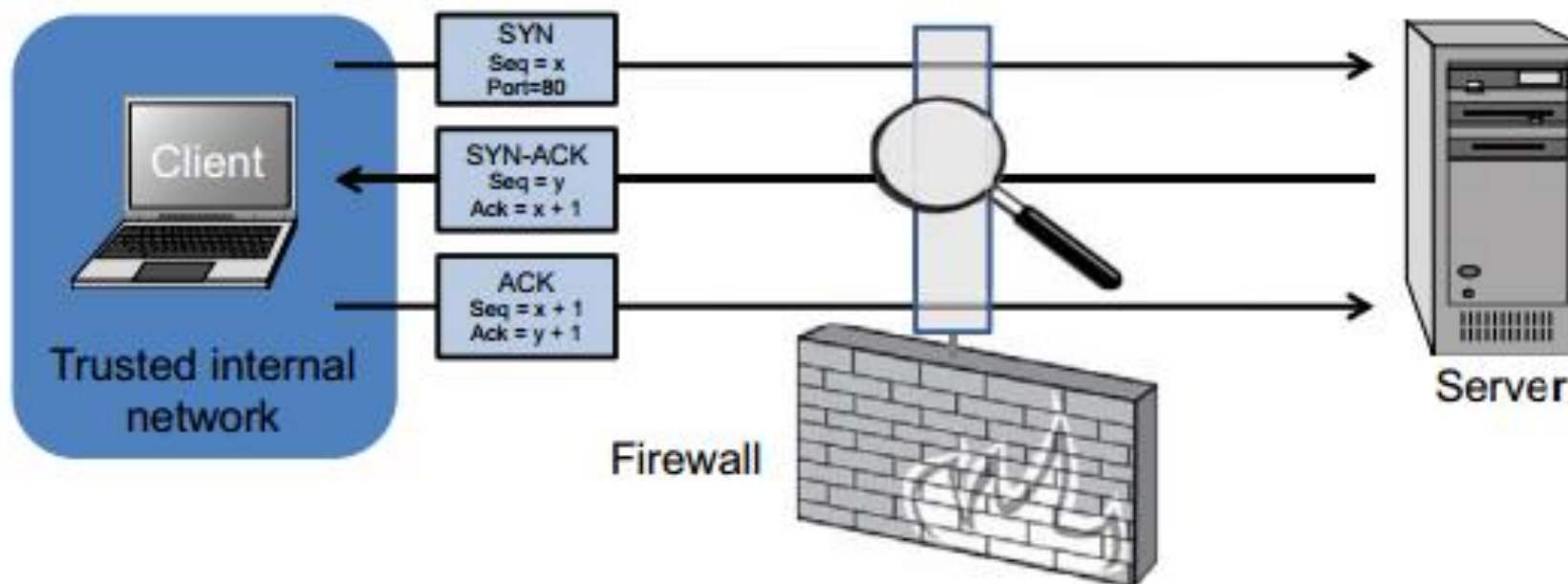
## 状态过滤器（状态防火墙）

- 维护通过它的所有连接的记录，并可以确定数据包是新连接的开始、现有连接的一部分还是无效数据包

## 应用层防火墙

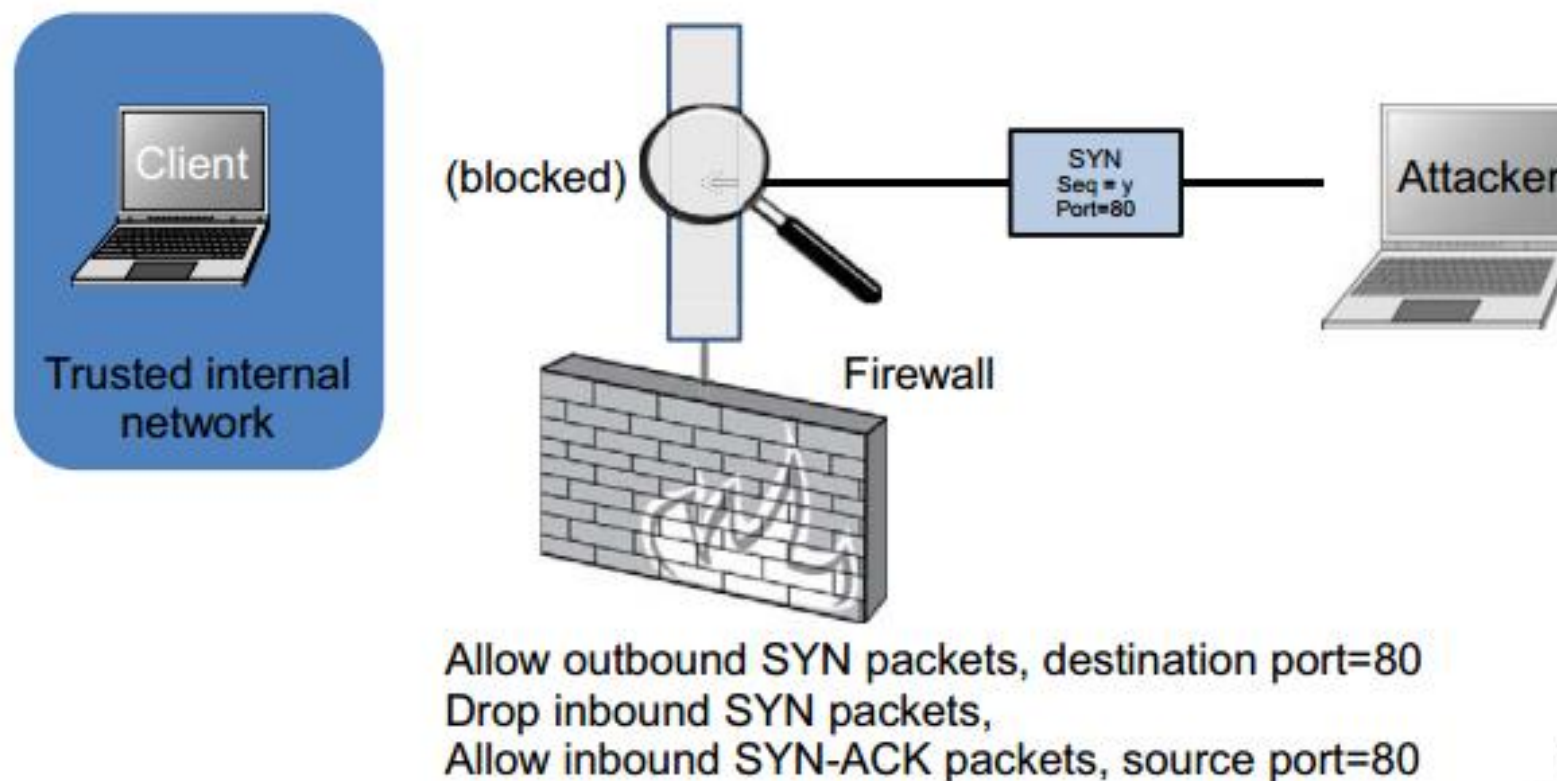
- 它就像一个代理，可以“理解”某些应用程序和协议
- 它可能会检查流量的内容，当其被视视为不当内容（即网站，病毒，漏洞.....）时阻止该流量

- 无状态防火墙不会为正在处理的数据包维护任何可存储的上下文（或“状态”）
- 相反，将每个尝试通过的数据包视为独立的，不考虑先前已经处理过的数据包



Allow outbound SYN packets, destination port=80  
Allow inbound SYN-ACK packets, source port=80

无状态防火墙可能必须具有严格的限制性，以防止大多数攻击

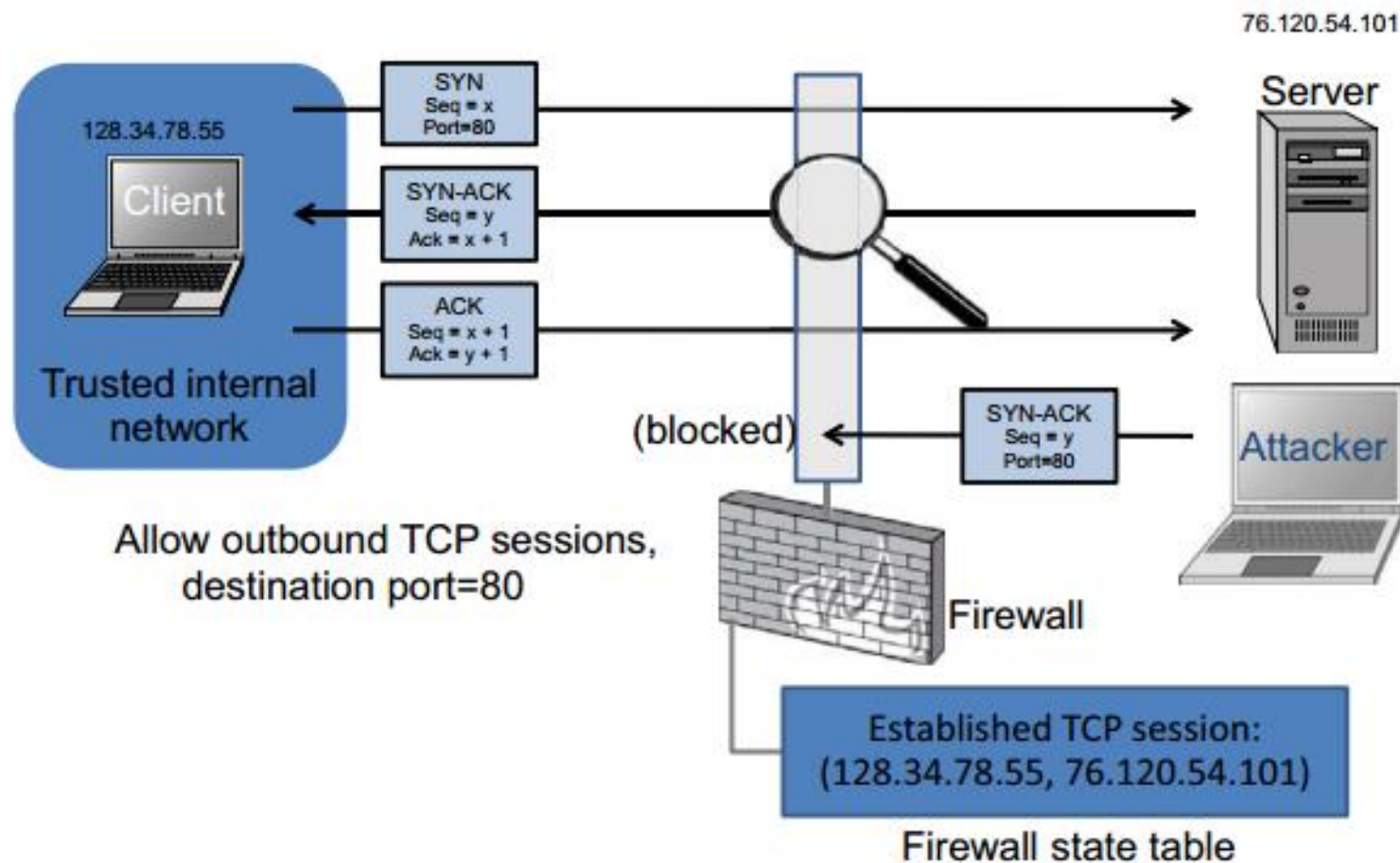




- 状态防火墙可以区分数据包是否是受信任网络内发起的合法会话的一部分
- 状态防火墙维护一些表，表中包含每个活动连接的信息，包括IP地址、端口和数据包的序列号
- 使用这些表，状态防火墙可以只允许响应内部网发起连接的TCP数据包流入



## ■ 仅允许请求的TCP连接





PART 1

域名系统DNS

PART 2

防火墙

**PART 3**

**隧道**

PART 4

入侵检测

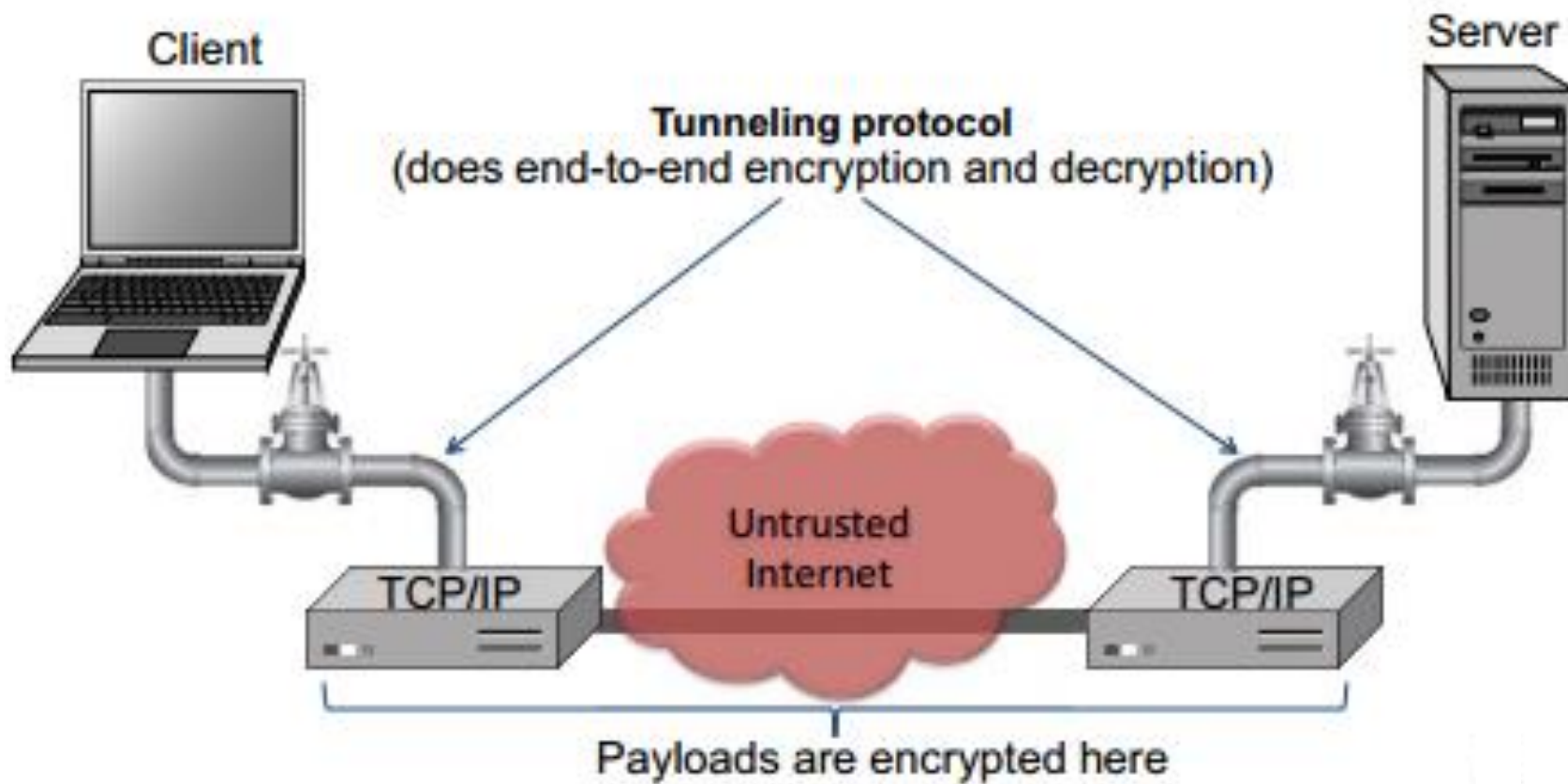
PART 5

无线网



- 通常TCP数据包的内容是不加密的，因此如果有人窃听TCP连接，他会知道该会话中有效载荷的所有内容
- 使用隧道协议无需改变软件的执行就能防止这种窃听
- 在隧道协议中，客户端和服务端之间的通信是自动加密的，窃听是不可行的

- 通过Internet发送的数据包会自动加密





## ■ 一次安全的交互式命令会话

- 客户端通过一个TCP会话连接到服务器
- 客户端与服务器交换管理细节的信息，如支持的加密方法、各自协议的版本，每一方都要选择另一方支持的一组协议
- 客户端和服务端进行密钥交换，创建共享的秘密会话密钥，用会话密钥加密双方的通信（但不用于身份验证）。这个会话密钥配合选择的块加密（通常是AES、3DES、Blowfish或IDEA）来加密所有后续的通信



- 服务器向客户端发送可以接受身份验证列表，客户端将按顺序尝试。最常见的机制是使用密码或以下的公共密钥身份验证方法
  - 如果选定的机制是公共密钥身份验证，则客户端向服务器发送自己的公钥
  - 然后服务器检查是否这密钥已存储在其授权的密钥列表之中。如果在，服务器使用客户的公钥加密挑战，并将其发送给客户端
  - 客户用自己的私钥解密挑战，并向服务器发回响应，证明自己的身份
- 一旦身份验证已顺利完成，服务器允许客户端访问相应的资源，如命令提示符



- IPSec定义了一组协议，为IP数据包提供机密性和真实性
- 每个协议都能运行在两种模式下，**传输模式**或**隧道模式**
  - 在传输模式下，在原数据包的数据之前，会插入额外的IPSec的头信息，只对数据包的有效载荷继续加密或身份验证
  - 在使用隧道模式时，会构造一个新的数据包，将IPSec头信息和整个原数据包，（包括它的头）一起封装为新数据包的有效载荷





- **虚拟专用网络（VPN）** 是一种安全地延长了私有网络的物理距离，利用公有网络（如互联网）进行通信的技术
- 尽管使用不受信任的网络进行传输，VPN也能提供数据的保密性、完整性
- VPN主要有两种类型
  - 远程访问VPN
  - 站点到站点的VPN



## ■ 远程访问VPN允许授权的用户访问私有网络，一般将这种私有网络称为**内网**

- 例如，组织可能允许员工远程访问公司的网络，员工就像在公司一样使用自己的系统或互联网
- 为了能做到这一点，组织会建立VPN端点，该端点被称为**网络接入服务器**。客户端通常在自己的计算机上安装VPN客户端软件，用于处理到NAS的连接约定

## ■ 站点到站点VPN解决方案旨在为两个或更多远程网络提供安全的桥梁

- 在使用VPN之前，组织为了安全地桥接自己的私有网络，需要购买昂贵的租用线路，并用电缆直接连接内网



PART 1

域名系统DNS

PART 2

防火墙

PART 3

隧道

**PART 4**

**入侵检测**

PART 5

无线网



## ■ 入侵

- 旨在检测一些威胁（机密性、完整性、计算/网络资源的可用性）

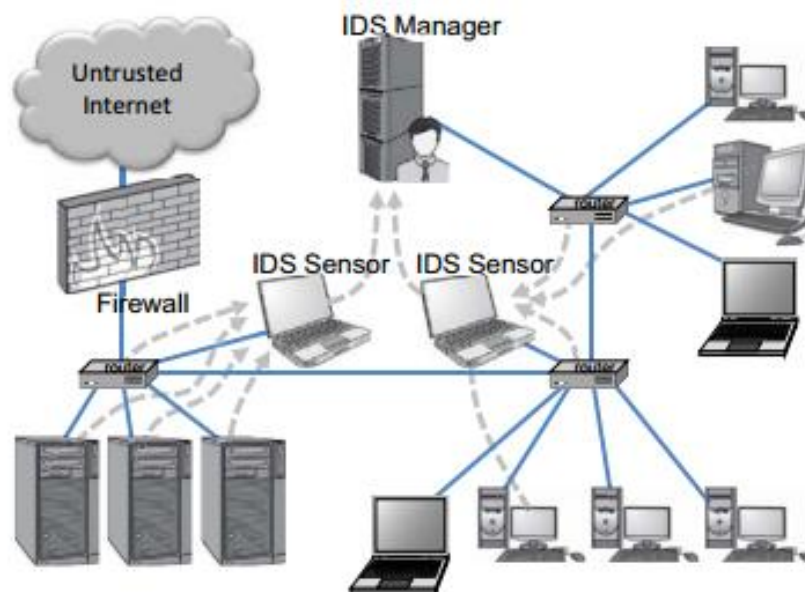
## ■ 入侵检测

- 通过入侵签名和入侵活动报告进行识别

## ■ 入侵防御

- 检测入侵活动和管理整个网络中的自动响应操作的过程

- IDS管理器编译来自IDS传感器的数据，以确定是否发生了入侵
- 此确定基于一组站点策略，这些策略是定义可能入侵的规则和条件
- 如果IDS管理员检测到入侵，则会发出警报





## ■ IDS旨在检测一些威胁，所包含的威胁如下：

- 伪装者，攻击者毛用合法用户的身份或凭据来获得对计算机系统或网络的访问
- 违法者，合法的用户执行了未经授权的操作
- 秘密用户，通过删除审计文件或系统日志，试图组织或掩盖自己行为的用户

## ■ 此外，IDS旨在检测自动攻击和威胁，所包含的相关攻击如下：

- 端口扫描:信息收集旨在确定主机开放哪个端口作为TCP连接
- 拒绝服务攻击：网络攻击意味着淹没主机，并将合法访问拒之门外
- 恶意软件攻击：复制恶意软件的攻击，特洛伊木马、计算机蠕虫和病毒等
- ARP欺骗：试图重定向局域网中的IP流量
- DNS缓存中毒：网络嫁接攻击旨在改变主机的DNS缓存，以创建伪造的域名/IP地址的关联







- 入侵检测系统可以部署在各种上下文中来执行不同的功能
- 传统的**网络入侵检测系统 (NIDS)** :
  - 位于网络边界，基于流量模式和内容检测恶意的行为
- **基于协议的入侵检测系统 (PIDS)** :
  - 专门检测特定协议中的恶意行为，通常部署在特定的网络主机中
- **基于主机的IDS (HIDS)** :
  - 驻留在单个系统之中，监控这台计算机上的活动



## ■ 入侵检测可能会出现两种类型的错误：

- 误报：当事件是良性活动而不是入侵时就发出警报（浪费时间和资源）
- 漏报：当事件是入侵的恶意事件，未发出警报（系统受到损害，管理员未察觉）

## ■ 下图为四种可能的检测结果：

	Intrusion Attack	No Intrusion Attack
Alarm Sounded	 NYPD 03539480 True Positive	 NYPD 03539480 False Positive
No Alarm Sounded	 False Negative	 True Negative



- 难以创建具有高真阳性率和低假阴性率的理想特性的入侵检测系统
- 如果实际入侵的数量与分析的数据量相比相对较小，则可以降低入侵检测系统的有效性
- 特别是，由于称为基本谬误的统计误差，某些IDS的有效性可能会被误解
- 当评估某些条件事件的概率而不考虑该事件的“基本速率”时，会发生此类错误



- 假设IDS准确度为99%，假阳性或假阴性的概率为1%。 假设进一步.....
- 入侵检测系统生成1,000,100个日志条目
- 1,000,100个条目中只有100个对应于实际的恶意事件
- 由于IDS的成功率，在100个恶意事件中，99个将被检测为恶意，这意味着我们有1个假阴性
- 然而，在1,000,000个良性事件中，10,000个将被错误地识别为恶意事件。 也就是说，我们有10,000个误报
- 因此，将有10,099个警报响起，其中10,000个是误报警。 也就是说，大约99%的警报都是误报警



在1987年，Dorothy Denning的一篇有影响力论文确定了在这类事件记录中的一些字段，这些字段如下：

- 主体：发起者
- 对象：目标资源、如文件、命令、设备或网络协议
- 操作：主体对对象正在执行的操作
- 异常条件：操作所产生的任何错误消息或异常条件
- 占用的资源：系统执行或响应该操作所需的定量项
- 时间戳：记录开始操作时刻的唯一标识符



## ■ 基于规则的入侵检测

- 规则标识与入侵攻击的某些已知配置文件匹配的操作类型，在这种情况下，规则将编码此类攻击的签名。因此，如果IDS管理器看到与该规则的签名匹配的事件，它将立即发出警报，甚至可能指示怀疑的特定类型的攻击

## ■ 基于统计的入侵检测

- 构建了一个配置文件，它是用户行为或主机使用的典型方式的统计表示；因此，它可用于确定用户或主机何时以非常不寻常的异常方式运行
- 一旦用户配置文件到位，IDS管理员就可以确定异常行为的阈值，然后在用户或主机显着偏离该人员或机器的存储配置文件时发出警报



- **端口扫描**：允许用户列举计算机的哪个端口正在接受连接的技术
- **端口有三个状态**：开放的（接受连接）、关闭的（不接受连接）、阻塞的（防火墙或其他设备防止一些流量到达目的端口）
- **端口扫描方法**：
  - TCP扫描
  - SYN扫描
  - 空闲扫描
  - UDP扫描



## ■ 蜜罐：检测入侵的另一种工具

## ■ 蜜罐计算机是非常有效的工具：

- 入侵检测：因为连接到蜜罐的尝试不会来自合法用户，所以对蜜罐的任何连接都被安全地确定为入侵
- 证据：蜜罐计算机中有吸引力的文件使入侵者逗留并留下证据，从而识别出入侵者或者确定他的位置
- 导流：与合法计算机相比，蜜罐对入侵者更有吸引力，从而分散入侵者对敏感信息和服务的注意力





PART 1

域名系统DNS

PART 2

防火墙

PART 3

隧道

PART 4

入侵检测

**PART 5**

**无线网**

- 2024年在瑞典Skillingaryd地区举行的“快速响应24”是北约近年来规模最大的一场军事演习（超过1.7万名美国军人和2.3万名多国军人参加），期间美军特种作战小队首次与颠覆性网络安全技术进行了深度融合训练。在此次演习中，美军特种作战小队成功使用远程访问设备（RAD）扫描了目标建筑，以识别运行其安全系统的WiFi网络
- 特战小队破解了WiFi密码，随后对内部网络进行了详细分析，团队在网络中四处移动，关闭闭路电视摄像头，打开安全门，并禁用其他安全系统
- 与此同时，另一支特种作战小队则进行了物理渗透行动。通过高空跳伞，并徒步七英里，他们顺利接近目标建筑。由于前一支小队的网络干扰，他们能够轻松进入大楼，并安放信号干扰设备，以清除行动痕迹，随后迅速撤离
- “我们现在可以通过信号设备接入目标的WiFi网络，监控目标的位置和活动，RAD让我们能够更清晰地掌握目标情况。”一位特种部队成员解释道





- 2024年，英国遭遇了一起大规模的网络攻击事件，导致全国多个主要火车站的公共WiFi服务瘫痪。根据英国铁路网公司（Network Rail）的声明，此次攻击发生在当地时间9月25日晚上，影响了伦敦尤斯顿站、曼彻斯特皮卡迪利站、伯明翰新街站、爱丁堡韦弗利站和格拉斯哥中央车站等19个火车站
- 在这次网络攻击中，当乘客尝试连接火车站的公共WiFi时，他们遇到了一个显示“我们爱你，欧洲”的页面，页面中包含宣扬宗教仇恨的信息，并列举了欧洲多地的恐怖袭击事件。这种信息的展示引起了公众的广泛关注和不安



We love you, Europe.

Below is a just a SMALL taste of what's coming.





## ■ 无线电波

- 无需物理插入网络
- 远程访问

## ■ 覆盖范围

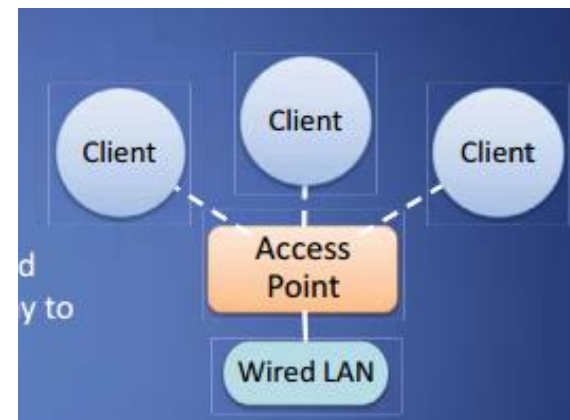
- 个人局域网 (PAN)
- 局域网 (LAN)
- 城域网 (MAN)

## ■ 安全问题

- 无线电信号泄漏到建筑物外面
- 检测未经授权的设备
- 拦截无线通信
- 中间人攻击
- 验证用户
- 限制访问

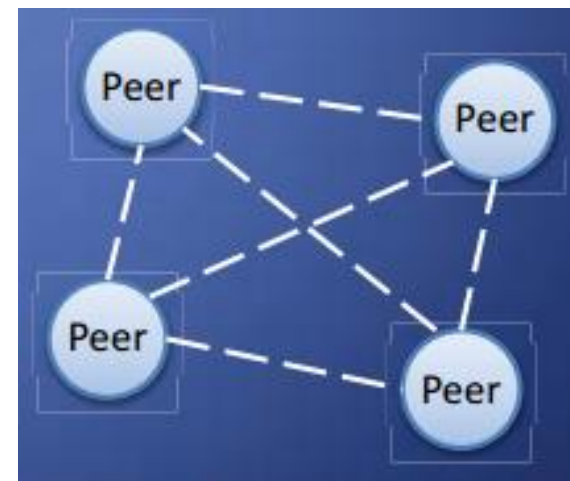
## ■ 基础设施

- 客户端计算机与称为接入点的特殊网络设备建立无线连接
- 连接到有线网络的接入点，提供到互联网的网关
- 最常见的无线网络类型



## ■ 点对点

- 多个对等机器相互连接
- 通常用于ad-hoc网络和Internet连接共享





## ■ 多个无线网络可以共存

- 每个网络由32个字符的服务集ID (SSID) 标识
- 制造商的名称是接入点的典型默认SSID
- 经常广播SSID以使潜在客户能够发现网络

## ■ SSID未被签名，因此可以进行简单的欺骗攻击

- 将恶意接入点放置在公共场所（例如，咖啡馆，机场）
- 使用ISP的SSID
- 设置类似于ISP的登录页面
- 等待客户端连接到恶意接入点并进行身份验证
- 可能会转发到ISP网络的会话
- 由自动连接默认值促成



- 可以窃听所有无线网络流量
- 基于MAC的身份验证通常用于识别公司网络中已批准的计算机
- MAC欺骗攻击可能，如在有线网络中
- 短暂断开连接后，会话保持活动状态
- 如果ISP客户端未明确结束会话，则MAC欺骗允许接管该会话



## ■ 协议

- DHCP提供IP地址
- 名称服务器将一切映射到认证服务器
- 防火墙阻止所有其他流量
- 任何URL都会重定向到身份验证页面
- 身份验证后，恢复常规网络服务
- 通过MAC地址识别的客户端
- 由无线ISP使用

## ■ 安全问题

- 如果客户端没有主动断开连接，则可以执行MAC欺骗和会话窃取攻击
- 如果在身份验证之前未阻止防火墙之外的DNS流量，则隧道攻击可以绕过强制网络门户





- 四处寻找无线局域网
- 有些人使用GPS设备记录位置，在线发布
- NetSumbler for Windows, KisMac for Macs和Kismet for Linux等软件可在线轻松获取
- 使用天线增加射程
- 未传输任何信息且未使用任何网络服务时，合法性不明确
- Warchalking涉及在侧面行走标记无线网络和相关信息上留下粉笔标记（源自流浪汉符号）



## ■ 目标

- 机密性：防止窃听
- 数据完整性：数据包不能被篡改
- 访问控制：仅路由正确加密的数据包

## ■ 设计约束

- 采用90年代的廉价硬件实现
- 符合美国早期加密设备出口管制法规（40位密钥）

## ■ 实施和限制

- 在数据链路级别加密每个帧的主体
- 要避免传统的IEEE 802.11标准



## ■ 初始化

- 接入点和客户端共享40bit密钥K
- 密钥在WEP会话期间永远不会更改

## ■ 加密

- 计算消息M的CRC-32校验和（帧的有效载荷）
- 选择24位初始化向量V
- 使用RC4流密码生成密钥流S(K,V)
- 计算密文:

$$C = (M \parallel CRC(M)) \oplus S(K, V)$$

## ■ 客户端认证

- 接入点向客户端发送未加密的随机质询
- 客户端响应加密挑战

## ■ 传输

- 发送V||C





## ■ 消息篡改

- 给定一个任意字符串 $\Delta$ ，我们想用  $M' = M \oplus \Delta$  替换消息 $M$
- 在中途用  $C' = C \oplus (\Delta \parallel CRC(\Delta))$  替换密文 $C$

## ■ 目标文本替换

- 如果我们知道消息中文本的位置，则可能发生
- E.g., 更改电子邮件中的日期

## ■ 脆弱性原因

- CRC校验和通过XOR分配
- 不是加密哈希函数



## ■ 攻击者利用物理接入点解密数据包

## ■ 方法

- 窃听入站IP数据包
- 将数据包重新发送到由攻击者控制的外部计算机
- 接收由接入点解密的数据包
- 重复出站数据包

## ■ 猜测目的地址

- 在LAN子网内

## ■ 更改目的地址

- 将原始目的地 $D$ 修改为由攻击者控制的外部机器 $D'$
- 使用上述消息篡改方法

## ■ 更改数据包校验和

- 新校验和与旧校验和之间的差为:

$$x' - x = (D_H' + D_L') - (D_H + D_L)$$

- 猜测  $x' \oplus x$

## ■ 几次尝试后成功



## ■ 重用IV意味着重用密钥流

- 攻击者获得两条消息的XOR
- 攻击者可以恢复消息和密钥流
- 攻击者可以使用恢复的密钥流来注入流量

## ■ 默认IV

- IV生成的几个有缺陷的实现
- 例如，当设备开启然后重复递增时从零开始

## ■ 随机IV

- 小长度（24位）即使随机生成也会在短时间内重复
- 例如，在  $2^{12} \approx 4000$  次传输之后，预计碰撞的概率很高



## ■ 攻击者想要欺骗合法的客户端

- 不知道秘密密钥K
- 可以窃听身份认证消息

## ■ 攻击

- 生成挑战R和加密挑战  $C = (R \parallel CRC(R)) \oplus S(K, V)$
- 计算密钥流  $S(K, V) = (R \parallel CRC(R)) \oplus C$
- 从接入点挑战时重用密钥流S(K,V)



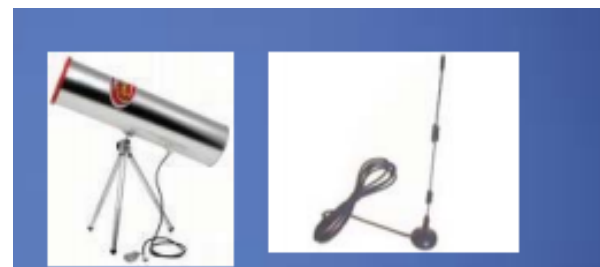
# DEMO: WARDRIVING AND WEP CRACKING



- Netstumbler wifi 扫描器



- 增益天线

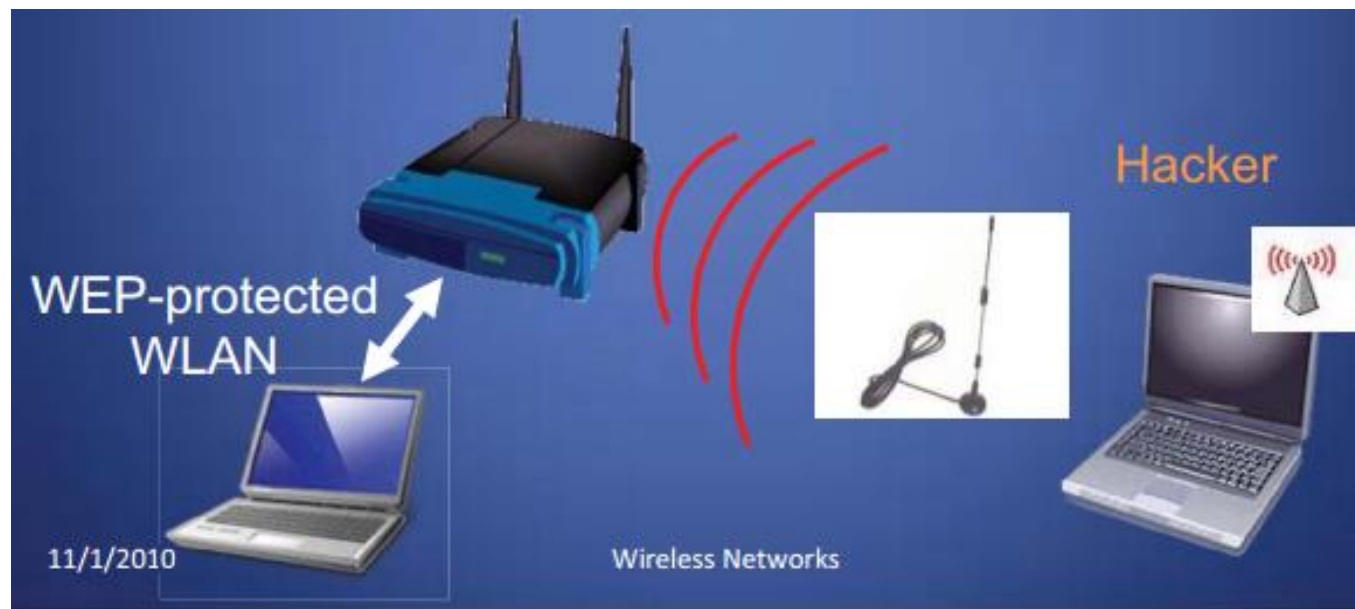


- 带监控模式的无线网卡

- GPS (可选)



- 接入点和客户端正在使用WEP加密
- 黑客利用驱逐工具嗅探



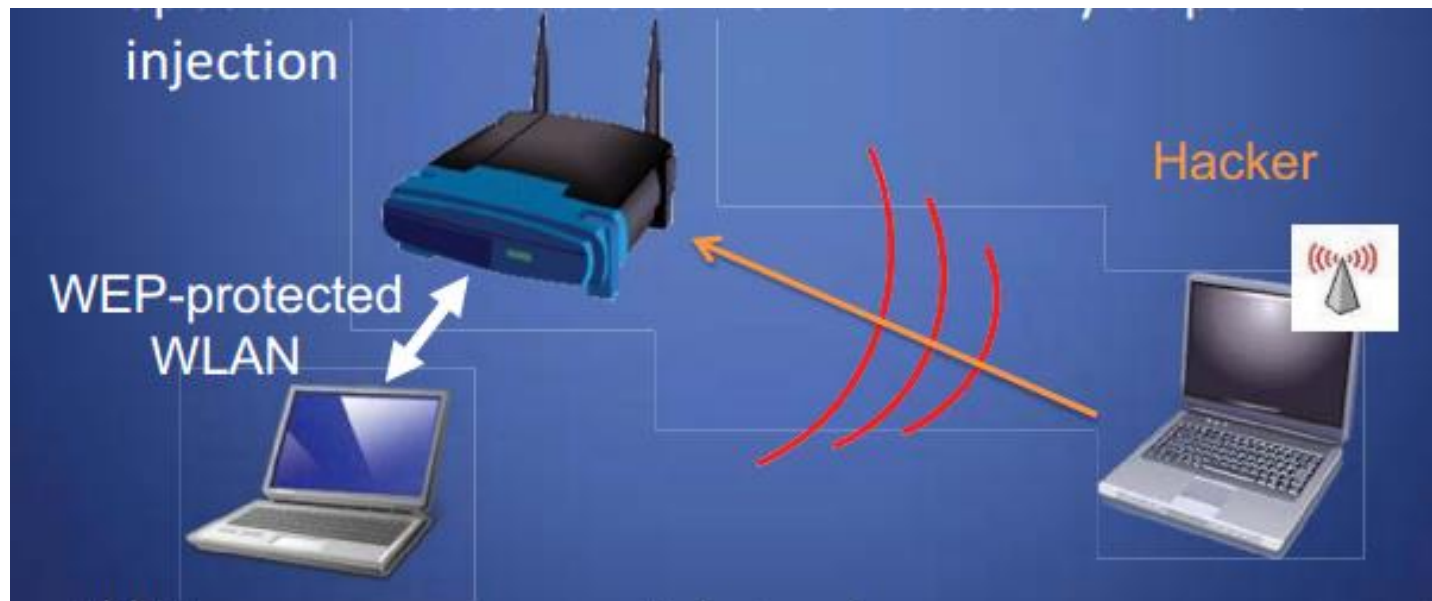


## ■ 要破解64位WEP密钥，您可以捕获：

- 包含初始化向量（IV）的50,000到200,000个数据包
- 只有大约1/4的数据包包含IV
- 所以你需要200,000到800,000个数据包

## ■ 捕获那么多数据包可能需要很长时间（通常是几小时甚至几天）

- 黑客注入数据包以创建更“有趣”的数据包
- 执行注入需要特殊的无线卡驱动程序





- 每个数据包一个，24bit的值
- 以邮件的明文部分发送
- 初始化向量的小空间保证了重用相同的密钥流
- IV碰撞：
  - 攻击两个明文消息的异或
  - IV通常是非可预测的，并引入了大量冗余



- 假设攻击者知道一个加密消息的一个明文,
  - $RC4(X) \oplus X \oplus Y = RC4(Y)$
  - 构造计算CRC32的新消息
- 即使不完全了解数据包，也可以翻转消息中的选定位并成功调整加密的CRC
- 我们知道ARP，重新注入：
  - ARP通常会重新广播并生成IV
  - Nikita Borisov, Ian Goldberg, David Wagner, Intercepting Mobile Communications: The Insecurity of 802.11. MOBICOM, 2001.



## ■ WEP被广泛认为是不安全的;

- 2005年, FBI在3分钟内公开破解了一个WEP密钥

## ■ 2003年提出WPA

## ■ 以多种方式改进WEP:

- 更大的密钥 (128位) 和初始化数据 (48位)
- 支持除共享密钥之外的各种类型的身份验证, 例如用户名/密码
- 在会话继续时动态更改密钥
- 用于检查完整性的加密方法
- 帧计数器以防止重放攻击



## ■ WPA是一个中间版本

- 最终版本：IEEE 802.11i，又名WPA2

## ■ 对WPA的改进是逐步的而非原理性的变化：

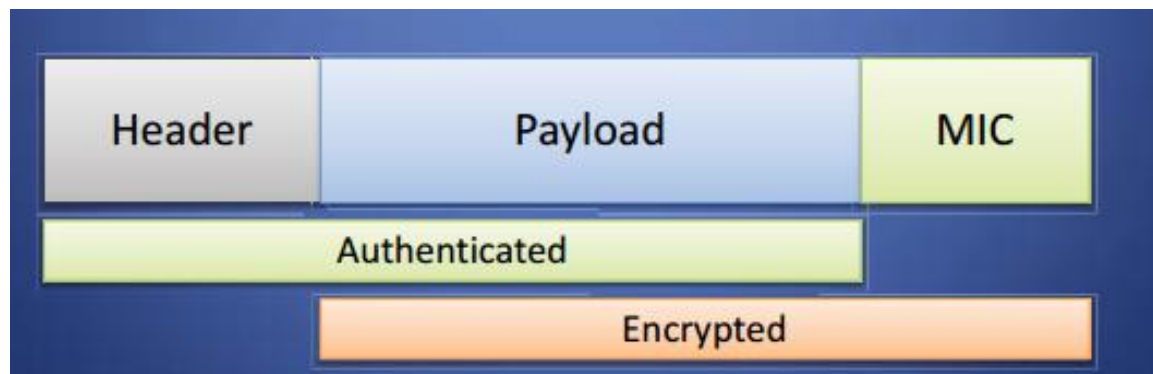
- 使用AES而不是RC4
- 处理加密，密钥管理和完整性
- 由反模式提供的MAC与密码块链接（CCMP）一起使用

## ■ WPA2需要最新的硬件才能正常运行，但随着时间的推移会越来越好





- 具有密码块链接消息认证码协议的计数器模式
- 使用Michael算法在明文标头和有效负载上计算64位消息完整性代码（MIC）
- 加密有效负载和MIC
- Michael不是一个强大的加密哈希函数





- **WEP, WPA和WPA2都只保护您的流量至接入点**
  - 在接入点之外没有提供安全性
- **其他方法可以实现端到端的加密**
  - SSL, SSH, VPN, PGP等
- **端到端加密通常比设置网络级加密更简单**
  - Brown无线网络未加密, 但不允许使用大多数明文协议 (仅允许HTTP, HTTPS, SSH, VPN, IMAPS, POPS)
  - Brown还在CIT中提供WPA网络
- **大多数这些解决方案都需要按应用程序配置**



## □思考题

- R-6.3、R-6.7、R-6.12、R-6.14
- C-6.2、C-6.8、C-6.12
- P-6.5
- 自学网上材料或课程

# 本章结束

~End~

但行好事，莫問前程。  
Those that can, do.  
Those that cannot,  
complain.