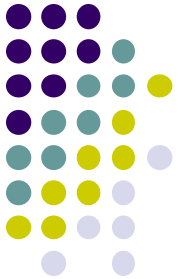
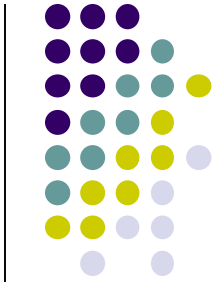
网络安全技术
课程信息



- 平时：30% （平时作业、课堂提问、实验）
- 期末考试： 70%
- 自选课程项目，可占20%
- 实验内容：包括书后每章的实践练习，SEED labs 的相关实验；可能会用到网络安全实验室
- http://qiqi789.github.io/teaching/network-security/

- TED > 日常生活中的网络犯罪——我们该做些什么
  - http://open.163.com/movie/2014/3/3/L/M9KC5G9MO_M9KGSBV3L.html

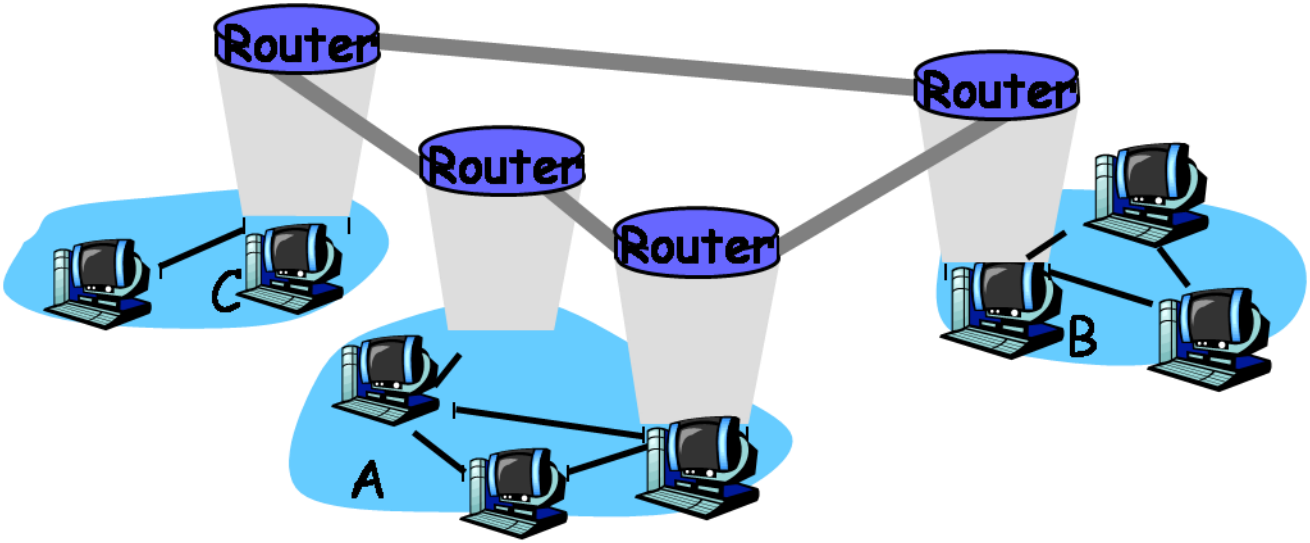


第1章
网络安全概论

《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年.

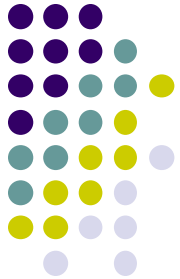
网络安全的重要性

- 因特网
  - –公共网络
  - – 基于TCP/IP
  - – 存储转发技术



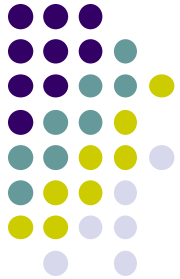
《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年.

第1章 网络安全概论



- 1.1 网络安全的任务
- 1.2 基本攻击类型和防范措施
- 1.3 攻击者类别
- 1.4 网络安全基本模型
- 1.5 网络安全信息资源网站

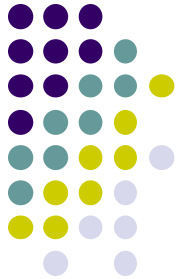
网络安全的任务



- 什么是数据？
  - 任何可以被计算机处理和执行的对象
- 数据的两种状态
  - 传输状态
  - 存储状态

网络安全的任务

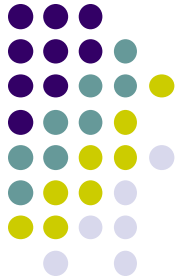
- 数据机密性
  - 包括数据的传输和存储两种状态
- 数据完整性
  - 包括数据的传输和存储两种状态
- 数据的不可否认性
- 数据的可用性



- 漏洞，瑕疵，缺陷
  - 软件
  - 协议设计
  - 系统配置
- 被动防御: 是什么人在何处发起的？
  - 多重防御机制
- 信息安全的其他领域

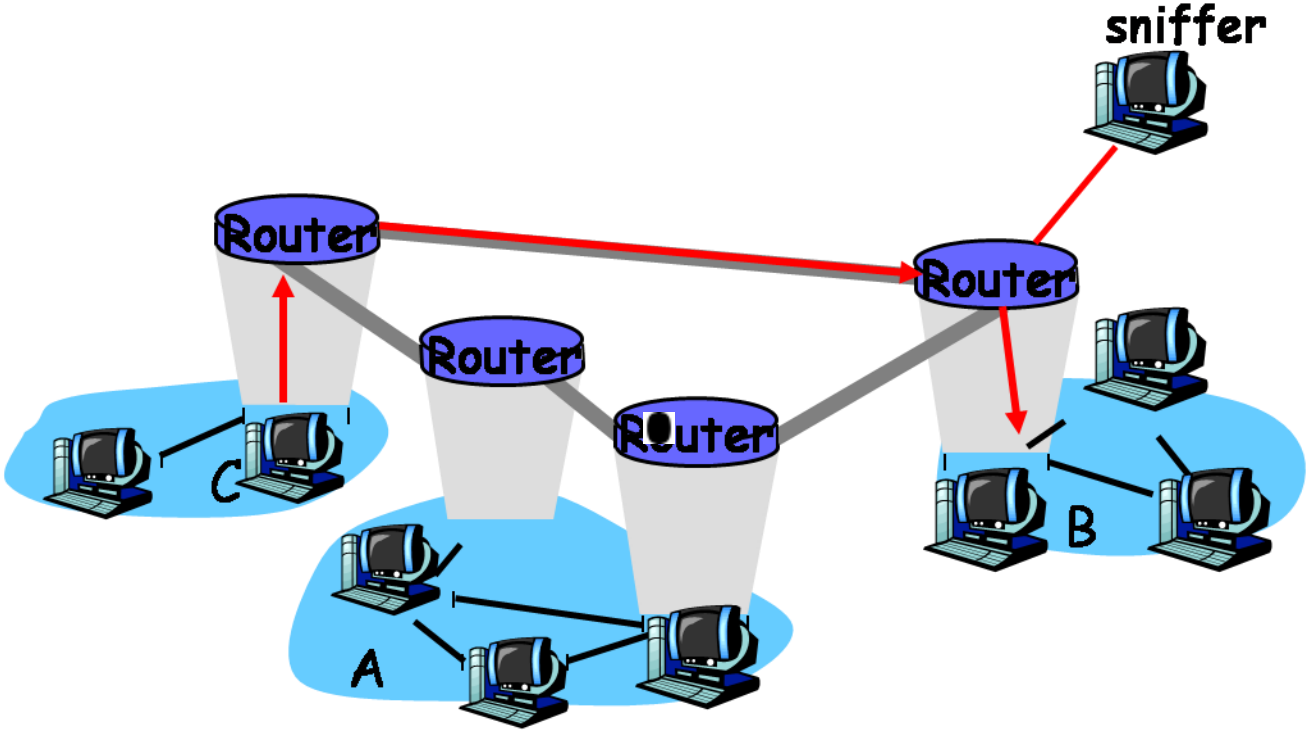
《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年.

第1章 网络安全概论



- 1.1 网络安全的任务
- 1.2 基本攻击类型和防范措施
- 1.3 攻击者类别
- 1.4 网络安全基本模型
- 1.5 网络安全信息资源网站

窃听

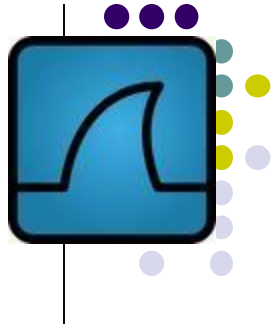


常用的网包嗅探软件: TCPdump, Wireshark

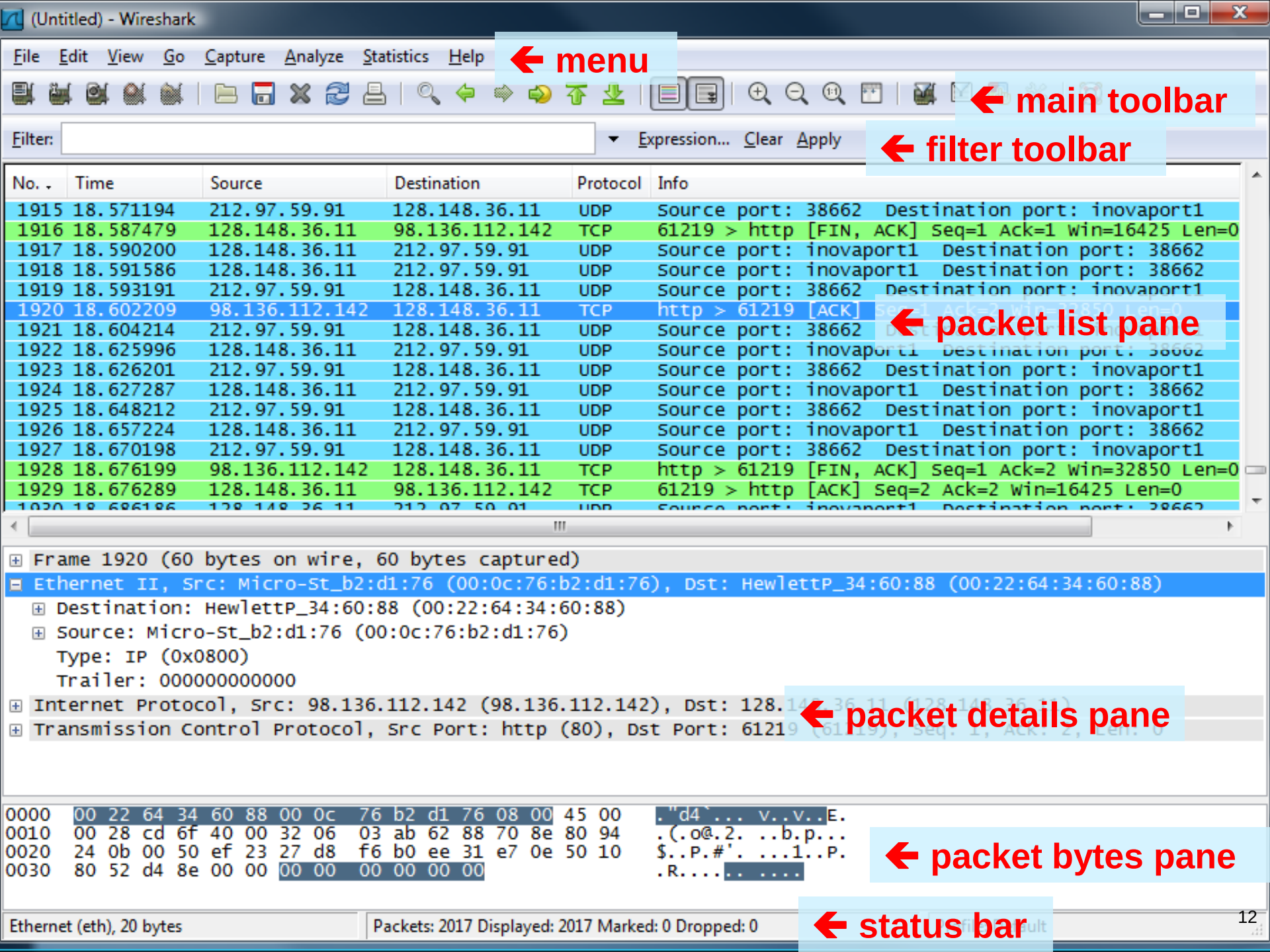
解决途径 - 数据加密

《计算机网络安全的理论与实践（第2版）》. 【美】王杰，高等教育出版社，2011年.

Wireshark



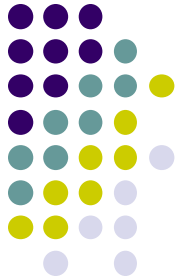
- Wireshark is a packet sniffer and protocol analyzer
  - Captures and analyzes frames
  - Supports plugins
- Usually required to run with administrator privileges
- Setting the network interface in promiscuous mode captures traffic across the entire LAN segment and not just frames addressed to the machine
- Freely available on www.wireshark.org


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
menu
main toolbar
Filter:
Expression... Clear Apply
filter toolbar
No. Time Source Destination Protocol Info
1915 18.571194 212.97.59.91 128.148.36.11 UDP Source port: 38662 Destination port: inovaport1
1916 18.587479 128.148.36.11 98.136.112.142 TCP 61219 > http [FIN, ACK] Seq=1 Ack=1 Win=16425 Len=0
1917 18.590200 128.148.36.11 212.97.59.91 UDP Source port: inovaport1 Destination port: 38662
1918 18.591586 128.148.36.11 212.97.59.91 UDP Source port: inovaport1 Destination port: 38662
1919 18.593191 212.97.59.91 128.148.36.11 UDP Source port: 38662
1920 18.602209 98.136.112.142 128.148.36.11 TCP http > 61219 [ACK]
1921 18.604214 212.97.59.91 128.148.36.11 UDP Source port: 38662
1922 18.625996 128.148.36.11 212.97.59.91 UDP Source port: inovaport1
1923 18.626201 212.97.59.91 128.148.36.11 UDP Source port: 38662 Destination port: inovaport1
1924 18.627287 128.148.36.11 212.97.59.91 UDP Source port: inovaport1 Destination port: 38662
1925 18.648212 212.97.59.91 128.148.36.11 UDP Source port: 38662 Destination port: inovaport1
1926 18.657224 128.148.36.11 212.97.59.91 UDP Source port: inovaport1 Destination port: 38662
1927 18.670198 212.97.59.91 128.148.36.11 UDP Source port: 38662 Destination port: inovaport1
1928 18.676199 98.136.112.142 128.148.36.11 TCP http > 61219 [FIN, ACK] Seq=1 Ack=2 Win=32850 Len=0
1929 18.676289 128.148.36.11 98.136.112.142 TCP 61219 > http [ACK] Seq=2 Ack=2 Win=16425 Len=0
packet list pane
Frame 1920 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: Micro-St_b2:d1:76 (00:0c:76:b2:d1:76), Dst: HewlettP_34:60:88 (00:22:64:34:60:88)
Destination: HewlettP_34:60:88 (00:22:64:34:60:88)
Source: Micro-St_b2:d1:76 (00:0c:76:b2:d1:76)
Type: IP (0x0800)
Trailer: 000000000000
Internet Protocol, Src: 98.136.112.142 (98.136.112.142), Dst: 128.
Transmission Control Protocol, Src Port: http (80), Dst Port: 6121
packet details pane
0000 00 22 64 34 60 88 00 0c 76 b2 d1 76 08 00 45 00 ."d4`... v..v..E.
0010 00 28 cd 6f 40 00 32 06 03 ab 62 88 70 8e 80 94 .(.o@.2. ..b.p...
0020 24 0b 00 50 ef 23 27 d8 f6 b0 ee 31 e7 0e 50 10 $..P.#'. ...1..P.
0030 80 52 d4 8e 00 00 00 00 00 00 00 00 .R...... ....
packet bytes pane
Ethernet (eth), 20 bytes
Packets: 2017 Displayed: 2017 Marked: 0 Dropped: 0
status bar

密码分析

- 密码分析
  从密文数据中寻找有用信息
  分析密文的统计特征
- 防御措施
  用更长的密钥和更安全的加密算法

盗窃登录密码



- 盗窃登录密码
  - 密码保护是第一道防御线
    - 也很有可能是系统唯一的防御
  - 窃取用户密码的方法：
    - 密码猜测
    - 社交工程
    - 字典攻击
    - 密码嗅探

《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年.

- 密码猜测

  最容易，特别是短小或缺省的密码

  10 中最常见的密码 (根据PC Magazine的统计):
  - password
  - 123456
  - qwerty (which are keys below 123456 on standard keyboard
  - abc123
  - letmein
  - monkey
  - myspace1
  - Password1
  - Blink182
  - The user’s own first name

- 社交工程

  用社交手段获取私密信息

  - 身份伪装

    攻击者伪装成别人去欺骗受害者

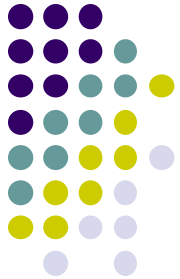
    (见课本第六页例子)

- 钓鱼、网转

  近些年最常见的一种大规模社交工程攻击形式

  伪造电子邮件或者网站进行的攻击

  - 参见下一节课件一个真实的网络钓鱼事件(注意钓鱼邮件中的不地道的英文表达), 邮件中的链接是陷阱



Date: Fri, 5 Oct 2007 16:11:46 -0700

From: US Bank SCD-Verify@usbank.com

Subject: US Bank – Internet Online Access is Locked – October 5, 2007 at 12:23:05 PM

Dear US Bank Customer,

We're sorry, but you reached the maximum number of attempts allowed to login into your US Bank account. For your protection, we have locked your account.

Consequently, we placed a temporary restriction on your account. We did this to protect your account from any fraudulent activity.

Please click below and complete the steps to Remove Limitations. This allows us to confirm your identity and unlock your US Bank online account

http://www4-usbank.com/

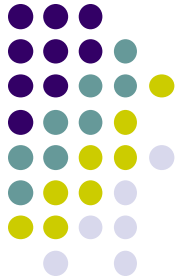
If we do no receive the appropriate account verification within 48 hours, then we will assume this US Bank account is fraudulent and will be suspented.

一般而言，任何钓鱼邮件都包括一个超级链接到一个假冒网站，称之为钓鱼网站

其他形式

- 收集垃圾废纸，找到有用信息
- 在用户上网时弹出新窗口，诱使用户登录

防御措施 – 浏览器抗钓附载模块新技术可用来检测和阻止用户进入诱饵网页



- 字典攻击

  登录密码经过加密后存储在主机系统中

  - UNIX/Linux:

    用户登录密码存储在/etc文件夹下一个叫 *shadows*的系统文件中

  - Windows XP:

    用户登录密码存储在系统的注册表中一个叫*SAM*的文件中

《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年.

一个典型的字典攻击过程如下：

- 收集、获取用户名信息和对应的加密密码
- 用散列算法逐一加密所有单词、日期、人名等
- 将盗取的密文和上一步骤计算出的密文逐一比较，找出相同者，则得到对应的明文即是登录密码

构造一个彩虹表帮助节约存储空间，节省计算成本

彩虹表

- 令r 是一个缩减函数
- 令h 是一个加密哈希函数
- W_{11}是一个给定的登录密码. 交替使用函数 h和 r ， 生成如下互不相同的密码链：

$$w_{11}, w_{12}, \ldots, w_{1n_1},$$

有, $w_{1i} = r(h(w_{1,i-1}), i = 2,3,\ldots,n_1$ 得到$(w_{11}, h(w_{1n1}))$， 即彩虹表的第一行

- 选一个之前链中未出现的 w_{j1}

Password	Hash value
w_{11}	$h(w_{1\,n1})$
w_{21}	$h(w_{2\,n2})$
…	…
w_{k1}	$h(w_{k\,nk})$

重复这一过程k次在彩虹表中产生 k行

《计算机网络安全的理论与实践（第2版）》. 【美】王杰，高等教育出版社，2011年.

假设两个函数 $f: A \rightarrow B$ ， $g: B \rightarrow A$. 令 $y \in B$ and $i \geq 0$.

定义:

$$(f \circ g)^i(y) = \begin{cases} y & if\ i = 0 \\ f\left(g\left((f \circ g)^{i-1}(y)\right)\right) & if\ i \geq 1 \end{cases}$$

令 Q_0 值为对密码 w加密后的值. 即 $Q_0 = h(w)$. 如果

$$h\left((h \circ r)^i(Q_0)\right) = h(w_{j\,n_j})$$

对一些 $i \geq 0$ 和 j 有 $1 \leq j \leq k$ 并且$i \leq j$, 那么 w 有可能出现在 $w_{j1}, \ldots w_{j,nj}$ 密码链的第 j项 .

- 在彩虹表中找到 w 的算法：

1. 令 $Q_1 \leftarrow Q_0$，$t \leftarrow 0$. 令 $n = \max\{n_1,\ldots,n_k\}$

2. 检查是否有一个 $1 \le j \le k$ 使得 $Q_1 = h(w_{j,nj})$ 并且 $t \le n$. 如果有，执行步骤3；否则，执行步骤 4

3. 对w_{j1} 交替使用r和h，使用i次，$0 \le i \le j$，直到 $w_{j,ni} = (r \circ h)^i(w_{j1})$ 产生出了$h(w_{j,ni}) = Q_0$ 如果找到了这样的一个 $w_{j,ni}$，返回 $w = w_{j,ni}$；否则，执行步骤4

4. 令 $Q_1 \leftarrow h(r(Q_1))$，$t \leftarrow t + 1$. 如果 $t \le$ n 那么跳转到步骤2，否则，返回“未找到登录密码。”(彩虹表不可能包含哈希值为Q_0 的登录密码)

《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年.

- 密码嗅探

密码嗅探是一种软件，用来获取远程登录信息，比如用户名和密码

防御方法 —加密所有信息，包括登录信息，使用远程登录软件，比如，SSH 和HTTPS

Cain & Abel, 就是这样的一个网络嗅探软件，能捕获、破解使用Windows操作系统的用户登录密码

密码保护

保护密码不被窃取的准则：

1. 用长密码，用字母，大写字母，特殊符号的组合做密码，不要使用常用单词，普通姓名和日期。
2. 不要轻易告诉他人你的密码，不要把密码提供给尽管看起来可信的人，如果一定要给密码，请当面交给可信者。
3. 不定期的更改密码，如要重复使用旧密码。
4. 不同的账户不要使用相同的密码。
5. 不要使用不加密登录信息和个人重要信息的远程软件。
6. 用切碎机切碎丢弃的有个人信息的纸张。
7. 避免进入任何弹出窗口，避免在可疑邮件中点击任何链接。

- 其他的用户认证方法

  - 生物识别技术，利用生物个体的唯一性—连接生物特征识别装置到计算机，比如指纹读写器或者视网膜扫描器。

  - 用身份认证技术 – 发行方给予电子认证

    使用用户的密码认证是最简单的方法

身份诈骗

- 身份诈骗攻击，冒充受害者身份，不用受害者密码即可实施攻击。
  - 中间人攻击
  - 重放攻击
  - 网络诈骗
  - 软件剥削

- 中间人攻击

攻击者在通信的二人之间或多人之间安装网络设备或窃听软件（或者在他自己的机器上装），用这些设备去解释、修改、伪造数据在通信者之间传输。

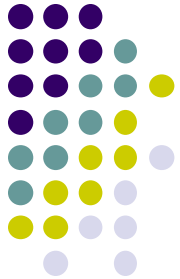
A认为自己在和B通信

攻击者解释修改了AB之间的通信

B认为自己在和A通信

防御措施—编码或验证IP包

《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年.



- 重放攻击

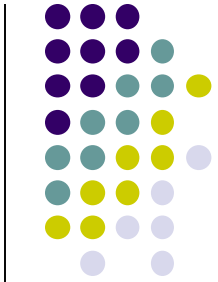
攻击者首次拦截了一个合法的信息，经过一段时间后，原封不动地将此消息发给最初的接受者。

例如，攻击者可能拦截了合法用户的认证消息，并用此消息去伪造用户身份得到系统的服务。

防御机制 –

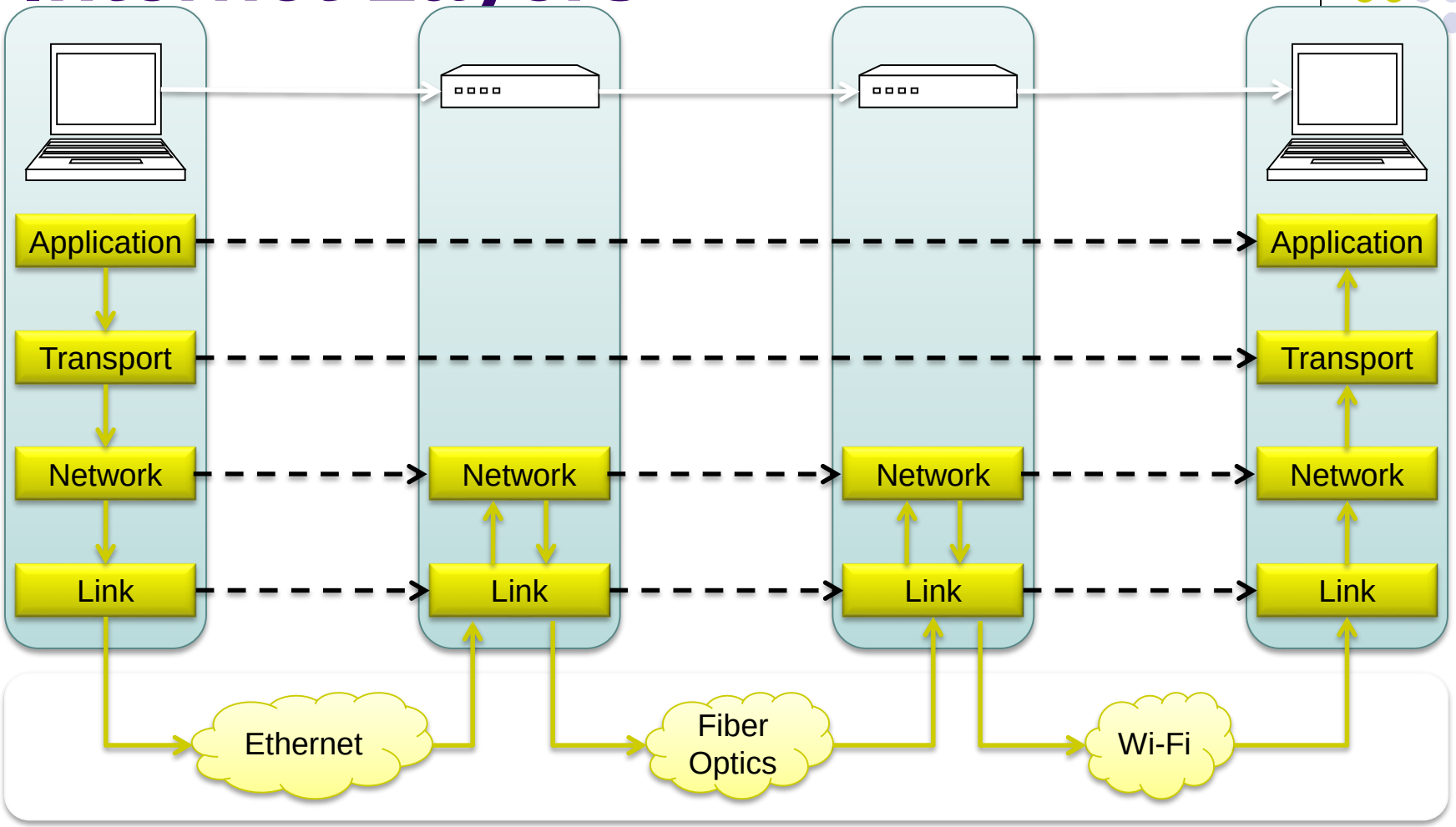
- 给消息附上一个随机数，用于代表某个特定信息。
- 给消息附上时间戳
- 最佳方法是同时使用随机数和时间戳

- 网络诈骗
  - IP诈骗是一种最主要的网络诈骗技术
  - SYN 充斥
    - 攻击者向攻击目标主机TCP缓冲区发送大量SYN 控制包
    - 目的：使目标计算机不能与其他计算机建立通信连接 (也就是成为哑巴计算机)
  - ARP 诈骗，也称之为APR投毒

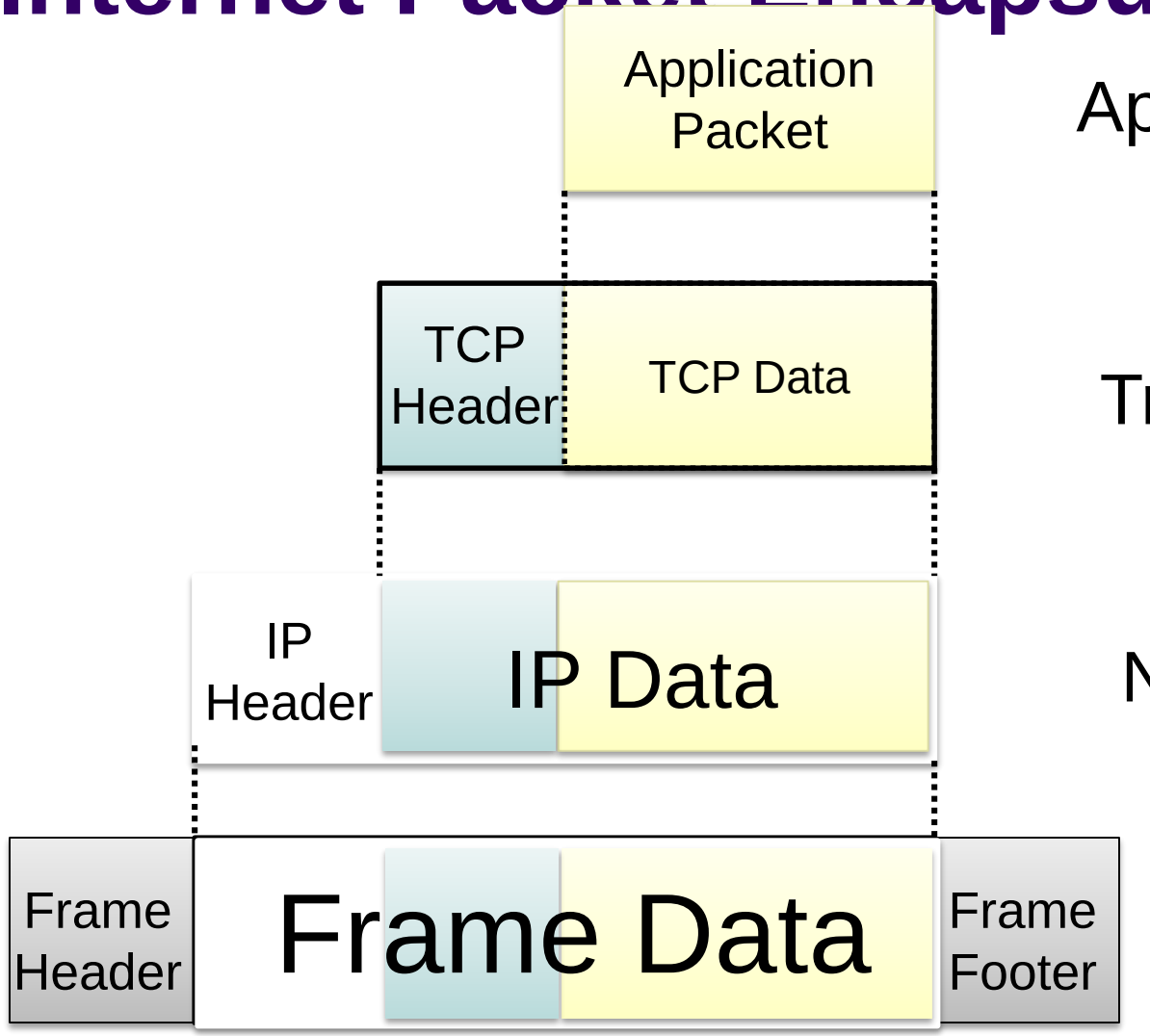


相关网络知识

Internet Layers



Internet Packet Encapsulation



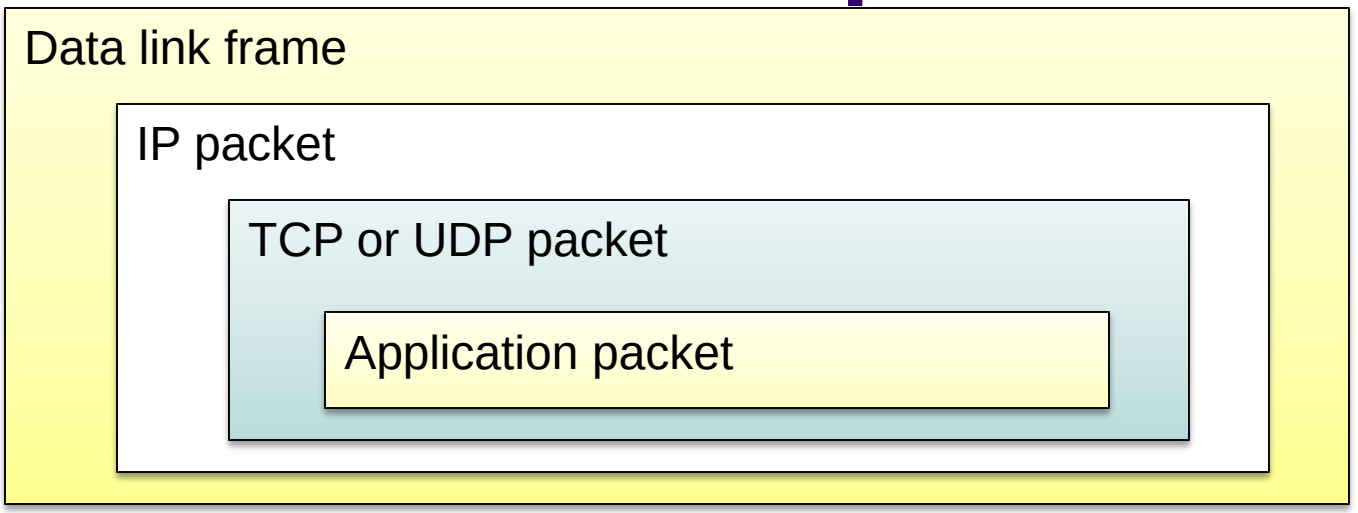
Application Layer

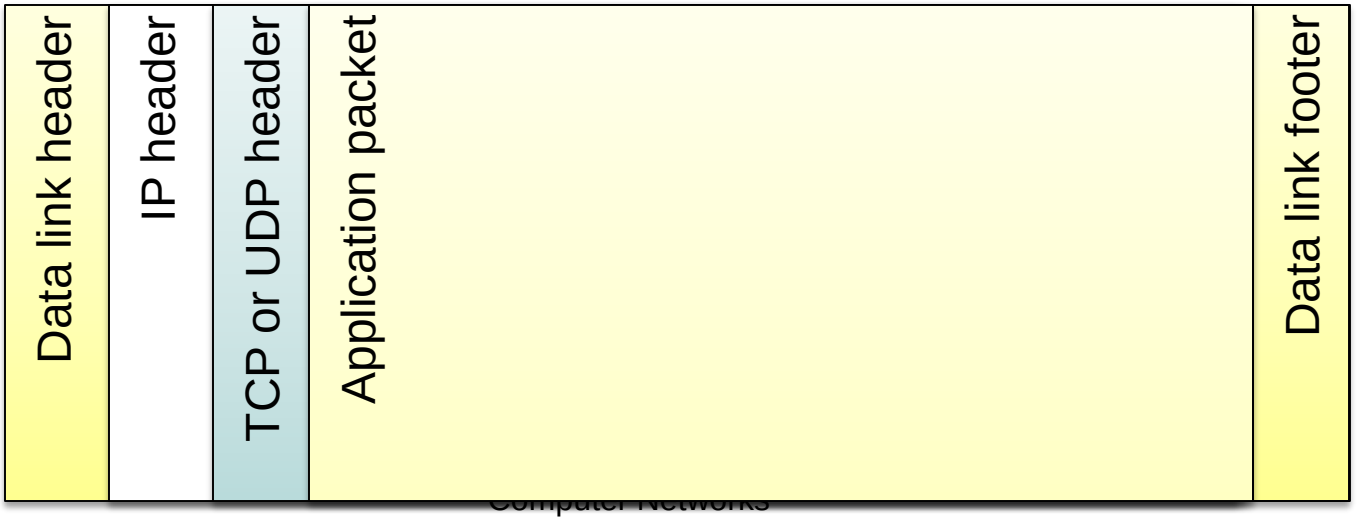
Transport Layer

Network Layer

Link Layer

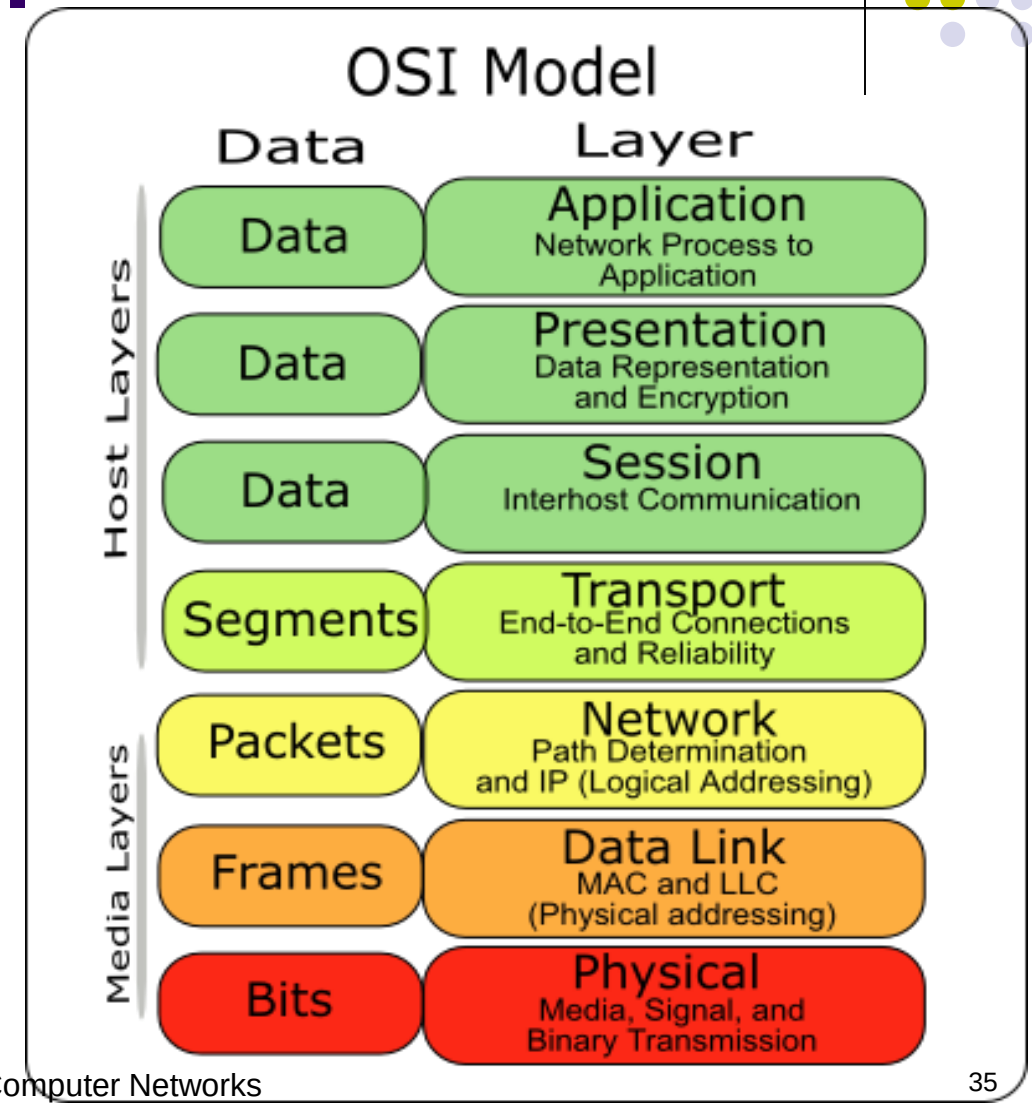
Internet Packet Encapsulation



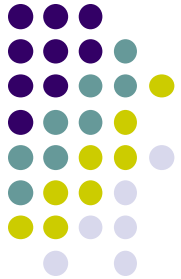


The OSI Model

- The OSI (Open System Interconnect) Reference Model is a network model consisting of seven layers
- Created in 1983, OSI is promoted by the International Standard Organization (ISO)

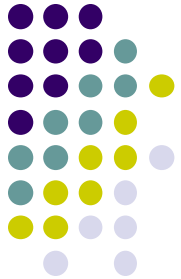


Transmission Control Protocol



- TCP is a transport layer protocol guaranteeing reliable data transfer, in-order delivery of messages and the ability to distinguish data for multiple concurrent applications on the same host
- Most popular application protocols, including WWW, FTP and SSH are built on top of TCP
- TCP takes a stream of 8-bit byte data, packages it into appropriately sized segment and calls on IP to transmit these packets
- Delivery order is maintained by marking each packet with a sequence number
- Every time TCP receives a packet, it sends out an ACK to indicate successful receipt of the packet.
- TCP generally checks data transmitted by comparing a checksum of the data with a checksum encoded in the packet

Ports



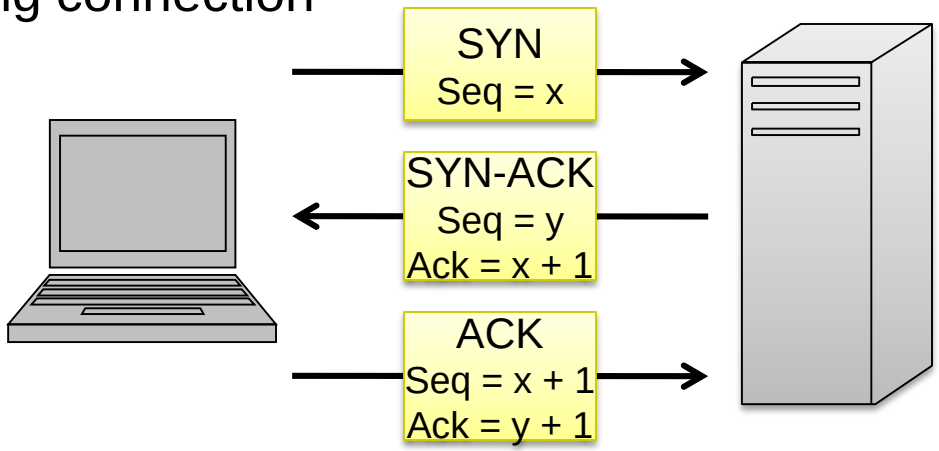
- TCP supports multiple concurrent applications on the same server
- Accomplishes this by having ports, 16 bit numbers identifying where data is directed
- The TCP header includes space for both a source and a destination port, thus allowing TCP to route all data
- In most cases, both TCP and UDP use the same port numbers for the same applications
- Ports 0 through 1023 are reserved for use by known protocols.
- Ports 1024 through 49151 are known as user ports, and should be used by most user programs for listening to connections and the like
- Ports 49152 through 65535 are private ports used for dynamic allocation by socket libraries

TCP Packet Format

Bit Offset	0-3	4-7	8-15	16-18	19-31
0	Source Port			Destination Port	
32	Sequence Number				
64	Acknowledgment Number				
96	Offset	Reserved	Flags	Window Size	
128	Checksum			Urgent Pointer	
160	Options				
>= 160	Payload				

Establishing TCP Connections

- TCP connections are established through a three way handshake.
- The server generally has a passive listener, waiting for a connection request
- The client requests a connection by sending out a SYN packet
- The server responds by sending a SYN/ACK packet, indicating an acknowledgment for the connection
- The client responds by sending an ACK to the server thus establishing connection



SYN充斥

攻击者向攻击目标计算机TCP缓冲区发送大量SYN控制包，使被攻击的计算机不能与其他计算机通信。

1. 攻击者给目标计算机发送大量诡诈SYN 控制包，目标计算机被迫给包含在SYN 控制包内的IP地址发送 ACK控制包
2. 因为SYN控制包将其封装的IP包首部所含的起始网址换成了另外一个IP地址，而此网址不可达，所以受害者计算机不可能收到他要等待的ACK包，因此诡诈SYN控制包继续停留在目标主机的TCP缓冲区中。
3. 目标机的 TCP 缓冲区完全被欺诈的SYN包所充斥

TCP劫持

V 是公司主机

Alice是公司的一名雇员，准备要远程登录到公司主机 V

她和V的 TCP连接有可能被TCP劫持，过程如下:

1. Alice 向主机V发了SYN包请求远程登录
2. 攻击者劫持了这个包，用SYN充斥的方法使V成为了哑巴机，使得V无法完成三次握手
3. 攻击者预测出正确的V的ACK回应控制包该用的回应号码，伪装成V发给Alice，用正确的序列号和ACK号码以V的名义发给Alice
4. Alice 证实ACK包并且发送ACK包回应给攻击者，至此，攻击者与Alice完成TCP握手，建立连接
5. TCP 连接就此在Alice和攻击者之间建立，而非Alice和V

- ARP 诈骗

  攻击者改变合法的连网计算机的 MAC 地址为一个其指定的 MAC地址

  防御方法 –

  检查 MAC地址和域名

ARP

- The address resolution protocol (ARP) connects the network layer to the data layer by converting IP addresses to MAC addresses
- ARP works by broadcasting requests and caching responses for future use
- The protocol begins with a computer broadcasting a message of the form

  who has <IP address1> tell <IP address2>

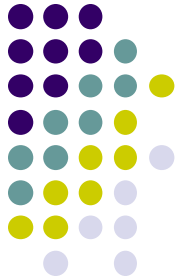
- When the machine with <IP address1> or an ARP server receives this message, its broadcasts the response

  <IP address1> is <MAC address>

- The requestor's IP address <IP address2> is contained in the link header
- The Linux and Windows command arp - a displays the ARP table

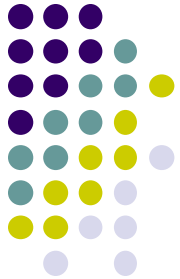
```
  Internet Address      Physical Address      Type
  128.148.31.1          00-00-0c-07-ac-00     dynamic
  128.148.31.15         00-0c-76-b2-d7-1d     dynamic
  128.148.31.71         00-0c-76-b2-d0-d2     dynamic
  128.148.31.75         00-0c-76-b2-d7-1d     dynamic
  128.148.31.102        00-22-0c-a3-e4-00     dynamic
  128.148.31.137        00-1d-92-b6-f1-a9     dynamic
```

ARP Spoofing



- The ARP table is updated whenever an ARP response is received
- Requests are not tracked
- ARP announcements are not authenticated
- Machines trust each other
- A rogue machine can spoof other machines

ARP Poisoning (ARP Spoofing)



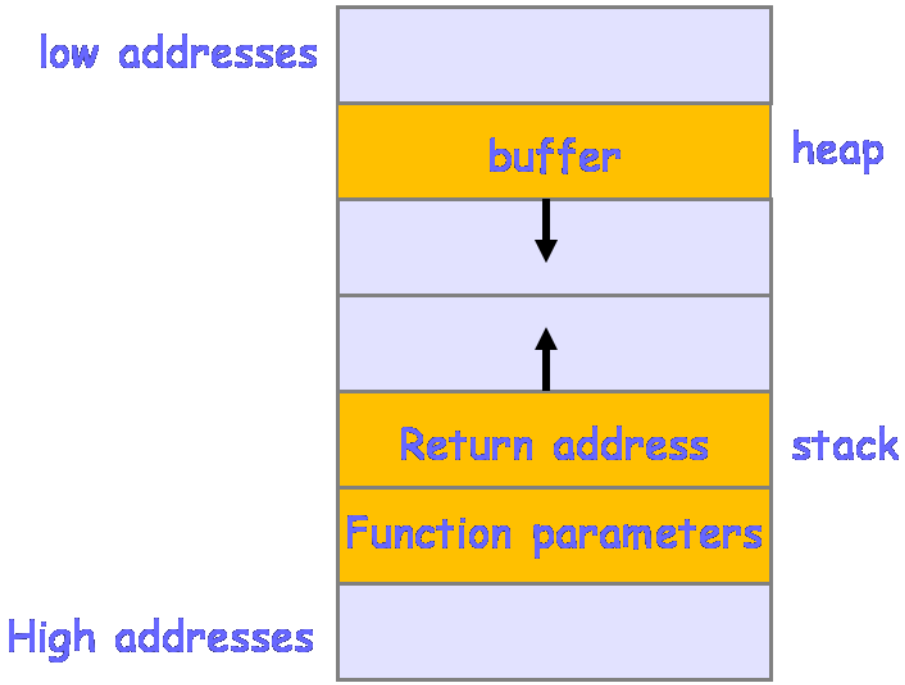
- According to the standard, almost all ARP implementations are ***stateless***
- An arp cache updates every time that it receives an arp reply… even if it did not send any arp request!
- It is possible to “poison” an arp cache by sending gratuitous arp replies
- Using static entries solves the problem but it is almost impossible to manage!

缓冲区溢出攻击

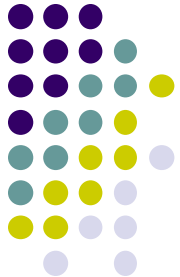
- 缓冲区溢出攻击

  缓冲区溢出，又名缓冲区超限，是一种常见的软件漏洞。即程序进程给该缓冲区写入多过其容量的内容，则缓冲区溢出。

有可能利用缓冲区溢出，重定向受害者的程序去执行攻击者自己的代码，这类攻击常常利用了某些函数，**数据放在堆，函数调用的返回地址放在栈内**。



《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年.



- 缓冲区溢出的攻击步骤：

1. 找到一个允许缓冲区溢出的程序（例如，找到一个程序使用了是不检查边界的函数）
2. 将攻击者的可执行代码存入内存
3. 算出需拷贝的足够长的字符串到缓冲区
4. 使缓冲区溢出，数据跨堆入栈，修改函数返回地址，使其执行攻击者程序

防御措施– 坚持进行语句检查并检查要写入缓冲区的内容的界限

抵赖

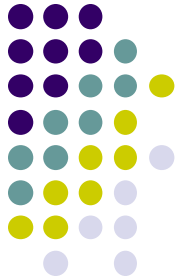
有些情况下，数据所有者可能会否认数据为自己所有或逃避法律后果

- 他可能争辩说他从未发送或收到有问题的数据

防御途径 –

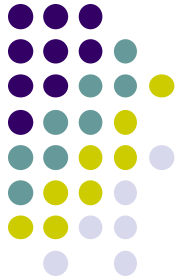
加密和身份认证

入侵



- 未授权用户进入他人计算机系统，利用系统配置漏洞、通信协议缺陷和软件漏洞实现非法入侵他人系统
- 入侵检测是一种探测入侵行为的技术，关闭TCP 和UDP 可能被入侵者利用的端口，也可有效降低入侵
- IP扫描和端口扫描是常用的攻击工具，同时，也可以来帮助用户发现自身系统哪些端口开启了，哪些开启的端口可能会遭受攻击

流量分析

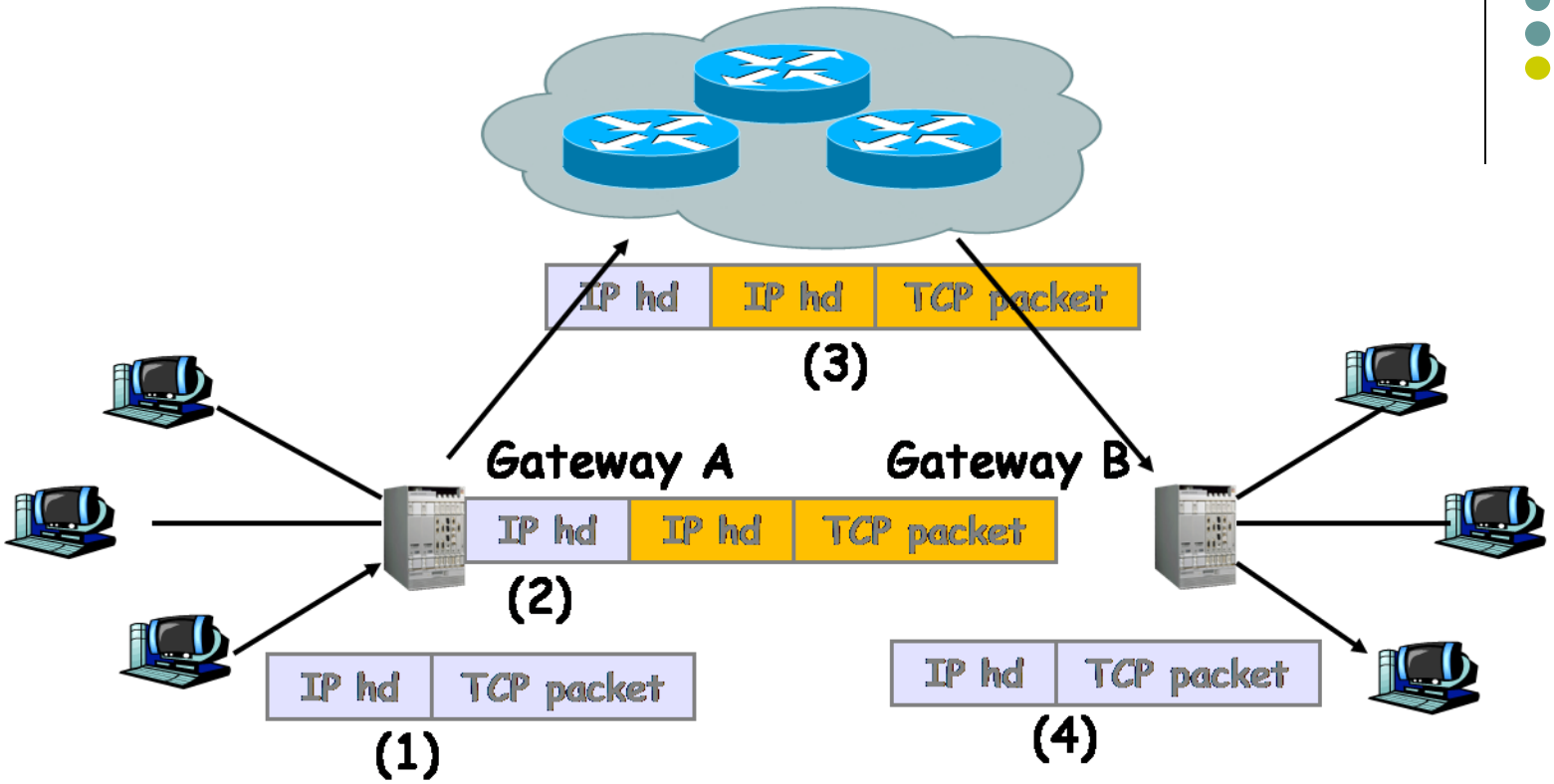


目的在于依靠分析IP包发现通话的双方及其通信量，尽管IP包已经加密，入侵者仍旧可以分析IP头文件获得有用的信息

防御措施 –

加密 IP包文件，但是一个IP头文件加密后的IP包不能送达目的地，因此，需要网关

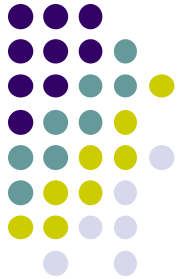
- 网关也可以保护内部网络拓扑



(1) 发 IP包到网关A. (2) 网关 A加密了发送者的IP包并传往下一个路由器 (3) IP包经由网关 A 传送到网关B. (4)网关B去掉头文件，解密发送者的IP包,并且将其发送给接受者。

《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年.

服务阻断攻击（Denial of Service）

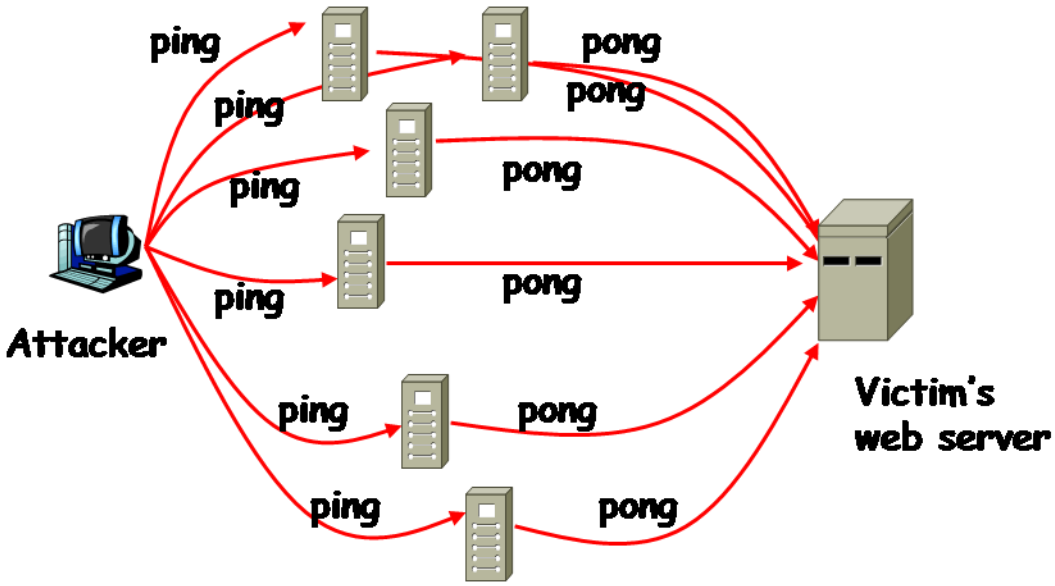


阻止合法用户得到正常通信和资源

- DoS –由单台计算机发起攻击
- DDoS – 操作多台计算机发起攻击

DoS

SYN 充斥是一种典型和有效的 DoS 攻击， smurf 攻击是另一种典型的 DoS攻击



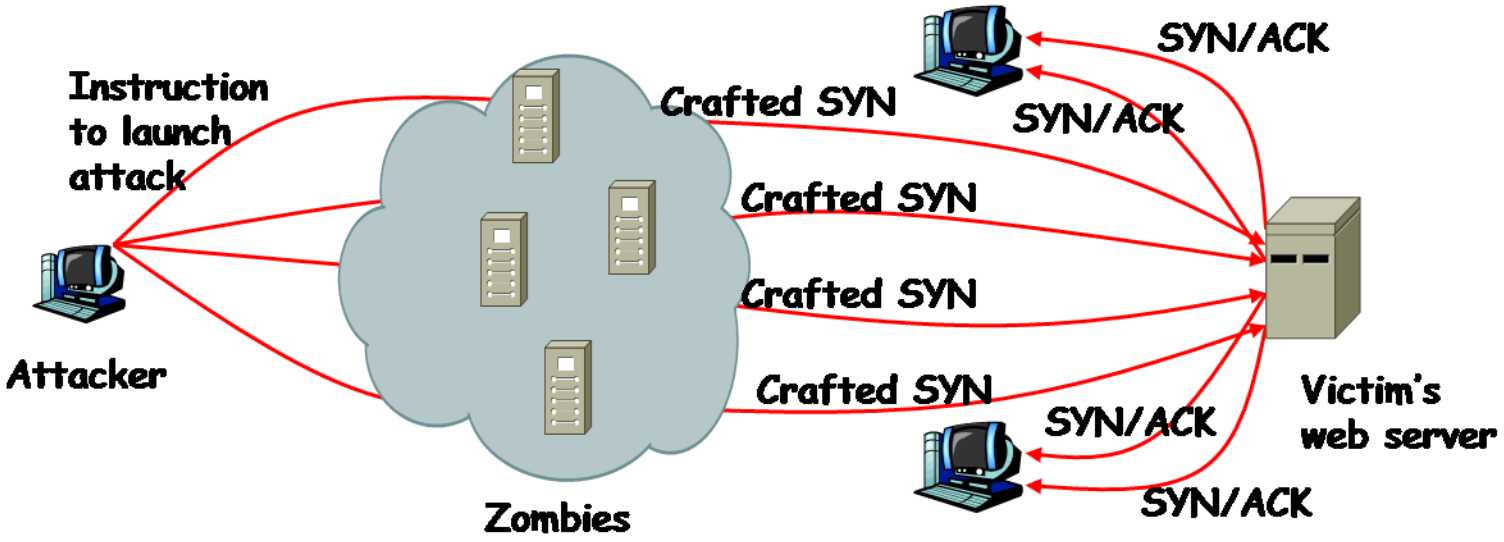
攻击者在一个很短的时间段内向网上的一组计算机发送大量**ping指令**， 并使得这些指令看起来出自其选取的受攻击的目标主机，因此这些计算机会向其回送pong消息。

《计算机网络安全的理论与实践（第2版）》. 【美】王杰，高等教育出版社，2011年.

DDoS

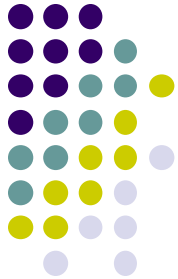
典型的 DDoS 攻击过程如下：

1. 利用操作主机扫描尽可能多的连网计算机
2. 安装一个特殊的攻击软件，然后命令所有被控制计算机发起DoS攻击，这些机器成为占比机
3. 操纵主机命令所有占比机同时向同一目标发起DoS攻击



《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年.

垃圾邮件



垃圾邮件是不请自来的信息，多是商业信息，或钓鱼信息

其目的虽然不是危害用户主机工作，但仍然消耗了计算资源

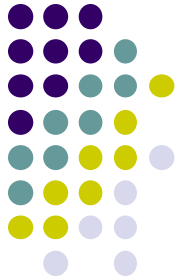
垃圾邮件也出现在万维网搜索引擎、即时消息、博客、手机等各种网络应用中

防御措施 – 垃圾过滤软件能够检测和阻止垃圾邮件进入用户邮箱

恶意软件

危害用户计算机的软件称之为恶意软件

- 病毒
- 蠕虫
- 特洛伊木马
- 逻辑炸弹
- 后门程序
- 间谍软件



病毒和蠕虫

- 病毒软件是可以自我复制的软件
  - 它不是一种孤立的程序，它必须依附一个主程序或文件中
  - 一个包含病毒的主程序或文件叫做受感染宿主
- 蠕虫可以自我复制的，但不同于病毒，蠕虫可以单独生存，不必依附载体

防御方法–

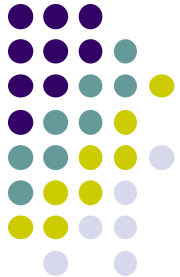
- 不要从非信任源下载软件
- 不要运行来路不明的程序
- 确保即时安装、更新补丁软件

- 特洛伊木马

特洛伊木马是一种软件，表面上看在在做一件事，实际上在做另一件事

特洛伊木马常常将自己伪装成具有诱惑力而无害的软件，诱使人们下载

防御方法 – 如同对付病毒和蠕虫一样，运用杀毒软件可以检测、隔离和删除它

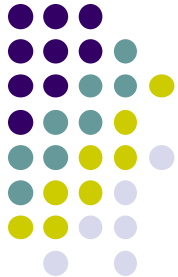


- 逻辑炸弹

  逻辑炸弹是植入在程序内的子程序或指令，当一定的条件满足后，会触发执行

  防御措施 –

- 雇主需关照你的职员，使他们不至于植入逻辑炸弹危害公司
- 项目管理者应该雇佣外面的公司或者组建专门的团队而不是让源代码开发者去检查源程序
- 必须建立相关的法律条款使有意植入逻辑炸弹的雇员面对法律的严惩



后门程序

后门程序有进入软件的密码通道

他们可能由程序开发者加在软件内，得以无需登录密码便可快速进入程序，修改和调试代码

防御方法 –

专门的团队来检查源代码

- 间谍软件

间谍软件是一种将自己安装在用户电脑上的软件

间谍软件常用于监视用户浏览习惯并且时常弹出商业广告骚扰用户

- 浏览器劫持 –篡改用户浏览器设置
- 僵尸软件– 一种软件可以接管用户的计算机并且把其变为占比机，用来实施DDoS 攻击或者变为一个病毒传播者，比如发送垃圾邮件或者传播病毒

《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年.

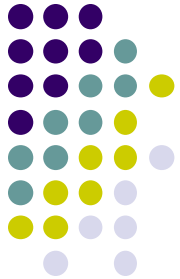
间谍软件还可以做的事包括：

- 浏览监视 – 监视用户浏览习惯，发送报告给网页服务器或攻击者主机，告知用户的网购习惯和模式
- 密码窃取 –通过击键记录软件记录用户敲击的按键来窃取用户的登录信息
- 广告软件 – 在用户的网页上自动显示广告窗口

防御方法 –

使用抗间谍软件来检测和消除间谍软件带来的危害

第1章 网络安全概论



- 1.1 网络安全的任务
- 1.2 基本攻击类型和防范措施
- 1.3 攻击者类别
- 1.4 网络安全基本模型
- 1.5 网络安全信息资源网站

黑客

- 黑客

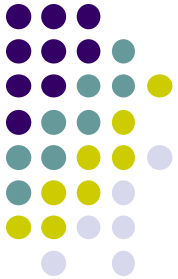
  骇客是指那些对计算机系统知识有特别钻研，对软件，算法，计算机配置的精巧细节有深入了解的一群人

  - *黑顶骇客* – 为了他们自身的利益专门破坏他人计算机系统的人
  - *白顶骇客*– 为了寻找安全漏洞和提供更多安全措施而探索网络安全漏洞的人
  - *灰顶骇客*–介乎于白顶骇客与黑顶骇客之间的人，大多数时间他们安分守己，但偶尔也会干点黑客干的事

  当发掘出软件产品的安全弱点，白顶骇客和灰顶骇客会首先与生产该产品的公司取得联系，寻找问题补救解决方案

《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年.

抄袭小儿



抄袭小儿是一群用黑客写的程序攻击他人计算机的人

尽管他们不知道如何写黑客软件或者并不理解黑客软件工作原理，但是却仍然具有不可忽视的危害性

《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年.

电脑间谍

拦截网络通信，获取情报就是电脑间谍的工作

每个国家都有自己的情报机关

每支军队有自己的情报系统

他们收集情报，破译各类密码通信

恶意雇员，电脑恐怖分子，假想敌

- 恶意雇员

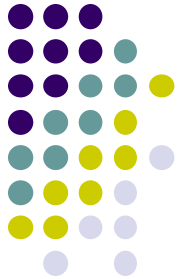
  恶意雇员是那些试图破坏雇主网络安全的雇员

- 电脑恐怖分子

  恐怖分子是那些运用电脑和网络技术从事危害计算机安全从而制造公众恐慌的极端分子

- 假想敌（本书所讨论的）
  - 黑客
  - 抄袭小儿
  - 电脑间谍（为经济目的背叛自己祖国或组织的贪婪的人）
  - 恶意雇员

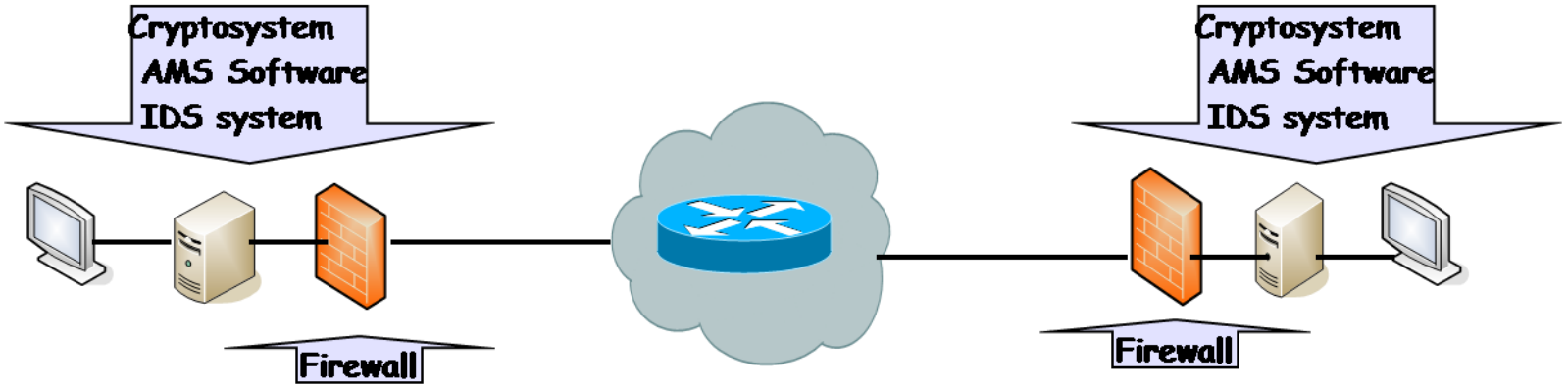
第1章 网络安全概论



- 1.1 网络安全的任务
- 1.2 基本攻击类型和防范措施
- 1.3 攻击者类别
- 1.4 网络安全基本模型
- 1.5 网络安全信息资源网站

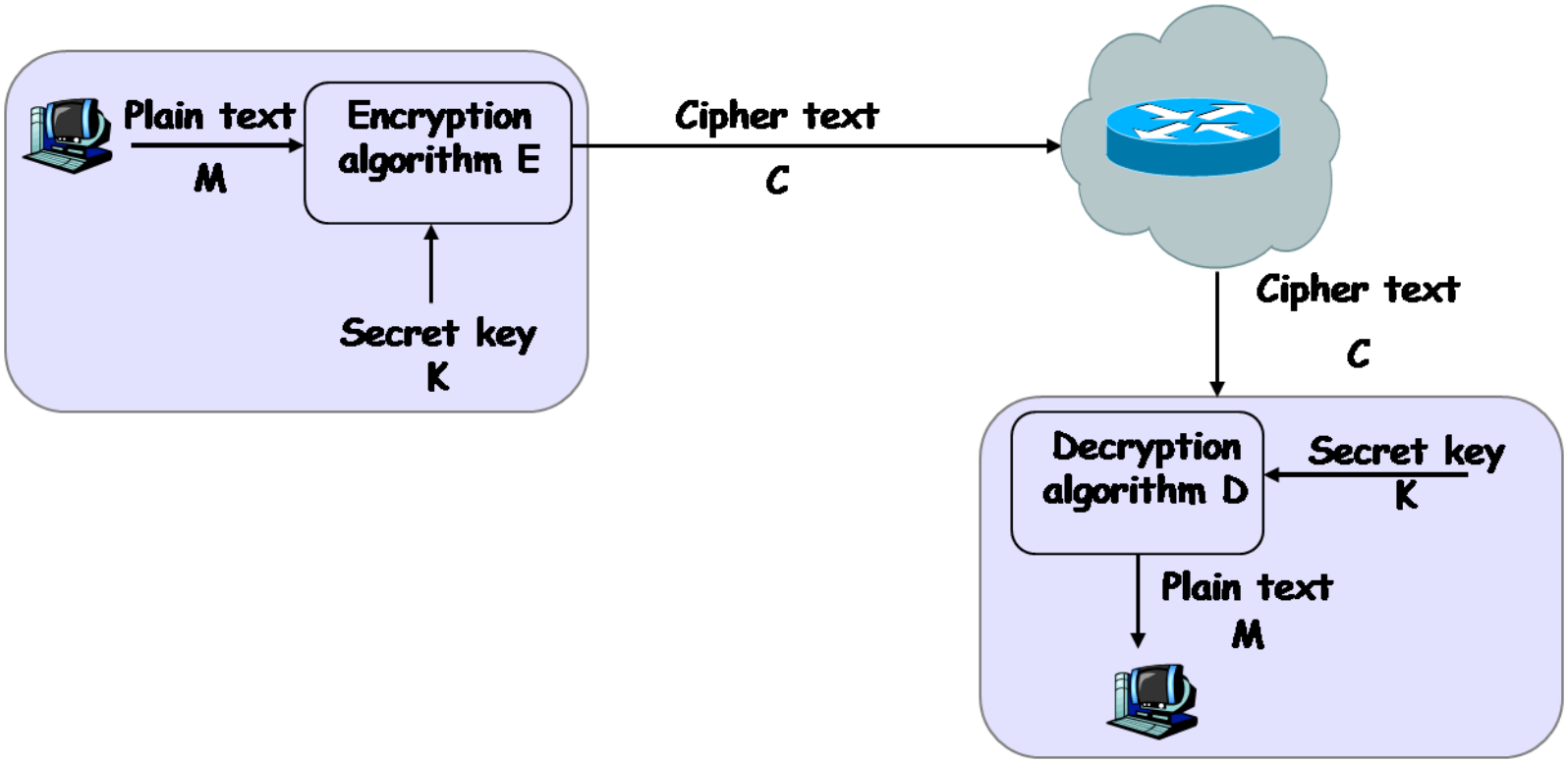
网络安全基本模型

网络安全基本模型由四部分组成：密码系统，防火墙，抗恶意软件(AMS software)，入侵检测系统 (IDS)



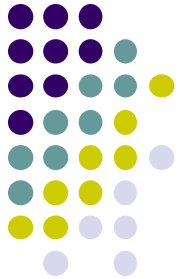
《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年.

网络密码系统模型



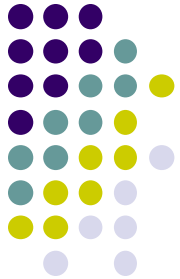
《计算机网络安全的理论与实践（第2版）》. 【美】王杰，高等教育出版社，2011年.

第1章 网络安全概论



- 1.1 网络安全的任务
- 1.2 基本攻击类型和防范措施
- 1.3 攻击者类别
- 1.4 网络安全基本模型
- 1.5 网络安全信息资源网站

网络安全信息资源网站



- CERT
  - www.cert.org
- SANS Institute
  - www.scans.org
- Microsoft Security
  - www.microsoft.com/security/default.mspx
- NTBugtraq
  - www.ntbugtraq.com