Chapter 6 IP Security

2017年4月1日 10:28

BY LSY

- Agenda
  - TCP/IP stack
  - TCP/IP issues

1. TCP/IP Protocol Stack
  -
    - local network
    - internet service provider (ISP)
    - backbone
    - ISP
  - TCP/IP
  - BGP
  - DNS

2.TCP

- application layer——HTTP,SMTP——类似于货物
- Transport layer——TCP，UDP——类似于快递
- Network——类似于地址
- Link——类似于路
- Data Format

3. IP

4. ICMP(Control Message Protocol) 用来检测网络消息

5. IP & TCP/UDP 完整性与可靠性

- 序列号sequencing numbers, 避免重复
- acknowledgment

6. User Datagram Protocol

- 分配端口号

7. Transmission Control Protocol

- synchronization or 3-way handshake

8. port numbers

9.DNS(domain name service)

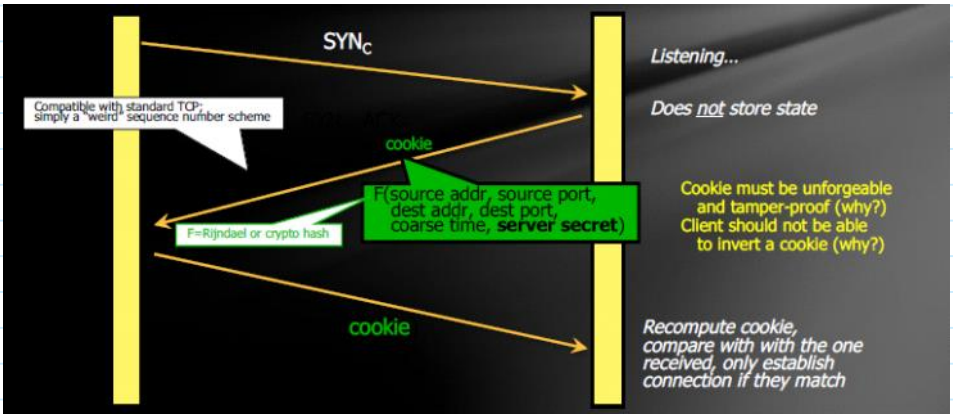
10. Security issues of TCP/IP

- sniffing：很多信息没有加密，截取信息
- ARP spoofing:

2017/4/5 8:15

  - smurf
    - src: victim's address; dest: broadcast address 广播地址(不用)
    - 通过发给局域网的所有机子，然后返回大量包给victim
  - ARP poisoning

- TCP SYN Flooding !!!!
  - 三次握手的时候client只发SYN不回复，然后把Server炸掉
  - client会伪装IP地址，所以server返回的包不会到攻击者，所以对攻击者没有损失，不对称性
  - DOS伪造成假的客户，DDOS利用肉机真的用户去攻击——availability
  - if SYN queue is full. randomly delete one
  - SYN Cookies: ensure that the server will not store the states, unless it receives at least two messages from the client, 只能由服务器产生
    - must be unforgeable, cookies不能被伪造——单向散列函数
    - should not be able to invert 不能被反向推算
    - simply a weird sequence number scheme



- TCP SYN Prediction Attack
  - TCP spoofing
  - TCP connection hijacking
  - TCP reset
- TCP congestion control:
  - 发现拥塞，立即减半
  - 不拥塞，慢慢上升
- DNS Spoofing
  - 将local DNS service的缓存伪造掉
  - solution: 对local DNS service进行验证

11.IPSEC——ip layser security mechanisms

- IPv6 must support IPSEC, IPv4 is optionally
- 加一点头来保证
- 三要素:
  - Authentication Headers, AH / 验证头，只验证不加密

Authentication Header format

Offsets	Octet16	0							1							2								3							
Octet16	Bit10	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Next Header								Payload Len								Reserved															
4	32	Security Parameters Index (SPI)																															
8	64	Sequence Number																															
C	96	Integrity Check Value (ICV)																															

  - Encapsulating Security Payloads, ESP / 载荷安全性封装,会直接加密，可以做AH可以做的所有事情并且加密
  - Security Associations, SA / 安全关联， reference
- Mode
  - IPv4 一个放在中间，一个放在前面
  - 传输模式：中间造个盒子
  - 隧道模式：整体加密
- 比如内网就不使用IPSEC，外网才使用IPSEC加密
- 但是用户没有选择，所以性能会下降

12. SSL/TLS
    - SSL Connection
    - SSL Session
    - SSL/TLS Protocol Stack
        - handshake layer
        - record layer
    - SSL Handshake protocol
        - client_hello: establish safety negotiation
            - 要选择一种算法
            - server需要知道client的版本号之类的用来支持旧的版本
        - server authentication and key exchange
            - server不能拒绝client选择的加密算法
        - client authentication and key exchange
        - end
    - SSL Record Protocol
        - 在包的开头写协议号