WA READING

✓ lec 01 cryptography

> share resources via communication
>
> to protect the communication

- What channel: wired & wireless
- How far: single-hop & multi-hop(单跳&多跳)
- How many routes: single-path & multi-path
- Who to reach: unicast & multicast & broadcast

  > IPv4: unicast, multicast, broadcast

  - Unicast: one-to-one communication
  - Multicast: one-to-group - multicast traffic addressed for a group of devices on the network.
  - Broadcast: one-to-all
- What data: data transmission & service
- **CIA Triad:**
  - confidentiality: 机密性--secrecy
  - integrity: 完整性--accuracy
  - authentication--ascription

    - non-repudiation--liability

- overhead/eavesdropped：窃听

- Encryption加密: with message and key as input – output encrypted message

  Decryption解密: with encrypted message and key as input – output the original message

- Symmetric cryptography对称加密

  > 如果一个实体同时与许多其他实体通信，特别是从许多其他实体接收消息，使用对称密钥，每个实体需要维护一个秘密密钥，要维护的密钥太多，开销高

- Asymmetric cryptography非对称加密

  > 无需安全通道即可共享密钥，因为任何人都可以知道公钥

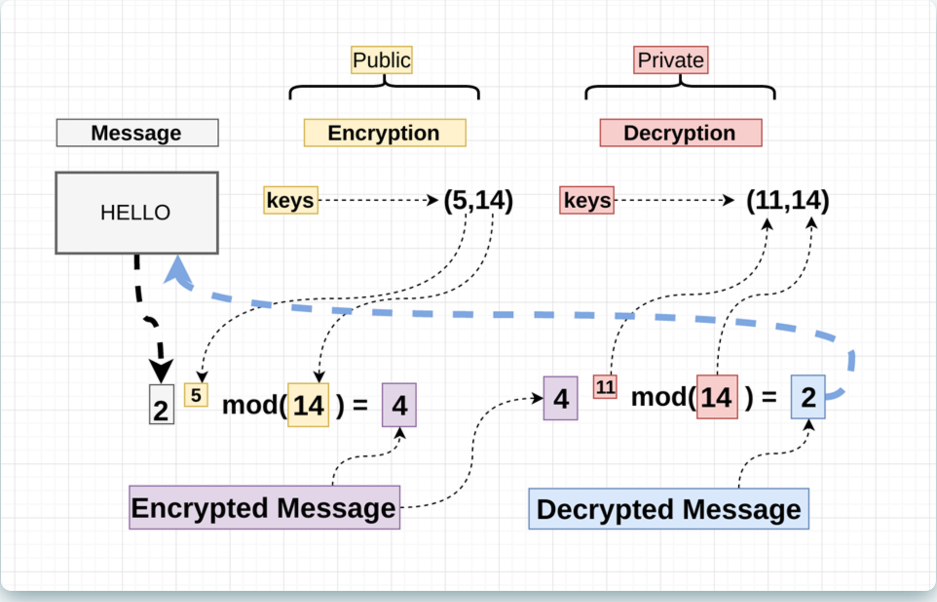
  公钥：广播给所有人

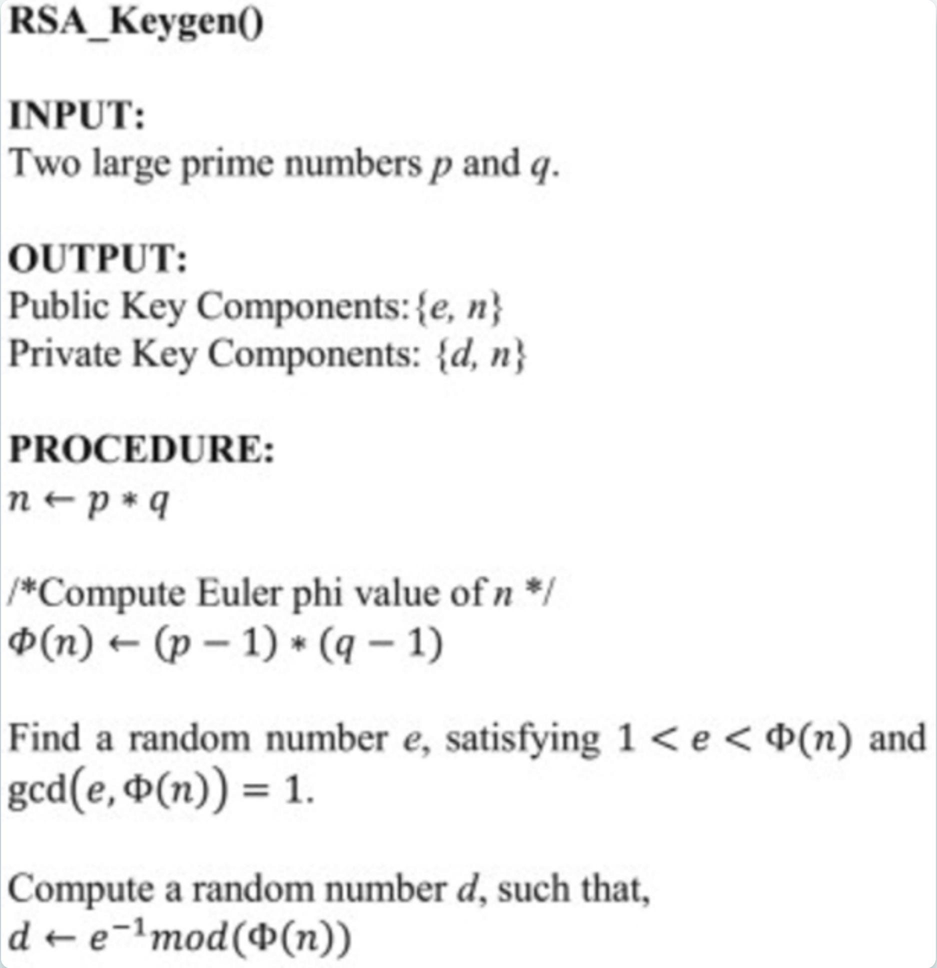
  私钥：本地保存

- Homomorphic Encryption同态加密

  允许在密文上进行计算，生成加密的结果，该结果在解密后与操作的结果相匹配，就好像在纯文本上执行了该操作一样。同态加密的目的是允许对加密数据进行计算。

- **RSA**





RSA_Keygen()

INPUT:
Two large prime numbers p and q.

OUTPUT:
Public Key Components: $\{e, n\}$
Private Key Components: $\{d, n\}$

PROCEDURE:

```
$n \leftarrow p * q$

/*Compute Euler phi value of $n$ */
$\Phi(n) \leftarrow (p-1) * (q-1)$

Find a random number $e$, satisfying $1 < e < \Phi(n)$ and $\gcd(e, \Phi(n)) = 1$.

Compute a random number $d$, such that,
$d \leftarrow e^{-1} mod(\Phi(n))$
```

- Cryptanalysis密码分析：即使密码密钥是未知的，密码分析也可用于破坏密码安全系统并获得对加密消息内容的访问。

- **Replay attack:** 攻击者向B重播相同的消息，让B相信这个消息来自于A

  解决方法：Limit Message Freshness, Timestamp, One-time session key

- **Man-In-The-Middle attack**中间人攻击

攻击者将与通信的两端建立独立的连接并交换双方的数据。 通讯的双方都认为，即使是真正由“中间人”控制的，他们也正在通过专用连接直接相互交谈。 在这种情况下，攻击者可以拦截双方之间的通信并插入新内容。

解决方法：Guarantee Connection Authenticity

- **Relay Attack**

  攻击者拦截请求并替换请求

  解决方法：Distance Bounding

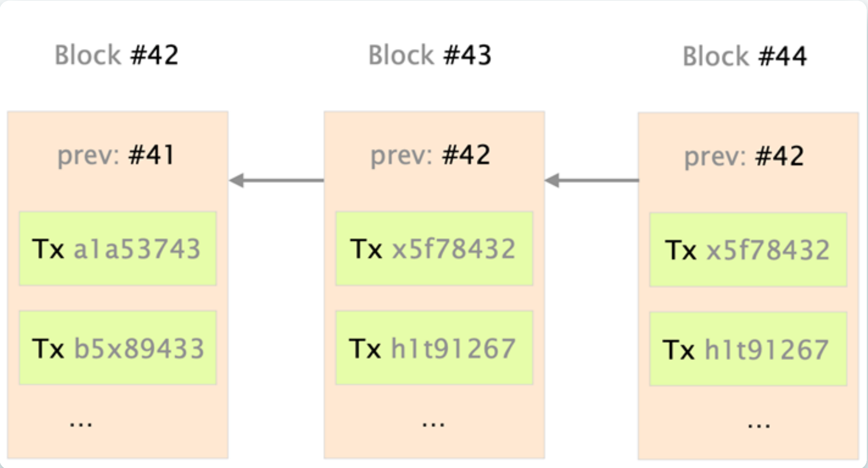
✓ lec 02 Blockchain

- **Bitcoin**:

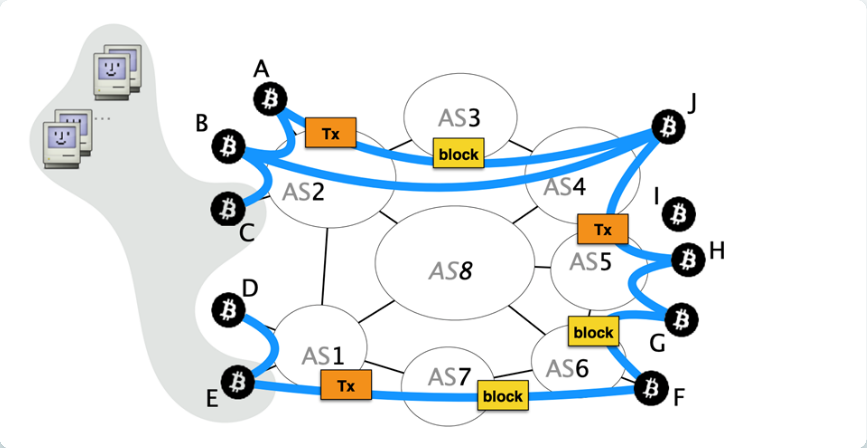
  a cryptocurrency & a form of electronic cash & a decentralized digital currency & without central bank or single admin

  can be sent from user to user on the peer-to-peer bitcoin network without the need for intermediaries

  - 各个节点之间形成随机关联
  - 每个节点保留所有交易的分类帐，表现为blockchain，被矿工不停向后扩展



  - 矿工都在矿池中集群，矿池通过multiple gateways连接比特币网络
  - 连接通过互联网路由。互联网由Autonomous System(ASes)组成。BGP计算跨它们的转发路径
  - 比特币消息未经加密地传播，并且没有任何完整性保证



- **Bitcoin Possession**

  digital signature using Alice's private key

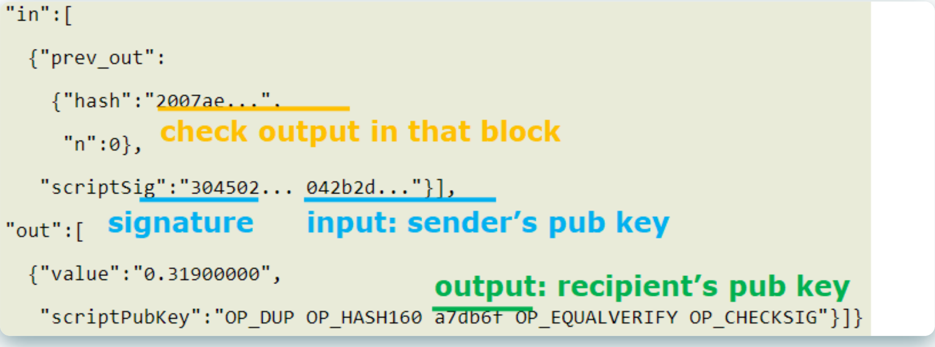
- serial number: 避免比特币重放

  transaction = I, Alice, am giving Bob bitcoin sn1.
  transaction = I, Alice, am giving Bob bitcoin sn2.

- is sn1 really belonging to Alice?

  ledger=blockchain：每个人都完整记录哪个比特币属于哪个人，显示所有比特币交易；让每个人都集体成为银行。

  A block contains one or more transactions



```
"in":[
  {"prev_out":
    {"hash":"2007ae...",
     "n":0},
   "scriptSig":"304502... 042b2d..."}],
"out":[
  {"value":"0.31900000",
   "scriptPubKey":"OP_DUP OP_HASH160 a7db6f OP_EQUALVERIFY OP_CHECKSIG"}]}
```

- who issues serial numbers? **hash of a block**: 也许有更多的交易指明使用的确切交易；

- **Double spending**--what if Alice pays sn1 to Charlie as well?

  - 过了一会儿才发sn1：sn1 appears in two [in] fields in prev blocks
  - 同时支付sn1：some users validate Alice-Bob; some Alice-Charlie

    fork emerge: follow the longest fork; accept the transaction until at least 5 more blocks follow it;

  - 同时put sn1 related A-B and A-C: easily spot it

  - what if Alice pays sn1 to Bob, wait till accepted; then repays sn1 to Charlie, compute another longer fork? make it hard to catch up

- **proof-of-work** make validating a block computationally costly; require enormous computation power to forge; 我们在区块中补增一个随机数(Nonce)，这个随机数要使得该给定区块的随机散列值出现了所需的那么多个0

  > find a nonce x, such that h(msg,x) leads with 10 zeros (hex).
  > prob $1/16^{10}$ for all 10 zeros
  > $1/(1/16^{10})$tries

  > find a nonce x, such that h(blockheader,x)<=target, how much comp power should Alice have to win?
  > **51% attack**: 单个矿工或一组矿工，他们控制着网络超过50%的挖掘能力（也称为哈希率或哈希能力）

- **proof-of stake**: （实现分布式共识distributed consensus）用一个公式来选择下一个区块的伪造者，这取决于用户最小hash值和股权的大小组合。因为股权的大小是公开的，每个节点通常都可以预测谁会成为下一个区块的伪造者。Nxt和BlackCoin是使用随机区块选择方法的加密货币。

  - every participant joins blockchain by paying stake
  - when choosing creator of a block,more stake with high probability
  - creator gets stake reward if created block passes verification, otherwise, penalty
  - only one creator per block; no huge computation waste

- **selfish mining attack**

  Attacker increases the share of the reward by not broadcasting mined blocks to the network for some time and then releasing several blocks at once, making other miners lose their blocks.

- **block withholding attack**

- **sybil attack**: 黑客控制多个节点，被病毒辐射的假节点会关闭他们的transaction
- **eclipse attack**: 黑客控制大量IP地址或分布式botnet，受害者所有传出连接都会被定向到攻击者控制的IP地址

✓ lec 03 Secure Connection

- 不安全的情况下，信息以plaintext形式保存
- 通过在公共Internet上创建用于私有通信的唯一加密通道来保护其数据。
- **protocal**: SLL/TLS

  Application: HTTPS

  1. The client sends a hello message to the server.

     Client hello:

     - SSL Protocol version
     - Session ID
     - List of Cipher Suites
     - CLIENT HELLO Extensions

  2. The server responds with a hello message and sends the server's certificate.

     > the purpose of a server's certificate is to couch for the server's private key that is signed by the CA's key and verified by the CA's key

     Server hello:

     - SSL Protocol version
     - Session ID
     - Selected Cipher
     - Server Certificate->Public Key
     - SERVER HELLO Extensions
     - Client Certificate Request **(optional)**

3. The client performs the following actions:
   Verifies that the SSL/TLS server certificate is signed by a root certificate that the client trusts.
   Extracts the public key from the server certificate.
   Generates a premaster secret and encrypts it with the server's public key.
   Sends the encrypted premaster secret to the server.

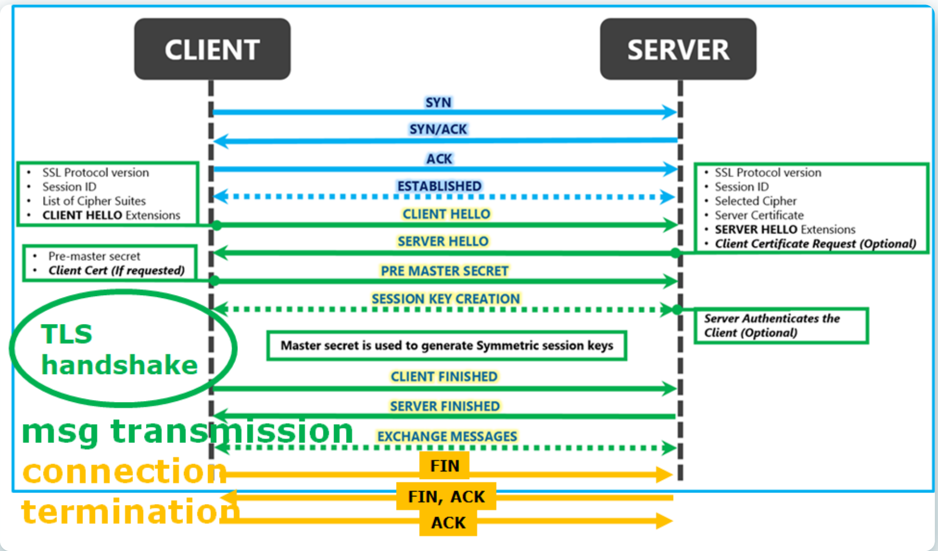
4. To decrypt the client's premaster secret, the server sends it to the HSM. The HSM uses the private key in the HSM to decrypt the premaster secret and then it sends the premaster secret to the server. Independently, the client and server each use the premaster secret and some information from the hello messages to calculate a master secret.

5. The handshake process ends. For the rest of the session, all messages sent between the client and the server are encrypted with derivatives of the master secret.

- **HTTPS**:

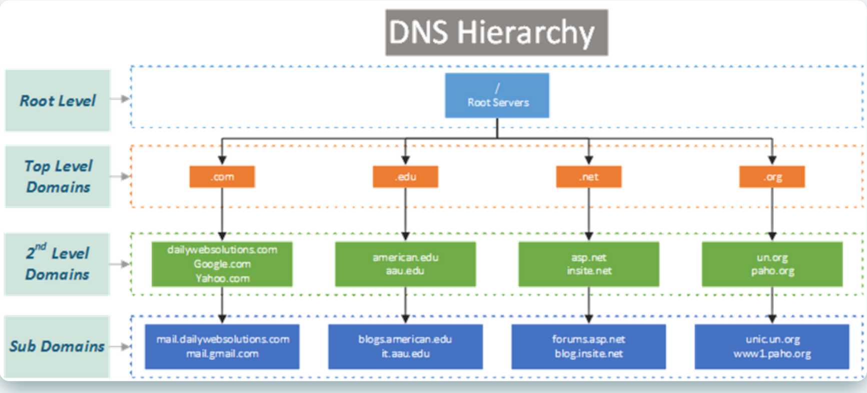
  - Threats: hard to prevent, possible to detect

    1. Eavesdropping攻击者窃听--encryption
    2. Manipulation重定向包--integrity（MAC）
    3. Impersonation攻击者冒充授权用户--signature



1. **connection request: 域名->IP**

   DNS: Domain Name System



- Iterative Resolution
- Recursive Resolution

域名系统（DNS）区域文件是描述DNS区域的文本文件。 DNS区域是DNS的分层域名结构的子集，通常是单个域。 区域文件包含域名和IP地址以及其他资源之间的映射，以资源记录（RR）的文本表示形式进行组织。 区域文件可以是权威地描述区域的DNS主文件，也可以用于列出DNS缓存的内容。

- frequently request rarely-accessed links;
- force DNS to evict cached hot links;
- slowdown DNS resolution.

DNS Poisoning: 危害DNS服务器；伪造目标链接的IP地址；

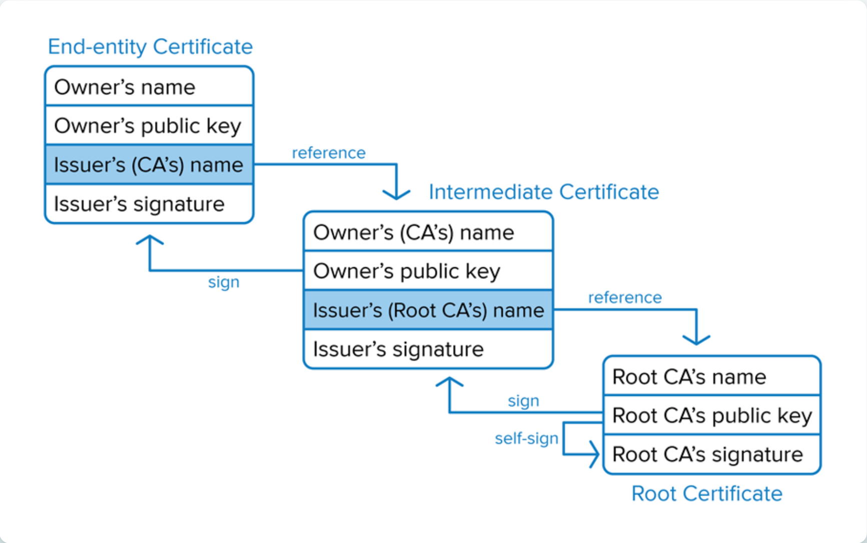
2. **server response:**

Certificate: 由第三方CA发行。给公钥提供担保。

- signed by CA's private key
- verifiable by CA's public key

3. **certificate verification**

Certificate Authority & Certificate Date & Certificate Revocation List & Domain Name



CRL check: 由签发CA吊销的证书将不可用(Certificate Revocation List)

- revoked: 如果发现发行证书不正确，或者认为私钥已被泄露，则证书将被不可撤销地吊销
- hold: 可逆状态可用于记录证书的临时无效，如用户不确定私钥是否丢失

> 证书被吊销与到达客户之间的时间间隔永远成立

> Always a time gap between when a certificate is revoked and when its revocation approaches a client

鉴权过程：

1. The certificate must be issued by a trusted Certificate Authority (CA).

2. The fully qualified hostname in the HTTPS request URL and the certificate owner (“Issued to” name) must match.

3. The certificate must be current (within its “Valid from...to...” date range).

4. The certificate must not be on a revocation list (either CRL or OCSP).

   - Periodically issued by a CRL issuer

CRL is the certificate revocation list. After the certificate is revoked, it will be recorded in CRL, and CA will publish CRL regularly. Applications can rely on CRL to check if the certificate has been revoked.

        - Query supported as well

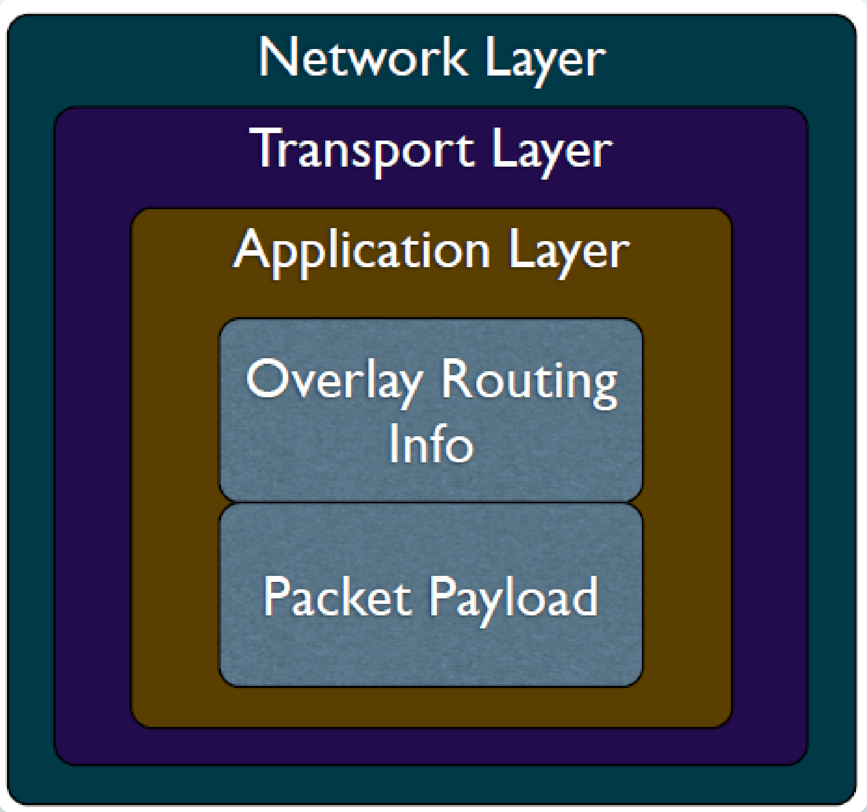
          OCSP is an online certificate status checking protocol. The application sends a request according to the standard, queries a certificate, and then the server returns the certificate status.

    5. Checks 1-4 are recursively applied to every certificate in the trust chain.
    6. key exchange
    7. secure communication
    8. bye

✓ lec 04 Anonymous Communication

> 用户在internet通信时被分配IP地址，通常固定在一个或多个通信会话中，可以推断关键隐私

- **hide destination address**：通过relay（转发）将数据包传递到目的地
- **Overlay Network**
    - 在应用层上解决路由
    - tunnel message inside other messages

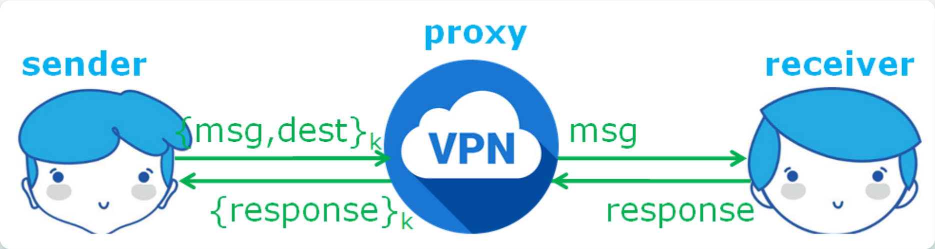


- Threat Model: 内部拜占庭式攻击者可能会严格控制网络（例如Z ASes），但不太可能观察到整个互联网

- Traceforward Attack: 被动的攻击者；从发件人处追踪并阻止收件人的匿名

- Marking Attack: 主动的攻击者，标记信件，并在另一处发现该信件

- **Anonymizing Proxy**匿名代理：
  - intermediary between sender & receiver
  - Sender relays all traffic through proxy
  - Encrypt destination and payload
  - Asymmetric technique: receiver not involved (or informed of) anonymity



如果攻击者在sender-proxy处，则receiver是匿名的

如果攻击者在proxy-receiver处，则sender匿名

如果两处都有攻击者，或攻击者在proxy处，则都不匿名

如果receiver是攻击者，proxy能保护sender的匿名性

- **匿名proxy的优点：**
  - Easy to configure
  - Require no active participation of receiver, which need not be aware of anonymity service
  - Have been widely deployed on Internet
- **匿名proxy的缺点：**
  - 被信任的第三方代理可能会泄露信息（使用proxy++去避开不可信赖的代理）
  - 不确定攻击者的位置（使用dynamize proxy location去避开攻击者）
- **source routing**: 指定数据包发送的路径specify on-path routers by source
  - POF-based Source Routing: Protocol Oblivious Forwarding：不保护匿名性，会泄露port sequence，为保护匿名性应该对非邻居隐藏端口
  - onion routing: anonymous overlay communication,使用覆盖性网络构架，否则，基础转发设备不支持修改
    1. Connect to Tor entry
    2. Randomly select a series of Tors
    3. Relay messages across them
    4. Tor exit relays messages to destination
    5. Reply traffic from destination traverses the reverse path
    6. Maintains a bidirectional persistent multi-hop path between source and destination

    只在邻居之间泄露信息

✓ lec 05 Secure Routing

> selecting a path for traffic in a network, or between or across multiple networks.

- **scheme**
  - unicast: 向单个节点传送msg
  - broadcast: 向网络中所有节点传送msg
  - multicast: 向网络中一组节点传送msg

    - anycast: 向一组节点中的任意一个传送msg
    - geocast: 依靠地理位置给一组节点传送msg

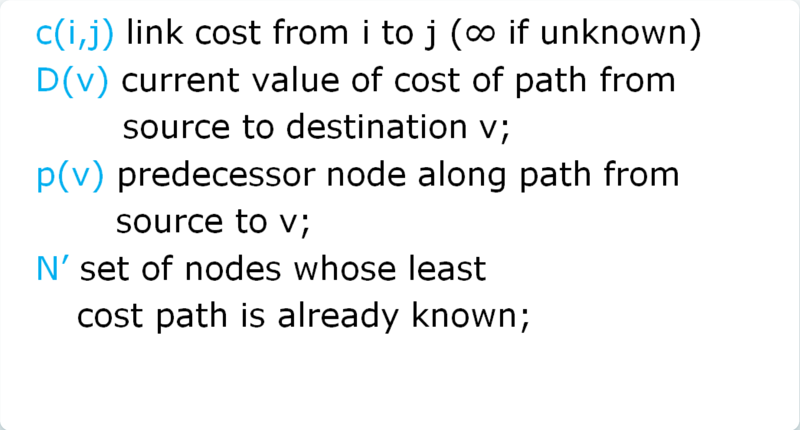
- intra-domain routing: 在一个autonomous系统内的节点间，consider A-F as routers

  inter-domain routing: 在多个autonomous系统的节点间查找路径，consider A-F as autonomous systems

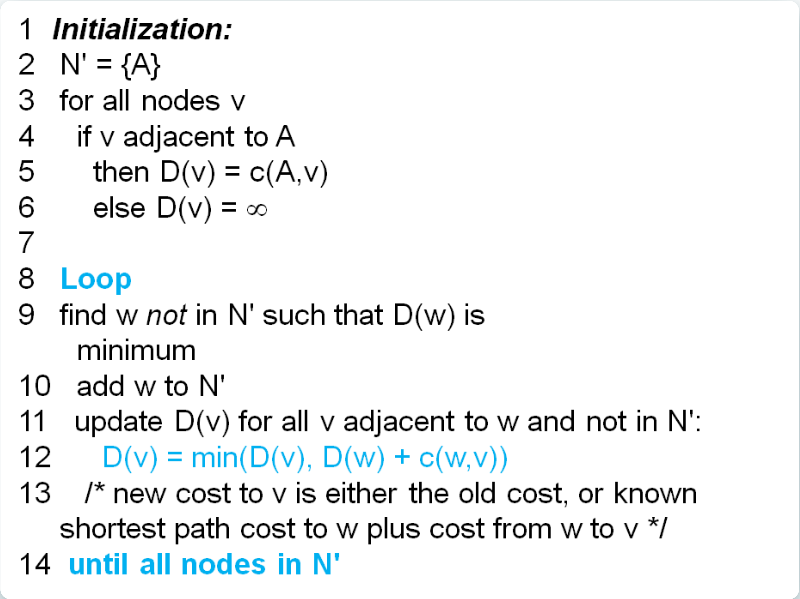
- **route computation**

    - Link-state algorithms--Dijkstra

        - 每个路由器都知道完整的拓扑和链路成本信息
        - 计算到达每个目的地的最短路径
        -



c(i,j) link cost from i to j (∞ if unknown)
D(v) current value of cost of path from source to destination v;
p(v) predecessor node along path from source to v;
N′ set of nodes whose least cost path is already known;

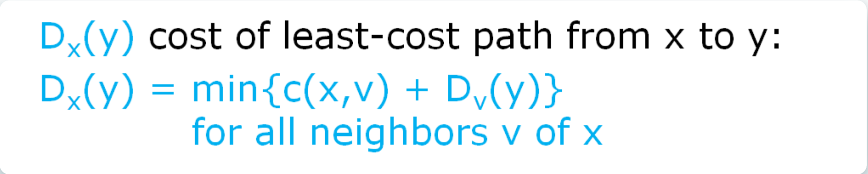


```
Initialization:
N' = {A}
for all nodes v
  if v adjacent to A
    then D(v) = c(A,v)
    else D(v) = ∞

Loop
find w not in N' such that D(w) is
  minimum
  add w to N'
  update D(v) for all v adjacent to w and not in N':
    D(v) = min(D(v), D(w) + c(w,v))
   /* new cost to v is either the old cost, or known
shortest path cost to w plus cost from w to v */
until all nodes in N'
```

    - Distance-vector--Bellman-Ford

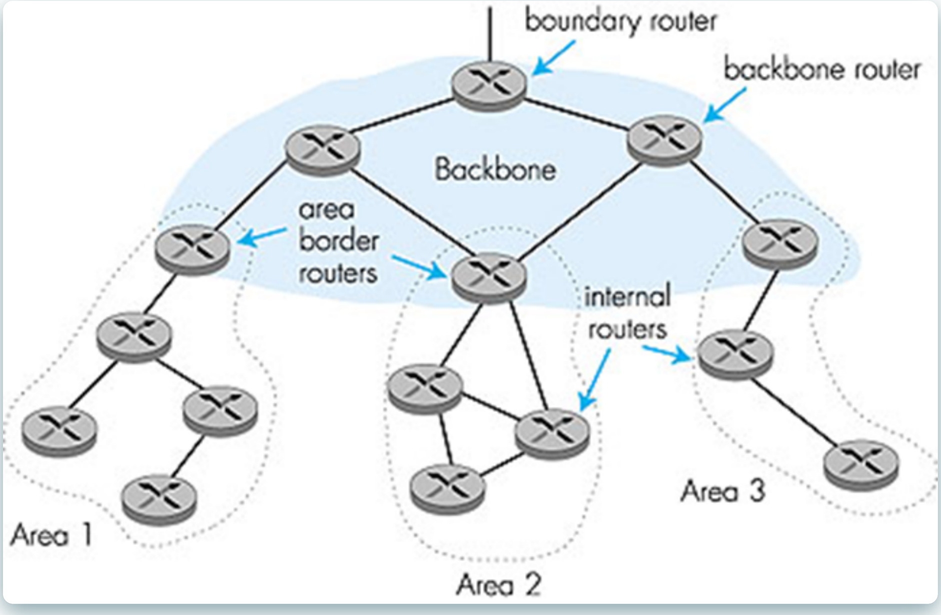
        - 每个路由器都知道直接邻居和与邻居的链接成本
        - 通过基于到每个目的地的邻居距离的迭代过程来计算到达每个目的地的最短路径



$D_x(y)$ cost of least-cost path from x to y:

$D_x(y) = \min\{c(x,v) + D_v(y)\}$ for all neighbors v of x

- **Hierarchical Routing**分层路由
  - 每个AS使用自己的IGP内部路由协议；
  - 边界路由器也运行BGP
- RIP路由信息协议
  - 距离矢量算法：
    - 距离度量标准：跳数（最大=15hops)
    - 邻居路由器每30秒交换一次路由通告
    - 如果再180秒后没有听到邻居N的更新，则N的链接宣告死亡，通过N的所有线路均无效：更新发送给邻0居；下一个邻居会发来新的消息；使用poison reverse来避免ping-pong loops（16 hops=inf)
  - Link-State Packet
    - one entry per neighbor router
    - ID of the node created the LSP
    - a list of direct neighbors with link cost
    - SEQ: sequence number for this LSP
    - TTL: time-to-live for info in this LSP
    - each node stores and forwards LSPs
    - Decrement TTL of stored SLPs
    - Discard info when TTL=0
    - Generate LSPs periodically with increasing SEQ
    - 使用source-ID和SEQ来检测重复
  - OSPF中所有信息都被authenticated
  - multiple same-cost paths are allowed
  - hierarchical OSPF is used in large dom
- **Hierarchical OSPF**



两级hierarchy: localArea，backbone（本地网，骨干网）

每个节点都有详细的拓扑信息，但只有通往其他area的最短路径

- **Area border routers:** “summarize” distances to nets in own area, advertise to other Area Border routers.
- **Backbone routers:** run OSPF routing limited to backbone.
- **Boundary routers:** connect to other AS’ s.

- **BGP**: Border Gateway Protocol

  - 对于每个AS:
    从邻居AS获取子网可达性信息;
    将可达性信息传播给所有内部路由器;
    根据可达性信息和策略确定到子网的路由

  - IBGP与EBGP

    - IBGP是AS与AS之间的
    - EBGP是AS内部的

  - dual-homed

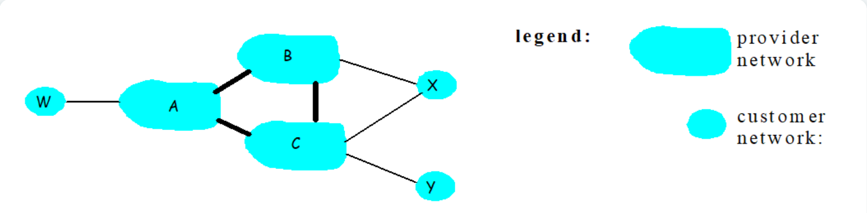


Figure 4.5-BGPnew: a simple BGP scenario

x是dual-homed的，它连接了两个网络

1. A告诉B路径AW

2. B告诉A路径BAW
3. B不会告诉C这个路径，因为w和c都不是B的客户，不能给B带来收益

- **routing attack**

  distance-vector: announce 0 distance to all other nodes

  link-state: drop links; claim direct link to other routers

  BGP: announce arbitrary prefix; alter paths

  使用cryptography或RPKI进行secure routing

- **RPKI**(resource public key infrastructure)

  进行原始身份验证，是IP前缀和他们的Ases之间的认证映射

  如果只是路由信息被更改，RPKI是不足够的

- **SBGP**：路径上的每个AS都以加密方式签署其公告，确保路径上的每个AS在路径中进行通告。

✓ lec 06 Wi-Fi

- 更高的风险：

  - channel：广播通信更容易受到窃听和干扰。无线网络也更容易受到利用通信协议漏洞的主动攻击；
  - mobility：更大的便携性和移动性会导致很多风险
  - resources: 无线设备应对威胁的内存和处理资源有限
  - accessibility: 某些无线设备可能无人看管，容易遭受物理攻击

- how to attack

  - **passive attack**：被动的信息收集；对收集到的信息进行离线攻击，监听数据包（key cracking）
  - **active attack**：主动攻击；操纵无线通信（packet injection, DoS）

- Rogue AP恶意访问点

  恶意攻击者添加但未被本地网络管理员明确授权而安装在无线网络上的访问点。如果攻击者安装了访问点，则他们能够运行各种类型的漏洞扫描程序，而不必亲自在组织内部，而是可以远程进行攻击

- Evil twins AP

通过设置与合法AP相同的SSID设置看似合法的欺诈性的WIFI接入点，设置为窃听无线通信。其孪生兄弟是网络钓鱼诈骗的无线局域网

- Man in the middle attack

  - **Frame Injection**: 更多更积极地注入帧，而不是简单地拦截通信

- replay attack

  传输数据被恶意重复，masquerading attack的一部分。攻击者拦截数据以进一步重传数据，具有使设计不佳的应用成分崩溃的能力

- Denial of Sleep

  通过信号触发无线设备，让其保持活动状态并消耗电力，更多的节点消耗会导致网络中断

- Collision Attack

  用户和攻击者之间的渠道重叠，攻击者通过发送与用户冲突的数据包导致用户的数据包被丢失

- Jamming

  物理干扰，用噪声信号淹没频射信号导致系统失效

  易于发起的无线ddos攻击

- **WEP: secure WIFI**

  wired equivalent privacy 让WiFi网络至少与有限LAN一样安全，不实现强大的安全性

  服务：access control to network, message confidentiality, message integrity

  - Access control: 在关联之前，设备STA需要向AP进行身份验证

    STA -> AP: authenticate request

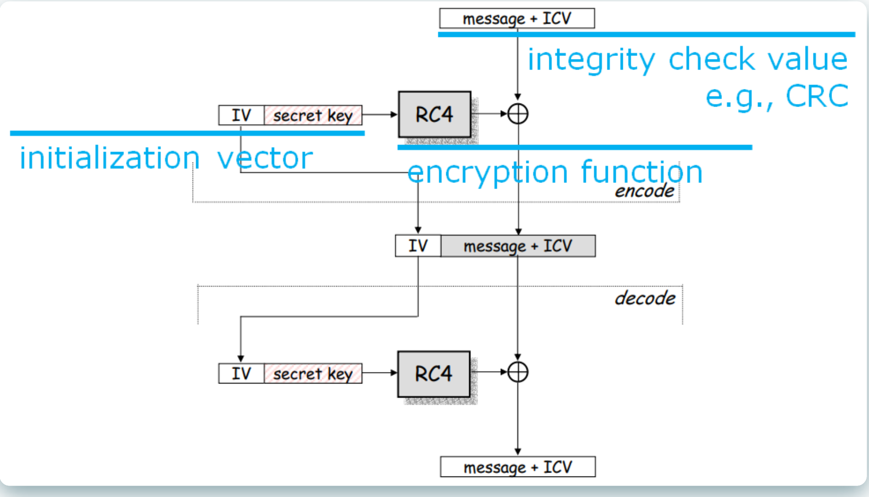
    AP -> STA: authenticate challenge r(128b)

    STA -> AP: authenticate response($E_k(r)$)

    AP -> STA: authenticate success/failure

    认真通过后，STA可以发送关联请求，AP会回应一个关联响应

- WEP Encryption



ICV：完整性检查值

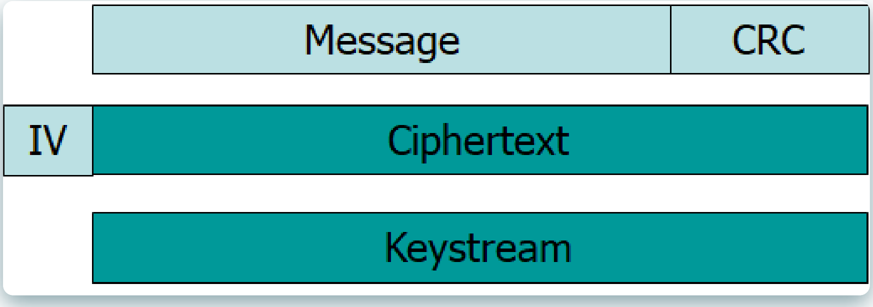
RC4：加密算法，在硬件中容易实现，降低加密带来的性能损失

IV (Initialization Vector): 24-bit number

Key: 40 or 104-bit number

Keystream: IV||Key

加密过程



1. compute CRC for the message (CRC-32 polynomial)
2. compute the keystream(IV与密钥连接，RC4加密算法用于64位或128位串联)
3. Encrypt the plaintext：源文本与keystream XOR获得加密文本。IV在密文之前

解密过程

1. build the keystream：从传入的帧中提取IV，讲IV置于密钥前，使用RC4构建密钥流
2. decrypt the plaintext and verify：将加密文本与keystream进行XOR，使用CRC验证

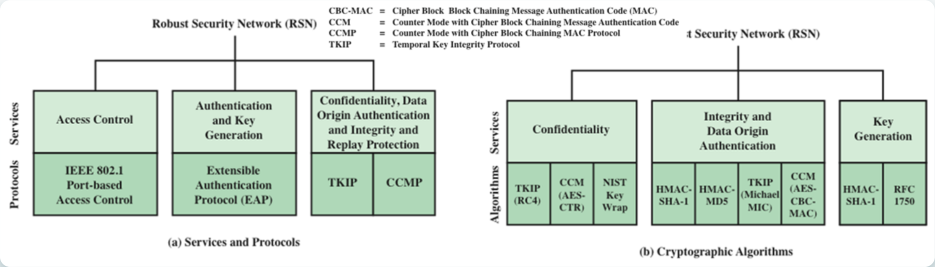
weakness

    - AP not authenticate to STA
    - 24-bit IV in plaintext
    - CRC is unkeyed function
    - RC4 cipher: week seeds (IV) make more easily calculated keystreams

- secure WIFI more & secure data trans: **IEEE 802.11i**

  STA和AP之间实现双向鉴权，authentication phase需要AS, AP, STA

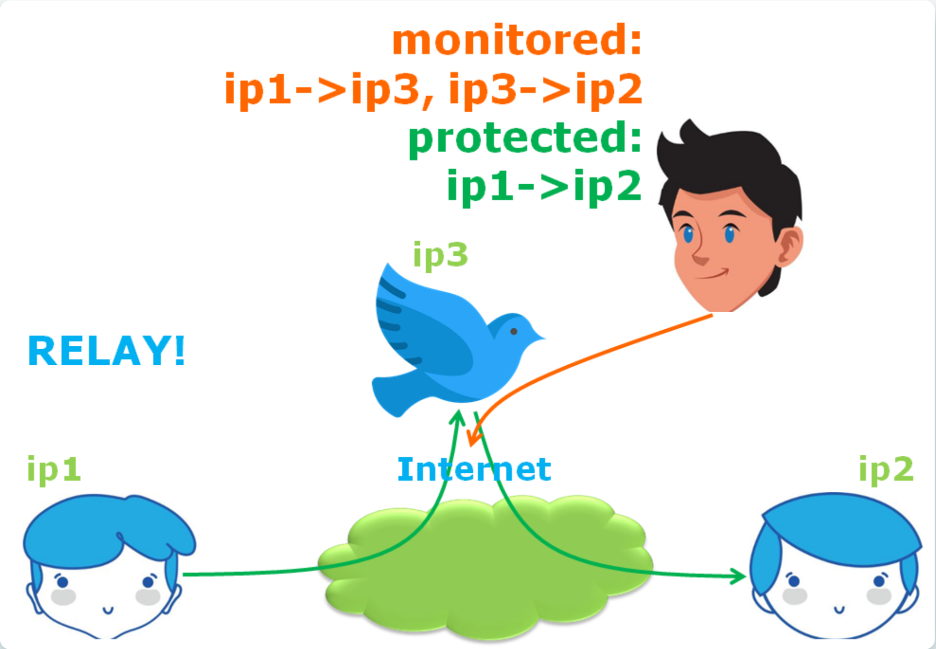
  访问控制：强制执行身份鉴权，routes messages properly，促进key exchange

  
  Robust Security Network (RSN)
CBC-MAC = Cipher Block Block Chaining Message Authentication Code (MAC)
CCM = Counter Mode with Cipher Block Chaining Message Authentication Code
CCMP = Counter Mode with Cipher Block Chaining MAC Protocol
TKIP = Temporal Key Integrity Protocol
Services
Protocols
Access Control
IEEE 802.1 Port-based Access Control
Authentication and Key Generation
Extensible Authentication Protocol (EAP)
Confidentiality, Data Origin Authentication and Integrity and Replay Protection
TKIP
CCMP
(a) Services and Protocols
t Security Network (RSN)
Services
Algorithms
Confidentiality
TKIP (RC4)
CCM (AES-CTR)
NIST Key Wrap
Integrity and Data Origin Authentication
HMAC-SHA-1
HMAC-MD5
TKIP (Michael MIC)
CCM (AES-CBC-MAC)
Key Generation
HMAC-SHA-1
RFC 1750
(b) Cryptographic Algorithms

  - **TKIP**: 对使用WEP实现的设备进行软件更改
    - 消息完整性：在数据字段后将消息完整性代码添加到802.11mac帧，Michael算法使用源和目标MAX地址以及数据字段、密钥作为输入来计算64位值。
    - 数据机密性：通过使用RC4加密MPDU和MIC
  - **CCMP**：适用于配置IEEE 802.11设备的硬件
    - 消息完整性：使用CBC-MAC
    - 数据机密性：使用CTR分组密码操作模式对AES进行加密

- **Relay Attack**

  拦截请求并替换



defense: distance bounding，响应时间如果大于RTT就拒绝该消息

RTT=2*distance/velocity\

limitation: the attack can still work if the distance is small. Because it's hard to distinguish attacker added RTT and the delay caused by normal network fluctuation.

✓ lec 07 DDoS

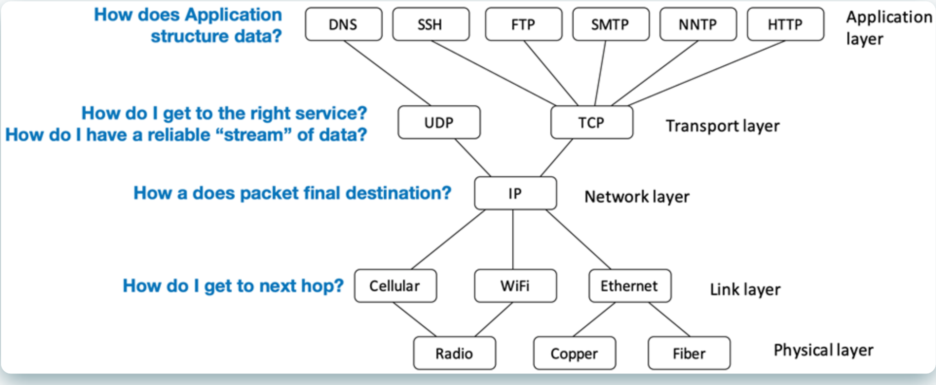
> Distributed Denial-of-Service Attack

- **DoS** (Denial-of-Service)：控制攻击的设备，用多余的请求淹没受害者，使受害者超载并阻止其满足某些合法要求

  defense：阻止攻击源

- **DDoS**: 控制许多不同的攻击源；仅通过阻止单个来源来避免攻击难以实现

- how to attack?


How does Application structure data?
DNS
SSH
FTP
SMTP
NNTP
HTTP
Application layer
How do I get to the right service?
How do I have a reliable “stream” of data?
UDP
TCP
Transport layer
How a does packet final destination?
IP
Network layer
How do I get to next hop?
Cellular
WiFi
Ethernet
Link layer
Radio
Copper
Fiber
Physical layer

link layer: send too much traffic for switches/routers to handle

transport layer: require servers to maintain large number of concurrent connections or state

application layer: require servers to perform expensive queries or cryptographic operations

- **TCP SYN Flood**

  具有随机源IP地址的SYN数据包填满服务器上的积压队列，但没有进一步的连接

  IP Spoofing: 根据随机伪造的IP地址制作SYN数据包；对于此类随机IP地址，在它们从服务器接收到SYN ACK数据包之后，由于这些IP地址根本没有发送过SYN请求，因此它们可能会简单地丢弃它们

- **symmetric DDoS attack**

  目标设备消耗的带宽量仅仅是每个攻击者发送的流量总和；攻击者需要大量流量才能实现；

- **asymmetric DDoS attack**

  攻击者使用相对较少数量或较低级别的资源，以使大量或较高级别的目标资源发生故障或失败

- **Smurf Attack**(asym的一种)

  攻击者向网络广播地址发送ICMP包，并将回复地址设置成受害网络的广播地址，通过使用ICMP应答请求数据包来淹没受害主机的方式进行，最终导致该网络的所有主机都对次ICMP应答请求作出答复，导致网络阻塞。

  solution: disable IP broadcast address on router and firewall, reject external packets to broadcast address

- **DNS放大攻击**：1 query vs many responses

“开放式DNS解析器”愿意为Internet上的任何人解析递归DNS查找。

1. 攻击者使用受感染的端点将具有伪造IP地址的UDP数据包发送到DNS递归器。 数据包上的欺骗地址指向受害者的真实IP地址。
2. 每个UDP数据包都会向DNS解析器发出请求，通常会传递一个参数（例如 “ ANY” ）以接收最大的响应。
3. 收到请求后，DNS解析器会尝试通过响应来提供帮助，它会对欺骗性的IP地址发送较大的响应。
4. 目标的IP地址会收到响应，并且周围的网络基础结构将被大量的流量淹没，从而导致拒绝服务。

EDNS: sends DNS data in larger UDP packets

solution: reduce the number of open resolvers; source IP verification--stop spoofed packets leaving network

- **NTP 放大攻击**

利用monlist命令触发对NTP服务器的请求的最后600个源IP地址进行响应。响应包按照每 6 个 IP 进行分割，最多有 100 个响应包。理论上这种恶意导向的攻击流量可以放大到伪造查询流量的100倍。

solution

reduce the number of NTP servers that support monlist;

source IP verification – stop spoofed packets leaving network;

- **DDoS defense**

make server harder to be attacked:

enrich server with more resources;

leverage the sources of others;(如 Google Project Shield)

detect and filter attack traffic

with spoofed IP addresses

- **Ingress filtering policy**: 网络服务商只转发具有合法IP地址的数据包

面临挑战：需要全球所有ISP都这么做，如果有10%的网络为实现就不会有防御力，没有鼓励ISP实施的动力

转运AS不能验证数据包的来源，只检测destination

- **Traceback**

  目标：given set of attack packets, determine path to source

  方法：change routers to record info in packets. router adds its own IP address to packet, victim reads path from packet

  假设：trusted routers, sufficient packets to track, stable route from attacker to victim

  局限性：requires space in packet, path can be long, no extra fields in current IP format