第六章--网络安全技术前沿选讲

1. 模糊测试技术
    - 模糊测试技术的概念
        - **Fuzzing**或模糊测试是一种**自动化的软件测试技**术，通常**用于识别程序中的潜在漏洞。**
        - 对程序进行模糊测试是通过向其提供随机输入语句并记录导致程序中的崩溃或非崩溃的内存损坏的测试用例来完成的。
        - 辅助以人工分析, 基于导致异常的输入数据进一步定位软件中漏洞的位置。
        - 在某种意义上，模糊测试就是通过蛮力搜索漏洞。
    - 模糊测试的测试用例生成
        - 模糊测试的测试用例生成方式有两种：基于生成和基于变异的。
        - **基于变异的模糊测试**：是通过变异已知的测试用例来创建新的测试用例，通过随机修改样本的方式生成测试用例。
        - **基于生成的模糊测试**：或者是基于语法的模糊测试，需要对语法有较好的理解并建立起模型，通过指定的输入模型来构造规范的输入，使得这类生成模型生成的输入很容易通过代码的完整性检测和语法检测，从而快速的绕过程序的语法检测。
    - 一些经典的工具
        - AFL：American fuzzy lop，号称是当前最高级的Fuzzing 测试工具之一，由谷歌的Michal Zalewski 所开发。通过记录输入样本的代码覆盖率，不断对输入进行变异，从而达到更高的代码覆盖率。

- Syzkaller：Google团队开发的一款针对Linux内核进行模糊测试的开源工具，基于覆盖率引导的Linux内核Fuzzer。

- RSA算法：$p=3$；$q=11$，$e=7$；$M=2$，写出公钥与私钥，加密与解密计算过程？

  答：

  1）
  - $n=pq=3\times 11=33$
  - $\Phi(n)=2\times 10=20$
  - $d\equiv e^{-1}\pmod{\Phi(n)}=7^{-1}\pmod{20}=3$
  - 公钥PU={7,33}；
  - 私钥PR={3,33}。

  2）
  - 加密过程：$C=2^7 \bmod 33=29$
  - 解密过程：$M=29^3 \bmod 33=2$

AES加密算法中，矩阵State中一列为

$$\begin{bmatrix}87\\6E\\46\\A6\end{bmatrix}$$

经过在有限域GF(2^8)（不可约多项式为$m(x) = x^8+x^4+x^3+x+1$）上运算的列混淆运算后，其输出列的值为多少？

答：列混淆即正向变换矩阵乘以该矩阵State中一列，即

$$\begin{bmatrix}02&03&01&01\\01&02&03&01\\01&01&02&03\\03&01&01&02\end{bmatrix}\begin{bmatrix}87\\6E\\46\\A6\end{bmatrix}$$

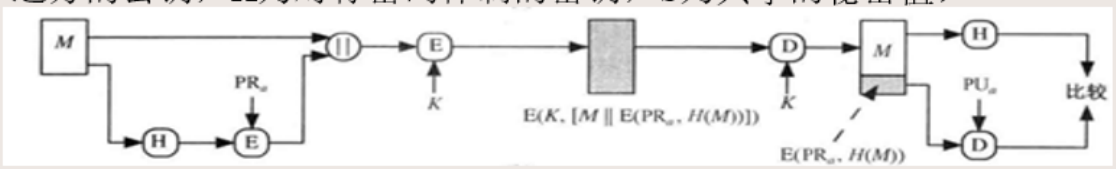
对于第一个值：

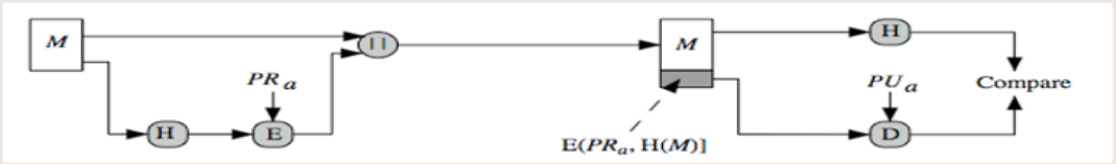
({02}•{87})⊕({03}•{6E})⊕{46}⊕{A6}

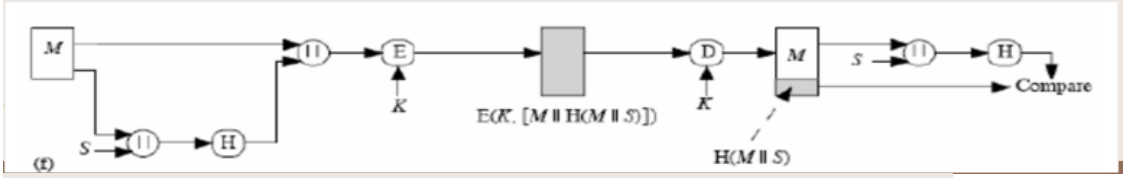
- {02}•{87} = (0000 0010) • (1000 0111) = (0000 1110) ⊕（0001 1011）=（0001 0101）
- {03}•{6E} = ({02}•{6E})⊕{6E} = {(0000 0010) • (0110 1110)} ⊕ (0110 1110)= (1101 1100) ⊕ (0110 1110)= (1011 0010)
- {02}•{87} = 0001 0101
  {03}•{6E} = 1011 0010
  {46} = 0100 0110
  ⊕ {A6} = 1010 0110
  0100 0111 = {47}

其他值可一一进行相应运算，最后可得 $\begin{bmatrix}47\\37\\94\\ED\end{bmatrix}$

密码学的目标包括机密性、真实性、完整性与不可否认性，分析如下处理过程分别能达到哪些目标？（其中：M为明文，H为散列算法，E为加密算法，D为解密算法，PRa为发送方的私钥，PUa为发送方的公钥，K为对称密码体制的密钥，S为共享的秘密值）







答：
1）机密性、真实性、完整性与不可否认性。
2）真实性、完整性。
3）真实性、完整性与不可否认性。
4）机密性、真实性、完整性。

- AES加密算法中，如果输入的以字节为单位的正方形矩阵State中有1个字节发生变化，则经过2轮次迭代后，其输出结果最多会有多少个字节发生变化？

答：16.

设某路由器建立了如下路由表：现共收到5个分组，其目的地址分别为：(1) 128.96.39.1；（2）128.96.40.1；（3）128.96.40.10；(4)128.96.40.100；5）192.4.153.10。试分别计算其下一跳

目的网络	子网掩码	下一跳
128. 96. 39. 0	255. 255. 255. 128	接口m0
128. 96. 39. 128	255. 255. 255. 128	接口m1
128. 96. 40. 0	255. 255. 255. 192	R2
128. 96. 40. 1	255. 255. 255. 255	R3
192. 4. 153. 0	255. 255. 255. 248	R4
0. 0. 0. 0	0. 0. 0. 0	R5

答：

（1）128.96.39.1与255.255.255.128进行逐位相与，得到128.96.39.0，与第一项目的网络匹配，因此其下一跳为：接口m0。

（2）路由表中第4项有目的地址为128.96.40.1的特定主机路由，因此其下一跳为：R3。

（3）128.96.40.10与255.255.255.192进行逐位相与，得到128.96.40.0，与第一项目的网络匹配，因此其下一跳为：R2。

（4）由于在路由表中找不到任意一行满足如下关系：用其子网掩码和128.96.40.100逐位相与运算，得到的结果与其目的网络匹配，因此该分组的下一跳为默认路由，即R5。

（5）由于在路由表中找不到任意一行满足如下关系：用其子网掩码和192.4.153.10逐位相与运算，得到的结果与其目的网络匹配，因此该分组的下一跳为默认路由，即R5。

- 以下为通过捕包软件捕获得到的一个以太网帧：

00 1B 38 A0 CC 26 00 0F E2 53 FC 08 08 00 45 00 00 28 E4 2D 40 00 2D 06 31 4D CA 76 E0 99 AC 10 E1 34 00 19 04 A7 B4 5A 72 EB 1E CC F7 88 50 11 16 D0 1E 53 00 00 00 00 00 00

- 请回答以下问题（写出具体理由）：
  - 求源IP地址、源端口、目的IP地址、目的端口？
  - 该以太网帧是从客户发送给服务器还是从服务器发送给客户？相应的服务器程序是什么？
  - 该以太网帧是在TCP运输连接的什么阶段捕获的？

熟知端口号

FTP	TELNET	SMTP	DNS	TFTP	HTTP
21	23	25	53	69	80

以太网帧格式

6	6	2	46 ~ 1500	4
目的地址	源地址	类型	数　据	FCS

IP 数据报格式

TCP 报文段格式

答：

- （1）根据以太网帧格式，类型字段中为“0x0800”，表明数据区中为IP数据报。IP数据报起始于“45”字段。根据IP数据报格式，协议字段为“0x06”表明IP数据报数据部分为TCP报文段，源地址为“CA 76 E0 99”，目的地址为“AC 10 E1 34”，TCP报文段起始于“00 19”。根据TCP报文段格式，源端口为“00 19”，目的端口为“04 A7”。于是：
  - 源IP地址：202.118.224.153
  - 源端口：25
  - 目的IP地址：172.16.225.52
  - 目的端口：1191

（2）由于源端口是熟知端口号“25”，因此该以太网帧是从服务器发送给客户，相应的服务器程序是：SMTP服务器程序。

- （3）根据TCP报文段格式，控制位为“0x11”，转换为二进制的形式：“010001”，报文FIN=1，表明要求释放运输连接，因此该以太网帧是在连接释放阶段捕获的。

某网络拓扑图如下图所示，路由器R1通过接口E1、E2、E3分别连接局域网1、局域网2、局域网3，通过接口L0连接路由器R2，并通过路由器R2连接域名服务器与 互联网。R1的L0接口的IP地址是202.195.2.1；R2的L0接口的IP地址是202.195.2.2，L1接口的IP地址是 61.167.60.22，E0接口IP地址是202.195.3.1；域名服务器的IP地址是202.195.3.2；R2通过路由器R3的L0接口接入互联网，其IP地址为61.167.60.23。R1与R2间链路的MTU=1420；R2与R3间链路的MTU=1020（注：MTU为最大传送单元，为能够通过的IP数据报最大长度）。请回答以下问题（写出具体理由及推演过程）：

a) 局域网1、局域网2与局域网3上的主机数分别为120，60，60。将IP地址空间 202.195.1.0/24 划分为3个子网，分别分配给局域网1、局域网2与局域网3，请给出每一个局域网的地址块（包括网络前缀与子网掩码)

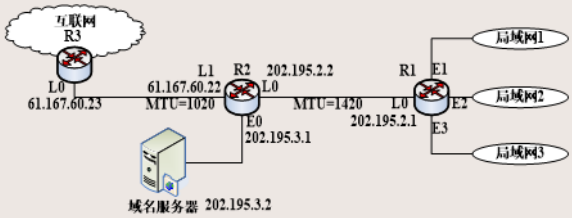
b) 给出R1的完整路由表，并要求包含的路由表项最少

c) 给出R2的完整路由表，并要求包含的路由表项最少

d) 若局域网1中某主机有一个IP数据报要发送给互联网的某一服务器，该IP数据报总长度为2020字节（固定首部长度），则经过R1时需要进行数据报分片，请给出分片结果？（包括每一个分片数据报的数据字段长度、片偏移和MF的值）

e) 请进一步给出d)中数据报经过R2时的分片结果？

附：路由表项包括如下内容：目的网络IP地址、子网掩码、下一跳IP地址、接口



a) 答案并不唯一，给出其中一种：

局域网 1 202.195.1.0/25；局域网 2 202.195.1.128/26；局域网 2 202.195.1.192/26

b) 基于 a)中给出的划分方法，给出相应的路由表：

目的网络 IP 地址	子网掩码	下一跳 IP 地址	接口
202.195.1.0	255.255.255.128	直接	E1
202.195.1.128	255.255.255.192	直接	E2
202.195.1.192	255.255.255.192	直接	E3
0.0.0.0	0.0.0.0	202.195.2.2	L0

c)

目的网络 IP 地址	子网掩码	下一跳 IP 地址	接口
202.195.1.0	255.255.255.0	202.195.2.1	L0
202.195.3.2	255.255.255.255	直接(或 202.195.3.2)	E0
0.0.0.0	0.0.0.0	61.167.60.23	L1

d)分成 2 个分片：

数据字段长度	片偏移	MF
1400	0	1
600	175	0

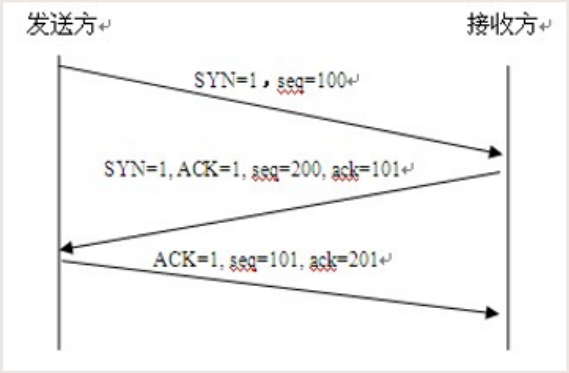
e) d)中的第 1 个分片继续被分片，第 2 个分片保持不变，总共 3 个分片：

数据字段长度	片偏移	MF
1000	0	1
400	125	1
600	175	0

- 用TCP传送512字节的数据。设窗口为300字节，而TCP报文段每次传送100字节的数据。再设发送方和接收方的起始序号分别为100和200。试回答下面问题：
  - 1) 画出TCP连接建立过程的示意图。
  - 2) 发送方发送完毕512个字节的数据以后，进行连接释放，这时连接释放报文段序号应该为多少？

答：

- 1）连接建立过程示意图：



- 2) 此时连接释放报文段序号为**613**。100+1+512=613

- 生日攻击 2的55次幂 抗强抗弱：2的80次幂