第十九节 网络安全问题概述、两类密码体制、鉴别

一、课程目标

了解教材 7.1-7.3。

二、课程内容

【网络安全问题概述】

1、网络安全威胁分为两类：被动攻击和主动攻击。

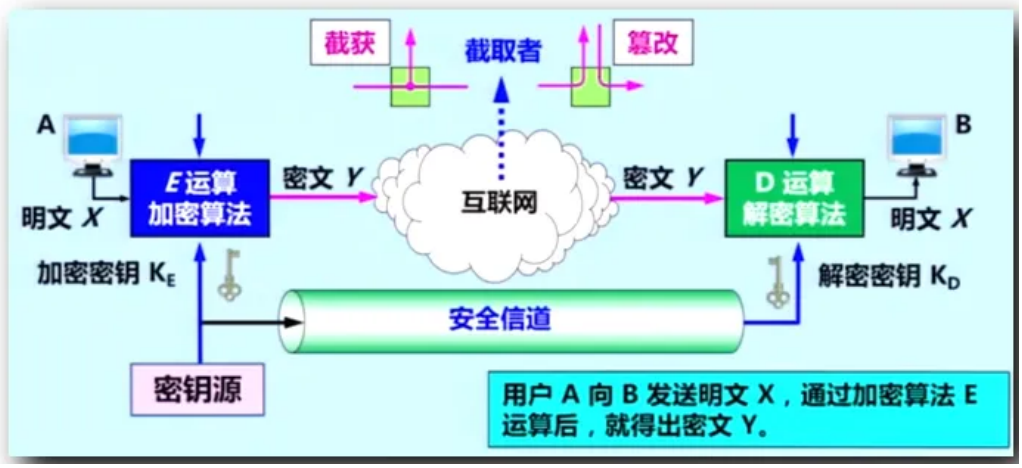
2、被动攻击是指攻击者从网络上窃听他人的通信内容，即截获。合理利用称为流量分析。

3、主动攻击类型众多，主要包括篡改、恶意程序（计算机病毒、计算机蠕虫、特洛伊木马、逻辑炸弹、后门入侵、流氓软件）、拒绝服务 DoS 等。

4、计算机网络安全的四个目标：**机密性、端点鉴别、信息完整性、运行安全性**。其中，

- 机密性应对被动攻击，只有发送方和接收方才能理解信息内容，截获者可见不可用。
- 端点鉴别应对主动攻击，避免身份假冒。
- 信息安全性确保信息内容未被他人篡改，通常与端点鉴别配合存在。
- 运行安全性代表性方案是访问控制，对用户访问权限加以控制。

5、**数据加密模型**：用户 A 向 B 发送明文 X，但通过加密算法 E 运算后，得到密文 Y。用户 B 执行解密算法 D，得到明文 X。



6、密码学包括两部分：密码编码学（设计密码体制）和密码分析学（破解密码）。

【两类密码体制】

7、20 世纪 70 年代后期，美国数据加密标准 DES 和共钥密码体制的出现，成为近代密码学发展史上的两个里程碑，分别对应两类密码体制：**对称密钥密码体制和公钥密码体制**。

8、对称密钥密码体制：加密密钥与解密密钥相同；密钥保密，算法公开。代表性方案包括 DES、三重 DES、AES。

- 数据加密标准 DES 由 IBM 公司研制，于 1977 年定为美国联邦信息标准。其在加密前，先对整个明文按照 64 位长二进制数据分组然后进行加密处理，得到一组 64 位密文数据，最后将各组密文串接得到整个密文。使用的密钥占有 64 位（实际密钥长度为 56 位，外加 8 位用于奇偶校验）。
- 三重 DES 把 64 位明文用第一个密钥 K1 加密，在用第二个密钥 K2 解密，再用第一个密钥 K1 加密。
- AES 有三种加密标准，其密钥分为 128 位、192 位和 256 位。

名称	秘钥长度	运算速度	安全性	资源消耗
DES	56 位	较快	低	中
3DES	112 位，168 位	慢	中	高
AES	128 位，192 位，256 位	快	高	低

9、公钥密码体制：加密密钥与解密密钥不同；加密密钥 PK（公钥）公开，解密密钥 SK（私钥）保密，加密算法 E 与解密算法 D 公开；又称非对称密钥密码体制。代表性方案包括 RSA。

公钥密码体制产生原因包括（1）对称密钥密码体制密钥分配复杂，高度依赖密钥分配中心；（2）数字签名需求。

名称	成熟度	安全性	运算速度	资源消耗
RSA	高	高	慢	高
DSA	高	高	慢	只能用于数字签名
ECC	低	高	快	低

10、共钥密码体制加解密过程特点：

- 密钥对产生器产生出接收者 B 的一对密钥：加密密钥 PK_B 和解密密钥 SK_B。发送者 A 所用的加密密钥 PK_B 就是接收者 B 的公钥，向公众公开。B 所用的解密密钥 SK_B 就是接收者 B 的私钥，对其他人保密。
- 从已知的 PK_B 推导出 SK_B 是“计算上不可能的”。
- 公钥可以用来加密，但不能用来解密。
- D 运算和 E 运算先后顺序可以任意。

11、任何加密方法的安全性取决于密钥的长度和攻破密文所需的计算量，而非体制。

【鉴别】

12、鉴别对象包括鉴别发信者（实体/端点鉴别，验证是否冒充）和鉴别报文完整性（未被他人篡改），对应两类鉴别：实体鉴别和报文鉴别。

13、数字签名基本原理：A 用其私钥 SK_A 对报文 X 进行 D 运算，将报文 X 转换为某种不可读密文，B 用 A 的公钥 PK_A 进行 E 运算得到明文，可以完成鉴别。

- 数字签名还可保证发送者时候不能抵赖对报文的签名，即不可否认。若

A 抵赖曾发送报文给 B，B 可将 X 及 D_{PKA}（X）公证，第三者很容易用 PK_A 证实 A 确实发送 X 给 B。

- 普通数字签名不具备机密性，为保证机密性，可采用教材图 7-5 所示方案，现实中难以实现。

14、密码散列函数，又称哈希函数，具备四个特点：哈希结果较短且固定（快）、抗碰撞、单向性、非线性（输入小改动，输出大改动）。代表性方案包括 MD5 和 SHA-1。

14、**实体鉴别**基本原理：A 向 B 发送带有自己身份 A 和口令的报文，并使用双方约定好的共享对称密钥 K_{AB} 进行加密；B 使用 K_{AB} 进行解密，完成 A 的身份鉴别。

- **重放攻击**：入侵者 C 截获 A 发给 B 的报文，C 不需要破译该报文，直接转发给 B；B 误认为 C 是 A，向伪装成 A 的 C 发送许多本应该发送给 A 的报文。
- 应对重放攻击的方法是**不重数法**：采用一次一数，一次一个不重复使用的大随机数，区分重复的鉴别请求和新的鉴别请求。具体流程为：A 首先用明文发送其身份 A 和一个不重数 R_A 给 B，B 使用共享密钥 K_{AB} 对 R_A 加密后发回给 A，捎带自己的不重数 R_B。A 用共享密钥 K_{AB} 对 R_B 加密后发回给 B。
- 中间人攻击：AB 通信中间存在中间人 C。C 用自己的私钥 SK_C 对 RB 加密后发回给 B，使 B 误认为是 A 发来的。A 收到 RB 后也用自己的私钥 SK_A 对 RB 加密后发回给 B，但中途被 C 截获并丢弃。B 向 A 索取其公钥，这个报文被 C 截获后转发给 A。C 把自己的公钥 PK_C 冒充是 A 的公钥发送给 B，同时也截获到 A 发送给 B 的公钥 PKA。B 用收到的公钥 PK_C（误认为是 A 的）对数据进行加密，并发送给 A。C 截获后用自己的私钥 SK_C 解密，复制一份留下，然后再用 A 得公钥 PK_A 对数据加密后发给 A。A 收到数据后可以用自己的私钥 SK_A 解密。

三、重点习题

P368：全部

四、参考资料

https://cloud.tencent.com/developer/techpedia/1806
https://www.jianshu.com/p/fff19c19eb09