> 教材十五章

- 身份识别的应用场景（强调实时性，登录的时候）
- 认证方式：口令（掌握），挑战/应答（了解），零知识认证协议（**不考**，匿名投票时可用到）
- 这些方式为什么不安全？
- 用哪些信息来证明自己的身份？

口令

> 怎么安全存用户口令？

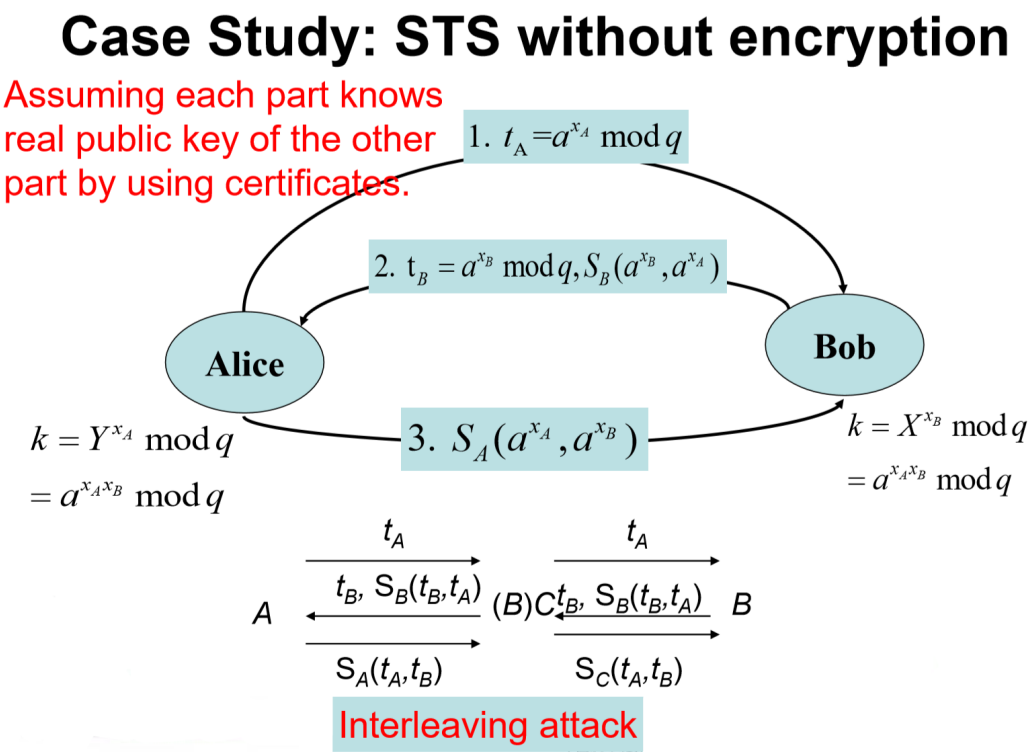
设置读写权限，存储口令的哈希值，加盐（盐值是随机生成的，可防碰撞攻击）

挑战/应答

以下方法可用于防止「重放攻击」：

1. 挑战/应答（随机数）：A 想要一个来自 B 的新消息，首先发给 B 一个临时交互号（询问），并要求后面从 B 收到的消息（回复）包含正确的临时交互号值
2. 序列号（开销较大）：为每一个用于认证交互的消息附上一个序列号，只有当新消息的序列号顺序正确时，它才被接受
3. 时间戳

- 基于对称密钥的挑战/应答
  - 第六张课件中有 NeedHam Schroeder 以及其改进方案。
- 基于公钥密码的挑战/应答
- 基于数字签名的挑战/应答
  - 站间协议（STS），https://xz.aliyun.com/t/2965 这里有中文描述。下图为无加密版本：



若不加密，可能遭遇交织攻击（PPT P38，让 A 误以为 ta 在和 B 通信，实际上在和 C 通信）

一些攻击手段

- 假冒攻击
- 重放攻击
- 交织攻击：一种模拟或其他欺骗行为，包括选择性地组合来自一个或多个先前或同时进行的协议执行（并行会话）的信息
- 反射攻击：反射攻击是一种攻击挑战/应答认证系统的方法，攻击的基本思想是诱使目标为自己的挑战提供答案。是一种交织攻击
- 选择文本攻击

思考题

15.2

> 列出三个常用的防止重放攻击的方法。

1. 随机数
2. 序列号（开销较大）
3. 时间戳

15.4

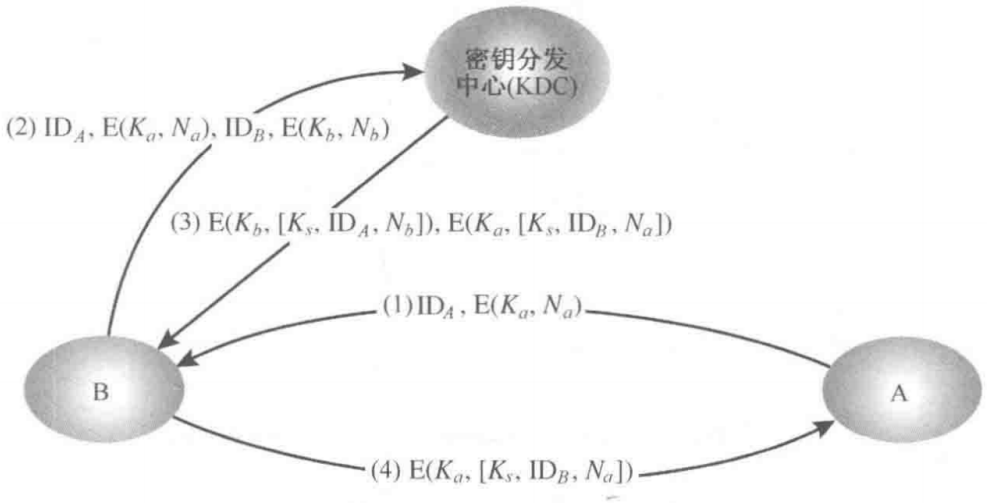
> Kerberos 主要处理什么问题?

假设一个开放的分布式环境，其中工作站上的用户希望访问分布在整个网络中的服务器上的服务。我们希望服务器能够限制对授权用户的访问，并能够对服务请求进行身份验证。在这种环境下，无法信任工作站为网络服务正确识别其用户。

习题

14.1

> 14.1 本地网络向量提供一个密钥分发方案，如图 14.18 所示。
> （a）描述该方案。
> （b）相比图 14.3 的方案，有哪些优点和缺点。



(a) A 向 B 发送一个连接请求，用 A 与 KDC 共享的密钥加密事件标记或 nonce（N_a）。如果 B 准备接受连接，它会向 KDC 发送一个会话密钥请求，包括 A 的加密 nonce 加上 B 生成的 nonce（N_b），并用 B 与 KDC 共享的密钥加密。KDC 向 B 返回两个加密的块，其中一个块供 B 使用，包括会话密钥、A 的标识符和 B 的 nonce。为 A 准备了一个类似的块，并从 KDC 传递到 B，然后传递给 A。A 和 B 现在已经安全地获得了会话密钥，并且由于这些非连续性，可以确保另一个是可信的。

(b) 该方案的一个优点是，在 B 拒绝连接的情况下，避免了与 KDC 交互的开销。

14.2

> “请描述下，该网络使用的通信协议。”福尔摩斯睁开眼睛，以告诉 Lestrade 他虽然一脸睡意但是他还是在认真听着。
> “协议如下，网络中的每个节点 N 都有唯一的密钥 K_n，用于节点和可信服务器之间的安全通信，即所有的密钥也在服务器中存放。用户 A 想要发送秘密消息 M 给 B 时，使用以下协议：
>
> （1）A 产生临时交互号 R，发送自己的名字 A、目的地 B 和 $\mathrm{E}(K_a, R)$ 给服务器。
> （2）服务器回复消息 $\mathrm{E}(K_b, R)$ 给 A。
> （3）A 发送 $\mathrm{E}(R, M)$ 和 $\mathrm{E}(K_b, R)$ 给 B。
> （4）B 使用 K_b 解密 $\mathrm{E}(K_b, R)$ 得到 R，随后应用 R 解密 $\mathrm{E}(R, M)$ 得到消息 M。
>
> 每次有消息发送时产生一个随机密钥，我承认他可能在几个节点之间发送时截获消息，但是，他不可能解密消息。”
> “我相信你有你的道理，Lestrade。这个协议是不安全，因为服务器不能鉴定谁发的请求。明显地，协议设计者相信发送 $\mathrm{E}(K_x, R)$ 就可以鉴定发送者为用户 X，因为只有 X 知道 K_x，但是你也知道 $\mathrm{E}(K_x, R)$ 可能被截获然后重放。只要知道漏洞在哪里，通过监控该男子对访问计算机的使用，可以得到更多的证据。他最有可能是这么做的：截获 $\mathrm{E}(K_a, R)$ 和 $\mathrm{E}(R, M)$ 后，我们称该男子为 Z，会假装 A，然后……”
> 完成福尔摩斯的话。

1. 向服务器发送源名称 A，目的地名称 Z（他自己的名称）和 $\mathrm{E}(K_a, R)$
2. 服务器将通过向 A 发送 $\mathrm{E}(K_z, R)$ 进行响应，而 Z 将截获
3. 因为 Z 知道他的密钥 K_z，所以他可以解密 $\mathrm{E}(K_z, R)$，因此可以动用 R 来解密 $\mathrm{E}(R, M)$ 并获得 M

15.10

> 在 Kerberos，当 Bob 收到一个来自于 Alice 的票据，如何得知其是否真实?

它包含 Alice 的 ID、Bob 的名字和 KDC-Bob 密钥加密的时间戳。

15.11

> 在 Kerberos，当 Bob 收到一个来自于 Alice 的票据，如何得知其确实来自于 Alice?

它包含由 KDC-Bob 密钥加密的 Alice 的名字。

15.12

> 在 Kerberos，若 Alice 收到一个回复，她如何得知该消息来自于 Bob（且是 Bob 最新的回复）?

它有一个用会话密钥加密的 Nonce（例如，时间戳）。