南開大學
Nankai University

网络空间安全学院

课堂题目

重放攻击及相关问题

姓名：魏伯繁

学号：2011395

专业：信息安全

2023 年 5 月 22 日

目录

1 消息重放的定义

消息重放就是重放攻击，是指攻击者发送一个目的主机已接收过的包，来达到欺骗系统的目的，主要用于身份认证过程，破坏认证的正确性。重放攻击可以由发起者，也可以由拦截并重发该数据的敌方进行。攻击者利用网络监听或者其他方式盗取认证凭据，之后再把它重新发给认证服务器。重放攻击在任何网络通过程中都可能发生，是计算机世界黑客常用的攻击方式之一。

重放攻击的基本原理就是把以前窃听到的数据原封不动地重新发送给接收方。很多时候，网络上传输的数据是加密过的，此时窃听者无法得到数据的准确意义。但如果他知道这些数据的作用，就可以在不知道数据内容的情况下通过再次发送这些数据达到愚弄接收端的目的。例如，有的系统会将鉴别信息进行简单加密后进行传输，这时攻击者虽然无法窃听密码，但他们却可以首先截取加密后的口令然后将其重放，从而利用这种方式进行有效的攻击。再比如，假设网上存款系统中，一条消息表示用户支取了一笔存款，攻击者完全可以多次发送这条消息而偷窃存款。

在重放攻击中，攻击者并不需要破解加密算法或窃取密码，只需要在目标系统与合法用户之间的通信过程中拦截数据包，记录其内容并在以后的某个时间再次发送这些数据包即可。重放攻击可以被视为一种类似于回放录像的攻击方式，攻击者将过去的通信数据包“重放”给目标系统，让目标系统误认为这些数据包是当前的合法请求。

重放攻击在许多场景下都会带来安全风险，如银行转账、电子票务、安全门禁等，因为在这些场景下，需要防止用户在短时间内重复提交同一请求，或者防止攻击者在发送一次合法请求之后多次利用该请求来进行欺诈行为。如果攻击者可以轻易地截获合法请求并重放，那么系统就会受到攻击。

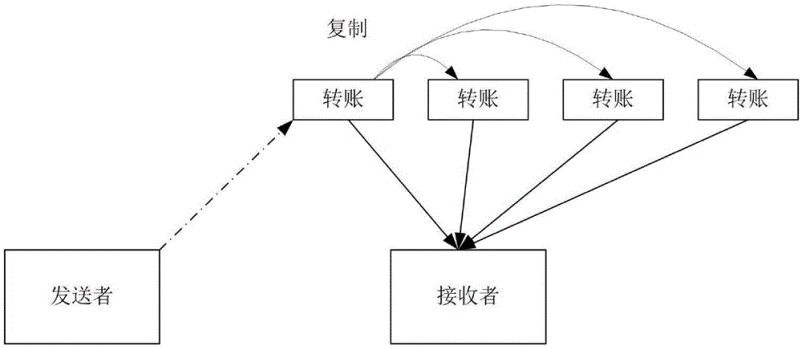

图 1.1: 重放攻击示意图

2 防御方法及优劣分析

2.1 加随机数

该方法优点是认证双方不需要时间同步，双方记住使用过的随机数，如发现报文中有以前使用过的随机数，就认为是重放攻击。缺点是需要额外保存使用过的随机数，若记录的时间段较长，则保存和查询的开销较大。

2.2 加时间戳

该方法优点是不用额外保存其他信息。缺点是认证双方需要准确的时间同步，同步越好，受攻击的可能性就越小。但当系统很庞大，跨越的区域较广时，要做到精确的时间同步并不是很容易。

2.3 加流水号

就是双方在报文中添加一个逐步递增的整数，只要接收到一个不连续的流水号报文 (太大或太小)，就认定有重放威胁。该方法优点是不需要时间同步，保存的信息量比随机数方式小。缺点是一旦攻击者对报文解密成功，就可以获得流水号，从而每次将流水号递增欺骗认证端。

2.4 时间戳 + 随机数

：在消息中注入一个时间戳和一个随机数，接收者检查时间戳和随机数是否都合法，以此判断消息的有效性。这种方法可以增加判断的准确性，但是增加了消息的大小，可能导致网络拥塞等问题。

2.5 消息签名

：使用对称密钥来生成一个 MAC，以此保证消息的完整性和真实性。但是，MAC 是基于对称密钥的，密钥管理和分发可能会带来安全问题。

2.6 数字证书

：使用公钥来加密数字证书，以此保证消息的完整性和真实性。数字证书中包含了公钥和相关的身份信息，可以用于实现身份验证和密钥管理。但是，数字证书的繁琐过程和管理维护成本可能较高。

以上方法各有优缺点，具体取决于应用场景和安全需求。例如，时间戳具有轻量级的优点，适用于对时效性要求较高的场景，但是不够安全；数字证书相对来说更加安全，但是相对较重量级，适用于对安全性要求较高的场景。

参考材料：**https://www.jianshu.com/p/a810a6b14841**

https://zhuanlan.zhihu.com/p/615133039