基于网络通信的会话窃取的研究

The Research of Session Attacking Based on Networking Communication

许力阳　王　康

（重庆大学网络中心　重庆400044）

Abstract　This article describes an attack against the TCP, which allows crackers to break the session of both client and server and to redirect the TCP stream to manipulate the system as a legal user. The principle of the attack is analyed, and TCP protocol and some schemes to detect this attack are presented.

Keywrods　Session attacking, TCP, Synchization, Desynchization, TCP series

1. 概述

随着 Internet 的发展与普及，远程调用变得十分常见，地理位置上跨洲和跨国的远程调用也变得十分普遍。一般而言随着空间距离的增加，信息流过的中间信息节点也相应增多，信息被截获的可能性也随之加大。为方便广大用户，一些企业、银行组织、政府机构甚至某些军事部门将原有的内部网络与公众信息网实现了互联。一方面，方便了信息的双向交流，使信息采集，移动办公成为可能；另一方面，也增加了信息的不安全性，信息被截获的可能性较大，使得“某个角落”的窃听者，实施通信过程中的“会话窃取”成为可能，进而造成立即的或潜在的信息安全威胁。本文研究会话窃取的原理、方法，将有助于对这一网络攻击手段的防范，有助于对其它基于 TCP（传输控制协议）传输信息网络破坏的预防。

网络攻击通常有两种方式：一是对网络应用程序中的漏洞进行攻击；二是利用网络通信协议（如 TCP 通信协议）的漏洞进行攻击。利用网络应用程序漏洞的攻击因计算机的型号，系统软件或应用软件的版本不同而不同。而利用网络通信协议漏洞进行的攻击则是跨平台，跨机型的，具有一定的“普遍性”和“通用性”。会话窃取是利用网络通信协议的漏洞进行攻击的众多方法之一，它利用 TCP/IP 协议的 TCP 和其上层应用层协议的“先天不足”而实施的攻击。TCP 是 TCP/IP 协议族中应用最为广泛的协议之一，因此会话窃取这种攻击是极具威胁性的网络攻击手段。

2. 会话窃取

会话窃取简而言之就是第三方（攻击者）通过一定的手段首先窃取到双方的对话，然后使其中的一方被中断，再冒充这一方和不知情的另一方继续对话。

进行会话窃取攻击需要攻击者熟知网络的信息交流情况，即：谁正在通过，向谁提供什么服务，或是向谁得到什么服务，通信 IP 地址，端口号是多少，服务内容是什么（即应用层使用什么协议）等等。显然攻击者需要借助一个网络侦听程序的帮助，通过耐心的网络侦听之后，攻击者总能得到诸如会话双方的 IP 地址、端口号、TCP 报文的序号、TCP 报文的确认序号等，甚至用户的注册密码等信息也能获取。攻击者要实施会话窃取攻击，通常只需要知道前面的四项内容就可以了。

如果应用层使用的通信协议是“容易下手”的协议，如 TELNET、FTP，加之有了会话双方的 IP 地址、端口号、TCP 报文的序号、TCP 报文的确认序号，攻击者就容易进行攻击。攻击者接下来要做的便是搅乱原有的 TCP 会话，使会话中断。攻击者中断原有会话的手段有多种，如可以通过 TCP 的复位直接中断原有连接（这是一种比较鲁莽的做法）。更为隐蔽的做法是通过修改 TCP 报文的序号和 TCP 报文的确认序号，来破坏原有的会话连接，此时攻击者就可以扮作会话的一方与另一方通信了。下面具体分析 TCP 连接传输的过程。

3. 同步建立一个 TCP 连接的过程

TCP 通信协议通过使用三次握手协议后，建立起双方的连接。三次握手协议是连接两端正确同步的充要条件。这是因为 TCP 建立在不可靠的分组投递服务之上，报文可能出现丢失、延迟、重复和混乱的情况。

在 TCP 的三次握手协议中，首先由 CLIENT 客户方发出第一个报文，报文的码元字段 SYN 被置1，报文序号是 CLT_SEQ0；SERVER 服务方收到第一个报文之后发出确认报文，该报文码元字段的 SYN 和 ACK 均被置1，表明这是对第一个报文的确认，报文序号是 SVR_SEQ0；最后由 CLIENT 方发出最后一个报文，该报文仅仅是一个确认信息，报文码元字段的 ACK 被置1，通知 SERVER 方已经建立了双方所同意的这个连接。到此，TCP 通信会话建立，此时有如下关系：

客户端报文序号 CLT_SEQ=CLT_SEQ0+1

客户端应答序号 CLT_ACK=SVR_SEQ0+1

服务端报文序号 SVR_SEQ=SVR_SEQ0+1

服务端应答序号 SVR_ACK=CLT_SEQ0+1

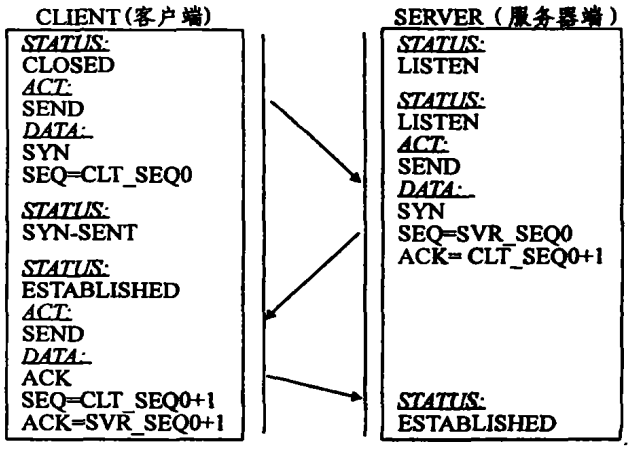

图1　TCP 通信双方建立连接过程

三次握手协议完成了两个重要的功能，确保了连接双方做好传输数据的准备，而且双方统一了初始序号；在握手期间传输序号并获得确认。每个机器随机地选择一个初始序号，用以区分报文在数据流中的位置。图1是 TCP 通信协议的 CLIENT 端与 SERVER 端建立连接的过程。

TCP 会话建立起来后，此时有如下关系：

CLT_SEQ=CLT_SEQ0+1

CLT_ACK=SVR_SEQ0+1

SVR_SEQ=SVR_SEQ0+1

SVR_ACK=CLT_SEQ0+1

4. TCP 传输接收过程中的会话窃取

在 TCP 会话过程建立之后，CLIENT 方和 SERVER 方均处于对等通信状态。TCP 提供了可靠的数据流投递服务，确保在计算机之间进行没有重复和丢失的数据流的投递。IP 层提供了分组报文的投递功能，并不确保数据流的可靠投递。大部分可靠投递的协议，都使用“确认-重传”机制作为提供可靠性的基础。这项技术要求接收方收到数据之后向发送方回送确认信息。发送方对发出的每个报文都保存一份记录，并在发送下一个报文之前等待确认。许多网络协议出于提高传输效率和流量控制的考虑，并引入了滑动窗口的概念。

滑动窗口允许发送方在得到确认信息之前发送多个分组报文。当窗口内第一个分组报文的确认到达时，发送窗口向后滑动，并发送下一个报文，随着确认的不断到达窗口也在向后滑动。接收方同样有滑动窗口控制着数据接收的步调。当窗口内第一个分组报文到达时，接收窗口向后滑动，并回应以 ACK 报文。随着分组报文的不断到达接收窗口也在向后滑动。然而报文序号落在接收滑动窗口之外的分组报文将被丢弃，接收方将回应以 ACK 报文指出希望得到的报文序号。

TCP 在传输中，使用 ACK 报文确认收到的数据报文，通过滑动窗口控制流量。ACK 报文中携带了它收到的报文的序号(sequence number)。因为 TCP 建立在不可靠的分组投递服务之上，报文在通过网络的传输过程中难免会发生误传、拥塞、丢失等现象。在报文到达接收方之后，接收方将对收到的报文依据报文序号进行排序、重组，对于落在接收滑动窗口之外的报文将会被丢弃。发送方发出报文的报文序号应当满足不等式 ACK≤SEQUENCE NUMBER≤ACK+WINDOW SIZE 才能被接受方所接受。

对于 CLIENT 方的 TCP 报文的序号，CLT_SEQ 应落在区间[SVR_ACK，SVR_ACK+SVR_WINDOW]

对于 SERVER 的 TCP 报文的序号，SVR_SEQ 应落在区间[CLT_ACK，CLT_ACK+CLT_WINDOW]。

4.1 同步缺失(DESYNCHRONIZTION)

当以上条件不能满足时，通信双方处于同步缺失状态。此时发送方的所有报文都将被接受方拒绝，接受方将应之以 ACK 报文，ACK 报文中带有接受方希望的报文的序号。

显然，同步缺失正是攻击者所希望的状态。通过造成同步缺失，攻击者将原有的连接断开，然后伪造报文，以他人的身份继续操作。

4.2 复位法制造同步缺失

复位法是指攻击者在 CLIENT 和 SERVER 在建立会话时利用复位报文中断 CLIENT 和 SERVER 的三次握手过程，冒充 CLIENT 继续和 SERVER 通信。复位法制造同步缺失的过程如下：

(1)攻击者侦听网络发现 SERVER 回应的 SYN/ACK 报文。

(2)攻击者向 SERVER 的同一端口发送 RST 报文，然后发送一个 SYN 报文，这个 SYN 报文与原有的 SYN 报文拥有相同的参数，但报文序号不同。

(3)RST 报文后 SERVER 将关闭第一次的连接，并对收到的 SYN 报文应之以 SYN/ACK 报文。

(4)攻击者在侦听到 SYN/ACK 报文后，回应 ACK 报文。SERVER 进入 ESTABLISHED 状态。

(5) CLIENT 在得到最早 SERVER 回应的 SYN/ACK 报文后进入 ESTABLISHED 状态。

这时，对于 CLIENT 的 TCP 报文的序号应当满足不等式：

SEQUENCE NUMBER＜ACK or SEQUENCE NUMBER＞ ACK + WINDOWS，即 CLT_SEQ 应落在区间[SVR_ACK，SVR_ACK + SVR_WINDOW] 之外。即 CLIENT 和 SERVER 进入了同步缺失状态。

4.3 通过应用层造成同步缺失

复位法制造同步缺失的方法依据应用层的具体协议而各不相同，但各种手法的指导思想是一致的。通过大量的数据报文造成同步缺失，而在此过程中 CLIENT 一端不会产生明显的迹象显示正在受到攻击。以 TELNET 应用为例来说明其过程。

(1) 攻击者侦听到 TELNET 会话。

(2) 攻击者发送大量的数据报，这些数据报仅包含 IAC NOP IAC NOP...，SERVER 的 TELNET DAEMON 在收到每对 IAC NOP 序列后，从数据流中取走 IAC NOP，而不做其他任何动作。但这时 SERVER 的 ACK 确认序号却在不停地变化，直到达到以下状态。

对于 CLIENT 的 TCP 报文的序号满足不等式：

SEQUENCE NUMBER＜ACK or SEQUENCE NUMBER＞ACK+WINDOWS

即 CLT_SEQ 应落在区间[SVR_ACK，SVR_ACK+SVR_WINDOW] 之外，为了达到会话窃取的目的攻击者要做的就是破坏原由会话双方的同步，破坏同步的前提是网络的窃听得到会话双方的 IP 地址，端口号，TCP 报文的序号，TCP 报文的确认序号等信息，进而使用伪造的报文使通信一方的报文序号不再满足 TCP 的传输接受要求，即实现原有通信双方的“同步缺失”，此时攻击者便可凭借伪造的应用层的数据报文展开攻击。

5. 会话窃取的预防与检测

要进行会话窃取必须要通过网络侦听之后，得到会话双方的 IP 地址、端口号、TCP 报文的序号、TCP 报文的确认序号等信息。在不同的网络拓扑结构下和不同的网络介质下，实现网络侦听的可能性和难度各不相同，但是在通常的树型拓扑结构和 CSMA 的协议下网络侦听变得异常容易。会话窃取虽然利用了 TCP 的“先天不足”，但是问题的症结仍在应用层。应用层的明文传输使得攻击易于得手。特别是象广泛应用的 TELNET，FTP 功能，用户通过 root 用户注册的应用就显得格外的脆弱。会话窃取的攻击检测有一定的难度，因为整个攻击过程因应用层的不同各有所异，并无固定的模式可循。而采用端口扫描和IP轰炸等手段进行攻击就易于主动被发现。

(下转第134页)

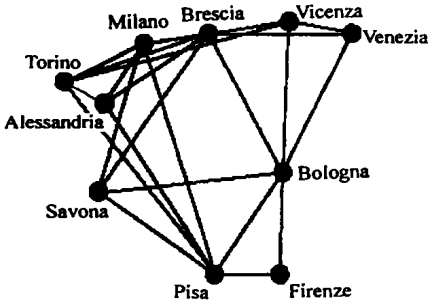

图2 上层网络拓扑

图3 下层网络拓扑

中，然后进行备用容量的规划。在进行备用容量规划时，分为两个阶段进行，第一阶段，在给定上下层联合业务分配矩阵和对下层单链路故障进行100%恢复条件下，对备用容量进行计算。对此问题的求解，可以通过专门的求解整数线性规划的软件如 LINGO 等进行求解，但要使用此工具求解，需要对节点对间的满足条件的备用路由进行事先计算。我们使用基于文[9]描述的算法思想自行编制的程序，使备用容量的计算同实际的动态恢复大体一致。恢复路由的可选路由的最大值设置为5。第二阶段，以此备用容量结果为基础，针对上下层的组合故障进行恢复，对总的备用容量进行计算，上层故障将在上层和下层同时进行恢复，并优先使用上层的恢复。整个过程分成两个阶段，在第一次备用容量规划的基础上，可以方便地了解，在进行第二次规划之前，下层的备用容量可以同时提供给上层进行恢复的百分比率。我们对给定的网络拓扑分别对上层和下层指定如下的本地业务，上层的均匀分布的业务量（以VC-4为单位）分别为：180和360个单位。下层以波长为单位的业务量分别为：78，156，234。上下层业务单位的粒度比例分别设置为1：1或1：4，即是 SDH 层的交叉粒度为 VC-4，而 WDM 的一个波长通道的容量为155Mb/s，或622Mb/s。

表1 不同业务分布情况下的备用容量使用情况

下层业务量（波长）	78				156				234			
单位容量比例（下/上）	1		4		1		4		1		4	
上层业务量（VC-4）	180	360	180	360	180	360	180	360	180	360	180	360
分配业务总量（波长）	815	1423	359	511	1022	1630	566	718	1229	1837	773	925
恢复下层故障所需备用容量	1006	1776	431	620	1240	2011	681	862	1482	2238	931	1112
恢复上下层故障所需备用容量	1275	2257	504	762	1524	2550	754	1008	1766	2806	1004	1258
备用容量增加率（%）	26	27	16	22	22	26	10	16	19	25	7	13

从以上结果可以看出，在下层本地业务量较小的情况下，上层业务对总的备用容量的影响较大，但上层业务量的容量的增加，对备用容量增加的增益较小。而在上层的业务量较大的情况下，上下层单位容量的比例越大备用容量的增加越小，但备用容量随着上层业务量的增加，其增量增益越大。这说明在本例情况：下层的网络连通度比较低，平均节点度 D=2.5，而上层网络的连通，其平均节点度 D=4.6较大的情况下，在下层本地业务量较大的情况下，网络容量利用更高，但增加上层网络的业务量，将导致网络容量利用率的更快下降。

小结 本文对 SDH/WDM 的 MESH 网络环境下，基于共享备用容量的一种恢复方式进行了研究。从全局方式的网络抗毁角度看，这种基于下层网络恢复机制的策略，可以作为一种补充机制，它可以在一定程度上动态地在上下层间调整网络的备用容量，为上层的网络业务提供一种疏导的手段。

（下转第112页）

（上接第144页）

对于采取会话窃取攻击的被攻击者来说，他感受到的也仅仅是连接异常中断，并不影响下一次的连接。因此，会话窃取的攻击手法较一般的攻击手段来得更隐蔽。

通过 TCP 协议传输会话窃取的手段虽然隐蔽，但仍有“马脚”可查。为了造成同步缺失状态，会产生大量的 ACK 报文，理论上 ACK 报文的多少与滑动窗口的大小成正比，在10 BASE-T 的网络条件下，滑动窗口的大小通常为4096位。在同步缺失状态下，当 SERVER 方收到了一个不可接受的数据报文后，会回应一个 ACK 报文要求所需要的分组报文。而这个报文会对于 CLIENT 来说同样是不可接受的，CLIENT 方也会回应一个 ACK 报文要求所需要的分组报文。如此反复，在网络通信中形成 ACK 风暴，又必然最终造成网络拥塞，网络拥塞一定会造成数据丢失。一旦有一个 ACK 报文丢失，整个 ACK 风暴即告结束。当然攻击者可以介入 ACK 应答，防止 ACK 风暴发生。因此加强对网络中的 ACK 风暴的监测，这也是防止会话窃取的重要手段。

因为攻击者伪造了合法用户的 TCP 报文，可通过防火墙的检测，而攻击的基础是网络监听，监听之后伪造用户报文是因为用户数据的明文传送为攻击者分析用户数据报文提供了极大的方便，因此最好的防范手段是谨慎使用未经加密的 TCP 应用。此外利用 IPSec，VPN 技术建立通信双方的通信加密数据通道可以有效地防止攻击者对数据报文的监听分析，从而防止攻击者利用伪造的数据报文展开攻击。

参考文献

1 Comer D E, Stevens D L. Internetworking With TCP/IP Vol I: Principles, Protocols, and Architecture (Third Edition). Prentice Hall

2 Comer D E, Stevens D L. Internetworking With TCP/IP Vol II: Design, Implementation, and Internals (Second Edition). Prentice Hall

3 Roberts D. Internet 协议手册. 海洋出版社，1998

4 Meinel C P. 黑客如何侵入. 科学，1998，12，44：51

5 谢希仁，陈鸣，张兴元. 计算机网络. 电子工业出版社，1998