基于 TCP/IP 的隐信道随机密钥方法的研究

Study on Random Cipher in Cover Channel Based on TCP/IP

李 岚　雷 洁　（南昌大学软件学院 江西南昌 330029）

摘　要： 本文针对在网络层上传输隐蔽信息的问题进行了探讨，提出了利用三次握手机制建立隐存储信道并进行隐蔽信息加密解密的方案。文中采用随机方式每次生成唯一的密钥序列对隐蔽信息进行加密。实验证明，这种加密方案使隐信道中隐秘信息的传输更有效率。

关键词： 三次握手 隐信道 TCP 运输连接 数据报

1　前言

隐通道是信息隐藏方法学的一个主要分支。在信息隐藏中，通信双方在符合系统安全策略的条件下进行互相通信，当使隐蔽通道时，通信双方在合法的内容上加上无法觉察的信息。面对网络世界中日益充斥着的多种黑客经常使用的攻击方式，人们对其识别的方法均已熟悉，且已存在比较成熟的体系对其进行对抗。而隐蔽通道技术由于其特殊的构造方式将给互联网带来前所未有的威胁。

隐蔽通道的概念由 Lampson[1] 首先定义。在开放系统互联模型中，通信双方原则上可针对七层模型中的每一层建立隐蔽通道[2]。而网络层则是处理端到端数据传输的最底层，可见，对这一层上的隐蔽通道算法的加密解密进行分析和研究具有十分重要的意义。

本文通过对 TCP 数据包头分析，设计了一种新颖的基于随机序列的隐存储信道算法。

2　隐信息的隐藏与识别方法

通过对图 1TCP 数据包头[4] 以及图 2 三次握手过程的分析，可知，ISN 字段可为三次握手建立虚拟回路提供有效的机制。在三次握手的建立过程中，一定有一数据包从客户端送至服务端，且在该数据包中 ISN 字段显示连接状态，即 SYN 的值为 ON。服务端收到报文后，返还一个数据包，写明自己的 ISN 号并且将已知报文附在其后（ISN +1），这时 SYN 和 ACK 字段为 ON。客户端随即将已知报文发还给服务端，三次握手即结束。

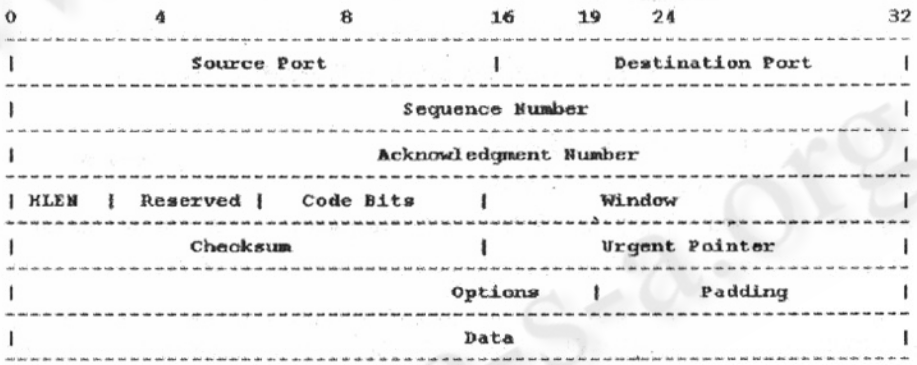

图 1　TCP 数据包头

在这里，32 位的 SN 字段可作为隐秘数据的存储空间加以利用。秘密消息的发送者可以在 SN 字段里加上需加入的数据，接收方可以据此接收数据。这样，在 SYN 数据包中使用 SN 字段我们可以建立一个独立的全双工隐秘通信信道。

客户端 > > > > > > > ISN1 + F[SYN] > > > > > > > > > > > > > > > 服务端
客户端 < < < ISN2 + ACK = (ISN1 + 1) + F[SYN,ACK] < < < < < < < 服务端
客户端 > > > > > > > ACK = ISN2 + 1 + F[ACK] > > > > > > > > > 服务端

图 2　三次握手

图 3 为隐存储信道的加密与解密过程。TCP 数据包的 ACK 字段为 32 位，令其为 i_k，k = 1,2,…32，标识字段 Sequence Number 为 32 位，令其为 f_k，k = 1,2,…,32。设隐蔽信息为 $[e_1, e_2, \cdots, e_{32}]$。

为使隐蔽信息在隐存储信道中传输，可构造唯一标识数据包的 32 位标识字段 Sequence Number。使

$$i'_k = [i_1, i_2, \cdots, i_{16}] = e_k \oplus f_k,\ k = 1,2,\ldots 16 \quad (a)$$

而 $i^*_k = [i_{17}, i_{18}, \ldots, i_{32}]$　(b)

为任意 16 位二进制数。由此可得

$$i_k = (a) + (b) = i'_k + i^*_k \quad (c)$$

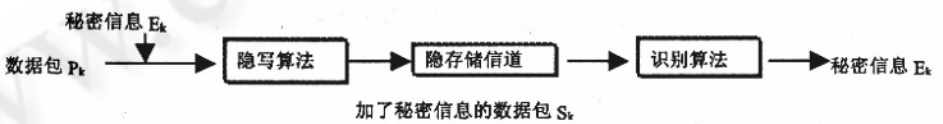

图 3　隐存储信道的加密与解密过程

可见，通过在数据包里传输由式(c)导出的 ik，隐存储信道可将隐蔽信息传输至目标主机而不考虑分段与否。本算法运用 one – time pad[3] 加密方案。显然，在该算法里，密钥为 f_k。对 f_k 稍加分析即可知其为一随机序列。

秘密信息 E_k 在隐存储信道中传输，最终到达目标主机。目标主机根据下文所述的识别算法将秘密信息解码。数据包到达后，相对应 ACK 字段以及标识字段被目标主机截获，目标主机通过等式 $E_k = f_k \oplus i'_k$ 获得隐蔽信息。

3　实验结果与算法分析

我们对本文提出的方案进行了模拟实验。实验中，我们将 1000 个藏有隐蔽信息的数据包由一台主机 A 发往另一台受防火墙保护的主机 B。实验证明，由于这种算法针对标识字段进行操作，使得这种形式的数据隐藏方法能抵御包过滤防火墙。标识字段的前 16 位由隐写算法构造，而后 16 位是随机产生的。这 16 位随机产生的数值可以保证加密后的数据为唯一的。因此，在隐信道中传输有相同标识符的内容相同的数据的概率为 $1/2^{16}$。也即说明，即使数据包内容相同，其标识符雷同以致被防火墙发现的概率也很小。可见，防火墙的过滤策略应针对这种情况作相应的改进，以增强识别隐信道传输隐密信息的能力。

参考文献

1 Lampson B W. A note on the confinement problem, Communications of the ACM, 1973, 16(10): 613 ~ 615.

2 Handel T G, Sandford M T. Hiding data in the OSI network model. Proceedings of Information Hiding: first international workshop, Cambridge, UK, Berlin: Springer – Verlag, 1996: 23 ~ 38.

3 D. Kahn, The Codebreakers: The Story of Secret Writing, New York: Macmillan Publishing Co., 1983.

4 U. S. C. Information Sciences Institute, "Internet protocol, darpa internet program, protocol specification," September 1981. Specification prepared for Defense Ad – vanced Research Projects Agency.