基于 TCP 时间戳的远程网络设备识别技术研究 *

徐书华[1],徐丽娜[2]
(1.华中科技大学 电子与信息工程系,湖北 武汉 430074;
2.武汉科技大学 管理学院,湖北 武汉 430074)

摘 要:不同于传统基于操作系统特性或者网络协议特性的软件识别机制,提出了一种基于TCP时间戳进行远程网络设备识别的方法。该方法依据RFC 1323协议中TCP时间戳理论,通过在发送数据包中加入时间戳选项,能够在没有测量工具协作的情形下远程利用细微的硬件设备偏差(时钟脉冲相位差)来识别网络设备。实验结果表明,这种方法能够有效地用于远程网络主机的识别。

关键词:TCP时间戳;网络设备识别;网络安全
中图分类号:TP393.4 **文献标识码**:A **文章编号**:1674-7720(2013)05-0046-03

Remote network device identification based on TCP timestamp

Xu Shuhua[1], Xu Lina[2]
(1.Department of Electronic and Information Engineering, Huazhong University of Science and Technology, Wuhan 430074, China;
2.School of Mangement, Wuhan University of of Science and Technology, Wuhan 430074, China)

Abstract: Unlike traditional software-based identify mechanisms based on operating system features or network protocol characteristics, the paper proposes a method of remote network device identification based on TCP timstamp. By using TCP timestamp theory based on RFC 1323 protocol, TCP timestamp option is sent in data packet. In the absence of measurement tools collaboration, the subtle hardware devices deviation (clock skew) from the remote network can be used to identify network equipment. The experimental results show that this method can be effectively used for identifying remote network host.

Key words: TCP timestamp; network device identification; network security

近年来,无线局域网以超乎想象的速度迅猛发展。在迅速普及的同时,相应的网络安全性问题日益凸现,开放式信道以及某些自组织组网形式导致了形形色色的安全威胁。在各类安全威胁中,非法接入设备对网络系统攻击造成的危害最大。在这类网络攻击中,MAC地址被非法盗用来窃取网络资源和数据,而目前对MAC地址盗用缺乏行之有效的办法。如果加入网络设备识别技术,即便MAC地址仍然被盗用,但是非法网络设备的特征不能匹配合法设备的特征,这将大大增强网络用户的安全性。

在网络设备安全鉴别中,侦测远程主机的操作系统不仅能够检测非法攻击,而且有利于制定和采取更为有效的反制措施。目前,研究人员已经提出了不少探测远程操作系统的方法和技术。参考文献[1]提出通过探测主机操作系统进行远程设备识别;参考文献[2]、[3]提出利用不同操作系统TCP协议中存在的差异来探测远程主机,并将不同操作系统在TCP协议中体现出来的差异视为TCP指纹特征。这种被动探测方式隐蔽性较强,具有一定的实用性。但是,这种依赖操作系统探测进行远程主机识别的方式具有很大的局限性。主要表现在两个方面:一是非法用户可以通过多种方式进行操作系统伪装;二是依赖操作系统特征识别目标网络设备数量极为有限,一旦设备增多就难以进行有效的安全识别。

为了解决上述问题,研究人员对网络设备自身的硬件设备差异进行了研究。参考文献[4]首次在网络时延测量中观测到物理设备时钟偏移现象,并提出了对时钟偏移的估计和消除方法;参考文献[1]分析了远程物理设备中存在的差异可能用作远程设备探测的两大类特征,包括操作系统差异和时钟偏差;参考文献[5]还进一

* 基金项目:中央高校基本科研业务费资助(HUST编号:2012QN082)

步对网络分组的精确时间戳进行了分析。在上述研究的基础上，本文提出了一种基于 TCP 时间戳（硬件设备时钟差异）进行远程网络设备识别的方法。与远程操作系统探测技术不同，这种技术能够在测量工具协作的情形下，利用细微的硬件设备偏差（时钟脉冲相位差）来识别远程网络设备。这种识别技术可以用来判断网络上两个可能在时间和 IP 地址上有变动的设备是否为同一物理设备，从而提高网络接入设备的安全性。

1 TCP 时间戳原理

RFC 1323 协议定义了两个新的 TCP 选项，即窗口扩大选项和时间戳（Timestamp）选项，选项格式如图 1 所示。其中，时间戳选项可以使 TCP 对报文段进行更加精确的 RTT 测量。即发送方在每个报文段中放置一个时间戳数值，接收方在确认中返回这个数值，从而允许发送方为每一个收到的 ACK 计算 RTT。时间戳是一个单调递增的值，RFC 1323 推荐在 1 ms~1 s 之间将时间戳值加 1。例如，BSD4.4 在启动时将时间戳始终设置为 0，然后每隔 500 ms 将时间戳时钟加 1。

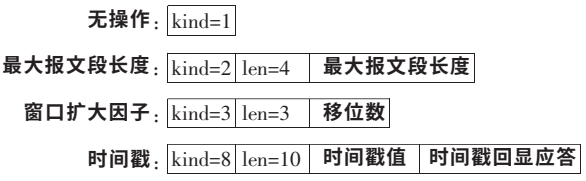


图 1 RFC 1323 TCP 选项

一个特定的网络设备可能具备多个独立的时钟脉冲，包括设备系统时间和设备自身的 TCP 堆栈时钟脉冲（时间戳选项时钟脉冲）。虽然专业管理下的设备系统时钟脉冲可以通过 NTP 协议与真实时间同步，然而对于大多数操作系统而言，它们的默认安装并不能使主机的系统时钟脉冲与真实时间保持同步或者只是偶尔能保持同步。这样，对于一个非专业管理设备，如果测量设备能够及时掌握设备系统时钟脉冲值，那么就能推断出系统时钟脉冲相位差的信息。事实上，任何网络通信设备的系统时钟脉冲都不是绝对稳定的，实际的时钟脉冲频率总是存在或大或小的相位偏差。基于上述硬件基础，可以利用 TCP 时间戳原理测量实际存在的网络设备相位差。

2 物理设备识别方法

本文用如下方法分析 TCP 时间戳信息。假定网络监测设备得到的被监测网络设备发送 TCP 数据包的网络路径为 P，为了估算网络设备的 TSopt 时钟脉冲相位差，本文使用 t_i 表示监测设备在路径 P 中观测到第 i 个数据包的时刻（以 s 为单位），P_i 表示在第 i 个数据包的 TCP 时间戳。定义如下：

$$x_i=t_i-t_1 \quad (1)$$

$$v_i=p_i-p_1 \quad (2)$$

$$w_i=v_i \quad (3)$$

$$y_i=w_i-x_i \quad (4)$$

$$O_P=\{(x_i,y_i):i\in\{1,\cdots,|P|\}\} \quad (5)$$

其中，w_i 是第 i 个数据包中可观测的偏差，是与路径 P 相对应的一系列偏差，其单位为 s；t 的数值代表真实的时间。假定被测量主机产生第 i 个数据包的时间和测量者记录第 i 个数据包的时间没有延时，那么 $y_i=\text{off}\ (x_i+t_1)$，进而 O_P 点的斜率可以近似为 CTcp 的相位差。为了从 O_P 中取得相位差，本文借用了 MOON S B 等人提出的线性规划解决方案[5]：线性规划可行解输出一条直线 $\alpha X+\beta$，是 O_P 上一系列点的上限。直线的斜率 α 是 CTcp 时钟脉冲相位差的估算值。这条直线的线性规划约束为：对于所有点 $i\in\{1,\cdots,|T|\}$，$\alpha x_i+\beta\geqslant y_i$，那么线性规划可行解是目标函数 $\frac{1}{|T|}\sum_1^{|T|}(\alpha\cdot X_i+\beta-y_i)$ 的最小值。

3 系统软件方案设计

本项目拟设计远程网络设备 TCP 时间戳捕获识别系统，对远程设备进行识别，进而判定网络接入设备的合法性。系统方案总体结构如图 2 所示。

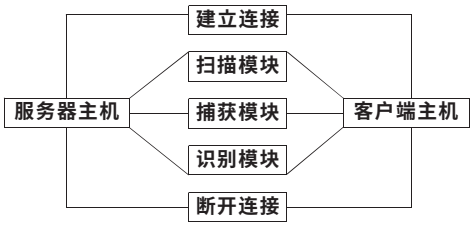


图 2 系统的总体结构图

其中，运行服务器程序的主机作为发起扫描的主机，运行扫描模块、捕获模块和控制平台，并建有设备识别模块。扫描模块直接从主机上通过网络以其他主机为对象对用户指定 IP 和端口发送各种数据包；捕获模块采集被扫描主机回送给系统的数据包，并取出其中的相应网络字段；识别模块完成数据包的解析与识别，通过回送数据包的各首部字段查找相应的设备特征，最后给出判断结果。

本项目构建的软件系统内部传递捕获数据包的各个首部字段以及发送和捕获的相关数据。根据对系统输入输出信息的分析，系统流程如图 3 所示。

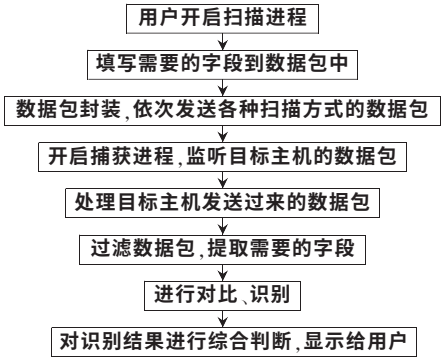


图 3 系统的工作流程

4 实验分析

对本文提出的前述基于 TCP 时间戳的远程网络设备识别技术进行实验验证，所搭建的网络实验环境如图 4 所示。实验中使用了 3 台主机，分别编为 1 号机、2 号机和 3 号机。其中，1 号主机作为服务器，其余两台主机用作待探测识别的主机。本项目在 1 号机和其余两台主机上分别运行服务器端程序和客户端程序。在两台主机进行网络通信的同时，在服务器端运行数据包解析程序，捕获数据包并提取 TCP 时间戳，然后通过线性规划分析对目标主机进行安全性识别。

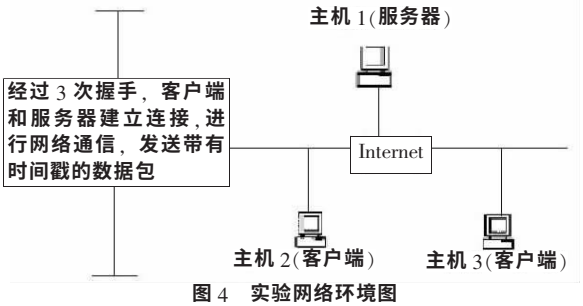
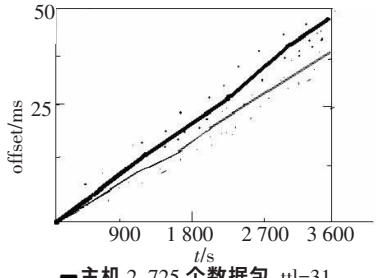


图 4 实验网络环境图

本项目进行了两组远程探测识别实验，实验过程和结果说明如下。

4.1 不同客户端主机在不同地址接入网络的识别实验

本实验中服务器主机（主机 1）IP 地址为 222.*.*.134，其他两台客户端主机（主机 2 和主机 3）IP 地址分别为 222.*.*.140 和 222.*.*.142。主机 2 在 1 小时内不间断地发送了 725 个数据包，主机 3 也同时不间断地发送了 810 个数据包。采用前文所述线性规划分析方法分析数据包提取的 TCP 时间戳信息，可以观察到主机 2 和主机 3 的可观测偏差和真实时间的关系，如图 5 所示。可以测量出主机 2 的 TSopt 时间脉冲相位差估算为 133.3 ppm（1 ppm 为百万分之一），而主机 3 的 TSopt 时间脉冲相位差估算为 108.3 ppm。

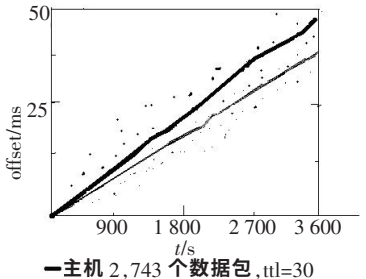


—主机 2，725 个数据包，ttl=31
–主机 3，810 个数据包，ttl=28

图 5 不同客户端主机在不同地址接入网络时 TSopt 时钟偏差

4.2 不同客户端主机在同一地址接入网络的识别实验

本实验中服务器主机 IP 地址为 222.*.*.134，其他两台客户端主机（主机 2 和主机 3）先后运行在同一 IP 地址 222.*.*.140 上。主机 2 在某时段 1 小时内不间断地发送了 743 个数据包，主机 3 随后也不间断地发送了 821 个数据包。仍然采用前文的分析方法，可以观测到主机 2 和主机 3 的可观测偏差和真实时间关系如图 6 所示。可以测量到主机 2 的 TSopt 时间脉冲相位差估算为 133.1 ppm，而主机 3 的 TSopt 时间脉冲相位差估算为 108.5 ppm。



—主机 2，743 个数据包，ttl=30
–主机 3，821 个数据包，ttl=29

图 6 不同客户端主机在同一地址接入网络时 TSopt 时钟偏差

从上述两组实验结果可以看到，不论是从不同的 IP 地址发出数据包还是从同一 IP 地址发出数据包，待探测客户端主机 2 和主机 3 的时钟脉冲相位差基本保持不变（差别没有超过 1 ppm），而且这两台主机的时钟脉冲相位差存在较大的区别（约为 25 ppm），因而可以对这两台远程网络设备进行有效的辨识，从而达到了项目预期目标。

本文基于 TCP 时间戳原理，利用现代网络设备微小的时钟脉冲相位偏差，成功地对远程设备进行了安全性辨识，并为网络体系的安全性增强提供了一个新的有效检测方法。这种技术将来可以有效应用到计算机安全取证、追踪从不同通路端连接入互联网的网络设备等领域。

基于 TCP 时间戳的远程主机识别是一种较新的研究方法和领域，还需要进一步对提高设备特征的提取精度和更多的实际目标进行研究；同时，如果结合尚未成熟的被动探测机制，并借助现代模式识别技术，本文的研究方法将在前景广阔的网络通信安全领域有着极大的应用价值。

参考文献

[1] KOHNO T, BROIDO A, CLAFFY K C. Remote physics device fingerprinting [J]. IEEE Transactions on Dependable and Secure Computing, 2005, 2(2): 93–108.

[2] 沙超.一种基于 TCP/IP 协议栈的操作系统识别技术[J]. 计算机技术和发展，2006，16(10)：125–127.

[3] 陈刚.基于 TCP 指纹的远程操作系统探测技术[J].信息系统与网络，2006，36(9)：7–11.

[4] MOON S B, SKELLY P, TOWSLEY D. Estimation and removal of clock skew from network delay measurements[C]. IEEE Proceedings of INFOCOM′99, Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies，1999(1)：227–234.

[5] MICHEEL J, DONNELLY S, GRAHAM I. Precision timestamping of network packets[C]. Proceedings of the 1st ACM SIGCOMM Workshop on Internet Measurement，2001：273–277.

（收稿日期：2012–10–07）

作者简介：

徐书华，男，1976 年生，博士，讲师，主要研究方向：无线通信网络安全、光通信系统等。