doi :10.3969/j.issn.1671-1122.2009.05.018

一种基于 Winsock2 SPI 架构的网络监控程序自我保护方案设计与实现

张亚航，文伟平

（北京大学软件与微电子学院信息安全系，北京 102600）

摘　要：如何保证涉密网络信息保密的问题一直受到政府、军队、航天等涉及国家秘密的行业所关注。在软件层次对计算机用户进行监控是一个较好的解决方案。这篇文章提出并实现了基于Winsock2 SPI框架的网络监控自我保护方案。监控程序本身的自我保护技术是保证网络监控抵抗非法用户攻击的关键。基于这种方案的网络监控程序能够将监控线程同系统关键进程进行绑定，既实现了程序的进程隐藏，又能够防止高级非法用户强制关闭监控程序，并且能够同Rootkit技术等其他相结合共同提高程序自我保护性能。

关键词：涉密网络；Winsock2 SPI；自我保护

中图分类号：TP393.08　　文献标识码：A

Design and Implementation of Self-Protection Scheme for Network Monitor Program Based on Winsock2 SPI Framework

ZHANG Ya-hang, WEN Wei-ping

(Department of Information Security, SSM, Peking University, Beijing 102600, *China)*

Abstract: The problem that how to protect the information without divulging in a secret-related network in terms of departments of government, army and energy is always be regarded by people. It is a good way to solve this problem by monitoring the computer user in the secret-related network using software. This paper presents and implements a self-protection scheme for network monitor program based on Winsock2 SPI Framework. The self-protection technology of the network monitor is the key point that protects the network monitor from being attacked by illegal users. The network monitor program based on this scheme can bind itself with the critical system process to hide the monitor process itself and protected itself being shut down or delete by senior attacker, besides, this technology can work with other technologies like rootkit to improve the performance of the monitor program.

Key words: secret-related network; Winsock2 SPI; self-protection

0 引言

随着信息化建设的加快，企业、政府网络的信息传递和信息共享日益频繁，信息安全已经受到越来越多的重视。特别是在政府、军队、能源等涉及国家秘密的行业，信息的安全保密显得尤为重要。目前在涉及国家秘密的行业系统中进行的涉密网建设与保密资格审查认证工作，把重视信息安全的工作推向一个崭新阶段。因此，涉密网安全保密方案是一个非常重要的研究课题[1]。

对于涉密网络保密解决方案，一般分为软硬件两种解决途径。在硬件层次，一般基于物理安全网闸从物理上将涉密网络直接隔离[2][3]，这种方案优点在于只要不出现物理接触，外网攻击者无法直接通过程序攻入内网，缺点在于这种方案灵活性较差，而且难以防范内部人员主动向外网泄露信息。在软件层次，一般采用监控软件的方式随软件系统启动而启动，在系统运行期间不断监控当前用户的网络状态[4][5]。这种方式优点在于部署灵活，而且能够防止内部合法用户主动向外网泄密的情况，缺点在于容易被高级攻击者通过各种非法手段强行关闭或令之失效。

因此，软件层次的网络监控程序最为核心的技术在于监控程序的自我保护功能是否足够强大以对抗高级攻击者。本文通过对 Winsock2 SPI 技术的研究，提出基于 Winsock2 SPI 框架的网络监控自我保护方案。基于这种方案的网络监控程序能够将监控线程同系统关键进程进行绑定，既实现了程序的进程隐藏，又能够防止高级非法用户强制关闭监控程序，并且能够同 Rootkit 技术等其他相结合共同提高程序自我保护性能。并且成功将这种思想在国家保密局网络监控程序上得到应用，在实践中证实了该程序能够成功的进行自我隐藏和保护，抵御各种手段的攻击和删除手段。

1 Winsock 2 SPI

在 Win 32 操作系统中，系统提供了一套为上层应用程序调用的标准网络接口 Winsock。上层应用程序不用关心 Winsock 实现细节，为上层应用程序提供了透明的服务[6][7][8]。

Winsock 2引入的一个新功能就是打破服务提供者的透明，让开发者可以编写自己的服务提供者接口程序，即 SPI 程序。SPI 以动态链接库（DLL）的形式存在，它工作在应用层，为上层 API 调用提供接口函数。

当自身编写 SPI 程序安装到系统之后，所有的 Winsock 请求都会先发送到这个程序并由它完成网络调用。Winsock 2

提供的服务提供者结构如图1所示。

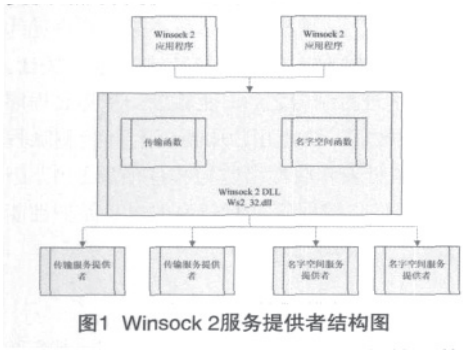

图1 Winsock 2服务提供者结构图

Winsock 2 SPI分为完成网络传输的传输服务提供者(Transport Service Provider)，还有提供友好名称服务的名字空间服务提供者(Name Space Service Provider)。传输服务提供者能够提供建立通信、传输数据、流量控制和错误控制等服务。名字空间服务提供者吧一个网络协议的地址属性和一个或多个用户友好名称关联起来。本程序主要关注传输服务提供者。

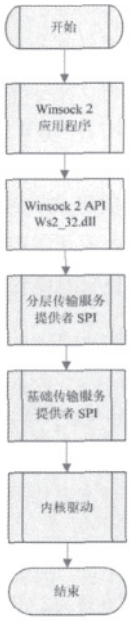

图2 Socket应用程序调用分层SPI提供者顺序图

传输服务提供者又分为基础服务提供者和分层服务提供者(Layered Service Provider)。基础服务提供者和分层服务提供者都开放相同的SPI接口，所不哦他能够的是基础服务提供者位于提供者的底层，因此安装的时候基础服务提供者必须安装在服务提供者加载顺序链的最低端，而分层服务提供者则根据需求分布在顺序链的中间。它们的调用关系如图2所示。

2 Rootkit

Rootkit技术已经并不是一个新鲜的事物，而是已经存在了很久，但直到最近几年才引起大量的深入使用和重视，它主要作用于windows、unix、linux等操作系统中。Root在英语中是根，扎根的意思，kit是包的意思。Rootkit可以理解为一个利用很多技术来潜伏在系统中的一个后门，并且包含了一个功能比较多的程序包，例如有、清除日志，添加用户，获取shell，添加删除启动服务等功能。当然它的设计者也要用一些技术来隐藏自己，确保不被发现。隐藏包括隐藏进程，隐藏文件，端口，或句柄，注册表的项，键值等等。总之，写Rootkit的人是狡尽乳汁利用很多办法不被发现[9]。

在本系统中，我们在程序自我保护的模块，主要采用了内核级Rootkit技术。因此这里主要介绍内核级Rootkit技术的实现方式。由于系统本身架构的隐蔽性，实际上系统本身并没有独立的进程。如果用户恶意删除系统安装文件，则系统虽然丧失了监控功能，却因为破坏了系统SPI，仍然能够阻碍系统上网。为了防止用户恶意强行删除软件，我们采用Rootkit进行文件和注册表隐藏。

3 系统设计

3.1 体系结构设计

本系统最核心的功能在于程序的自我保护和网络监控模块上面，这两大功能决定了软件的基本实现理论和架构。为了实现监控进程的隐藏和保护，本系统借用进程注入的思想，将核心监控线程同系统关键进程进行绑定；而为了实现系统关键文件保护，可以考虑Rookit内核级隐藏技术。对于邮件通信，程序可以采用Socket完成SMTP协议，从而将非法用户的信息进行收集，并发送到管理员指定邮箱。

本程序主要分为安装/卸载程序、管理员控制、网络监控主题模块三个大模块，各自分别又分为具体的小模块，系统总体模块结构图如图3所示。

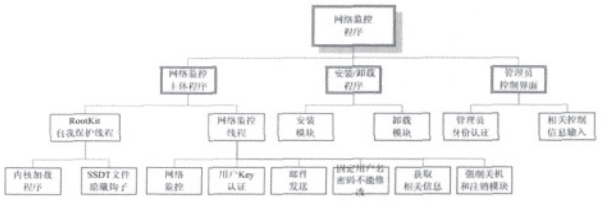

图3 涉密网络监控程序总体结构图

3.2 程序处理流程设计

为了实现网络监控程序的自我保护功能，系统的基本处理流程是：首先通过加载函数，将处理TCP、UDP和RAW等协议的分层服务提供者注册成为系统默认SPI。之后，当系统启动的时候，部分需要使用使用网络TCP、UDP和RAW协议的关键系统进程(如svchost.exe<network>)在初始化网络配置的时候，自动加载网络监控程序动态链接库。

动态链接库中设置了计数器m_iDllCount计算当前加载动态链接库的进程数，当第一个主动加载网络监控程序动态链接库的时候，将进入该动态链接库的Dllmain函数以初始化动态链接库。如果当前进程为第一个关键进程，则开始启动监控线程，并初始化Rootkit启动保护线程。如此一来，将监控线程同系统关键进程进行绑定，实现了程序的自我隐藏和自我保护。同时通过Rootkit，将对应的注册表删除，防止了高级攻

图4 网络监控程序总体流程图

击者通过修改注册表的方式将网络监控程序所属SPI卸载。其总体流程图如图4所示。

4 试验测试结果

该网络监控程序设计方案在国家保密局涉密网络监控系统中得到实施。在实际中，针对该程序各个性能的测试结果如下。

4.1 网络监控系统自启动

操作系统启动之后，不做任何操作，插入外网网线，使得系统能够连接外网，将当前用户信息提取发送到管理员邮箱之后，系统自动强行关机。证明成功实现了网络监控程序系统自启动功能。

4.2 进程自我隐藏

系统启动之后，通过进程查看等各种方法，无法观察到监控进程的存在，同时真正用户体验也无法感受到该监控程序的存在，证明成功实现了自我隐藏功能。

4.3 Rootkit自我保护

系统启动之后，原先位于程序安装目录的关键动态链接库消失不见，系统注册表也无法查询到本系统的网络监控SPI，证明成功实现了Rootkit自我保护功能。

4.4 程序防止强制关闭

根据调试，发现程序被加载到svchost.exe<network>进程中，强行将该进程删除，系统提示核心进程遭到破坏，系统启动强行关机程序。证明成功实现了防止攻击者强行关闭功能。

5 结论

通过上面的分析和测试，我们可以看到，将基于Winsock2 SPI框架的网络监控程序能够成功将自身监控线程同系统关键进程进行绑定，这种程序能够在不被用户察觉的基础上，实现进程的自我隐藏，并且防止攻击者强行关闭。在同Rootkit等其他技术进行结合之后，能够进一步提高程序的自我保护和自我隐藏性能，防止用户从硬盘上直接删除程序关键文件或者通过注册表卸载网络监控程序所属SPI。因此，基于SPI技术的网络监控程序具有较高的自我保护性能和自我隐藏性能。（责编 张岩）

参考文献：
[1] 何波，董世都，涂飞，程勇军. 涉密网安全保密整体解决方案[J]. 微计算机信息，2006年，第22卷，第9-3期:116-118.
[2] 蒲天银. 安全隔离网闸技术发展探讨[J]. 计算机时代，2006年，第6期: 18-19.
[3] 董惠勤，陆魁军. 跨安全网闸的内外网数据库同步的实现. 科技通报，2007年，23卷(2期): 266-270.
[4] 吴晓昶，李名世. 办公业务网信息监控系统设计[J]. 厦门大学学报，2004年，增刊: 332-335.
[5] 李焕洲，张健，陈麟. 涉密网资源监控体系的研究与实现[J]. 计算机应用，2006年，26卷(5期): 1090-1092.
[6] 甘利杰，丁明勇，杨永斌. 基于Winsock SPI技术的包过滤研究[J]. 计算机科学，2007年，08期: 112-114.
[7] 田磊，李祥和，辛志东，潘军. 基于Winsock2 SPI技术的木马植入新方案[J]. 计算机工程，2006，7期: 166-168.
[8] Jones A. Network Programming for Microsoft Windows (SecondEdition) [M]. Microsoft Press, 2002.
[9] Greg Hoglund, James Butler, Rootkit-subverting the windows kernel, Addison Wesley Professional, July 22, 2005.

作者简介：张亚航(1985-)，男，硕士研究生，主要研究方向：网络安全；文伟平(1976-)，男，副教授，主要研究方向：网络攻击与防范、恶意代码研究、信息系统逆向工程和可信计算技术等。

（上接37页）

当前进程从链表中删除以后的结果。以上就是使用DKOM方法实现进程隐藏的基本思路，即平常所说的“摘链法”。

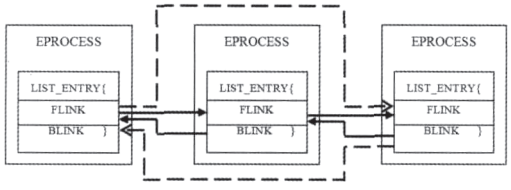

图2 DKOM方法删除当前进程示意图

3 结论

从上面可以看出，木马实现常用的技术很多，木马用于进程隐藏的技术手段也是多种多样的：从应用层到操作系统内核，由表及里，越来越深入。对于各种进程隐藏技术，我们可以在研究和分析其基本原理与方法的基础上，一方面，考虑把它们应用到我们实际的系统管理工作中去，如某些安全控制程序；另一方面，可以为开发防病毒和木马软件打下良好的基础，从而使我们更好地检测和防御木马，确保我们系统的安全。（责编 张岩）

作者简介：卢立蕾(1971－)，女，高级讲师，硕士研究生，主要研究方向：系统与网络安全；文伟平(1976－)，男，副教授，主要研究方向：网络攻击与防范、恶意代码研究、信息系统逆向工程和可信计算技术等。

参考文献：
[1] 孙淑华，马恒太，张楠，卿斯汉. 内核级木马隐藏技术研究与实践[J]. 微电子学与计算机，2004，21(3): 76-80 .
[2] 许国顺. 木马攻击与防范技术研究[D]. 四川大学：工程硕士学位论文，2006，03 .
[3] 贾建忠，姜锐. 新型木马技术剖析及发展预测[J]. 网络安全技术与应用，2007，5: 43-45.
[4] 刘牧星. 木马攻击与隐蔽技术研究[D]. 天津大学：硕士学位论文，2006.
[5] 文伟平. 恶意代码机理与防范技术研究[D]. 中国科学院研究生院(软件研究所)：博士论文，2005.
[6] 康治平，向宏. 特洛伊木马隐藏技术研究与实践[J]. 计算机工程与应用，2006，09: 103-105，119.
[7] 彭迎春，谭汉松. 基于DLL 的特洛伊木马隐藏技术研究[J]. 信息技术，2005年，第12期: 41-43.
[8] 于继江. 动态嵌入式DLL木马实现方法[J]. 电脑知识与技术，2005年，21期: 47-49.
[9] Greg Hoglund，James Butler.Rootkits:Subverting the Windows Kernel. July 22，2005.
[10] 杨彦，黄皓.Windows Rootkit隐藏技术研究.计算机工程，2008，6，Vol.34，No.12:152-156.