安全体系结构 Project 1

2053182 王润霖

实验内容：

分析一个典型的 Windows 10-x86 主机安全体系结构，典型的 Windows 10-x86 笔记本主机：Windows 10+sql+office。

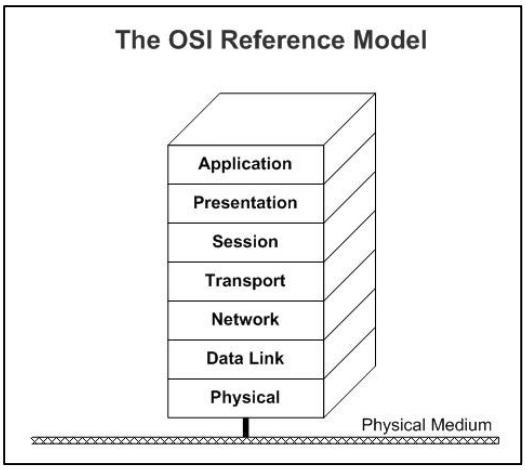
（1）用 OSI 7 层和 tcp/ip4 层模型分解或划分其系统组件或软硬件结构。

（2）简要概括其实现 cia 的安全策略和安全机制，一一对应到基本组件。

一、用 OSI 7 层和 tcp/ip4 层模型分解或划分其系统组件或软硬件结构

1.1 Windows10[2]

Microsoft Windows 网络驱动程序实现 OSI 模型底部四层。



1.1.1 物理层

物理层是 OSI 模型的最低层。 此层通过物理介质管理非结构化原始位流的接收和传输。 它描述了物理介质的电气/光学、机械和功能接口。 物理层承载所有较高层的信号。

在 Windows 中，物理层由网络接口卡(NIC) 、其涂层和 NIC 附加到的介质实现。

1.1.2 数据链接层

数据链接层在物理地址之间发送帧，负责物理层中发生的错误检测和恢复。

数据链接层由电气和电子工程师研究所 (IEEE) 进一步划分为两个子层：媒体访问控制 (MAC) 和逻辑链接控制 (LLC) 。可以由例如 k57xp32.sys 等驱动完成，不同的网卡此驱动可能不同，它相当于一个 Ndis Miniport 驱动，和 Ndis 协议驱动一样，都是运行在 Ndis 库营造的一个运行环境中，主要完成例如以内网数据包的构成，操作网卡发送数据包，以及注册中断接收数据包以及其它信息的工作。

MAC

MAC 子层管理对物理层的访问、检查帧错误和管理接收帧的地址识别。

在 Windows 网络体系结构中，MAC 子层在 NIC 中实现。 NIC 由称为 微型端口驱动程序的软件设备驱动程序控制。 Windows 支持多种微型端口驱动程序变体，包括 WDM 微型端口驱动程序、微型端口呼叫管理器 (MC) ，以及微型端口中间驱动程序。

LLC

LLC 子层提供从一个节点到另一个节点的无错误数据帧传输。 LLC 子层建立和终止逻辑链接、控制帧流、序列帧、确认帧以及重新传输未确认的帧。 LLC 子层使用帧确认和重

新传输，通过指向上述层的链接提供几乎无错误传输。

在 Windows 中，LLC 子层由称为协议驱动程序的软件驱动程序实现。

1.1.3 网络层

网络层控制子网的操作。 此层根据以下情况确定数据应采用的物理路径：

网络状况、服务的优先级、其他因素，例如路由、流量控制、帧碎片和重新汇编、逻辑到物理地址映射以及使用情况会计。

网络层由协议驱动程序实现。

具体而言，tcp/ip 协议的传输层和网络层实现是在 tcpip.sys 里完成的，它主要完成两部分工作，传输层实现和网络层实现，在传输层部分完成 TCP, UDP, RawIp 的绑定，连接等功能，主要服务于 afd.sys 发下来的 TDI 命令，然后进入到网络层，来完成路由以及 IP 包的构成，网络层部分相当于一个 Ndis 协议驱动，一般来讲它会绑定所有的网卡来监听和发送 IP 包。

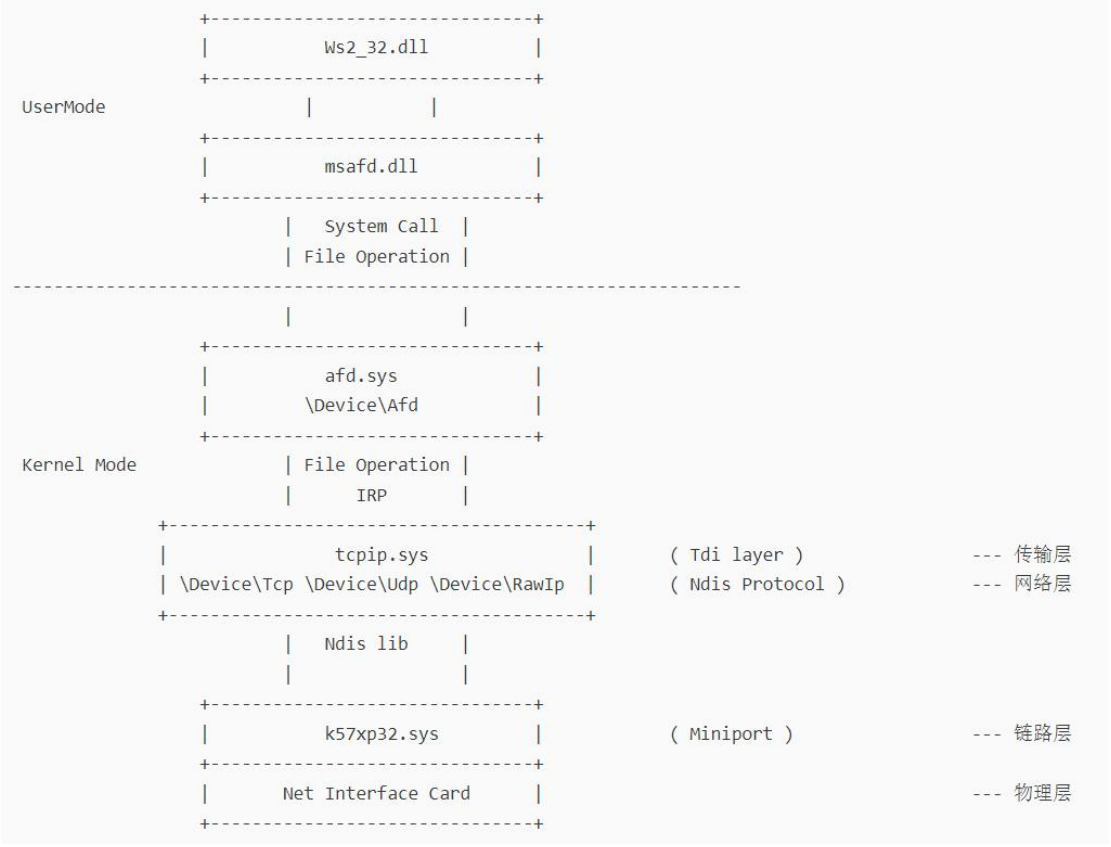
1.1.4 传输层

传输层可确保消息按顺序免费传递，且不会丢失或重复。 此层可缓解高层协议，使其担心与对等方进行数据传输。

协议堆栈中需要最小传输层，其中包括提供虚拟线路功能的可靠网络或 LLC 子层。 例如，由于适用于 Windows 的 NetBEUI 传输驱动程序是符合 OSI 的 LLC 子层，因此其传输层函数最少。 如果协议堆栈不包含 LLC 子层，并且网络层不可靠且/或支持数据报 (与 TCP/IP 层或 NWLink 的 IPX 层) 一样，传输层应包括帧序列化和确认，以及重新传输未确认帧。

在 Windows 网络体系结构中，传输层由协议驱动程序实现，有时称为传输驱动程序。

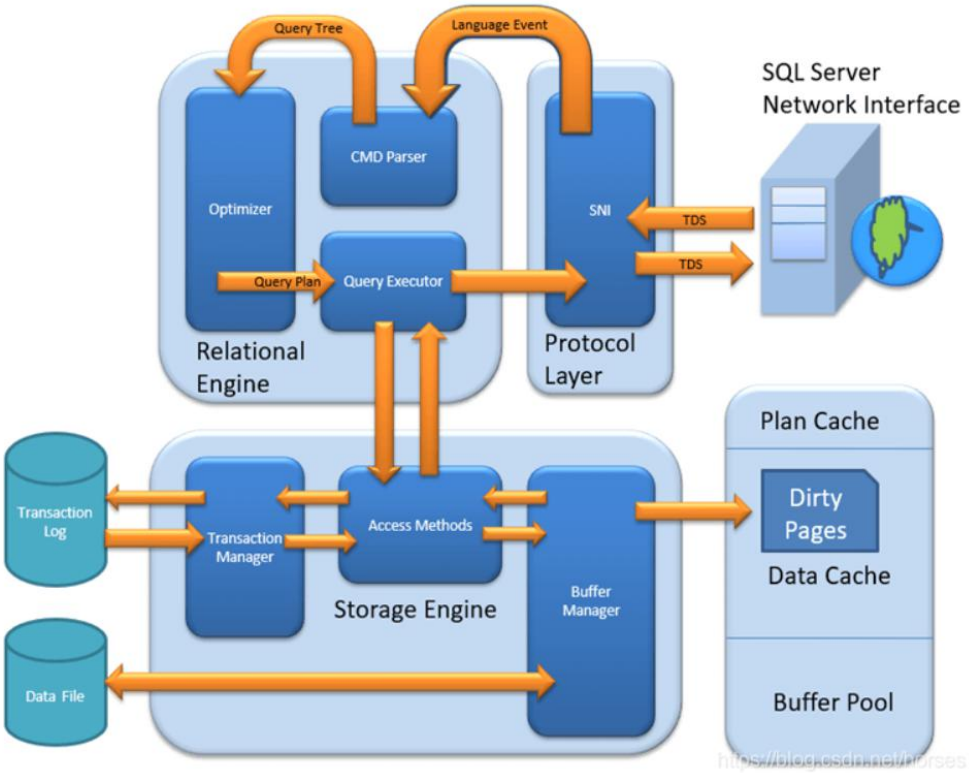
对应到具体实现的系统组件，如下图所示：



1.2 Sql Server[3]

Microsoft SQL Server 服务由一个实例（Instance）和多个数据库（Databases）组成，实例包含了后台线程和占用的内存，默认的系统数据库包括 master、model、msdb、Resource 以及 tempdb。

Microsoft SQL Server 的整体系统结构如下：



主要包含以下三个组件：

（1）协议层（Protocol Layer），主要负责客户端的连接请求和数据通信。

（2）关系引擎（Relational Engine），主要负责 SQL 语句的解析、优化和执行。

（3）存储引擎（Storage Engine），主要负责数据和日志的存储和访问、内存和缓存管理、事务和锁管理。

客户端应用首先需要通过 SNI 网络接口（SQL Server Network Interface）与服务器建立连接，Microsoft SQL Server 提供了以下三种协议方式：TCP/IP 协议；共享内存（Shared Memory）协议；命名管道（Named Pipes）协议。

二、简要概括其实现 cia（保密性、可用性、完整性）的安全策略和安全机制，一一对应到基本组件

1.Windows 10 安全策略和安全机制

1.1 安全策略

1.1.1 加密策略

（1）BitLocker 加密：BitLocker 是 Windows 10 中的一种全磁盘加密技术，可以对整个硬盘进行加密，以保护计算机中的所有数据。BitLocker 使用高级加密标准（AES）算法进行加密，可以有效地防止数据泄露和信息窃取。

（2）EFS 加密：EFS 是 Windows 10 中的一种文件级别加密技术，可以对单个文件或文件夹进行加密。EFS 使用公共密钥加密技术（PKI）来加密和解密文件，可以保护计算机中的敏感数据。

（3）Credential Guard：Credential Guard 是 Windows 10 中的一种硬件虚拟化技术，可

以将用户凭据存储在一个安全的硬件隔离区域中，以防止攻击者窃取用户凭据。

（4）Device Guard：Device Guard 是 Windows 10 中的一种硬件保护技术，可以防止未经授权的代码运行在 Windows 10 系统上。Device Guard 使用硬件虚拟化技术和代码签名来保护系统安全。

（5）Windows Hello：Windows Hello 是 Windows 10 中的一种生物识别技术，可以使用面部识别、指纹识别或虹膜扫描等方式来验证用户身份，以防止未经授权的访问。

（6）防火墙：Windows 10 中的防火墙可以帮助阻止未经授权的网络访问，以保护计算机中的数据安全。

1.1.2 口令防护策略

（1）强制口令复杂度：强制用户创建复杂的口令，包括长度、大小写字母、数字和特殊字符等。

（2）口令历史记录：限制用户不能使用之前已经使用过的口令。

（3）口令锁定：当用户多次输入错误的口令时，系统会自动锁定用户账户一段时间，以防止恶意攻击。

（4）口令过期：强制用户定期更换口令，以增加安全性。

（5）口令复杂度检查：系统会检查用户输入的口令是否符合要求，并给出提示。

（6）双因素认证：在口令认证的基础上，增加另一种认证方式，例如指纹或者智能卡等。

1.1.3 反病毒策略

（1）Windows Defender 防病毒软件：Windows 10 系统自带了 Windows Defender 防病毒软件，可以对系统进行实时监测和防护。

（2）自动更新：Windows 10 系统会自动更新病毒库和防病毒软件，以保证最新的病毒和威胁可以得到及时的防护。

（3）防火墙：Windows 10 系统自带了防火墙，可以阻止未经授权的网络访问和攻击。

（4）安全浏览器：Microsoft Edge 浏览器内置了安全浏览器功能，可以防止用户访问被感染的站点和下载恶意软件。

（5）应用程序控制：Windows 10 系统的应用程序控制功能可以帮助用户限制应用程序的运行和访问权限，以防止恶意应用程序的攻击。

1.1.4 数据库策略

数据库访问控制：Windows 10 系统提供了多种访问控制技术，如用户账户控制、应用程序控制等，可以帮助管理员限制用户对数据库的访问和操作权限，以保护数据库的安全性。

数据库备份和恢复：Windows 10 系统提供了多种备份和恢复技术，如系统还原、文件历史记录等，可以帮助管理员及时备份数据库，并在需要时快速恢复数据，以避免数据丢失和损坏。

1.1.5 安全审计策略

基本组件包括：“本地组策略编辑器”、“组策略管理器”、“事件查看器”、“PowerShell”、“Sysmon”、“SIEM 系统”和日志聚合工具等。

本地安全策略或组策略对象设置：可以通过“本地组策略编辑器”或“组策略管理器”设置安全审计策略。审计日志设置：可以通过“事件查看器”设置审计日志的大小、保留时间和清除方式。审计事件过滤：可以通过“事件查看器”设置审计事件的筛选规则。审计事件分析：可以使用“事件查看器”、“PowerShell”、“Sysmon”、第三方工具等分析审计日志。审计事件报告：可以通过安全信息和事件管理（SIEM）系统、日志聚合工具等生成审计事件报告。

1.1.6 Internet 连接策略

（1）防火墙策略：Windows 10 系统内置了防火墙功能，可以通过控制面板中的 Windows

Defender 防火墙选项来进行配置。可以设置阻止所有的入站连接、允许所有的入站连接、允许指定的入站连接等。

（2）代理服务器策略：如果需要通过代理服务器连接 Internet，可以在 Internet 选项中进行配置。可以设置自动检测代理服务器、手动配置代理服务器、使用脚本等。

（3）IE 安全设置：可以通过 Internet 选项中的安全选项卡来设置 Internet Explorer 的安全级别，包括 Internet、本地 Intranet、受信任的站点和受限制的站点四个区域。可以设置允许或阻止 ActiveX 控件、脚本、Java Applet 等。

（4）Windows Update 策略：可以通过 Windows Update 设置来自动更新 Windows 系统，包括安全更新、功能更新等。

（5）Microsoft Edge 浏览器策略：可以通过 Microsoft Edge 浏览器中的设置来配置其 Internet 连接策略，包括 Cookie、弹出窗口、JavaScript、Flash 等。

1.1.7 VPN 安全策略

VPN 协议选择：Windows 10 系统支持多种 VPN 协议，包括 PPTP、L2TP/IPSec、SSTP 和 IKEv2 等。在选择 VPN 协议时，需要根据实际情况和安全要求进行选择。

连接认证方式：Windows 10 系统支持多种 VPN 连接认证方式，包括用户名/密码、数字证书等。为了提高安全性，建议使用数字证书等强认证方式进行连接认证。

VPN 日志记录：Windows 10 系统可以开启 VPN 日志记录功能，记录 VPN 连接的详细信息，例如连接时间、连接 IP 地址、认证方式等。可以通过 VPN 日志记录检测异常连接行为，提高 VPN 连接的安全性。

VPN 加密策略：Windows 10 系统支持多种 VPN 加密策略，包括 AES、3DES、DES 等。为了保证 VPN 连接的安全性，建议使用强加密算法进行数据加密。

1.2 安全机制[1]

1.2.1 访问控制

Windows 操作系统与 Linux 不同，不支持强制访问控制，而是**采用自主访问控制**，开且没有可支持不同访问控制模型的通用框架。

Windows 访问控制模型有两个主要的组成部分，访问令牌和安全描述符，分别属于被访问主体和被访问主体。当 Windows 账户登录时，系统仍自身数据库中查询账户信息，用信息生成令牌，并且将令牌的副本赋给在账户环境里启动的进程。当进程在对对象进行访问时，系统会通过进程的令牌来进行访问检查。

1.2.2 数据完整性

在 CW 模型中，有以下性质：

（1）系统需要一个 IVP 来确认任何 CDI 的完整性；

（2）CDI 只能由转换过程（TP）来进行更改，且所有 TP 必须维护 CDI 的完整性；

（3）主体只能对特定的 CDI 执行与其关联的特定操作；

（4）访问规则必须满足责任分离要求；

（5）能够对 UDI 运用的 TP 将其转换为 CDI；

（6）所有执行的 TP 必须留下只写的日志;

（7）只有特殊的主体被系统允许更改相关于验证的列表。

相应的在 Windows 中，分别有以下实现：

（1）LSA 负责检查主体访问令牌的安全信息

（2）除管理员等少量用户可以直接更改任何客体的属性之外，其余用户不具有此能力；

（3）主体带有的访问令牌包含了其被允许的操作；

（4）只有管理员可以访问任何客体；

（5）用户可将无 ACL 的客体转为有 ACL；

（6）只写日志存在于 WindowsNT;

（7）只有管理员能够查看和执行需要高安全等级的操作。

从上面一段的介绍中可以看出，WindowsNT 满足 CW 模型，也就是 CW 模型的安全机制可以由 Windows 实现。

Windows 中每个安全对象具有一定的完整性等级（IL），并且由一个 SID 来标记，默认值为中等。由低进程产生的对象，其完整性等级为低 L。当一个进程试图访问一个对象时，"SeAccessCheck”接口将检查该进程的完整性等级，并判断进程是否符合访问控制列表。当访问控制列表允许访问，但是主体的完整性等级低于客体，访问也不会被执行。

1.2.3 用户界面特权隔离

完整性等级还被用于 Windows 消息子系统，用来实现用户界面特权隔离(UIPI)。UIPI 的主要功能是防止低完整性等级处理窗口向高完整性等级窗口发送消息。在 Vista 之前的 Windows 操作系统，许多程序请求下管理员权限运行，但是实际上并没有必要。在 Vista 中增加了对这些请求的控制，但是为了兼容 Vista 之前编写的 32 位并且没有运行在管理员权限下的程序，在 Vista 之后的 Windows 版本新引入了文件虚拟化与注册表虚拟化机制。在用户使用标准账户时，若标准账户下的程序试图对系统范围的文件或注册表进行修改，系统会将这个操作映射到用户范围的虚拟位置。

1.2.4 用户账户控制

用户账户控制（UAC）是在 Vista 中为了提高安全性引入的功能,通知用户是否允许应用程序使用驱动器和系统文件以防止恶意软件损害系统。但是此功能在 Vista 中只有开启和关闭两种选项,这导致频繁的弹窗通知。Windows7 上则加入了两种 UAC 级别,这两种级别的区别在于其中一个在弹窗时会进入安全桌面,这个安全桌面属于 SYSTEM 账户，原用户账户下的程序无法知道 UAC 弹窗的情况，也无法绕过 UAC 提示框;而另一个弹窗则没有进入安全桌面，依然使用原有账户的桌面环境，相对前一级别来说安全性有所降低。

1.2.5 服务隔离

在以往的 Windows 版本中，服务与用户进程都运行在同一个会话下。Vista 后的版本中服务运行在“隔离会话 0”中。这意味着正常服务不会显示事件或者任何弹出对话框与用户的互动,它会一直静默而用户将无法注意到它。如果有个进程尝试弹出通知框给用户以获取用户输入，它会一直待命，因为用户无法看到对话框。用户所登录的交互会话实质上是一个终端的服务器。微软认可的从在隔离会话中运行的服务发送消息方法是使用 WTSSendMessage，它是 Windows 终端服务 API 的一部分。用服务隔离的方式可以提高服务的安全性。

1.2.6 内核保护

Windows 保护机制主要由 DEP(数据执行保护)、GS (一种编译选项)、ASLR(地址随机化)及 SafeSEH(安全结构化异常处理)等安全技术组成。这些安全技术通过从不同方面给攻击者制造障碍，增加攻击者实施缓冲区溢出攻击的难度，进而提升系统内存的安全性。其中，DEP 技术能够在内存上(如栈和堆)执行额外检查以阻止恶意代码的运行，GS 栈保护技术对栈中内容进行检查保护程序的返回地址，ASLR 技术通过对栈和堆等线性区布局的随机化加大攻击者预测目的地址的难度,防止攻击者定位 shellcode 地址和系统调用地址，SafeSEH 技术通过 SEH 句柄验证及链验证来保护 SEH 节点。这几种安全技术既相互独立又互为补充，共同组成了 Windows 抵御缓冲区溢出攻击的完整的安全机制。

参考文献：

[1]伍唤宇,李亚茹,龙瀚林.Windows 系统安全机制与安全技术分析[J].网络安全技术与应用,2019,No.225(09):11-13.

[2]Windows 网络体系结构和 OSI 模型.https://learn.microsoft.com/zh-CN/windows-hardware/drivers/network/windows-network-architecture-and-the-osi-model
[3]Microsoft SQL Server 数据库体系结构图解.https://blog.csdn.net/horses/article/details/109462399