第五章应用与数据安全

1浏览器安全

1.1服务器端

服务器端是指网络中能对其他计算机和终端提供某些服务的计算机系统，比如新浪网站服务器等。

1.2客户端

客户端与服务器端相对应，是指为客户提供本地服务的程序，一般安装在普通的客户机上，需要与服务器端互相配合运行，如安装在移动智能终端上的地图导航程序。

1.3C/S结构

客户端/服务器结构( Client/ Server,简称为C/S结构)是一种软件系统的体系结构。

此结构中客户端程序和服务器端程序通常分布于两台计算机上,客户端程序的任务是将用户的要求提交给服务器端程序,再将服务器端程序返回的结果以特定的形式显示给用户。

服务器端程序的任务是接收客户端程序提出的服务请求,并进行相应的处理,再将结果返回给客户端程序。

1.4B/S结构

浏览器/服务器结构( Browser/ Server,简称为B/S结构)中终端用户不需要安装专门的软件,只需要安装浏览器即可。

这种结构将系统功能的核心部分集中到服务器上。

以新浪网网站为例,用户所使用的浏览器即为客户端程序,在浏览器中输入新浪的网址,用户就向新浪的网站服务器发出访问请求,新浪的服务器接受客户端访问请求并进行处理,将结果返回给浏览器,由浏览器显示,提供给用户查看。

随着因特网和移动互联网的快速发展,B/S模式得以快速发展,针对浏览器的安全威胁也越来越多,因此保护浏览器的安全就显得非常重要

1.5浏览器

浏览器是可以显示网页文件并提供用户与服务器交互功能的一种软件。

个人计算机上常见的网页浏览器有 Internet ExplorerFirefox、 Chrome、360安

全浏览器等

下面介绍一些常用浏览器的安全措施

1.6浏览器安全措施

删除和管理Cookies

Cookie是指网站放置在个人计算机上的小文件,用于存储用户信息和用户偏好的资料。 Cookie可以记录用户访问某个网站的账户和口令,从而避免每次访问网站时都需要使用输入账户和口令登录。

Cookie给用户访问网站带来便利的同时,也存在一些安全隐患。因为Cookie中保存的信息中常含有一些个人隐私信息,如果攻击者获取这些Cookie信息,就会危及个人隐私安全。

所以在公用计算机上使用浏览器后需删除 Cookie信息

删除浏览器历史记录

浏览历史记录是在用户浏览网页时,由浏览器记住并存储在计算机中的信息。

这些信息包括输入表单的信息、口令和访问的网站等,方便用户再次使用浏览器访问网站

如果用户使用公用计算机上网,而且不想让浏览器记住用户的浏览数据,用户可以有选择地删除浏览器历史记录。

禁用ActiveX控件

Activex控件是一些嵌入在网页中的小程序,网站可以使用这类小程序提供视频和游戏等内容。

浏览网站服务器时,用户还可以使用这些小程序与工具栏和股票行情等内容进行交互。

但是, Activex控件会导致一些安全隐患,攻击者可以使用 Activex控件向用户提供不需要的服务。

某些情况下,这些程序还可以用来收集用户计算机的个人信息、破坏计算机的信息,或者在未获取用户同意的情况下安装恶意软件。

1.7C/S和B/S模式的区别

C/S模式就是客户端( client)/服务器( server)模式,客户端的电脑也可以参与整个系统的事务处理,可以处理一些不需要服务器处理的事务。

B/S模式就是浏览器( brower)/服务器( server)模式,浏览器端只能通过浏览程序(IE等)访问服务器,显示服务器提供的信息,整个系统的事务处理都要由服务器来完成。

2网上金融交易安全

2.1网上金融交易

网上金融交易是指用户通过因特网完成各种网络金融服务和网络电子商务支付。网络金融服务包括账户开户、查询、对帐、行内转账、跨行转账、信贷、网上证券、投资理财等服务项目,用户可以是不出户就完成各种金融业务。

网络电子商务支付可以使用银行卡或者第三方支付平台完成网络购物,如购买飞机票和火车票等。

为保障安全,网上金融交易一般不采用简单的账户/口令的验证方式来识别用户身份,多采取双因素身份认证识别用户身份,只有通过身份认证的用户才能通过网络完成各种转账、支付等操作。

2.2网上金融交易常用的安全措施如下

U盾（USB-Key）

U盾是用于网上电子银行签名和数字认证的工具,它内置微型智能卡处理器,采用非对称加密体制对网上数据进行加密、解密和数字签名用户选择使用U盾后,所有涉及资金对外转移的网银操作,都必须使用U盾才能完成。使用U盾时,除了需要将∪盾插入计算机,还需要输入设置的口令才能完成身份认证。

手机短信认证

用户向网络金融交易平台发出交易请求后,网络金融平台通过短信向用户绑定的手机号码发出一次性口令,只有在输入正确的用户口令和短信验证口令后,整个交易才能被确认并完成。

口令卡

口令卡相当于—种动态的电子银行口令。

口令卡上以矩阵的形式印有若干字符串,用户在使用电子银行进行对外转账、缴费等支付交易时,电子银行系统就会随机给出一组口令卡坐标,用户根据坐标从卡片中找到口令组合并输入。

只有口令组合输入正确时,用户才能完成相关交易这种口令组合是动态变化的,用户每次使用时输入的口令都不一样,交易结束后即失效,从而防止攻击者窃取用户口令。

采用安全超文本传输协议

安全超文本传输协议是以安全为目标的HTTP通道协议( Hyper Text Transfer protocol over Secure Socket Layer, HTTPS)是HTTP协议的安全版

HTTPS协议提供了身份验证与加密通信的方法,广泛用于因特网上安全敏感的通信,例如银行网站登录采用的是 HTTPS方式,该安全协议可以很大程度上保障用户数据传输的安全。

3.电子邮件安全

3.1电子邮件系统

电子邮件(Electronic mail , Email)是一种用电子手段提供信息交换的服务方式,是因特网上应用最为广泛的服务之一

3.2电子邮件安全威胁

随着电子邮件的广泛应用,电子邮件面临的安全威胁越来越多。这些威胁包括邮件地址欺骗、垃圾邮件、邮件病毒、邮件炸弹、邮件拦截、邮箱用户信息泄露等。

邮件地址欺骗

邮件地址欺骗是黑客攻击和垃圾邮件制造者常用的方法。由于在SMTP协议中,邮件发送者可以指定SMTP发送者的发送账户、发送账户的显示名称、SMTP服务器域名等信息,如果接收端未对这些信息进行认证就可能放过一些刻意伪造的邮件。攻击者可以通过自行搭建SMTP服务器来发送伪造地址的邮件。目前,正规的邮件服务器都有黑名单和反向认证等机制,如检査邮件来源IP、检查邮件发送域、反向DNS查询、登录验证等。伪造邮件一般很难通过严格设置的邮件服务器,但用户还是要对邮件内容涉及敏感信息的邮件来源保持高度警惕。

垃圾邮件

垃圾邮件是指未经用户许可就强行发送到用户邮箱的电子邮件。垃圾邮件一般具有批量发送的特征,其内容包括赚钱信息、成人广告、商业或个人网站广告、电子杂志、连环信等。垃圾邮件可以分为良性和恶性的良性垃圾邮件是对收件人影响不大的信息邮件,例如各种宣传广告;恶性垃圾邮件是指具有破坏性的电子邮件,例如携带恶意代码的广告

邮件病毒

邮件病毒和普通病毒在功能上是一样的,它们主要是通过电子邮件进行传播,因此被称为邮件病毒般通过邮件附件发送病毒,接收者打开邮件,运行附件会使计算机中病毒

邮件炸弹

邮件炸弹指邮件发送者利用特殊的电子邮件软件,在很短的时间内连续不断地将邮件发送给同一收信人,由于用户邮箱存储空间有限,没有多余空间接收新邮件,新邮件将会丢失或被退回,从而造成收件人邮箱功能瘫痪。同时,邮件炸弹会大量消耗网络资源,常常导致网络阻塞,重时可能影响到大量用户邮箱的使用。

3.3电子邮件安全防护技术

垃圾邮件过滤技术

垃圾邮件过滤技术是应对垃圾邮件问题的有效手段之一。下面介绍实时黑白名单过滤和智能内容过滤两种垃圾邮件过滤技术。

黑白名单过滤采用最简单直接的方式对垃圾邮件进行过滤。由用户手动添加需要过滤的域名、发信人或发信IP地址等。对于常见的广告型垃圾邮件,此方法的防范效果较为明显。但此种方式属于被动防御,需要大量手工操作,每次需要对黑白名单手工添加。

内容过滤主要针对邮件标题、邮件附件文件名和邮件附件大小等选项设定关键值。当邮件标题,邮件附件文件名和邮件附件大小等选项被认为是垃圾邮件,邮件系统就会将其直接删除。

邮件加密和签名

未经加密的邮件很容易被不怀好意的偷窥者看到,如果对带有敏感信息的邮件进行加密和签名,就可以大大提高安全性

用于电子邮件加密和签名的软件有许多, Gnupg( GNU Privacy Guard是其中常见的一种开源软件。

Gnupg是一个基于RSA公钥密码体制的邮件加密软件,可以加密邮件以防止非授权者阅读,同时还可以对邮件加上数字签名,使收信人可以确认邮件发送者,并确认邮件没有被篡改。

4.数据安全

4.1数据备份

在系统运行和维护的过程中,常会有一些难以预料的因素导致数据丢失如天灾人祸、硬件毁损、操作失误等。为确保数据的安全性,需对数据进行备份。

数据备份是容灾的基础,是为防止系统出现操作失误或系统故障导致数据丢失,而将全部或部分数据集合,从应用主机的硬盘或阵列复制到其它异地存储介质或移动硬盘的过程。

数据备份的方式有多种,传统方式是采用内置或外置的磁带机进行冷备份

备份后的磁带机数据保存在安全的位置,这种备份方式恢复数据的时间很长。随着技术的不断发展,海量数据的增加,不少企业开始采用网络备份。网络备份一般通过专业的数据存储管理软件结合相应的硬件和存储设备来实现。

随着云计算和云技术的发展,越来越多人们常使用云备份的方式来保存重要资料。个人和企业可以将重要数据备份到云服务器上,需要使用时,从云服务器上下载到本地使用。

4.2数据恢复

人们在日常生活和工作中会经常遇到数据丢失的情况,比如U盘误格式化、误删除某个文件、计算机硬件出现故障等,因此数据恢复引起越来越多地关注和重视。了解数据恢复原理并掌握一些常用的数据恢复工具,可以恢复各种丢失的数据,挽回用户的损失。如果不慎删除硬盘分区信息或者误格式化硬盘,造成系统信息区破坏,无法读取数据资料,首先应关机,不要轻易对硬盘数据资料进行写操作,否则会增加数据恢复的难度。重新开机后,再使用数据恢复工具恢复硬盘上的数据。

Easy Recovery是一款常用的数据恢复工具,当硬盘受病毒影响、格式化分区、误删除、断电或瞬间电流冲击造成的数据毁坏、程序的非正常操作或系统故障造成的数据毁坏等意外操作时,它可以帮助用户恢复丢失的数据以及重建文件系统。

Easy recovery不会向用户的原始驱动器写入任何数据,它的工作原理是在内存中重建文件分区表,然后将数据安全地传输到其他驱动器中。使用数据恢复软件找回数据文件的前提是硬盘中还保留有误删除文件的信息和数据块。当用户误删除文件或者误格式化U盘后,不要在该分区中写入任何文件,否则这些需要恢复的数据就有可能被写入的数据覆盖,恢复数据的难度就会加大。因此,为了恢复误删除的数据,就不能对要修复的分区或硬盘进行新的读写操作。

4.3数据加密

数据加密是保护数据安全的主要手段之一,可以避免用户在传输或存储重要信息过程中,被第三方窃取信息。常见的数据加密工具可以分为硬件加密和软件加密。硬件加密工具直接通过硬件单元,如利用USB接口或者计算机并行口等对数据进行加密,加密后可以有效地保

护用户信息、隐私或知识产权。软件加密工具主要有文件加密工具、光盘加密工具和磁盘加密工具。对单个文件或文件夹进行加密的工具有很多。例如,ZIP和RAR等压缩包可以用来加密大文件,压缩时可以设置密码,获取压缩包内的内容需要输入正确的口令才能解压。WPS、Word、PPT、PDF等也可以通过设置口令的方式来加密文件。光盘加密工具可以防止光盘数据被复制,可采用的方法很多。用户可以给光盘添加密码

例如, Secure Burn软件可以在正式刻录之前对光盘进行密码保护,然后通过软件内置的刻录功能即可直接获得有密码保护的光盘。用户也可以上文件只能在光盘中运行

又如,CD- Protector制作的加密光盘,他人无法通过直接复制文件获得光盘中的重要文件,即使把文件复制到硬盘再运行也会出现出错提示信息而不能使用。光盘加密工具可以对镜像文件进行可视化修改,隐藏光盘镜像文件。此外,还可以放大一般的文件,将普通目录改成文件目录由此保护光盘中的机密文件和有关隐私的信息。磁盘加密工具则是对磁盘数据进行加密。

目前磁盘加密工具主要有

PGPDisk，该软件是美国PGP公司开发的PGP系列安全软件中的一个套件，它的核心思想是通过建立虚拟磁盘来存放并保存加密数据。用户在使用虚拟磁盘时需要输入口令，所有存放并保存在虚拟磁盘中的文件都是加密的，如果用户不需要这个虚拟磁盘，可以删除。

TrueCrypt，这是一款免费开源的加密软件，同时支持多种操作系统。该软件通过在计算机上产生一个或几个虚拟盘来存放敏感数据，每个虚拟盘使用高强度密码算法进行加解密，加解密过程全部自动实现，用户只要输入正确的口令，能读取这些文件，否则不能读取数据。

为了数据安全，加密数据时应尽量保证

加密过程足够强壮并且覆盖整个磁盘，包括剩余空间，交换文件等

加密密钥足够长，能够抵御暴力破解攻击

加密密钥自身的机密性能够得到保障，例如用于加密磁盘的密钥从不存储在被加密保护的磁盘中

除了采用数据加密保证数据的保密性，用户还可以通过对数据文件添加数字签名来保证数据文件的完整性和真实性，防止数据被篡改或伪造，也可避免可能存在的欺骗和抵赖。一些应用软件可以对数据文件进行签名，如word，邮件客户端，Foxmail等。

4.4数据删除

硬盘等存储介质作为数据存储和交换的媒体,在日常工作中使用频繁。这些介质的处置不当,往往使得不法分子有机会通过对存储介质进行数据恢复来窃取曾经存储的重要数据,导致涉密,这成为了信息安全的重要隐患。因此,如何彻底删除计算机数据,防止信息泄露,已成为当今信息安全技术的一个重要研究内容。

在 Windows系统中,系统的文件删除命令是" delete"”,使用“ delete”删除文件以后,文件并没有真正删除,而是被移动到一个称为“回收站”的系统目录中,除非回收站满,或使用" shift+delete"组合键来删除,或当清空回收站时,才真正删除了文件。由于 Windows操作系统只考虑了由操作系统本身对系统资源存取,因此无论是在文件分配表(File location Table,FAT还是新技术文件系统( New Technology File System,NTFS)下,操作系统刷除文件的标准都是“对操作系统不可见”,事实上,只是对文件的目录作了删除标记,保证了文件在删除前所占用的空间确实得到释放,而文件实际存放在数据区的内容毫无改变。从以上原理可知,只要数据区没有被破坏,数据就没有完全删除,就存在被恢复的可能。

数据安全删除就是要安全删除了要删除的文件,包括文件相关属性信息,即完全破坏数据,使数据恢复无法进行,从而实现保护数据的目的。目前安全删除的方法归纳起来,大体上可以分为硬销毁和软销毁两类。

硬删除

数据硬销毁即破坏性销毁,是指采用物理破坏或化学腐蚀的方法把记录涉密数据的物理载体完全破坏掉,从而从根本上删除数据的销毁方式,是对保护数据不被恢复的安全、彻底的方法。数据硬销毁可分为物理销毁和化学销毁两种方式物理销毁又可分为消磁、熔炉中焚化和熔炼、借助外力粉碎及硏磨磁盘表面等方法。物理销毁方法费时、费力,一般只适用于保密要求较高的场合。化学销毁是指采用化学药品(比如高腐蚀性的浓盐酸和浓硫酸等)腐蚀、溶解、活化及剥离磁盘记录表面的数据销毁方法。化学销毁方法只能由专业人员在特定场所中进行

软销毁

软清除即逻辑销毁,是指通过软件编程实现对数据及其相关信息的反复覆盖擦除,达到不可恢复的安全删除目的,一般情况下,认为低级格式化以后,数据恢复的可能性依然存在要保证安全,必须通过多次写入新数据来覆盖旧数据才能真正达到数据安全删除的目的。数据软销毁通常采用数据覆写法。数据覆写是将非保密数据写入以前存有敏感数据的硬盘簇的过程,其技术原理是依据硬盘上的数据都是以二进制的“1”和“0″形式存储的,而使用预先定义的无意义、无规律的信息反复多次覆盖硬盘上原先存储的数据,就无法知道原先的数据,也就达到了销毁数据的目的。

由于经过数据覆写法处理后的硬盘可以循环使用,适用于密级要求不是很高的场合,特别是需要对某一具体文件进行销毁而其他文件不能破坏时,这种方法更为实用。现在常见的数据销毁软件,例如Bcwipe, Eraser等,主要是针对文件、剩余空间和物理磁盘的销毁。所采用的方式都是通过软件对磁盘进行相应的覆写。数据覆写技术犹如碎纸机,是安全、经济的数据软销毁方式之一

5账户口令安全

当用户在使用各种应用时,需通过账户和口令来验证身份从而访问某些资源,因此,账号口令的安全性非常重要。当前攻击者窃取用户口令的方式主要有以下三种

5.1暴力破解

暴力破解又称口令穷举,就是通过计算机对所有可能的口令组合进行穷举尝试。如果攻击者已知用户账户,用户的口令又比较简单,例如简单的数字组合,攻击者使用暴力破解工具可以很快破译口令。因此在一些安全性较高的系统,如网银系统,会限制口令的输入次数,降低暴力破解口令的成功率

5.2键盘记录木马

如果用户的计算机被植入键盘记录木马,当用户通过键盘输入口令时键盘记录木马程序会记住用户输入的口令,然后木马程序通过自带邮件发送功能把记录的口令发送到攻击者指定的邮箱。

5.3屏幕快照木马

如果用户的计算杋被植入屏幕快照木马,木马程序会通过屏幕快照将用户的登录界面连续保存为两张黑白图片,然后通过自带的发信模块将图片发送到指定邮箱。攻击者通过对照图片中鼠标的点击位置,就能破译出用户账号和口令。

5.4用户在设置账户的口令时,应遵循以下原则

严禁使用空口令

严禁使用与账号相同或相似的口令

不要设置简单字母和数字组成的口令(如 password1);

不要设置短于6个字符或仅包含字母或数字的口令;

不要使用与个人有关的信息作为口令内容,如生日、身份证号码、亲人或者伴侣的姓名、宿舍号等。

为了保证口令的安全性,建议用户每隔一段时间更新一次账号口令。如果用户是在公共场所使用计算机上网,登录账户时不要选择保存口令和自动登录,离开时要清除使用过的记录。