第3章 网络安全基础

3.1 网络安全概述

3.1.1 网络安全现状及安全挑战


网络安全现状及安全挑战

1969年，美国国防部国防高级研究计划局（DOD/DARPA）资助建立了ARPANET（阿帕网），标志着互联网的诞生。计算机网络及分布式系统的出现给信息安全带来了第二次变革。人们通过各种通信网络进行数据的传输、交换、存储、共享和分布式计算。网络的出现给人们的工作和生活带来了极大的便利，但同时也带来了极大的安全风险。在信息传输和交换时，需要对通信信道上传输的机密数据进行加密；在数据存储和共享时，需要对数据库进行安全的访问控制和对访问者授权；在进行多方计算时，需要保证各方机密信息不被泄露。这些均属于网络安全的范畴。

1. 网络安全现状

在今天的计算机技术产业中，网络安全是急需解决的最重要的问题之一。由美国律师联合会（American Bar Association）所做的一项与安全有关的调查发现，有40%的被调查者承认在他们的机构内曾经发生过计算机犯罪事件。在过去的几年里，Internet继续快速发展，Internet用户数量急剧攀升。随着网络基础设施的建设和Internet用户的激增，网络与信息安全问题越来越严重，因黑客事件而造成的损失也越来越巨大。

第一，计算机病毒层出不穷，肆虐全球，并且逐渐呈现新的传播态势和特点。其主要表现是传播速度快，与黑客技术结合而形成的“混种病毒”和“变异病毒”越来越多。病毒能够自我复制，其主动攻击与主动感染能力增强。当前，全球计算机病毒已达8万多种，每天会产生5～10种新病毒。

第二，黑客对全球网络的恶意攻击势头逐年攀升。近年来，网络攻击还呈现出黑客技术与病毒传播相结合的趋势。2001年以来，计算机病毒的大规模传播与破坏都与黑客技术的发展有关，二者的结合使病毒的传染力与破坏性倍增。这意味着网络安全遇到了新的挑战，即集病毒、木马、蠕虫和网络攻击为一体的威胁，可能造成快速、大规模的感染，造成主机或服务器瘫痪，数据信息丢失，损失不可估量。在网络和无线电通信普及的情况下，尤其是在计算机网络与无线通信融合、国家信息基础设施网络化的情况下，黑客加病毒的攻击很可能构成对网络生存与运行的致命威胁。如果黑客对国家信息基础设施中的

任何一处目标发起攻击,都可能导致巨大的经济损失。

第三,由于技术和设计上的不完备,导致系统存在缺陷或安全漏洞。这些漏洞或缺陷主要存在于计算机操作系统与网络软件之中。例如,微软的 Windows XP 操作系统中含有数项严重的安全漏洞,黑客可以通过此漏洞实施网络窃取、销毁用户资料或擅自安装软件,乃至控制用户的整个计算机系统。正是因为计算机操作系统与网络软件难以完全克服这些漏洞和缺陷,使得病毒和黑客有了可乘之机。由于操作系统和应用软件所采用的技术越来越先进和复杂,因此带来的安全问题就越来越多。同时,由于黑客工具随手可得,使得网络安全问题越来越严重。所谓"网络是安全的"的说法只是相对的,实际上根本无法达到"绝对安全"的状态。

第四,世界各国军方都在加紧进行信息战的研究。近几年来,黑客技术已经不再局限于修改网页、删除数据等惯用的伎俩,而是堂而皇之地登上了信息战的舞台,成为信息作战的一种手段。信息战的威力之大,在某种程度上不亚于核武器。在海湾战争、科索沃战争及巴以战争中,信息战发挥了巨大的威力。

今天,"制信息权"已经成为衡量一个国家实力的重要标志之一。信息空间上的信息大战正在悄悄而积极地酝酿,小规模的信息战一直不断出现、发展和扩大。信息战是信息化社会发展的必然产物。在信息战场上能否取得控制权,是赢得政治、外交、军事和经济斗争胜利的先决条件。信息安全问题已成为影响社会稳定和国家安危的战略性问题。

2. 敏感信息对安全的需求

与传统的邮政业务和有纸办公不同,现代的信息传递、存储与交换是通过电子和光子完成的。现代通信系统可以让人类实现面对面的电视会议或电话通信。然而,流过信息系统的信息有可能十分敏感,因为它们可能涉及产权信息、政府或企业的机密信息,或者与企业之间的竞争密切相关。目前,许多机构已经明确规定,对网络上传输的所有信息必须进行加密保护。从这个意义上讲,必须对数据保护、安全标准与策略的制定、安全措施的实际应用等各方面工作进行全面的规划和部署。

根据多级安全模型,通常将信息的密级由低到高划分为秘密级、机密级和绝密级,以确保每一密级的信息仅能让那些具有高于或等于该权限的人使用。所谓机密信息和绝密信息,是指国家政府对军事、经济、外交等领域严加控制的一类信息。军事机构和国家政府部门应对信息施加严格的保护,特别应对那些机密和绝密信息施加严格的保护措施。对于那些被认为敏感但非机密的信息,也需要通过法律手段和技术手段加以保护,以防止信息泄露或被恶意修改。事实上,一些政府部门的信息是非机密的,但它们通常属于敏感信息。一旦泄露这些信息,有可能对社会的稳定造成危害。因此,不能通过未加保护的通信媒介传送此类信息,而应该在发送前或发送过程中对此类信息进行加密保护。当然,这些保护措施的实施是要付出代价的。除此之外,在系统的方案设计、系统管理和系统的维护方面还需要花费额外的时间和精力。近年来,一些采用极强防护措施的部门也面临着越来越严重的安全威胁。今天的信息系统不再是一个孤立的系统,通信网络已经将无数个独立的系统连接在一起。在这种情况下,网络安全也呈现出许多新的形式和特点。

3. 网络应用对安全的需求

Internet 从诞生到现在只有短短几十年的时间,但其爆炸式的技术发展速度远远超

过人类历史上任何一次技术革命。然而，从长远发展趋势来看，现在的 Internet 还处于发展的初级阶段，Internet 技术存在着巨大的发展空间和潜力。

随着网络技术的发展，网络视频会议、远程教育等各种新型网络多媒体应用不断出现，传统的网络体系结构越来越显示出局限性。1996 年，美国政府制定了下一代 Internet (Next Generation Internet，NGI)计划，与目前使用的 Internet 相比，它的传输速度将更快、规模更大，而且更安全。

3.1.2　网络安全威胁与防护措施


网络安全威胁与防护措施

1. 基本概念

安全威胁，是指某个人、物、事件或概念对某一资源的保密性、完整性、可用性或合法使用所造成的危险。攻击就是某个安全威胁的具体实施。

防护措施，是指保护资源免受威胁的一些物理的控制、机制、策略和过程。脆弱性是指在实施防护措施中或缺少防护措施时系统所具有的弱点。

风险，是对某个已知的、可能引发某种成功攻击的脆弱性的代价的测度。当某个脆弱的资源的价值越高且成功攻击的概率越大时，风险就越高；反之，当某个脆弱资源的价值越低且成功攻击的概率越小时，风险就越低。风险分析能够提供定量的方法，以确定是否应保证在防护措施方面的资金投入。

安全威胁可分为故意(如黑客渗透)和偶然(如信息被发往错误的地方)两类。故意的威胁又可进一步分为被动攻击和主动攻击。被动攻击只对信息进行监听(如搭线窃听)，而不对其进行修改。主动攻击却对信息进行故意的修改(如改动某次金融会话过程中货币的数量)。总之，被动攻击比主动攻击更容易以更小的代价加以实施。

目前尚没有统一的方法对各种威胁加以区别和进行分类，也难以理清各种威胁之间的相互关系。不同威胁的存在及其严重性随着环境的变化而变化。然而，为了解释网络安全服务的作用，我们将现代计算机网络及通信过程中常遇到的一些威胁汇编成图表，如图 3-1 和表 3-1 所示。下面分三类对威胁进行分析：①基本的威胁；②主要的可实现威胁；③潜在威胁。

表 3-1　典型的网络安全威胁

威　　胁	描　　述
授权侵犯	被授权以特定目的使用系统的人，却将此授权用于其他非授权的目的
旁路控制	攻击者发掘系统的安全缺陷或安全脆弱性，以绕过访问控制措施
拒绝服务 *	对信息或其他资源的合法访问被无条件地拒绝
窃听攻击	信息在被监视的通信过程中泄露出去
电磁/射频截获	信息从电子或机电设备所发出的无线频率或其他电磁场辐射中被提取出来
非法使用	资源被某个非授权的人或以非授权的方式使用
人员疏忽	被授权的人为了金钱等利益或因疏忽，将信息泄露给非授权的人

续表

威　胁	描　述
信息泄露	信息被泄露或暴露给某个非授权的人
完整性侵犯 *	数据的一致性由于非授权的增删、修改或破坏而受到损害
截获/修改 *	通信数据在传输过程中被改变、删除或替换
假冒攻击 *	一个实体(人或系统)假装成另一个不同的实体
媒介废弃	信息从被废弃的磁带或打印的废纸中泄露出去
物理入侵	入侵者通过绕过物理控制(如防盗门)而获得对系统的访问
消息重发 *	对所截获的某次合法通信数据备份,出于非法的目的而重新发送该数据
业务否认 *	参与某次通信交换的一方,事后错误地否认曾经发生过此次信息交换
资源耗尽	某一资源(如访问接口)被故意地超负荷使用,导致其他用户服务中断
服务欺骗	某一伪造的系统或部件欺骗合法的用户或系统,自愿放弃敏感的信息
窃取	某一安全攸关的物品被盗,例如令牌或身份卡
流量分析 *	通过对通信流量进行监听和分析,机密信息有可能泄露给非授权的实体
陷门	将某一“特征”嵌入某个系统或其部件中,当输入特定数据时,允许违反安全策略
特洛伊木马	一个不易察觉或无害程序段的软件,当其被运行时,就会破坏用户的安全性

说明:带 * 的威胁表示在计算机通信安全中可能发生的威胁。

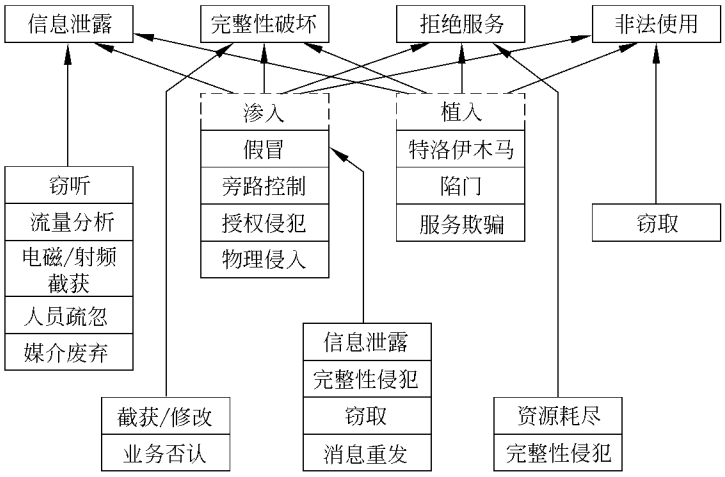

图 3-1　典型的威胁及其相互关系

2. 安全威胁的来源

(1) 基本威胁。

在信息系统中,存在以下 4 种基本安全威胁。

① 信息泄露:信息被泄露或透露给某个非授权的人或实体。这种威胁来自诸如窃

听、搭线或其他更加错综复杂的信息探测攻击。

② 完整性破坏：数据的一致性通过非授权的增删、修改或破坏而受到损坏。

③ 拒绝服务：对信息或资源的访问被无条件地阻止。这可能由以下攻击所致：攻击者通过对系统进行非法的、根本无法成功的访问尝试，使系统产生过量的负荷，从而导致系统的资源在合法用户看来是不可使用的。拒绝服务也可能是因为系统在物理上或逻辑上受到破坏而中断服务。

④ 非法使用：某一资源被某个非授权的人或以某种非授权的方式使用。例如，侵入某个计算机系统的攻击者会利用此系统作为盗用电信服务的基点，或者作为侵入其他系统的“桥头堡”。

(2) 主要的可实现威胁。

在安全威胁中，主要的可实现威胁应该引起高度关注，因为这类威胁一旦成功实施，就会直接导致其他任何威胁的实施。主要的可实现威胁包括渗入威胁和植入威胁。

主要的渗入威胁有如下几种。

① 假冒。某个实体(人或系统)假装成另外一个不同的实体。这是突破某一安全防线最常用的方法。这个非授权的实体提示某个防线的守卫者，使其相信它是一个合法实体，此后便攫取了此合法用户的权利和特权。黑客大多采取这种假冒攻击方式来实施攻击。

② 旁路控制。为了获得非授权的权利和特权，某个攻击者会发掘系统的缺陷和安全漏洞。例如，攻击者通过各种手段发现原本应保密但又暴露出来的一些系统“特征”。攻击者可以绕过防线守卫者侵入系统内部。

③ 授权侵犯。一个授权以特定目的使用某个系统或资源的人，却将其权限用于其他非授权的目的。这种攻击的发起者往往属于系统内的某个合法的用户，因此这种攻击又称为“内部攻击”。

主要的植入威胁有如下几种。

① 特洛伊木马(Trojan Horse)。软件中含有一个不易觉察的或无害的程序段，当被执行时，它会破坏用户的安全性。例如，一个表面上具有合法目的的应用程序软件，如文本编辑软件，它还具有一个暗藏的目的，就是将用户的文件复制到一个隐藏的秘密文件中，这种应用程序就称为特洛伊木马。此后，植入特洛伊木马的那个攻击者就可以阅读到该用户的文件。

② 陷门(Trapdoor)。在某个系统或其部件中设置“机关”，使得在提供特定的输入数据时，允许违反安全策略。例如，如果在一个用户登录子系统上设有陷门，当攻击者输入一个特别的用户身份号时，就可以绕过通常的口令检测。

(3) 潜在威胁。

在某个特定的环境中，如果对任何一种基本威胁或主要的可实现的威胁进行分析，就能够发现某些特定的潜在威胁，而任意一种潜在的威胁都可能导致一些更基本的威胁发生。例如，在对信息泄露这种基本威胁进行分析时，有可能找出以下几种潜在的威胁。

① 窃听(Eavesdropping)。

② 流量分析(Traffic Analysis)。

③ 操作人员的不慎所导致的信息泄露。

④ 媒体废弃物所导致的信息泄露。

图 3-1 列出了一些典型的威胁及它们之间的相互关系。注意,图中的路径可以交错。例如,假冒攻击可以成为所有基本威胁的基础,同时假冒攻击本身也存在信息泄露的潜在威胁。信息泄露可能暴露某个口令,而用此口令攻击者也可以实施假冒攻击。表 3-1 列出了各种威胁之间的差异,并分别进行了描述。

对 3000 种以上的计算机误用案例所做的一次抽样调查显示,最主要的几种安全威胁如下(按照出现频率由高至低排列)。

① 授权侵犯。

② 假冒攻击。

③ 旁路控制。

④ 特洛伊木马或陷门。

⑤ 媒体废弃物。

在 Internet 中,网络蠕虫(Internet Worm)就是将旁路控制与假冒攻击结合起来的一种威胁。旁路控制就是利用已知的 UNIX、Windows 和 Linux 等操作系统的安全缺陷,避开系统的访问控制措施,进入系统内部。而假冒攻击则通过破译或窃取用户口令,冒充合法用户使用网络服务和资源。

3. 安全防护措施

在安全领域中,存在多种类型的防护措施。除了采用密码技术的防护措施外,还有其他类型的安全防护措施。

(1) 物理安全。包括门锁或其他物理访问控制措施、敏感设备的防篡改和环境控制等。

(2) 人员安全。包括对工作岗位敏感性的划分、雇员的筛选,同时也包括对人员的安全性培训,以增强其安全意识。

(3) 管理安全。包括对进口软件和硬件设备的控制,负责调查安全泄露事件,对犯罪分子进行审计跟踪,并追查安全责任。

(4) 媒体安全。包括对受保护的信息进行存储,控制敏感信息的记录、再生和销毁,确保废弃的纸张或含有敏感信息的磁性介质被安全销毁。同时,对所用媒体进行扫描,以便发现病毒。

(5) 辐射安全。对射频(RF)及其他电磁(EM)辐射进行控制(又称 TEMPEST 保护)。

(6) 生命周期控制。包括对可信系统进行系统设计、工程实施、安全评估及提供担保,并对程序的设计标准和日志记录进行控制。

一个安全系统的强度与其最弱链路的强度相同。为了提供有效的安全性,需要将不同种类的威胁对抗措施联合起来使用。例如,当用户将口令遗忘在某个不安全的地方或受到欺骗而将口令暴露给某个未知用户时,即使技术上是完备的,用于对付假冒攻击的口令系统也将无效。

防护措施可用来对付大多数安全威胁，但是采用每种防护措施均要付出代价。网络用户需要认真考虑这样一个问题：为了防止某个攻击所付出的代价是否值得。例如，在商业网络中，一般不考虑对付电磁(EM)或射频(RF)泄露，因为它们对商用环境来说风险很小，而且其防护措施又十分昂贵。但对于机密环境，人们会得出不同的结论。对于某一特定的网络环境，究竟采用什么安全防护措施，这种决策属于风险管理的范畴。目前，人们已经开发出各种定性和定量的风险管理工具。如果要进一步了解有关的信息，请参看有关文献。

3.1.3　安全攻击的分类及常见形式


安全攻击的分类及常见形式

X.800 和 RFC 2828 对安全攻击进行了分类。它们把攻击分成两类：被动攻击和主动攻击。被动攻击试图获得或利用系统的信息，但不会对系统的资源造成破坏。而主动攻击则不同，它试图破坏系统的资源，影响系统的正常工作。

1. 被动攻击

被动攻击的特性是对所传输的信息进行窃听和监测。攻击者的目标是获得线路上所传输的信息。信息泄露和流量分析就是两种被动攻击的例子。

第一种被动攻击是窃听攻击，如图 3-2(a)所示。电话、电子邮件和传输的文件中都可能含有敏感或秘密信息。攻击者通过窃听，可以截获这些敏感或秘密信息。我们要做的工作就是阻止攻击者获得这些信息。

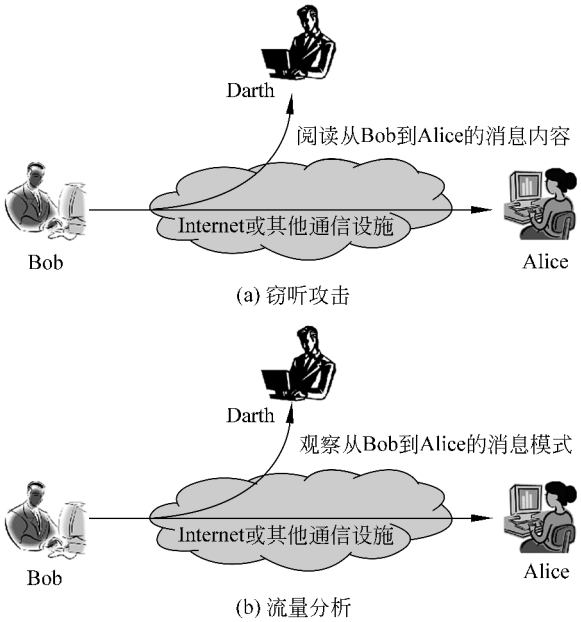

图 3-2　被动攻击

第二种被动攻击是流量分析，如图 3-2(b)所示。假设用户已经采取了某种措施来隐藏消息内容或其他信息的流量，使攻击者即使捕获了消息也不能从中发现有价值的信息。

加密是隐藏消息的常用方法。即使对信息进行了合理的加密保护,攻击者仍然可以通过流量分析获得这些消息的模式。攻击者可以确定通信主机的身份及其所处的位置,可以观察传输消息的频率和长度,然后根据所获得的这些信息推断本次通信的性质。

被动攻击由于不涉及对数据的更改,所以很难被察觉。通过采用加密措施,完全有可能阻止这种攻击。因此,处理被动攻击的重点是预防,而不是检测。

2. 主动攻击

主动攻击是指恶意篡改数据流或伪造数据流等攻击行为,它可分成以下 4 类:

(1) 伪装攻击(Impersonation Attack)

(2) 重放攻击(Replay Attack)

(3) 消息篡改(Message Modification)

(4) 拒绝服务(Denial of Service)攻击

伪装攻击是指某个实体假装成其他实体,对目标发起攻击,如图 3-3(a)所示。伪装攻击的例子有:攻击者捕获认证信息,然后将其重发,这样攻击者就有可能获得其他实体所拥有的访问权限。

重放攻击是指攻击者为了达到某种目的,将获得的信息再次发送,以在非授权的情况下进行传输,如图 3-3(b)所示。

消息篡改是指攻击者对所获得的合法消息中的一部分进行修改或延迟消息的传输,以达到其非授权的目的,如图 3-3(c)所示。例如,攻击者将消息 Allow John Smith to read confidential accounts 修改为 Allow Fred Brown to read confidential file accounts。

拒绝服务攻击则是指阻止或禁止人们正常使用网络服务或管理通信设备,如图 3-3(d)所示。这种攻击可能目标非常明确。例如,某个实体可能会禁止所有发往某个目的地的消息。拒绝服务的另一种形式是破坏某个网络,使其瘫痪,或者使其过载以降低性能。

主动攻击与被动攻击相反。被动攻击虽然难以检测,但采取某些安全防护措施就可以有效阻止;主动攻击虽然易于检测,但却难以阻止。所以对付主动攻击的重点应当放在如何检测并发现它们,并采取相应的应急响应措施,使系统从故障状态恢复到正常运行。由于检测主动攻击能起到威慑攻击者的作用,所以在某种程度上可以阻止主动攻击。

3. 网络攻击的常见形式

在前面已经讨论了网络中存在的各种威胁,这些威胁的直接表现形式就是黑客常采取的各种网络攻击方式。下面将对常见的网络攻击进行分类。通过分类,可以针对不同的攻击类型采取相应的安全防护措施。

(1) 口令窃取

进入一台计算机最容易的方法就是采用口令登录。只要在许可的登录次数范围内输入正确的口令,就可以成功地登录系统。

口令攻击有以下三种基本方式:

① 利用已知或假定的口令尝试登录。虽然这种登录尝试需要反复进行十几次甚至更多,但往往会取得成功。一旦攻击者成功登录,网络的主要防线就会崩溃。很少有操作

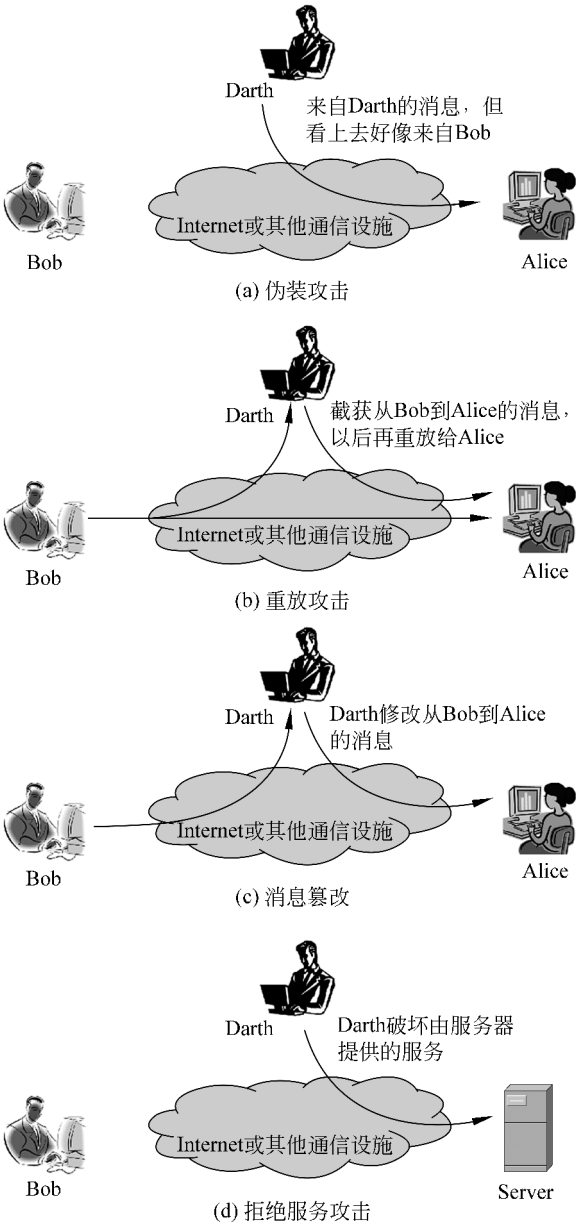

图 3-3　主动攻击

系统能够抵御从内部发起的攻击。

② 根据窃取的口令文件进行猜测(如 UNIX 系统中的/etc/passwd 文件)。这些口令文件有的是从已经被攻破的系统中窃取的,有的是从未被攻破的系统中获得的。由于用户习惯重复使用同一口令,当黑客得到这些文件后,就会尝试用其登录其他机器。这种攻击称为“字典攻击”,通常十分奏效。

③ 窃听某次合法终端之间的会话,并记录所使用的口令。采用这种方式,不管用户

的口令设计得有多好,其系统都会遭到破坏。

要彻底解决使用口令的弊端,就要完全放弃使用口令机制,转而使用基于令牌(Token-based)的机制。如果暂时还不能做到,起码要使用一次性口令方案,如 OTP(One-Time Password)。

(2) 欺骗攻击

黑客的另外一种攻击方式是采用欺骗的方式获取登录权限。常用的欺骗攻击是攻击者会向受害者发送钓鱼邮件。钓鱼邮件指利用伪装的电邮,欺骗收件人将账号、口令等信息回复给指定的接收者;或引导收件人连接到特制的网页,这些网页通常会伪装成和真实网站一样,如银行或理财的网页,令登录者信以为真,输入信用卡或银行卡号码、账户名称及密码等而被盗取。不幸的是,很多人都会上当,因为这个钓鱼邮件可能是自己的"朋友"或"熟人"发送的。

(3) 缺陷和后门攻击

网络蠕虫传播的方式之一是通过向 finger 守护程序(Daemon)发送新的代码实现的。显然,该守护程序并不希望收到这些代码,但在协议中没有限制接收这些代码的机制。守护程序的确可以发出一个 gets 呼叫,但并没有指定最大的缓冲区长度。蠕虫向"读"缓冲区内注入大量的数据,直到将 gets 堆栈中的返回地址覆盖。当守护程序中的子程序返回时,就会转而执行攻击者写入的代码。

缓冲器溢出攻击也称为"堆栈粉碎"(Stack Smashing)攻击。这是攻击者常采用的一种扰乱程序的攻击方法。长期以来,人们试图通过改进设计以消除缓冲器溢出缺陷。有些计算机语言在设计时就尽可能不让攻击者做到这点。一些硬件系统也尽量不在堆栈上执行代码。此外,一些 C 编译器和库函数也使用了许多对付缓冲器溢出攻击的方法。

所谓缺陷(Flaws),就是指程序中的某些代码并不能满足特定的要求。尽管一些程序缺陷已经由厂家逐步解决,但是一些常见问题依然存在。最佳解决办法就是在编写软件时,力求做到准确、无误。然而,软件上的缺陷有时是很难避免的,这正是今天的软件中存在那么多缺陷的原因。

Morris 蠕虫及其许多现代变种给我们的教训极为深刻,其中最重要的一点是:缺陷导致的后果并不局限于产生不良的效果或造成某一特定服务的混乱,更可怕的是因为某一部分代码的错误而导致整个系统的瘫痪。当然,没有人有意要编写带有缺陷的代码。只要采取相应的步骤,就可以降低其发生的可能性。

最后需要指出,不要为了追求效率而牺牲对程序正确性的检查。如果仅为了节约几纳秒的执行时间而将程序设计得既复杂又别出心裁,并且又需要特权,那么你就错了。现在的计算机硬件速度越来越高,节约的这点时间毫无价值。一旦出现安全问题,在清除入侵上所花费的时间和付出的代价将是非常巨大的。

(4) 认证失效

许多攻击的成功都可归结于认证机制的失效。即使一个安全机制再好,也存在遭受攻击的可能性。例如,一个源地址有效性的验证机制,在某些应用场合(如有防火墙地址过滤时)能够发挥作用,但是黑客可以使用 rpcbind 重发某些请求。在这种情况下,最终的服务器就会被欺骗。对于这些服务器来说,这些消息看起来好像源于本地,但实际上来

自其他地方。

如果源机器是不可信的，基于地址的认证也会失效。虽然人们可以采用口令机制以控制自己的计算机，但是口令失窃也是常见的。窃听者可以很容易地从未加密的会话中获得明文的口令，有时也可能对某些一次口令方案发起攻击。对于一个好的认证方案来说，再次登录必须具有唯一的有效口令。有时攻击者会将自己置于客户机和服务器中间，它仅转发服务器对客户机发出的“挑战”(Challenge，实际上为一随机数)，并从客户机获得一个正确的“响应”。此时，攻击者可以采用此“响应”信息登录到服务器上。有关此类攻击可参见相关文献。

(5) 协议缺陷

前面讨论的是在系统完全正常工作的情况下发生的攻击。但是，有些认证协议本身就有安全缺陷，这些缺陷的存在会直接导致攻击的发生。

例如，攻击者可对 TCP 发起序列号攻击。由于在建立连接时所生成的初始序列号的随机性不够，攻击者很可能发起源地址欺骗攻击。为了做到公平，TCP 的序列号在设计时并没有考虑抵御恶意的攻击。其他基于序列号认证的协议也可能遭受同样的攻击。这样的协议有很多，如 DNS 和许多基于 RPC 的协议。

在密码学上，如何发现协议中存在的安全漏洞是非常重要的研究课题。有时错误是由协议的设计者无意造成的，但更多的安全漏洞是由不同的安全假设所引发的。要证明密码协议的安全性非常困难，人们正在加强这方面的研究工作。现在，各种学术刊物、安全公司网站和操作系统开发商经常公布一些新发现的安全漏洞，我们必须对此加以重视。

802.11 无线数据通信标准中的 WEP 在设计上也存在缺陷。目前，针对 WEP 的攻击软件在网络上随处可见。这一切说明，真正的安全是很难做到的。工程师在设计密码协议时，应当多向密码学家咨询，而不是随意设计。信息安全对人的技术素质要求非常高，没有进行专业学习和受过专门培训的人员很难胜任此项工作。

(6) 信息泄露

许多协议都会丢失一些信息，这就给那些想要使用该服务的攻击者提供了可乘之机。这些信息可能成为商业间谍窃取的目标，攻击者也可借助这些信息攻破系统。Finger 协议就是这样一个例子。这些信息除了可以用于口令猜测之外，还可以用来进行欺骗攻击。

另一个丰富的数据来源是 DNS。在这里，黑客可以获得从公司的组织结构到目标用户的非常有价值的数据。要控制数据的流出是非常困难的，唯一的办法是对外部可见的 DNS 加以限制，使其仅提供网关机器的地址列表。

精明的黑客当然深谙其理，他根本不需要你说出有哪些机器存在。他只需进行端口号和地址空间扫描，就可寻找感兴趣的服务和隐藏的主机。这里，对 DNS 进行保护的最佳防护措施是使用防火墙。如果黑客不能向某一主机发送数据包，他也就不能侵入该主机并获取有价值的信息。

(7) 指数攻击——病毒和蠕虫

指数攻击能够使用程序快速复制并传播攻击。当程序自行传播时，这些程序称为蠕虫(Worms)；当它们依附于其他程序传播时，这些程序就叫作病毒。病毒传播的数学模型是相似的，病毒的流行传播与生物感染病毒非常相似。

这些程序利用很多系统或用户中普遍存在的缺陷和不良行为取得成功。它们可以在几小时或几分钟之内扩散到全世界,从而使许多机构蒙受巨大损失。Melissa 蠕虫能够阻塞基于微软软件的电子邮件系统达 5 天之久。各种各样的蠕虫给 Internet 造成巨大的负担。这些程序本身更倾向于攻击随机的目标,而不是针对特定的个人或机构。但是,它们所携带的某些代码却可能对那些著名的政治目标或商业目标发起攻击。

对于已知的计算机病毒,采用流行的查杀病毒软件来清除非常有效。但是这些软件必须经常升级,因为病毒的制造者和杀毒软件厂商之间始终在进行着较量。现在,病毒隐藏的隐蔽性越来越高,使得杀毒软件不再局限于在可执行代码中寻找某些字符串。它们必须能够仿效这些代码并寻找滤过性病毒的行为特征。由于病毒越来越难以发现,病毒检测软件就必须花更多的时间检查每个文件,有时所花费的时间会很长。病毒的制造者可能会巧妙地设计代码,使杀毒软件在一定时间内不能识别出病毒。

(8) 拒绝服务攻击

在前面讨论的攻击方式中,大多数是基于协议的弱点、服务器软件的缺陷和人为因素而实施的。拒绝服务(Denial-of-Service,DoS)攻击则不同,它们是通过过度使用服务,使网络连接数超出其可以承受的并发连接数,从而造成自动关机或系统瘫痪,或降低服务质量。这种攻击通常不会造成文件删除或数据丢失,因此是一种比较温和的攻击。

这类攻击往往比较容易发现。例如,关闭一个服务很容易被检测并发现。尽管攻击很容易暴露,但要找到攻击的源头却十分困难。这类攻击往往生成伪装的数据包,其中含有随机和无效的返回地址。

分布式拒绝服务(Distributed Denial-of-Service,DDoS)攻击使用很多 Internet 主机,同时向某个目标发起攻击。通常,参与攻击的主机却不明不白地成为攻击者的帮凶。这些主机可能已经被攻击者攻破,或者被植入恶意的木马。DDoS 攻击通常难以恢复,因为攻击有可能来自世界各地。

目前,黑客采用 DDoS 攻击成功地攻击了几个著名的网站,如 Yahoo、微软及 SCO 等,已经引起广泛关注。DDoS 其实是 DoS 攻击的一种,不同的是它能够使用许多台计算机通过网络同时对某个网站发起攻击。有关 DDoS 攻击原理,可以查阅相关文献。


开放系统互连模型与安全体系结构

3.1.4 开放系统互连模型与安全体系结构

研究信息系统安全体系结构的目的,就是将普遍性的安全理论与实际信息系统相结合,形成满足信息系统安全需求的安全体系结构。应用安全体系结构的目的,就是从管理上和技术上保证完整、准确地实现安全策略,满足安全需求。开放系统互连(Open System Interconnection,OSI)安全体系结构定义了必需的安全服务、安全机制和技术管理,以及它们在系统上的合理部署和关系配置。

由于基于计算机网络的信息系统以开放系统 Internet 为支撑平台,因此本节重点讨论开放系统互连安全体系结构。

OSI 安全体系结构的研究始于 1982 年,当时 ISO 基本参考模型刚刚确立。这项工作是由 ISO/IEC JTC1/SC21 完成的。国际标准化组织(ISO)于 1988 年发布了 ISO

7498-2 标准，作为 OSI 基本参考模型的新补充。1990 年，国际电信联盟（International Telecommunication Union，ITU）决定采用 ISO 7498-2 作为其 X.800 推荐标准。因此，X.800和 ISO 7498-2 标准基本相同。

我国的国家标准《信息处理系统开放系统互连基本参考模型——第二部分：安全体系结构》（GB/T 9387.2—1995）（等同于 ISO 7498-2）和《Internet 安全体系结构》（RFC 2401）中提到的安全体系结构是两个普遍适用的安全体系结构，用于保证在开放系统中进程与进程之间远距离安全交换信息。这些标准确立了与安全体系结构有关的一般要素，适用于开放系统之间需要通信保护的各种场合。这些标准在参考模型的框架内建立起一些指导原则与约束条件，从而提供了解决开放互连系统中安全问题的统一方法。

下面重点介绍安全体系结构中所定义的安全服务和安全机制及两者之间的关系。

1. 安全服务

X.800 对安全服务做出定义：为了保证系统或数据传输有足够的安全性，开放系统通信协议所提供的服务。RFC 2828 也对安全服务做出了更加明确的定义：安全服务是一种由系统提供的对资源进行特殊保护的进程或通信服务。安全服务通过安全机制来实现安全策略。X.800 将这些服务分为 5 类共 14 个特定服务，如表 3-2 所示。这 5 类安全服务将在后面逐一进行讨论。

表 3-2　X.800 定义的 5 类安全服务

分　类	特 定 服 务	内　容
认证（确保通信实体就是它所声称的实体）	同等实体认证	用于逻辑连接建立和数据传输阶段，为该连接的实体的身份提供可信性保障
	数据源点认证	在无连接传输时，保证收到的信息来源是所声称的来源
访问控制		防止对资源的非授权访问，包括防止以非授权的方式使用某一资源。这种访问控制要与不同的安全策略协调一致
数据保密性（保护数据，防止非授权泄漏）	连接保密性	保护一次连接中所有用户数据
	无连接保密性	保护单个数据单元里的所有用户数据
	选择域保密性	对一次连接或单个数据单元里选定的数据部分提供加密保护
	流量保密性	保护那些可以通过观察流量而获得的信息
数据完整性（保证接收到的数据确实是授权实体发出的数据，即没有修改、插入、删除或重发）	具有恢复功能的连接完整性	为一次连接中所有用户数据提供完整性保护。检测整个数据序列内存在的修改、插入、删除或重发，且试图将其恢复
	无恢复功能的连接完整性	同具有恢复功能的连接完整性基本一致，但仅提供检测，无恢复功能
	选择域连接完整性	为一次连接中传输的单个数据单元用户数据中选定部分提供数据完整性保护，并判断选定域是否有修改、插入、删除或重发
	无连接完整性	为单个无连接数据单元提供完整性保护；判断选定域是否被修改

续表

分　类	特定服务	内　容
不可否认性(防止整个或部分通信过程中,任意一个通信实体进行否认的行为)	源点的不可否认性	证明消息由特定的一方发出
	信宿的不可否认性	证明消息被特定方收到

(1) 认证

认证服务与保证通信的真实性有关。在单条消息下,如一条警告或报警信号认证服务是向接收方保证消息来自所声称的发送方。对于正在进行的交互,如终端和主机连接,就涉及两个方面的问题:首先,在连接的初始化阶段,认证服务保证两个实体是可信的,也就是说,每个实体都是它们所声称的实体;其次,认证服务必须保证该连接不受第三方的干扰,例如,第三方能够伪装成两个合法实体中的一方,进行非授权的传输或接收。

该标准还定义了如下两个特殊的认证服务:

① 同等实体认证。用于在连接建立或数据传输阶段为连接中的同等实体提供身份确认。该服务提供这样的保证:一个实体不能实现伪装成另外一个实体或对上次连接的消息进行非授权重发的企图。

② 数据源认证。确认数据的来源,但对数据的复制或修改不提供保护。这种服务支持电子邮件这种类型的应用。在这种应用下,通信实体之间没有任何预先的交互。

(2) 访问控制

在网络安全中,访问控制对那些通过通信连接对主机和应用的访问进行限制和控制。这种保护服务可应用于对资源的各种不同类型的访问。例如,这些访问包括使用通信资源、读/写或删除信息资源或处理信息资源的操作。为此,每个试图获得访问控制权限的实体必须在经过认证或识别之后,才能获取其相应的访问控制权限。

(3) 数据保密性

保密性是防止传输的数据遭到诸如窃听、流量分析等被动攻击。对于数据传输,可以提供多层的保护。最常使用的方法是在某个时间段内对两个用户之间所传输的所有用户数据提供保护。例如,若两个系统之间建立了 TCP 连接,这种最通用的保护措施可以防止在 TCP 连接上传输用户数据的泄露。此外,还可以采用一种更特殊的保密性服务,它可以对单条消息或对单条消息中的某个特定的区域提供保护。这种特殊的保护措施与普通的保护措施相比,所使用的场合更少,而且实现起来更复杂、更昂贵。

保密性的另外一个用途是防止流量分析。它可以使攻击者观察不到消息的信源和信宿、频率、长度或通信设施上的其他流量特征。

(4) 数据完整性

与数据的保密性相比,数据完整性可以应用于消息流、单条消息或消息的选定部分。同样,最常用和直接的方法是对整个数据流提供保护。

面向连接的完整性服务可保证收到的消息和发出的消息一致,不存在消息的复制、插入、修改、倒序、重发和破坏。因此,面向连接的完整性服务能够解决消息流的修改

和拒绝服务两个问题。用于处理单条消息的无连接完整性服务通常仅防止对单条消息的修改。

另外，我们还可以区分有恢复功能的完整性服务和无恢复功能的完整性服务。因为数据完整性的破坏与主动攻击有关，所以重点在于检测而不是阻止攻击。如果检测到完整性遭到破坏，那么完整性服务能够报告这种破坏，并通过软件或人工干预的办法恢复被破坏的部分。在后面可以看到，有些安全机制可以用于恢复数据的完整性。通常，自动恢复机制是一种非常好的选择。

(5) 不可否认性

不可否认性防止发送方或接收方否认传输或接收过某条消息。因此，当消息发出后，接收方能证明消息是由所声称的发送方发出的。同样，当消息接收后，发送方能证明消息确实是由所声称的接收方收到的。

(6) 可用性服务

X.800 和 RFC 2828 对可用性的定义是：根据系统的性能说明，能够按照系统所授权的实体的要求对系统或系统资源进行访问。也就是说，当用户请求服务时，如果系统设计时能够提供这些服务，则系统是可用的。许多攻击可能导致可用性的损失或降低。可以采取一些自动防御措施(如认证、加密等)来抵御这些攻击。

X.800 将可用性看作与其他安全服务相关的性质。但是，对可用性服务进行单独说明很有意义。可用性服务能够确保系统的可用性，能够抵御由拒绝服务攻击引起的安全问题。由于它依赖于对系统资源的恰当管理和控制，因此它依赖于访问控制和其他安全服务。

2. 安全机制

表 3-3 列出了 X.800 定义的安全机制。由表可知，这些安全机制可以分成两类：一类在特定的协议层实现，另一类不属于任何的协议层或安全服务。前一类称作特定安全机制，共有 8 种；后一类称为普遍安全机制，共有 5 种。

表 3-3　X.800 定义的安全机制

	分　类	内　　容
特定安全机制(可以嵌入合适的协议层以提供一些 OSI 安全服务)	加密	运用数学算法将数据转换成不可知的形式。数据的变换和复原依赖于算法和一个或多个加密密钥
	数字签名	附加于数据单元之后的数据，它是对数据单元的密码变换，可使接收方证明数据的来源和完整性，并防止伪造
	访问控制	对资源实施访问控制的各种机制
	数据完整性	用于保证数据元或数据流的完整性的各种机制
	认证交换	通过信息交换以确保实体身份真实性的各种机制
	流量填充	在数据流空隙中插入若干位以阻止流量分析
	路由控制	能够为某些数据动态地或预定地选取路由，确保只使用物理上安全的子网络、中继站或链路
	公证	利用可信的第三方以保证数据交换的某些性质

续表

	分　类	内　　容
普遍安全机制(不属于任何OSI安全服务或协议层的机制)	可信功能度	根据某些标准(如安全策略所设立的标准)被认为是正确的,就是可信的
	安全标志	资源(可能是数据元)的标志,以指明该资源的属性
	事件检测	检测与安全相关的事件
	安全审计跟踪	收集潜在可用于安全审计的数据,以便对系统的记录和活动进行独立地观察和检查
	安全恢复	处理来自诸如事件处置与管理功能等安全机制的请求,并采取恢复措施

3. 安全服务与安全机制的关系

根据X.800的定义,安全服务与安全机制之间的关系如表3-4所示。该表详细说明了实现某种安全服务应该采用哪些安全机制。

表3-4　安全服务与安全机制之间的关系

安全服务	加密	数字签名	访问控制	数据完整性	认证交换	流量填充	路由控制	公证
对等实体认证	Y	Y			Y			
数据源认证	Y	Y						
访问控制			Y					
保密性	Y						Y	
流量保密性	Y					Y	Y	
数据完整性	Y	Y		Y				
不可否认性		Y		Y				Y
可用性				Y	Y			

注:Y表示该安全机制适合提供该种安全服务,空格表示该安全机制不适合提供该种安全服务。

4. 在OSI层中的服务配置

OSI安全体系结构最重要的贡献是总结了各种安全服务在OSI参考模型的7层中的适当配置。安全服务与协议层之间的关系如表3-5所示。

表3-5　安全服务与协议层之间的关系

安全服务	协　议　层						
	1	2	3	4	5	6	7
对等实体认证			Y	Y			Y
数据源点认证			Y	Y			Y
访问控制			Y	Y			Y

续表

安全服务	协议层						
	1	2	3	4	5	6	7
连接保密性	Y	Y	Y	Y		Y	Y
无连接保密性		Y	Y	Y		Y	Y
选择域保密性							Y
流量保密性						Y	Y
具有恢复功能的连接完整性	Y		Y				Y
不具有恢复功能的连接完整性				Y			Y
选择域有连接完整性			Y	Y			Y
无连接完整性							Y
选择域无连接完整性			Y	Y			Y
源点的不可否认							Y
信宿的不可否认							Y

注：Y 表示该服务应该在相应的层中提供，空格表示不提供。第 7 层必须提供所有的安全服务。

3.1.5　网络安全模型

一个最广泛采用的网络安全模型如图 3-4 所示。通信一方要通过 Internet 将消息传送给另一方，那么通信双方(也称为交互的主体)必须通过执行严格的通信协议共同完成消息交换。在 Internet 上，通信双方要建立一条从信源到信宿的路由，并共同使用通信协议(如 TCP/IP)建立逻辑信息通道。

从图 3-4 中可知，一个网络安全模型通常由 6 个功能实体组成，它们分别是消息的发送方(信源)、消息的接收方(信宿)、安全变换、信息通道、可信的第三方和攻击者。

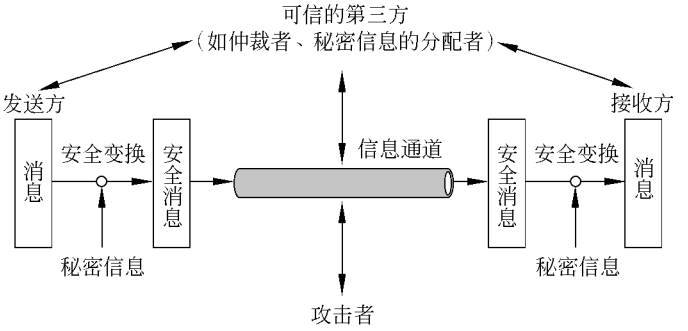

图 3-4　网络安全模型

在需要保护信息传输以防攻击者威胁消息的保密性、真实性和完整性时，就会涉及信息安全，任何用来保证信息安全的方法都包含如下两方面。

(1) 对被发送信息进行安全变换。例如对消息加密，它打乱消息使攻击者不能读懂消息，或者将基于消息的编码附于消息后，用于验证发送方的身份。

(2) 使通信双方共享某些秘密信息,而这些消息不为攻击者所知。例如加密和解密密钥,在发送端加密算法采用加密密钥对所发送的消息加密,而在接收端解密算法采用解密密钥对收到的密文解密。

图 3-4 中的安全变换就是密码学课程中所学习的各种密码算法。安全信息通道的建立可以采用密钥管理技术和后面即将讨论的 VPN 技术实现。为了实现安全传输,需要有可信的第三方。例如,第三方负责将秘密信息分配给通信双方,而对攻击者保密,或者当通信双方就关于信息传输的真实性发生争执时,由可信第三方仲裁。

网络安全模型说明,设计安全服务应包含以下 4 个方面的内容。

(1) 设计一个算法,它执行与安全相关的变换,该算法应是攻击者无法攻破的。

(2) 产生算法所使用的秘密信息。

(3) 设计分配和共享秘密信息的方法。

(4) 指明通信双方使用的协议,该协议利用安全算法和秘密信息实现安全服务。

前面讨论的安全服务和安全机制基本上遵循如图 3-4 所示的网络安全模型。但是,还有一些安全应用方案不完全符合该模型,它们遵循如图 3-5 所示的网络访问安全模型。该模型希望保护信息系统不受有害的访问。大多数读者都熟悉黑客引起的问题,黑客试图通过网络渗入可访问的系统。有时访问者可能没有恶意,只是对非法闯入计算机系统有一种满足感;或者入侵者可能是一个对公司不满的员工,想破坏公司的信息系统以发泄自己的不满;或者入侵者是一个罪犯,想利用计算机网络获取非法的利益(如获取信用卡号或进行非法的资金转账)。

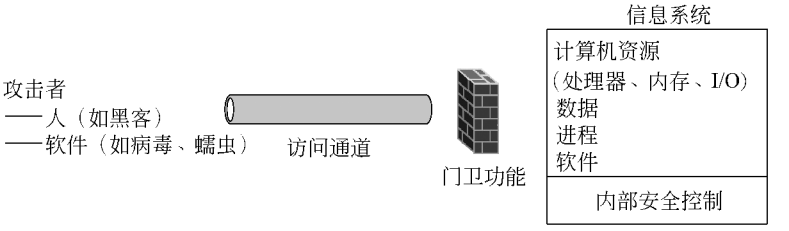

图 3-5 网络访问安全模型

3.2 网络安全边界防护技术


边界访问控制

3.2.1 边界访问控制

基于边界安全防护的前提是假定防护者与攻击者站在边界的两边,攻击者只有通过这个边界点,才能进入被攻击者的领地,实施攻击活动。因此,若能在这个边界点上部署安全措施,就可以有效地阻止攻击者的入侵。

1. 安全边界的由来

古人为保护自己领地和资源,首先会挖一条护城河,将自己与外界隔离开来。当然仅有河水还挡不住进攻者,就再修一堵围墙,如古城堡。护城河与城墙,不仅增加了攻击者

的进攻难度，还为防护者提供了充足的时间，组织人员抗击攻击者。挖的河和筑的墙就构成了人类居住点的安全边界。然而只有河和墙还不够，攻击者也可以在晚上偷偷地过河翻墙。为防止偷袭，还要在城墙上部署哨兵，及时发现外部的入侵者与内部的可疑者，并告警。这就是动态监控安全措施。

网络访问是一种对网络资源的远程访问，访问者可以是用户，也可以是攻击者；被访问的客体资源，可以是主机、数据库，也可以是服务、文件、进程。将被访问的客体资源安全隔离在一个局部的网络区域内，主体远程访问客体时必须经过的网络节点就是安全边界点，如图 3-6 所示。安全边界点可以是多个，但是不能被绕过。

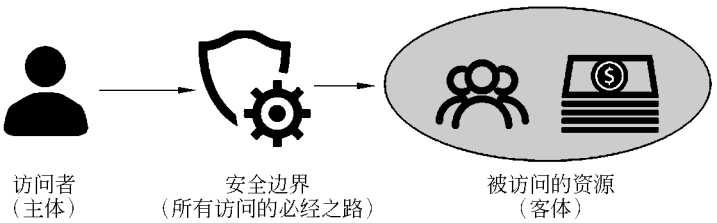

图 3-6　安全边界的概念

当然，这两种措施都是对付外部攻击者的。城堡里的人平常还要正常生活劳作，人们要进出城堡，难免会混入不法分子。这就需要第三种安全措施——信用机制，即对每个城内的人建立档案，进出城时确认其身份和权限，确认其行为是否符合管理规范。一旦发现其失信，就撤销其进出城堡的权限。

由此可见，网络边界上的安全措施有三大类：一是“挖河筑墙”的基础防护措施，二是“内外瞭望”的动态监控措施，三是对付“内鬼破坏”的安全信任机制。此外，还需要一个全局指挥的安全平台，负责管理各种安全设备，并做应急处置。

若攻击者绕过了边界，与防护者站在一边，基础防护措施就会失效，但对内的监控措施与安全信任机制仍可以发现攻击者的“异常行为”，阻止其进一步的入侵与破坏。

2. 建立安全域

将古人安全边界防护的思想用于网络上，就可以将一个单位的内部网络与外界隔离，形成一个网络区域，其内部用户业务的安全需求一致。该区域通过几个网络出口与外界相连，这几个网络出口就是进出该区域的边界点。这个网络区域就是我们要保护的内部网络，称其为“网络安全域”。

（1）网络安全域的定义

网络安全域是指同一系统内有相同的安全保护需求，相互信任，并具有相同的安全访问控制和边界控制策略的子网或网络，且域内用户共享相同的安全策略。网络安全域在广义上可理解为具有相同业务要求和安全需求的 IT 系统要素的集合。

（2）网络安全域的安全目标

通过在网络安全域的边界上部署安全措施，实现对网络安全域的安全防护。最理想的安全目标就是让攻击者“进不来”。网络安全是攻与防的对抗，随着攻击者能力的增强，安全目标可能会逐步降级。若不能阻止攻击者进入，还可以让其进来也“看不懂”，不能获

得有用信息;若攻击者看懂了,还可让其“改不了”,故不能破坏我们的数据和系统;若攻击者可以改数据,还可让其“拿不走”,故不会造成数据外泄;若攻击者可以拿走数据,还可让其“赖不掉”,通过安全审计、取证和追踪技术,我们还可抓到他。

(3) 安全域概念的由来

安全域的概念最早出自美国国家安全局(NSA)于 1998 年制定的《IATF 信息保障技术框架》,IATF 中提出了信息安全的防护是由人、技术、操作(预防、检测、相应、恢复)相互协同,而构成的深度防御体系,IATF 概括起来就是:一个核心思想,即纵深防御;三个核心要素,即人、技术、操作;四个焦点领域,也称为四个信息安全保障区域,即网络基础设施、边界接入、计算环境、支撑性基础设施,如图 3-7 所示。

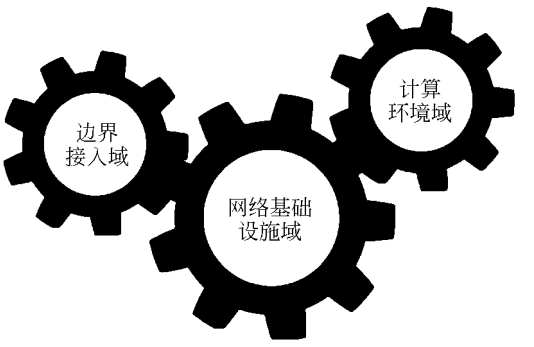

图 3-7 IATF 的信息安全保障框架

3. 边界防护体系

图 3-8 是小偷偷盗金库的场景,其中,Pt 是小偷打开多道防盗门的时间总和,Dt 是安全监控措施发现小偷需要的时间,Rt 是警察赶到金库现场捉住小偷需要的时间。当 Pt>Dt+Rt 时,警察到现场时小偷还没有打开所有的门,金子还在,防护体系是安全的。但是,若 Pt<Dt+Rt,警察到现场时,小偷已经拿到金子跑了,则防护体系就是不安全的。

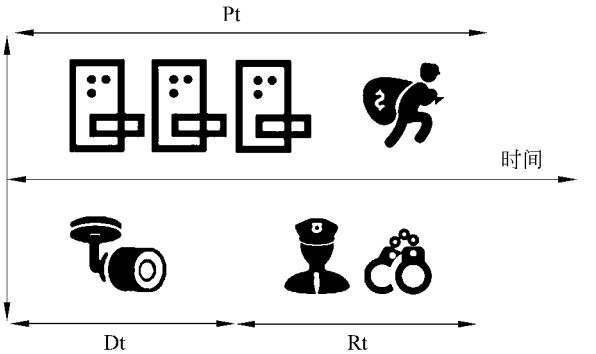

图 3-8 警察抓小偷游戏举例

因此,虽然边界防护的目标是发现并阻断入侵,但并非只实现身份识别与访问控制。网络边界上部署的防护措施,应能形成一个基于安全事件处置的立体纵深边界防护体系。