项目 1　认识网络安全

1.1　项 目 导 入

近年来，网络越来越深入人心，它是人们学习、工作、生活的便捷工具和丰富资源，但是我们应注意到，网络虽然有强大的功能，可也有易受到攻击、非常脆弱的一面。据美国 FBI 统计，美国每年因网络安全问题所造成的经济损失高达 75 亿美元，而全球平均每 20 秒钟就发生一起计算机入侵事件。在我国，每年因网络安全问题也造成了巨大的经济损失，所以网络安全问题是我们绝不能忽视的问题。据国外媒体报道，全球计算机行业协会（CompTIA）近日评出了“全球最急需的 10 项 IT 技术”，结果安全和防火墙技术排名首位。这说明安全方面的问题是全世界都急需解决的重要问题，人们在利用网络的优越性的同时，也不要忽视网络安全问题。

1.2　职业能力目标和要求

在网络高速发展的今天，人们在享受网络便捷所带来益处的同时，网络的安全也日益受到威胁。

网络攻击行为日趋复杂，各种方法相互融合，使网络安全防御变得更加困难。随着智能手机、平板电脑等无线终端的处理能力和功能通用性的提高，其功能越来越接近个人计算机，针对这些无线终端的网络攻击已经开始出现，并将进一步发展。

总之，网络安全问题变得更加错综复杂，影响将不断扩大，很难在短期内得到全面解决。

网络安全问题已经被摆在了非常重要的位置上，如果不加以防护，会严重地影响到网络的应用。学习完本项目，要达到以下职业能力目标和要求。

- 掌握网络安全的概念。
- 了解典型的网络安全事件。
- 了解网络安全的防护体系和安全模型。
- 了解网络安全体系、标准和目标。
- 掌握 Wireshark 的安装与使用。
- 掌握 TCP 和 UDP 的抓包分析。

1.3 相 关 知 识

1.3.1 网络安全的概念

1. 网络安全的重要性

（1）计算机存储和处理会涉及有关国家安全的政治、经济、军事、国防的情况及一些部门、机构、组织的机密信息或是个人的敏感信息、隐私，成为敌对势力、不法分子的攻击目标。

（2）随着计算机系统功能的日益完善和速度的不断提高，系统组成越来越复杂，系统规模越来越大，特别是随着 Internet 的迅速发展，存取控制、逻辑连接数量不断增加，软件规模空前膨胀，任何隐含的缺陷、失误都可能造成巨大的损失。

（3）人们对计算机系统的需求在不断增加，这类需求在许多方面都是不可逆转、不可替代的，而使用计算机系统的场所正在转向工业、农业、野外、天空、海上、宇宙空间、核辐射环境等，这些环境都比机房恶劣，出错率和故障的增加必将导致可靠性和安全性的降低。

（4）随着计算机系统的广泛应用，各类应用人员队伍迅速发展壮大，教育和培训却往往跟不上知识更新的需要，操作人员、编程人员和系统分析人员的失误或缺乏经验都会造成系统的安全功能不足。

（5）计算机网络安全问题涉及许多学科领域，既包括自然科学，又包括社会科学。就计算机系统的应用而言，安全技术涉及计算机技术、通信技术、存取控制技术、校验认证技术、容错技术、加密技术、防病毒技术、抗干扰技术、防泄露技术等，因此是一个非常复杂的综合问题，并且其技术、方法和措施都要随着系统应用环境的变化而不断变化。

（6）从认识论的高度看，人们往往首先关注系统功能，然后才被动地注意到系统应用的安全问题，因此广泛存在着重应用、轻安全、法律意识淡薄的问题。计算机系统的安全是相对不安全而言的，许多危险、隐患和攻击都是隐蔽的、潜在的、难以明确却又广泛存在的，这也使目前不少网络信息系统都存在先天性的安全漏洞和安全威胁，有些甚至产生了非常严重的后果。

2. 网络脆弱的原因

（1）开放的网络环境。Internet 的开放性使网络变成众矢之的，可能会遭受各方面的攻击；Internet 的国际性使网络可能遭受本地用户或远程用户、国外用户或国内用户等的攻击；Internet 的自由性没有给网络的使用者规定任何的条款，导致用户“太自由了”，可以自由地下载、自由地访问、自由地发布；Internet 使用的傻瓜性使任何人都可以方便地访问网络，基本不需要技术，只要会使用鼠标就可以上网冲浪，这也会带来很多的隐患。

（2）协议本身的缺陷。网络应用层服务存在隐患，如 IP 层通信的易欺骗性和针对 ARP 的欺骗性。

（3）操作系统的漏洞。例如，系统模型本身存在缺陷，操作系统存在 Bug，操作系统

程序配置不正确。

（4）人为因素。有些人缺乏安全意识，缺少网络应对能力。有相当一部分人认为自己的计算机中没有什么重要的东西，不会被别人攻击，存在侥幸心理，所以不认真对待安全问题，就会造成特别多的隐患。

（5）设备不安全。我们购买的国外的网络产品到底有没有留“后门”，我们根本无法得知，这无疑是最大的安全隐患。

（6）线路不安全。无论是有线介质（如双绞线、光纤），还是无线介质（如微波、红外、卫星、Wi-Fi 等），窃听其中一小段线路的信息是可以实现的，没有绝对安全的通信线路。

3. 网络安全的定义

网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭受到破坏、更改、泄露，系统能够连续、可靠、正常地运行，网络服务不中断。网络安全包含网络设备安全、网络信息安全、网络软件安全。从广义上说，凡是涉及网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论，都是网络安全的研究领域。网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。

4. 网络安全的基本要素

（1）机密性（保密性）：确保信息不暴露给未授权的实体或进程，防泄密。

（2）完整性：只有得到允许的人才能修改实体或进程，并且能够判别出实体或进程是否已被修改。完整性鉴别机制保证只有得到允许的人才能修改数据，同时应防篡改。

（3）可用性：得到授权的实体可获得服务，攻击者不能占用所有的资源而阻碍授权者的工作。用访问控制机制来阻止非授权用户进入网络。使静态信息可见，动态信息可操作。另外要防中断。

（4）可鉴别性（可审查性）：对危害国家的信息（包括加密的非法通信活动）的监视审计。控制授权范围内的信息流向及行为方式。使用授权机制来控制信息传播范围、内容，必要时能恢复密钥，实现对网络资源及信息的可控。

（5）不可抵赖性：建立有效的责任机制，防止用户否认其行为，这一点在电子商务中是极其重要的。

1.3.2　典型的网络安全事件

1999 年，中国台湾地区大学生陈盈豪制造的 CIH 病毒在 4 月 26 日发作，引起全球震荡，有 6000 多万台计算机受害。

2002 年，黑客用 DDoS 攻击影响了 13 个根 DNS 中的 8 个，作为整个 Internet 通信路标的关键系统遭到严重的破坏。

2006 年，“熊猫烧香”木马感染了我国数百万台计算机，并波及周边国家。

2007 年 2 月，“熊猫烧香”木马制作者李俊被捕。

2008 年，一个全球性的黑客组织利用 ATM 欺诈程序，在一夜之间从世界 49 个城市的银行中盗走了 900 万美元。

2009 年，韩国遭受了有史以来最猛烈的一次黑客攻击。韩国总统府、国会、国情院

和国防部等国家机关，以及金融界、媒体和防火墙企业网站遭受攻击，造成网站一度无法访问。

2010 年，维基解密网站在《纽约时报》《卫报》和《镜报》配合下，在网上公开了多达 9.2 万份的驻阿美军秘密文件，引起轩然大波。

2011 年，堪称中国互联网史上最大的泄密事件发生了。12 月中旬，CSDN 网站用户数据库被黑客在网上公开，600 余万个注册邮箱账户和与之对应的明文密码泄露。2012 年 1 月 12 日，CSDN 泄密的两名嫌疑人已被刑事拘留，其中一名为北京籍黑客，另一名为外地黑客。

2013 年 6 月 5 日，美国前中情局（CIA）职员爱德华 • 斯诺顿披露给媒体两份绝密资料。一份资料称美国国家安全局有一项代号为“棱镜”的秘密项目，要求电信巨头威瑞森公司必须每天上交数百万用户的通话记录。另一份资料更加惊人，美国国家安全局和联邦调查局通过进入微软、谷歌、苹果等九大网络巨头的服务器，监控美国公民的电子邮件、聊天记录等秘密资料。

2014 年 4 月 8 日，“地震级”网络灾难降临。在微软 Windows XP 操作系统正式停止服务同一天，互联网筑墙被划出一道致命裂口——常用于电商、支付类接口等安全性极高网站的网络安全协议 OpenSSL 被曝存在高危漏洞，众多使用 https 的网站均可能受到影响。在“心脏出血”漏洞逐渐修补结束后，由于用户很多软件中也存在该漏洞，黑客攻击目标存在从服务器转向客户端的可能性，下一步有可能出现“血崩”式攻击。

2015 年，我国国家旅游局系统漏洞致 6 套系统沦陷，涉及全国 6000 万客户，包括超过 6 万个旅行社账户密码、百万名导游信息；并且攻击者可利用该漏洞进行审核、拒签等操作。

2016 年 10 月 22 日，美国网络中介服务商遭到大规模的网络攻击，包括 Twitter、Spotify、Visa、《华尔街日报》官网等在内的上百家网站。大半个美国的网络瘫痪，来自用户的网页访问请求无法被正确接收和解析，从而导致访问错误，这是迄今为止美国最严重的集体断网事件。

2017 年 5 月 12 日，WannaCry 勒索病毒在全球爆发，以类似于蠕虫病毒的方式传播，攻击主机并加密主机上存储的文件，然后要求以比特币的形式支付赎金。WannaCry 爆发后，至少 150 个国家的 30 万名用户中招，造成损失达 80 亿美元。

2018 年，某黑客攻击事件的嫌疑人被指控攻击了美国 144 所大学、其他 21 个国家的 176 所大学、47 家私营公司，以及联合国、美国联邦能源监管委员会以及夏威夷州和印第安纳州等其他目标。美国司法部表示，黑客窃取了 31TB 的数据以及预估价值为 30 亿美元的知识产权信息。在黑客攻击的 10 万个账户中，他们能够获得大约 8000 个凭证。

2019 年 1 月，超 2 亿名中国求职者简历疑遭泄露，数据“裸奔”将近一周。HackenProof 的网络安全人员 Bob Diachenko 在推特上爆料称，一个包含 2.02 亿名中国求职者简历信息的数据库被泄露，这被称为中国有史以来最大的数据曝光之一。

2020 年 5 月 5 日，委内瑞拉国家电网干线遭到攻击，造成全国大面积停电。国家电网的 765 干线遭到攻击，除首都加拉加斯外，全国 11 个州府均发生停电。

2021 年 3 月 2 日，微软发布了 Microsoft Exchange Server 的安全更新公告，其中包含多个 Exchange Server 严重安全漏洞，危害等级为“高危”。未经身份验证的攻击者能够通

过这些漏洞来构造 HTTP 请求，扫描内网并通过 Exchange Server 进行身份验证。

1.3.3　信息安全的发展历程

1. 通信保密阶段

通信保密阶段始于 20 世纪 40 年代，又称通信安全时代，重点是通过密码技术解决通信保密问题，保证数据的保密性和完整性。主要安全威胁是搭线窃听、密码学分析。主要保护措施是加密技术。主要标志是 1949 年 Shannon 发表的《保密通信的信息理论》、1997 年美国国家标准局公布的数据加密标准（DES）、1976 年 Diffie 和 Hellman 在 *New Directions in Cryptography* 一文中提出的公钥密码体制。

2. 计算机安全阶段

计算机安全阶段始于 20 世纪 70 年代，重点是确保计算机系统中硬件、软件及正在处理、存储、传输信息的机密性、完整性和可用性。主要安全威胁扩展到非法访问、恶意代码、脆弱口令等。主要保护措施是安全操作系统设计技术。主要标志是 1985 年美国国防部公布的《可信计算机系统评估准则》（TCSEC，橘皮书），它将操作系统的安全级别分为 4 类和 7 个级别（D、C1、C2、B1、B2、B3、A），后补充红皮书 TNI（1987 年）和紫皮书 TDI（1991 年）等，构成彩虹（rainbow）系列。

3. 信息技术安全阶段

信息技术安全阶段始于 20 世纪 80 年代，重点需要保护信息，确保信息在存储、处理、传输过程中及信息系统不被破坏，确保合法用户的服务和限制非授权用户的服务，以及防范必要的防御攻击。强调信息的保密性、完整性、可控性、可用性等。主要安全威胁发展到网络入侵、病毒破坏、信息对抗的攻击等。主要保护措施包括防火墙、防病毒软件、漏洞扫描、入侵检测、PKI、VPN、安全管理等。主要标志是提出了新的安全评估准则 CC（ISO 15408、GB/T 18336）。

4. 信息保障阶段

信息保障阶段始于 20 世纪 90 年代后期，重点放在保障国家信息基础设施不被破坏，确保信息基础设施在受到攻击的前提下能够最大限度地发挥作用。强调系统的鲁棒性和容灾特性。主要安全威胁发展到有组织地对集团、国家的信息基础设施进行攻击等。主要保护措施是灾备技术、建设面向网络恐怖与网络犯罪的国际法律秩序，以及应对与国际联动的网络安全事件的应急响应技术。主要标志是美国推出的“保护美国计算机空间”（PDD-63）的体系框架。

1.3.4　网络安全所涉及的内容

1. 物理安全

网络的物理安全是整个网络系统安全的前提。在网络工程建设中，由于网络系统属于弱电工程，耐压值很低。因此，在网络工程的设计和施工中，必须优先考虑保护人和网络设备不受电、火灾和雷击的侵害；其次要考虑布线系统与照明电线、动力电线、通信线路、暖气管道及冷热空气管道之间的距离；另外也要考虑布线系统和绝缘线、裸体线以及接地

与焊接的安全；还必须建设防雷系统，防雷系统不仅要考虑建筑物防雷，也要考虑计算机及其他弱电耐压设备的防雷。总体来说，物理安全的风险主要有：地震、水灾、火灾等，电源故障，人为操作失误或错误，设备被盗、被毁，电磁干扰，线路截获。不仅要注意这些安全隐患，同时还要尽量避免网络的物理安全风险。

2. 网络安全

网络安全是指网络拓扑结构设计会影响到网络系统的安全性。假如在外网和内部网络进行通信时，内部网络的安全就会受到威胁，同时也会影响在同一网络上的许多其他系统。通过网络传播，还会影响到联上 Internet/Intranet 的其他网络；还可能涉及法律、金融等安全敏感领域。因此，在设计时有必要将公开服务器（Web、DNS、E-mail 等）和外网及内部其他业务网络进行必要的隔离，避免网络结构信息外泄；同时还要对外网的服务请求加以过滤，只允许正常通信的数据包到达相应主机，其他的请求服务在到达主机之前就应该遭到拒绝。

3. 系统安全

系统安全是指整个网络操作系统和网络硬件平台是否可靠且值得信任。恐怕没有绝对安全的操作系统可以选择，无论是 Microsoft 的 Windows 系统，还是其他任何商用的 UNIX 操作系统，其开发厂商必须有其 Back-Door（“后门”）。因此，我们可以得出如下结论：没有安全的操作系统。不同的用户应从不同的方面对其网络做详尽的分析，选择安全性尽可能高的操作系统。因此，不但要选用尽可能可靠的操作系统和硬件平台，并对操作系统进行安全配置；而且必须加强登录过程的认证（特别是在到达服务器主机之前的认证），确保用户的合法性；还应该严格限制登录者的操作权限，将其完成的操作限制在最小的范围内。

4. 应用安全

应用安全涉及很多方面，以 Internet 上应用最为广泛的 E-mail 系统来说，其解决方案有 SendMail、Netscape Messaging Server、SoftwareCom Post.Office、Lotus Notes、Exchange Server、SUN CIMS 等 20 多种。其安全手段涉及 LDAP、DES、RSA 等各种方式。应用系统是不断发展且应用类型是不断增加的。在应用系统的安全性上，主要考虑尽可能建立安全的系统平台，而且通过专业的安全工具不断发现漏洞、修补漏洞，提高系统的安全性。

信息的安全性涉及机密信息泄露、未经授权的访问、破坏信息的完整性和可用性、假冒等。某些网络系统中会涉及很多机密信息，如果一些重要信息遭到窃取或破坏，它的经济、社会和政治影响将是很严重的。因此，必须对使用计算机的用户进行身份认证；必须对重要信息的通信进行授权，传输必须加密。采用多层次的访问控制与权限控制手段，实现对数据的安全保护；采用加密技术，保证网上传输信息（包括管理员口令与账户、上传信息等）的机密性与完整性。

5. 管理安全

管理安全是网络安全中重要的组成部分。责权不明、安全管理制度不健全及缺乏可操作性等都可能引起管理安全的风险。例如，当网络出现攻击行为或网络受到其他一些安

全威胁时（如内部人员的违规操作等），无法进行实时的检测、监控、报告与预警；同时，当事故发生后，也无法提供黑客攻击行为的追踪线索及破案依据，即缺乏对网络的可控性与可审查性。这就要求我们必须对站点的访问活动进行多层次的记录，确保能及时发现非法入侵行为。

建立全新的网络安全机制，必须深刻理解网络并能提供直接的解决方案，因此，最可行的做法是将制定健全的管理制度和严格管理相结合。保障网络的安全运行，使其成为一个具有良好的安全性、可扩充性和易管理性的信息网络便成为首要任务。一旦上述的安全隐患成为事实，对整个网络所造成的损失都是难以估计的。因此，网络的安全建设是网络建设过程中重要的一环。

1.3.5　网络安全防护体系

1. 网络安全的威胁

所谓网络安全的威胁，是指某个实体（人、事件、程序等）对某一资源的机密性、完整性、可用性可能造成的危害。这些可能出现的危害，是某些别有用心的人通过采取一定的攻击手段来实现的。

网络安全的主要威胁有非授权访问、冒充合法用户、破坏数据完整性、干扰系统正常运行、利用网络传播病毒、线路窃听等。

2. 网络安全的防护体系

网络安全防护体系是由安全操作系统、应用系统、防火墙、网络监控、安全扫描、通信加密、网络反病毒等多个安全组件共同组成的，每个组件只能完成其中的部分功能。

3. 数据保密

为什么需要做好数据保密工作呢？请看下面的案例。

某网游公司因核心开发人员外泄相关技术及营业秘密而向法院提出诉讼，要求赔偿65亿韩元的损失费。该网游公司很多项目也只能从零开始。

某军工科研所的多份保密资料和文件落入境外情报机关之手。间谍发送伪造的官方邮件并暗藏木马程序，在工作人员单击后就迅速控制了该计算机，盗取了绝密资料。

某央企因机器中病毒，单位办公系统中的红头文件被窃取并发往中国台湾地区的途中被网监部门截获，被国资委多次点名批评。

据专业机构调查，数据泄密造成的经济损失每年可达百亿元，并呈逐年上升的态势。

从上面的案例中不难看出，数据是各行各业的核心，如果各行各业不对数据做保密措施，很容易造成数据外泄，从而造成重大损失，那么如何做好数据保密工作？下面介绍数据信息保密性安全规范。

数据信息保密性安全规范用于保障重要业务数据信息的安全传递与处理应用，确保数据信息能够被安全、方便、透明地使用。为此，业务平台应采用加密等安全措施完成数据信息保密性工作。

- 应采取加密措施实现重要业务数据信息传输的保密性。
- 应采取加密措施实现重要业务数据信息存储的保密性。

加密安全措施主要分为密码安全和密钥安全。

1）密码安全

密码的使用应该遵循以下原则。

- 不能将密码写下来，不能通过电子邮件传输。
- 不能使用默认设置的密码。
- 不能将密码告诉别人。
- 如果系统的密码泄露了，必须立即更改。
- 密码要以加密形式保存，加密算法强度要高，加密算法要不可逆。
- 系统应该强制指定密码的使用策略，包括密码的最短有效期、最长有效期、最短长度、复杂性等。
- 如果需要特殊用户的口令（如 UNIX 下的 Oracle），要禁止通过该用户进行交互式登录。
- 在要求较高的情况下可以使用强度更高的认证机制，如双因素认证。
- 要定时运行密码检查器来检查口令强度，对于保存机密和绝密信息的系统，应该每周检查一次；对于其他系统，应该每月检查一次。

2）密钥安全

密钥管理对于有效使用密码技术至关重要。密钥的丢失和泄露可能会损害数据信息的保密性、重要性和完整性。因此，应采取加密技术等措施来有效保护密钥，以免密钥被非法修改和破坏；还应对生成、存储和归档保存密钥的设备采取物理保护。此外，必须使用经过业务平台部门批准的加密机制进行密钥分发，并记录密钥的分发过程，以便审计跟踪，统一对密钥、证书进行管理。

密钥的管理应该基于以下流程。

① 密钥产生：为不同的密码系统和不同的应用生成密钥。

② 密钥证书：生成并获取密钥证书。

③ 密钥分发：向目标用户分发密钥，包括在收到密钥时如何将之激活。

④ 密钥存储：为当前或近期使用的密钥或备份密钥提供安全存储，包括授权用户如何访问密钥。

⑤ 密钥变更：包括密钥变更时机及变更规则，处置被泄露的密钥。

⑥ 密钥撤销：包括如何收回或者去激活密钥。

⑦ 密钥恢复：作为业务平台连续性管理的一部分，对丢失或破坏的密钥进行恢复。

⑧ 密钥归档：归档密钥，以用于归档或备份数据信息。

⑨ 密钥销毁：密钥销毁将删除该密钥管理下数据信息客体的所有记录，并且无法恢复。因此，在密钥销毁前，应确认不再需要用此密钥保护的数据信息。

4. 访问控制技术

访问控制技术可防止对任何资源进行未授权的访问，从而保证在合法的范围内使用计算机系统。这是指以用户身份及其所归属的某项定义组来限制用户对某些信息项的访问，或限制对某些控制功能使用的一种技术，如 UniNAC 网络准入控制系统的原理就是基于此技术。访问控制技术通常用于系统管理员控制用户对服务器、目录、文件等网络资源的访问。

访问控制是系统保密性、完整性、可用性和合法使用性的重要基础，是网络安全防护

和资源保护的关键策略之一，也是主体依据某些控制策略或权限对客体本身或其资源进行的不同授权访问。

访问控制包括以下三个要素。

（1）主体（subject）。主体是指提出访问资源的具体请求方。主体是某一操作动作的发起者，但不一定是动作的执行者，可以是某一用户，也可以是用户启动的进程、服务和设备等。

（2）客体（object）。客体是指被访问资源的实体。所有可以被操作的信息、资源、对象都可以是客体。客体可以是信息、文件、记录等集合体，也可以是网络上硬件设施、无线通信中的终端，甚至可以包含另外一个客体。

（3）控制策略。控制策略是指主体对客体的相关访问规则集合，即属性集合。访问策略体现了一种授权行为，也是客体对主体某些操作行为的默认。

5. 网络监控

网络监控是针对局域网内的计算机进行监视和控制，如美国 Emulex 公司针对内部的计算机互联网活动（上网监控）、非上网相关的内部行为与资产等过程实行的监控管理（内网监控）。互联网的飞速发展使互联网的使用越来越普遍，网络和互联网不仅成为企业内部的沟通桥梁，也是企业和外部进行各类业务往来的重要管道。

6. 病毒防护

病毒防护主要从以下几个方面着手。

（1）进行数据备份，特别是非常重要的数据及文件，避免被病毒入侵后无法恢复。

（2）对于新购置的计算机、硬盘、软件等，先用查毒软件检测后才可使用。

（3）尽量避免在无防毒软件的机器上或公用机器上使用可移动磁盘，以免感染病毒。

（4）对计算机的使用权限进行严格控制，禁止来历不明的人和软件进入系统。

（5）采用一套公认最好的病毒查杀软件，以便在对文件和磁盘操作时进行实时监控，及时控制病毒的入侵，并及时可靠地升级反病毒产品。

1.3.6　网络安全模型

网络安全模型是动态网络安全过程的抽象描述。通过对安全模型的研究，了解安全动态过程的构成因素，是构建合理而实用的安全策略的前提之一。为了达到安全防范的目标，需要合理的网络安全模型来指导网络安全工作的部署和管理。目前，在网络安全领域存在较多的网络安全模型，下面介绍常见的 PDRR 安全模型和 PPDR 安全模型。

1. PDRR 安全模型

PDRR 安全模型是美国国防部提出的常见安全模型，概括了网络安全的整个环节，即防护（protect）、检测（detect）、响应（react）、恢复（restore），这 4 个部分构成了一个动态的信息安全周期，如图 1-1 所示。

2. PPDR 安全模型

PPDR 安全模型是美国国际互联网安全系统公司提出的可适应性网络安全模型，它包括策略（policy）、保护（protection）、检测（detection）、响应（response）4 个部分。

PPDR 安全模型如图 1-2 所示。

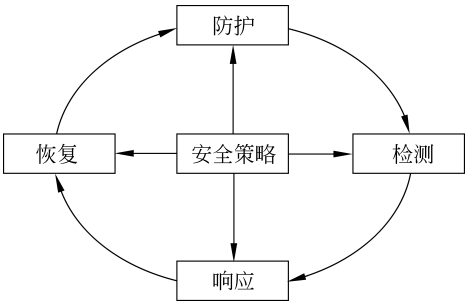

图 1-1　PDRR 安全模型

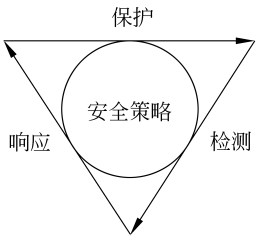

图 1-2　PPDR 安全模型

1.3.7　网络安全体系

CNNIC 报告显示，截至 2020 年 12 月，中国网民规模达 9.89 亿人（手机网民规模达 9.86 亿人），互联网普及率达 70.4%。可以说，中国目前已经成为当之无愧的世界第一网络大国。几乎每一天，互联网与移动端的 App 上会出现大量包含着虚假、谩骂、攻击、暴力的信息，甚至还包括一些鼓吹极端主义甚至是恐怖主义的信息，这些都需要相关部门不断地进行打击。

安全是发展的前提，发展是安全的保障，安全和发展要同步推进。值得警醒的是，我国的网络安全现状仍然严峻。公安部发布的信息显示，2020 年全国共破获电信网络诈骗案件 32.2 万起，抓获犯罪嫌疑人 36.1 万名，止付、冻结涉案资金 2720 余亿元。构建一个健全的网络安全体系，需要对网络安全风险进行全面评估，并制定合理的安全策略，采取有效的安全措施，才能从根本上保证网络的安全。

1.3.8　网络安全标准

1. TCSEC

《可信计算机系统评估准则》（TCSEC）由美国国防科学委员会提出，并于 1985 年 12 月由美国国防部公布。它将安全分为 4 个方面，即安全政策、可说明性、安全保障和文档。TCSEC 将以上 4 个方面分为 7 个安全级别，按安全程度从低到高依次是 D、C1、C2、B1、B2、B3、A，如表 1-1 所示。

表 1-1 《可信计算机系统评估准则》

类　别	级　别	名　　称	主 要 特 征
D	D	低级保护	保护措施很少，没有安全功能
C	C1	自主安全保护	自主存储控制
	C2	受控存储控制	单独的可查性，安全标识
B	B1	标识的安全保护	强调存取控制，安全标识
	B2	结构化保护	面向安全的体系结构 较好的抗渗透能力
	B3	安全区域	存取监控、高抗渗透能力
A	A	验证设计	形式化的最高级描述、验证和隐秘通道分析