Network Security Technology
网络安全技术

第十一章 网络安全发展与未来

主讲：李强

E-mail: dr_qiangli@163.com

Office：明实楼（3号楼）A410

本章内容安排

- 12.1 网络安全现状与挑战
- 12.2 网络安全的发展趋势
- 12.3 网络安全与法律法规
- 12.4 小结

12.1 网络安全现状与挑战

- 12.1.1 网络安全现状
- 12.1.2 网络安全面临的新挑战

12.1.1 网络安全现状

- 过去的数年中，互联网遭受了一波又一波的攻击——传播速度超快、影响范围广泛、造成损失巨大的恶意攻击不断出现。

网络安全现状(2)

- 典型攻击：
  - Melissa(1999) 和 LoveLetter(2000)
  - 红色代码(2001)
  - 尼姆达(2001)
  - 熊猫烧香(2006-2007)
  - 分布式拒绝服务攻击(2000-2007)
  - 远程控制特洛伊木马后门(1998-2007)

Melissa和LoveLetter

- 1999年3月爆发的Melissa 病毒和2000年5月爆发的LoveLetter 病毒非常相似，都是利用Outlook电子邮件附件迅速传播。
- Melissa是MicrosoftWord宏病毒，LoveLetter则是VBScript病毒，其恶意代码都是利用Microsoft公司开发的Script语言缺陷进行攻击，因此二者非常相似。

Melissa和LoveLetter(2)

- 用户一旦在Microsoft Outlook里打开这个邮件，系统就会自动复制恶意代码并向地址簿中的所有邮件地址发送带有病毒的邮件。
- 很快，由于Outlook用户数目众多，其病毒又可以很容易地被复制，很快许多公司的邮件服务器就被洪水般的垃圾邮件塞满而中断了服务。

Melissa和LoveLetter(3)

- **Melissa 和 LoveLetter 的爆发可以说是信息安全的唤醒电话，它引起了当时人们对信息安全现状的深思，并无形中对信息安全的设施和人才队伍的发展起了很大的刺激作用:**
  - Melissa 和 LoveLetter 刺激了企业和公司对网络安全的投资，尤其是对防病毒方面的投入；
  - 许多公司对网络蠕虫病毒的应急响应表现出的无能促使了专业网络安全应急响应小组的发展与壮大。

红色代码

- **2001年7月的某天，全球的IDS几乎同时报告遭到未知蠕虫攻击。**
- **信息安全组织和专业人士纷纷迅速行动起来，使用蜜罐(honeypots)技术从因特网上捕获数据包进行分析，最终发现这是一利用微软IIS缓冲溢出漏洞进行感染的变种蠕虫。**

红色代码(2)

- 其实这一安全漏洞早在一个月以前就已经被**eEye Digital Security**发现，微软也发布了相应的补丁程序，但是却很少有组织和企业的网络引起了足够的重视，下载并安装了该补丁。

红色代码(3)

- 在红色代码首次爆发的短短9个小时内，这一蠕虫迅速感染了250，000台服务器，其速度和深入范围之广也迅速引起了全球媒体的注意。
- 最初发现的红色代码蠕虫还只是篡改英文站点的主页，显示“**Welcome to http://www.worm.com! Hacked by Chinese!**”等信息。

红色代码(4)

- 随后的红色代码蠕虫便如同洪水般在互联网上泛滥，发动DoS（拒绝服务）攻击以及格式化目标系统硬盘，并会在每月20日～28日对白宫的WWW站点的IP地址发动DoS攻击，使白宫的WWW站点不得不全部更改自己的IP地址。
- 之后，红色代码又不断的变种，其破坏力也更强，在红色代码II肆虐时，有近2万服务器/500万网站被感染。红色代码就是凭着这样过硬的“本领”，在我们的1997至2002年网络攻击之最的民意调查中红色代码与Nimda以占选票44%的绝对优势位居榜首。

红色代码的启示

- 只要注意及时更新补丁和修复程序，对于一般的蠕虫传播是完全可以避免的。
- 在网络遭到攻击时，为进行进一步的分析，使用蜜罐是一种非常行之有效的方法。
- 红色代码猛攻白宫之所以被成功扼制，是因为**ISP**们及时将路由表中所有白宫的**IP**地址都清空了，在这一蠕虫代码企图阻塞网络之前，在因特网边界就已被丢弃。另外，白宫网站也立即更改了所有服务器的**IP**地址。

尼姆达

- 尼姆达（**Nidma**）是在 **9.11** 恐怖袭击后整整一个星期后出现的。地区之间的冲突和摩擦常会导致双方黑客互相实施攻击。
- 当时传言尼姆达病毒的散布为了试探美国对网络恐怖袭击的快速反应能力，一些安全专家甚至喊出了“我们现在急需制定另一个‘曼哈顿计划’，以随时应对网络恐怖主义”的口号，由此可见尼姆达在当时给人们造成的恐慌。

尼姆达(2)

- 尼姆达病毒是在早上9：08发现的，它明显地比红码病毒更快、更具有摧毁功能，半小时之内就传遍了整个世界。随后在全球各地侵袭了830万部电脑，总共造成将近10亿美元的经济损失。

尼姆达(3)

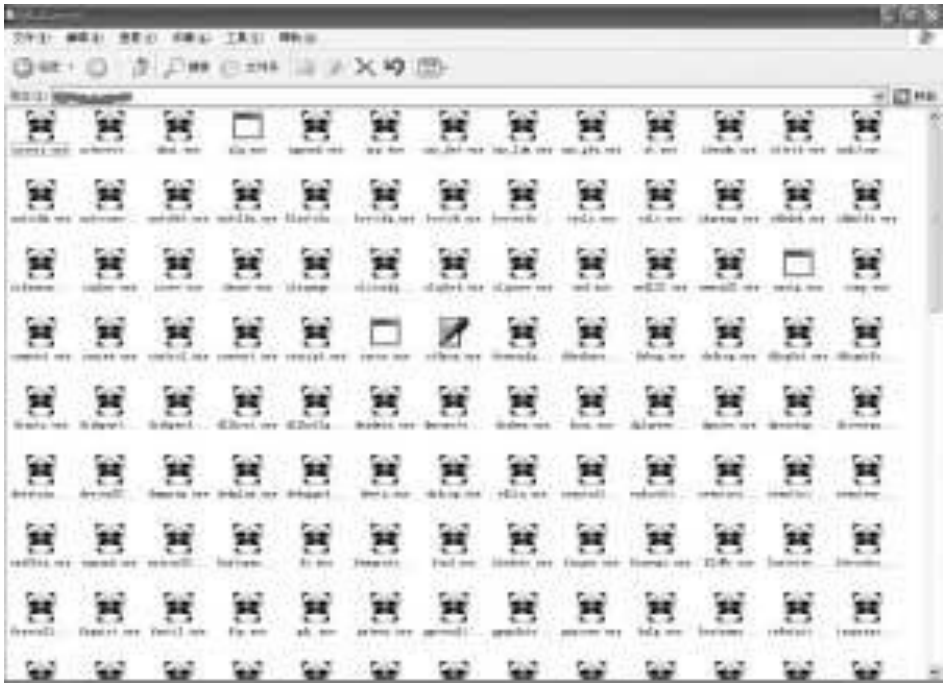
- 同“红色代码”一样，“尼姆达”也是通过网络对**Windows**操作系统进行感染的一种蠕虫型病毒。但是它与以前所有的网络蠕虫的最大不同之处在于，“尼姆达”通过多种不同的途径进行传播，而且感染多种**Windows**操作系统。
- **"红色代码"只能够利用IIS的漏洞来感染系统，而"尼姆达"则利用了至少四种微软产品的漏洞来进行传播:**
  - 在 IIS 中的缺陷
  - 浏览器的JavaScript缺陷
  - 利用 Outlook 电子邮件客户端的一个安全缺陷乱发邮件
  - 利用硬盘共享的一个缺陷，将guest用户击活并非法提升为管理员。
- **在一个系统遭到感染后，Nimda又会立即寻找突破口，迅速感染周边的系统，并占用大部分的网络带宽。**

尼姆达的启示

- 对网络攻击事件的紧急响应能力以及和安全专家们建立良好的关系是非常重要的。
- 为阻断恶意蠕虫的传播，往往需要在和广域网的接口之间设置过滤器，或者干脆暂时断开和广域网的连接。
- 在电子邮件客户端和网络浏览器中禁止任意脚本的执行对网络安全性来说是很关键的。

熊猫烧香

- “熊猫烧香”是一个由**Delphi**工具编写的蠕虫，终止大量的反病毒软件和防火墙软件进程。病毒会删除扩展名为**gho**的文件，使用户无法使用**ghost**软件恢复操作系统。



熊猫烧香(2)

- “熊猫烧香”病毒利用的传播方式囊括了漏洞攻击、感染文件、移动存储介质、局域网传播、网页浏览、社会工程学欺骗等。
- 它能感染系统的**.exe**、**.com**、**.pif**、**.src**、**.html**、**.asp**文件，添加病毒网址，导致用户一打开这些网页文件，**IE**就会自动连接到指定的病毒网址中下载病毒。
- 在硬盘各个分区下生成文件**autorun.inf**和**setup.exe**，可以通过**U**盘和移动硬盘等方式进行传播，并且利用**Windows**系统的自动播放功能来运行，搜索硬盘中的**.exe**可执行文件并感染，感染后的文件图标变成“熊猫烧香”图案。
- 它还能终止大量的反病毒软件和防火墙软件进程。病毒会删除扩展名为**.gho**的文件，使用户的系统备份文件丢失。
- 具有极强的变种能力，仅两个多月的时间，变种就多达**70**余种。

分布式拒绝服务攻击

- 在新千年的到来之季，信息安全领域的人们都以为由于存在千年虫的问题，在信息网络安全领域中应该暂时还不会出现什么涟波。
- 然而， 一月之后却来了一场谁也意想不到的洪潮：在全球知名网站雅虎第一个宣告因为遭受分布式拒绝服务攻击而彻底崩溃后， 紧接着 **Amazon.com**， **CNN**， **ZDNet**， **Buy.com**， **Excite** 和 **eBay** 等其它七大知名网站也几乎在同一时间彻底崩溃。这无疑又一次敲响了互联网的警钟。

分布式拒绝服务攻击(2)

- DDoS 的闪击攻击使人们认识到互联网远比他们想象得更加脆弱，分布式拒绝服务攻击产生的影响也远比他们原来想象中的要大得多。利用互联网上大量的机器进行DDoS，分布式扫描和分布式口令破解等，一个攻击者能够达到意想不到的强大效果。
- DDoS攻击从2000年开始，就一直是互联网安全的致命危害，就在2006年，即使是有着上千台服务器的百度在遭受DDoS攻击时也难逃一劫，致命服务停止半个小时。

分布式拒绝服务攻击的启示

- **从雅虎遭到强大的DDoS攻击中得到的启示：**
  - 要阻止这种攻击关键是网络出口反欺骗过滤器的功能是否强大。也就是说如果你的Web服务器收到的数据包的源IP地址是伪造的话，你的边界路由器或防火墙必须能够识别出来并将其丢弃。
  - 网络安全事件响应小组们认识到他们必须和他们的ISP共同去阻止数据包的flood攻击。如果失去ISP的支持，即使防火墙功能再强大，网络出口的带宽仍旧可能被全部占用。
  - 不幸地，DDoS攻击即使在目前也仍旧是互联网面临的主要威胁，当然这主要是因为ISP在配合阻断DDoS攻击上速度太慢引起的，无疑使事件应急响应的效果大打折扣。

远程控制特洛伊木马后门

- 在1998年7月，黑客 Cult of the Dead Cow（cDc）推出的强大后门制造工具 Back Orifice（或称BO）使庞大的网络系统轻而易举地陷入了瘫痪之中。安装BO主要目的是：黑客通过网络远程入侵并控制受攻击的Win95系统，从而使受侵机器“言听计从”。
- 如果仅仅从功能上讲，Back Orifice完全可以和市场上最流行的商业远程控制软件相媲美。因此，许多人干脆拿它来当作远程控制软件来进行合法的网络管理。

远程控制特洛伊木马后门(2)

- **BO的成功后来也迅速地带动和产生了许多类似的远程控制工具，像 SubSeven，NetBus， Hack-a-Tack 和 Back Orifice 2000 (BO2K)等。**
- 木马技术不发展，发生了众多功能强大的软件，灰鸽子就是其典型代表。
- 这些攻击工具和方法甚至一直保留到现在，作为黑客继续开发新的和更加强大的特洛伊木马后门，以避开检测，绕过个人防火墙和伪装自己的设计思想基础。

“敲诈”型木马

- 木马从最初的仅仅获取信息，转变为专门以营利为目的。如盗取银行账号信息掠夺金钱、盗取网游账号倒卖等。
- 此外，还出现了一种新型功能的木马——“敲诈”型木马，它的主要特点是试图隐藏用户文档，让用户误以为文件丢失，木马乘机以帮助用户恢复数据的名义，要求用户向指定的银行账户内汇入定额款项。国内已出现不少这类专门对用户进行“敲诈勒索”的木马。

12.1.2 网络安全面临的新挑战

- 针对网络安全的挑战更是层出不穷，下面列出了目前网络安全面临的几大问题：
  - 更多网络犯罪直接以经济利益为目的
  - 拒绝服务攻击泛滥
  - 垃圾邮件与反垃圾邮件之间的斗争愈演愈烈
  - 恶意软件横行，web攻击频发
  - 对非PC设备（例如手机）的威胁增加

更多网络犯罪直接以经济利益为目的

- 最吸引国人眼球的应该是腾讯，2004年两次QQ大规模无法使用，尤其是此后影影绰绰的勒索传言，有人惊呼：中国网络恐怖主义诞生了。
- 传言毕竟只是传言，相比之下，一群巴西网络银行骇客的落网或许更能让你真切感受到网络犯罪离你多近，仅仅一年多的时间，他们从银行中窃取了大约2758万美元……
- 依稀能看见商业间谍、军事间谍或者是一群仅仅为了金钱彻夜不眠地进行攻击攻击再攻击的人们……勿庸置疑，这些事实仅仅是冰山一角。技术进步加上道德感的缺失，黑客们开始看清自己要的东西。

更多网络犯罪直接以经济利益为目的

- 经济利益毫无疑问已经成为病毒和木马制造者最大的驱动力。病毒制造者已经不再是以炫耀自己的技术为目的，也不再是单打独斗，而是结成了团伙，制造、传播、盗窃信息、第三方平台销赃、洗钱，分工明确，形成了一整条黑色产业链。

令全国网民闻“猫”色变的熊猫烧香病毒

熊猫烧香背后的巨大利润

- 据湖北省公安厅介绍，李俊以自己出售和由他人代卖的方式，每次要价**500～1000**元不等，将该病毒销售给**120**余人，非法获利**10**万余元。
- 经病毒购买者进一步传播，该病毒的各种变种在网上大面积传播，通过入侵可盗取证券、银行、信用卡的账号，其非法所得通过购买网络货币，完成“漂白”的洗钱过程；而通过病毒盗取的游戏账号、虚拟钱币，则通过中间批发商直接变现，再进入传统销售渠道。另一部分非法收入则是通过入侵网站，勒索网站收取佣金。
- 据湖北省公安厅估算，被“熊猫烧香”病毒控制的“网络僵尸”数以百万计，按其访问流量付费的网站，一年下来可为整个“烧香”入侵之后一整套“推广”网络累计获利数千万元。

职业黑客的网络时代

- “300元，两天之内破解一个电子邮箱；1000元，攻击一次或一个服务器……”
- 这个价钱是一个职业黑客开出的价钱。随着网络技术不断进步、网络经济的繁荣，黑客这一概念，已开始从原先的对于不断追求网络技术的人群转变成了以提供相应服务，获得经济利益的职业人群。

拒绝服务攻击泛滥

- 我们所看到的拒绝服务已经不仅仅是一台或几台机器发起的了，攻击者们控制成百上千的僵尸电脑(Zombie)，甚至由蠕虫来进行传播和攻击。DoS凭借它的便捷有效，吸引了大量热衷者，互联网上因此充斥这类垃圾流量。
- 除了常规的拒绝服务攻击、DoS讹诈之外，我们面临的各种有意无意的DoS越来越多，例如，邮件蠕虫发送邮件，产生的大量DNS查询报文，对DNS服务器产生事实上的DoS等等，事件日渐频发。

垃圾邮件与反垃圾邮件之间的斗争愈演愈烈

- 网络服务商和邮件运营商们纷纷提出了自己的技术方案：雅虎的“**DomainKeys**”，它利用公/私钥加密技术为每个电子邮件地址生成一个唯一的签名，实现对邮件发送者的身份验证；微软的“电子邮票”有偿发送邮件方案；而**AOL**正在试验一种名为“**Sender permitted From**”（**SPF**）的新电子邮件协议，禁止通过修改域名系统（**DNS**）伪造电子邮件地址；等等……
- 但垃圾邮件发送者并不是坐以待毙，而是主动出击，继续他们没完没了的“发送事业”。

垃圾邮件与反垃圾邮件之间的斗争愈演愈烈(2)

- 道高一尺，魔高一丈，世界永远在此消彼长中发展。**2008**年，垃圾邮件事件依然在以惊人的速度增长，垃圾邮件厂商与反垃圾邮件厂商究竟是一起赚钱，或者能拼出个高下，尚无从得知，斗争依然热闹非凡。

恶意代码横行，web攻击频发

- MYDOOM/Netsky/Bagle/震荡波/SCO炸弹/QQ尾巴/MSN射手等一系列新病毒和蠕虫的出现，造成了巨大的经济损失。而且病毒和蠕虫的多样化明显，甚至蠕虫编写组织开始相互对抗，频繁推出新版本。
- 根据调查，平均每台家用PC有28个间谍软件，它们已经被更多的公司及个人利用，其目的也从初期简单收户信息演化为可能收集密码、帐号等资料。
- 至于web攻击，各大政府的门户网站成为别有用心的攻击者的首选目标，2008年政府网站被篡改的事件比例大幅增加。而网络钓鱼方面，且不谈多年受其困扰的ebay，只看网络钓客以“假网站”试钓中国银行、中国工商银行的用户，就可以想像其猖獗程度了。

对非PC设备（如手机）的威胁增加

- 手机的PC化为手机病毒的制造和传播准备了基础，智能手机的加速普及又将降低手机病毒在传播过程中因为手机制式的不同而形成的障碍，3G的到来终将引爆无线互联网，包括手机病毒在内的手机安全问题将日益凸现。
- 目前，手机病毒已经具有了计算机病毒的许多特点，而通过蓝牙等无线技术，手机病毒可以同时以手机网络和计算机网络为传播平台，其传播范围大大增加。手机漏洞挖掘技术的发展，也将促进这一领域内手机病毒的大量滋生。显然，手机等这类移动终端的安全问题，正面临着严峻的考验。

对非PC设备（如手机）的威胁增加

- 自2000年西班牙出现第一例手机病毒以来，到目前为止，总共超过200种手机病毒，并以每周新出现2-3款手机病毒的速度增长。2007年3月出现了一款运行为Symbian S60平台的“熊猫烧香”手机版病毒。
- 流氓软件也转战手机平台，一条基于以流氓软件为载体，基于智能手机平台服务的黑色产业链正在形成。
- 2002年，xfocus研究人员对手机的漏洞进行过研究，但手机病毒从没有这两年距离我们这样近过，手机蠕虫的大规模传播又成为了我们的心腹之患。

12.2 网络安全的发展趋势

- 12.2.1 网络攻击的发展趋势
- 12.2.2 防御技术的发展趋势
- 12.2.3 动态安全防御体系
- 12.2.4 加强安全意识与技能培训
- 12.2.5 标准化进程

12.2.1 网络攻击的发展

- 通过对大量网络攻击事件的分析和归纳得出，网络攻击技术正在朝以下几个方面迅速发展：
  - 趋势1：网络攻击阶段自动化
  - 趋势2：网络攻击工具智能化
  - 趋势3：漏洞发现、利用速度愈来愈快
  - 趋势4：防火墙等的渗透率愈来愈高
  - 趋势5：安全威胁的不对称性在增加
  - 趋势6：对网络基础设施产生的破坏力越来越强

趋势1：网络攻击阶段自动化

- 自动化攻击一般涉及四个阶段：
  - 扫描阶段：攻击者采用各种新出现的扫描技术（隐蔽扫描、智能扫描、指纹识别等），使得攻击者能够利用更先进的扫描模式来改善扫描效果，提高扫描速度。
  - 渗透控制阶段：先进的隐蔽远程植入方式，如基于数字水印远程植入方式、基于DLL和远程线程插入的植入技术，能够成功的躲避防病毒软件的检测将受控端程序植入到目的主机中。
  - 传播攻击阶段：以前依靠人工启动攻击软件工具发起的攻击，现在发展到由攻击工具本身只能发起新的攻击。
  - 攻击工具协调管理阶段：随着分布式攻击工具的出现，攻击者可以容易地控制和协调分布在Internet上的大量已部署的攻击工具。

趋势2：网络攻击工具智能化

- **目前攻击工具的开发者正在利用更先进的思想和技术来武装攻击工具，攻击工具的特征比以前更难发现。相当的工具已经具备了反侦破、智能动态行为、攻击工具变异等特点。**
  - 反侦破－是指攻击者越来越多地采用具有隐蔽攻击工具特性的技术，使得网络管理人员和网络安全专家需要耗费更多的时间分析新出现的攻击工具和了解新的攻击行为；
  - 智能动态行为－是指现在的攻击工具能根据环境自适应地选择或预先定义决定策略路径来变化对它们的模式和行为。并不像早期的攻击工具那样，仅仅以单一确定的顺序执行攻击步骤；
  - 攻击工具变异－是指攻击工具已经发展到可以通过升级或更换工具的一部分迅速变化自身，进而发动迅速变化的攻击，且在每一次攻击中会出现多种不同形态的攻击工具。

趋势3：漏洞发现、利用速度愈来愈快

- 安全漏洞是危害网络安全的最主要因素，安全漏洞在所有的操作系统和应用软件都是普遍存在的，特别是软件系统的各种漏洞。
- 安全漏洞并没有厂商和操作系统平台的区别，即并非人们印象中那样：**UNIX**系统更安全一些。新发现的各种系统与网络安全漏洞每年都要增加一倍，每年都会发现安全漏洞的新类型，这些漏洞在补丁未开发出来之前很难防御攻击者的破坏。
- 网络安全管理员需要不断用最新的补丁修补相应漏洞。攻击者经常能够抢在厂商修补漏洞前，发现这些未修补漏洞同时发起攻击。

趋势4：防火墙等的渗透率愈来愈高

- 配置防火墙目前仍然是企业和个人防范网络入侵者的主要防护措施。但是，一直以来，黑客都在研究攻击防火墙的技术和手段。攻击的手法和技术越来越只能化和多样化。
- 从黑客攻击防火墙的过程看，大概可以分为两类：
  - 第一类攻击防火墙的方法是探测在目标网络上安全的是何种防火墙系统，并且找出此防火墙系统允许哪些服务开放——防火墙的探测攻击；
  - 第二类攻击防火墙的方法是采取地址欺骗，TCP序列号攻击等手法绕过防火墙的认证机制，达到攻击防火墙和内部网络的目的。

趋势5：安全威胁的不对称性在增加

- Internet上的安全是相互依赖的。每个Internet系统遭受攻击的可能性取决于连接到全球Internet上其他系统的安全状态。
- 由于攻击技术水平的进步，一个攻击者可以比较容易地利用那些不安全系统，对一个受害者发动破坏性的攻击。
- 随着部署自动化程度和攻击工具管理技巧的提高，威胁的不对称性将继续增加。

趋势6：对网络基础设施的破坏力越来越大

- 由于用户越来越多地依赖计算机网络提供各种服务，完成日常相关业务，黑客攻击网络基础设施造成的破坏影响越来越大。
- 黑客对网络基础设施的攻击，主要手段有分布式拒绝服务攻击、蠕虫病毒攻击、对**Internet**域名系统**DNS**的攻击和对路由器的攻击。

12.2.2 防御技术的发展趋势

- 病毒防御技术发展趋势
- 反垃圾邮件发展趋势
- 防火墙技术发展趋势
- 反间谍技术的应用尝试与发展
- **IDS技术的发展趋势**

病毒防御技术发展趋势

- 对于企业来说，面临的最大问题是基于签名的识别技术不能有效防御新病毒。
- 企业要想有效地制止攻击，行为识别是首选的解决方案。

病毒防御技术发展趋势(2)

- 综合采用行为识别和特征识别技术，可非常高效的实现对计算机病毒、蠕虫、木马等恶意攻击行为的主动防御，能较好地解决现有产品或系统以被动防御为主、识别未知攻击行为能力弱的缺陷。
- 基于行为的反防毒保护并不依靠一对一的签名校对来实现恶性代码的识别，而是通过检查病毒及蠕虫的共有特征发现可能的恶性软件。

病毒防御技术发展趋势(3)

- 采用这一技术的优势在于：该技术可识别未知的病毒，以抵御“零日”攻击。
- 可以说由签名识别技术转移到行为识别技术，是大势所趋。但是，目前的事实是，行为识别技术暂时还没有走向商业化。

反垃圾邮件发展趋势

- 国内外主要的反垃圾邮件系统，普遍采用的是关键字内容过滤技术，采取“截获样本，解析特征，生成规则，规则下发，内容过滤”这种类似传统杀病毒系统的原理。
- 这种技术存在着许多难以克服的问题。

传统反垃圾邮件难以克服的问题

- 垃圾邮件内容变化快，数量远远大于病毒，任何一家安全公司都很难保证样本采集的数量和及时性，也就很难保证反垃圾邮件的使用效果和效果的持久性；
- 必须比对完所有的关键字规则，一封信才能被确信不是垃圾邮件，导致效率低下、资源消耗大、网关系统不稳定，尤其是在遭受巨量邮件攻击时，可能导致系统崩溃；
- 依赖关键字规则判别垃圾邮件，导致误判率较高，垃圾邮件识别准确性低，效果差；

传统反垃圾邮件难以克服的问题(2)

- 系统自维护能力差，管理员维护大量规则库，工作量大；
- 信件必须接收完整才能进行内容过滤，导致国际网络流量费用高；
- 通过拆信检查内容的方式进行反垃圾邮件，侵犯了公民电子邮件通信自由权和隐私权，这种内容过滤技术将受到广泛的法律质疑。

反垃圾邮件发展趋势(cont.)

- 传统反垃圾邮件技术，只能提升信噪比，以免垃圾邮件淹没正常邮件，但垃圾邮件与病毒邮件仍然占用了大量带宽与存储资源，垃圾邮件的发送仍处于非受控状态。
- 要想从根本上解决反垃圾邮件的技术难题，就要采用主动型垃圾邮件行为模式识别的技术，这样才能做到主动的邮件攻击行为防御、主动的垃圾邮件阻断，从而最大程度地提高垃圾邮件识别率、拦截率，降低资源消耗，真正达到电信级的网关处理速度。

反垃圾邮件发展趋势(cont.)

- 行为模式识别模型包含了邮件发送过程中的各类行为要素，例如：时间、频度、发送IP、协议声明特征、发送指纹等。
- 在统计分析中，可以发现在行为特征上，垃圾邮件与正常邮件具有极高的区分度，且不论内容如何均相对为固有特征，特别是对大量的采用动态IP发送的邮件更是如此。

反垃圾邮件发展趋势(cont.)

- 采用垃圾邮件行为模式识别模型不仅大大提高了垃圾邮件辨别的准确率，而且不需要对信件的全部内容进行扫描，所以又可以大大提高计算处理能力，为电信级的邮件过滤打下了坚实的基础。
- 此外，采用垃圾邮件行为模式识别模型识别垃圾邮件，也可以从另一方面给垃圾邮件攻击者以压力，迫使发送者必须按照一定的规范发送邮件。也就是说迫使邮件发送者只能从正常渠道，以正常方式发送邮件，从而使得邮件的发送处于受控状态。

防火墙技术发展趋势

- 目前的防火墙已经不仅仅只是进行状态检测，还需提供更多的安全功能，从各个方面对网络安全威胁进行防护，主动扩大战线。
  - 新一代NP技术
  - 防火墙深度检测
  - 应用状态检测
  - 安全技术融合
  - VPN功能集成

新一代NP技术

- NP是网络处理器（Net Processor）的简称，顾名思义，NP是专门设计用于网络封包处理的一种处理器，作为被业内普遍推崇的一种革命性技术，NP至今尚未能达到人们预期的应用水平。
- 作为NP技术的主要目标客户群，通信厂商们的态度正由热捧回归冷静，而在网络安全设备特别是硬件防火墙市场上，NP的应用却正呈现出一片欣欣向荣的景象。
- 国内的大部分重量级防火墙厂商纷纷推出了自己的NP架构防火墙产品。

新一代NP技术(2)

- 用CPU、ASIC还是NP，一直是大家不断争论的一个问题，其实这个问题非常简单。在能达到同样性能的情况下，优选CPU，其次是NP，然后是ASIC。目前很多厂商使用CPU+特定业务ASIC来实现高速处理，这是比较常见的方式。在性能不能解决的情况下，选择NP是必然的做法。
- 但不管是IBM，还是Intel的NP，一个主要问题是开发成本太高，代码的开发难度和进度都不是普通公司能够短期搞定的，而带来的维护成本和对客户的响应速度都是很大的问题。

新一代NP技术(3)

- 这两年推出的新一代网络业务NP，通过直接集成多个通用CPU在一个处理器中，既可以保证高性能，又能借助软件的灵活性处理高层业务数据。
- 新一代NP直接支持C语言和标准协议栈，性能高达10G，是期望中的业务网关处理芯片。使用新一代NP技术的防火墙将会获得性能和功能上两全的保障。

防火墙深度检测

- 防火墙最初的功能就是进行访问控制、状态检测，以及地址转换功能。通过对报文网络层信息的检测，来实现在网络层上对报文的控制。
- 随着网络应用的发展，高层协议得到越来越多的应用，互联网也从多种协议并驾齐驱发展成少数应用协议成为主流。而针对这些协议，用户需要进行控制。比如，需要控制用户不能访问非法网址，带有恶意信息的报文不能进入内网。
- 而这些功能，仅仅依靠传统防火墙技术实现的对网络层信息进行检查和判断，是不能实现的，需要检查报文中的更深层次的内容，于是发展出了深度检测技术。

防火墙深度检测(2)

- 深度检测可以检测报文中的内容信息，从而实现**URL**过滤、**FTP**命令过滤、网页中**ActiveX**控件过滤等功能，达到控制应用内容的目的。
- 集成深包检测的防火墙将会越来越多。通过深包检测对内容进行控制，而不仅仅是对网络层信息进行控制，使防火墙对智能攻击有了主动防护能力。

应用状态检测

- 安全领域中长期依赖、发挥最大作用的无非是状态防火墙，通过协议状态检测技术实现数据访问单向流动，从而有效的保护内部网络不受攻击。而对服务器，采取暴露端口的形式。
- 随着应用的增多和对安全性要求的提高，对这种开放端口的服务器同样需要保护，在网络层状态检查的基础上需要扩展到应用层的状态检查，从而对暴露在网络中的服务器进行保护。
- 这种趋势会产生一系列的应用层安全网关，比如**Web**安全网关、语音安全网关等专用协议网关。

安全技术融合

- 传统的网络层安全技术，如**NAT**、状态防火墙、**VPN**将不再作为专有设备，网络中路由器、交换机性能的提升和硬件构架的换代将直接提供网络层的安全功能，传统意义上的防火墙功能可以集成在路由器中。
- 而另一方面，随着协议和接口的统一，防火墙也可以取代路由器或者交换机的位置。安全厂商或许会变化成网络设备厂商，网络设备厂商也能变为安全厂商，而由于积累的不同，网络设备厂商具有更大的优势。

安全技术融合(2)

- 比如，现在的交换机成本和以前的Hub一样，但是抛弃了原来的交换芯片，使用新的硬件，不但提供交换，而且提供安全和业务特性，将来会直接把安全延伸到整个内部网络，彻底解决目前的内网安全问题。那么，传统的安全厂商如何发展？
  - 把自己融合进网络设备厂商。
  - 向安全的新领域—业务安全(而不是网络安全)进军。
  - 组建安全联盟，形成一个大的安全体系，自己成为其中一个基石。

VPN功能集成

- 从厂商的角度来说，希望一个环境中既使用**VPN**设备，又使用防火墙。但是，由于**VPN**设备对数据的隧道封装会导致防火墙设备上对**VPN**数据检测出现失准的现象，而同时维护两套配置策略也是没有必要的。
- 为了减少重复处理，降低维护工作，提高防火墙的防护范围，直接在防火墙上集成**VPN**功能是非常有效的方法。如**IPSec VPN**、**SSL VPN**、**L2TP VPN**直接通过防火墙来支持，应用效果提高，而且降低了用户的投入成本。

VPN功能集成(2)

- 防火墙技术在新的挑战下会继续向前发展，提供越来越多的智能和主动防御功能。
- 防火墙中各个功能的协调工作，以及和网络中其他硬件、软件组件的配合联动，才能达到真正意义上的智能安全和主动防御。

反间谍技术的应用尝试与发展

- 与其他网络安全产品相比，反间谍软件可谓后起之秀。应对间谍软件的首要任务就是要有一个清晰的标准来定义什么是间谍软件，然后以此为准绳进行判断和查杀。但难点恰巧是这个标准很难定义。
- 通常的定义：任何在计算机用户不知不觉的情况下，秘密搜集使用者的相关信息，并将其发给幕后操纵者的软件都可以称之为间谍软件。
- 但是，很多合法的广告软件实现的也是类似的功能。有人认为，可以通过传送信息的最终结果是否带有恶意来进行判定，但实际上，是否具有“恶意”，人类能够通过智力和直觉来判断，但要没有意识的计算机软件来进行区分，却难以实现。

反间谍技术的应用尝试与发展(2)

- 反间谍软件和防病毒类似，都需要一种可靠的解决方案和专门的研究及响应机制，来跟踪新的间谍软件风险，并及时提供随威胁变化而变化的升级版本。
- 虽然恶意软件与传统病毒存在区别，但是防范它们的目标是相同的，即保护客户电脑不受有害软件的侵扰。

反间谍技术的应用尝试与发展(3)

- 一款好的反间谍软件工具，要给用户提供实时的保护。不仅应该能够检测尽可能多的间谍软件，毫无残留地消除“间谍”在系统每一个角落中留下的残渣余孽，避免死灰复燃，还应该安装和部署简便，可以方便地升级间谍软件特征表。
- 好的反间谍工具应该提供迅捷明了的状态显示报告，可以让用户及时了解间谍软件给公司造成多大的损害，最大的风险和威胁在哪里。

反间谍技术的应用尝试与发展(3)

- 目前，“从什么位置阻挡间谍软件是最有效的”这个问题还有争论。
- 有的厂商认为应当从桌面阻止，保证每一个“内部成员”的可靠性。因为移动技术在企业内的大量应用，使得越来越多的计算设备脱离了由网关所划定的安全疆域，如果用户在网关的保护之外感染了间谍软件，然后又再次接入网络，这台机器本身就成了协助“间谍”潜入的跳板。
- 而另外一部分厂商则认为，桌面工具始终是被动防线，“更好的”间谍软件总会突破这道防线。因此，应该在网关处采取防护措施。如果资金足够，企业应该采取多层次的防护措施来阻止间谍软件，这样才能收到理想的效果

IDS技术的发展趋势

- 长期以来，IDS的“漏报”和“误报”问题一直困扰着用户。加强攻击检测是减少“漏报”和“误报”现象的首要手段。过去，攻击检测是IDS的全部。
- 而今天，它只是IDS的一个重要方面。IDS要实现全面关注网络健康，还应该能够做到帮助用户对检测内容进行深层次的分析，主动防御，最终提交给用户一份有意义的报告。

IDS技术的发展趋势(2)

- 在某些**IDS**产品中已经新增加了内容恢复和应用审计功能，能针对常用的多种应用协议，比如**HTTP**、**FTP**、**SMTP**、**POP3**、**Telnet**、**NNTP**、**IMAP**、**DNS**、**Rlogin**、**MSN**等进行内容恢复，能完全真实地记录通信的全部过程与内容，并将其进行回放。
- 此功能对于了解攻击者的攻击过程、监控内部网络中的用户是否滥用网络资源、发现未知的攻击具有重要和积极的作用。例如，在恢复**HTTP**的通信内容时，可恢复出其中的文本与图形等信息；而应用内容的审计则可发现内部的攻击，了解哪些人员查看了不该查看的内容。

IDS技术的发展趋势(3)

- 此外，实时监测网络流量并及时发现攻击行为，亦是IDS的一项基本特征。现在的IDS产品增加了对网络实时监控和诊断功能，尤其是增加了扫描器，能对全网络进行主动扫描，实时发现网络中的异常，并给出详细的检测报告。
- 这种在审计和监控等多项功能上得到加强的IDS已经超越了传统意义上的IDS，是适用于用户需求、保护用户网络健康的新型IDS。

12.2.3 动态安全防御体系

- 动态安全过程
- 动态安全防御体系

动态安全过程

- 由于黑客攻击手法层出不穷、千奇百怪、日新月异，迫使安全防御技术必须同步跟进，否则有时前期的安全投资不再有效，造成巨额的浪费。
- 因此在准备实施一个安全项目工程，构筑自身的防御体系机制时，网络安全不能仅仅依赖于众多安全产品的作用，也不能仅仅只停留在“三分技术，七分管理”的概念上，安全不应该作为一个目标去看待，而应该作为一个过程去考虑、设计、实现、执行。通过不断完善的管理行为，形成一个动态的安全过程。

动态安全防御体系

- 人们目前接受的安全策略建议普遍存在着“以偏盖全”的现象，它们过分强调了某个方面的重要性，而忽略了安全构件（产品）之间的关系。因此在可定制的、可操作的安全策略基础上，需要构建一个具有全局观的、多层次的、组件化的安全防御体系。
- 它应涉及网络边界、网络基础、核心业务和桌面等多个层面，涵盖路由器、交换机、防火墙、接入服务器、数据库、操作系统、**DNS**、**WWW**、**MAIL**及其它应用系统。

动态安全防御体系(2)

- 静态的安全产品不可能解决动态的安全问题，应该使之可定制、可定义、可管理。
- 无论静态或动态（可管理）安全产品，简单的叠加并不是有效的防御措施，应该要求安全产品构件之间能够相互联动，以便实现安全资源的集中管理、统一审计、信息共享。

动态安全防御体系(3)

- 目前黑客攻击的方式具有高技巧性、分散性、随机性和局部持续性的特点，因此即使是多层面的安全防御体系，如果是静态的，也无法抵御来自外部和内部的攻击。
- 只有将众多的攻击手法进行搜集、归类、分析、消化、综合，将其体系化，才有可能使防御系统与之相匹配、相耦合，以自动适应攻击的变化，从而形成动态的安全防御体系。

12.2.4 加强安全意识与技能培训

- 网络安全保护的对象由人创建、由人在用、由人在管。而网络攻击的发起者也是人，攻击目的来源于他的思想意识。所以网络安全的核心必然是人。
- 对攻击者进行安全法律法规教育，对执行者进行安全技能培训，这项工作应贯穿整个安全过程。

加强安全意识与技能培训(2)

- 与安全技术相比，涉及人的安全管理非常重要，应包括安全策略管理、安全组织规范、资产分类与控制、人员安全管理措施、物理与环境安全保障、通讯与操作管理程序、访问控制要求、系统开发与维护规程、业务连续性管理办法和法律法规一致性规定等内容。

加强安全意识与技能培训(3)

- 安全意识和相关技能的教育是组织安全管理中重要的内容，其实施力度将直接关系到组织安全策略被理解的程度和被执行的效果。
- 为了保证安全的成功和有效，高级管理部门应当对组织各级管理人员、用户、技术人员进行安全培训。
- 所有的组织人员必须了解并严格执行组织安全策略。

加强安全意识与技能培训(4)

- 在安全教育具体实施过程中应该有一定的层次性：
  - 主管网络安全工作的高级负责人或各级管理人员。重点是了解、掌握组织网络安全的整体策略及目标、网络安全体系的构成、安全管理部门的建立和管理制度的制定等。
  - 负责网络安全运行管理及维护的技术人员。重点是充分理解网络安全管理策略，掌握安全评估的基本方法，对安全操作和维护技术的合理运用等。
  - 用户。重点是学习各种安全操作流程，了解和掌握与其相关的安全策略，包括自身应该承担的安全职责等。
- 对于特定的人员要进行特定的安全培训。安全教育应当定期的、持续的进行。
- 在组织中建立安全文化并容纳到整个组织文化体系中才是最根本的解决办法。

12.2.5 标准化进程

- 国际信息安全标准化工作的情况
- 我国信息安全标准化的现状
- 信息安全标准化工作的发展趋势
- 现有标准

国际信息安全标准化工作的情况

- 国际上的信息安全标准化工作，兴起于20世纪70年代中期，在80年代有了较快的发展，于90年代引起了世界各国的普遍关注。
- 目前世界上约有近300个国际和区域性组织，制定标准或技术规则，与信息安全标准化有关的主要的组织有：
  - 国际标准化组织(ISO)
  - 国际电工委员会（IEC）
  - 国际电信联盟（ITU）
  - Internet工程任务组（IETF）

国际标准化组织(ISO)

- 国际标准化组织(ISO) 于1947年2月23日正式开始工作，ISO/IEC JTC1（信息技术标准化委员会）所属SC 27（安全技术分委员会）其前身是SC20（数据加密分技术委员会），主要从事信息技术安全的一般方法和技术的标准化工作。
- 而ISO/TC68负责银行业务应用范围内有关信息安全标准的制定，它主要制定行业应用标准，在组织上和标准之间与SC27有着密切的联系。
- ISO/IEC JTC1负责制定标准主要是开放系统互连、密钥管理、数字签名、安全的评估等方面的内容。

国际电工委员会（IEC）

- 国际电工委员会（IEC）正式成立于1906年十月，是世界上成立最早的专门国际标准化机构。
- 在信息安全标准化方面，主要与ISO联合成立了JTC1下分委员会外，还在电信、电子系统、信息技术和电磁兼容等方面成立技术委员会，如TC56可靠性、TC74 IT设备安全和功效、TC77 电磁兼容、TC 108音频/视频、信息技术和通讯技术电子设备的安全等，并制定相关国际标准，如信息技术设备安全（IEC 60950）等。

国际电信联盟（ITU）

- 国际电信联盟（ITU）成立于1865年5月17日，所属的SG17组，主要负责研究通信系统安全标准。SG17组主要研究的有：通信安全项目、安全架构和框架、计算安全、安全管理、用于安全的生物测定、安全通信服务。
- 此外SG16和下一代网络核心组也在通信安全、H323网络安全、下一代网络安全等标准方面进行了研究。目前ITU-T建议书中大约有40多个都是与通信安全有关的标准。

Internet工程任务组（IETF）

- Internet工程任务组（IETF）史创于1986年，其主要任务是负责互联网相关技术规范的研发和制定。目前，IETF已成为全球互联网界最具权威的大型技术研究组织。
- IETF标准制定的具体工作由各个工作组承担，工作组分成八个领域，分别是Internet路由、传输、应用领域等等，著名的IKE和IPsec都在RFC系列之中，还有电子邮件，网络认证和密码标准，也包括了TLS标准和其它的安全协议标准。

我国信息安全标准化的现状

- 目前，我国按照国务院授权，在国家质量监督检验检疫总局管理下，由国家标准化管理委员会统一管理全国标准化工作，下设有**255**个专业技术委员会。
- 中国标准化工作实行统一管理与分工负责相结合的管理体制，有**88**个国务院有关行政主管部门和国务院授权的有关行业协会分工管理本部门、本行业的标准化工作，有**31**个省、自治区、直辖市政府有关行政主管部门分工管理本行政区域内、本部门、本行业的标准化工作。

我国信息安全标准化的现状(2)

- 成立于**1984**年的全国信息技术安全标准化技术委员会（**CITS**），在国家标准化管理委员会和信息产业部的共同领导下负责全国信息技术领域以及与**ISO/IEC JTC1**相对应的标准化工作，目前下设**24**个分技术委员会和特别工作组，是目前国内最大的标准化技术委员会。
- 这是一个具有广泛代表性、权威性和军民结合的信息安全标准化组织，它的工作范围主要是负责信息和通信安全的通用框架、方法、技术和机制的标准化，在安全技术方面包括定义开放式安全体系结构、各种安全信息交换的语义规则、有关的应用程序接口和协议引用安全功能的接口等。

我国信息安全标准化的现状(3)

- 我国信息安全标准化工作，虽然起步较晚，但是近年来发展较快，标准化工作在公开性、透明度等方面更加取得实质性进展。
- 从20世纪80年代开始，本着积极采用国际标准的原则，转化了一批国际信息安全基础技术标准，制定了一批符合中国国情的信息安全标准，同时一些重点行业还颁布了一批信息安全的行业标准，为我国信息安全技术的发展做出了很大的贡献。
- 据统计，我国从1985年发布了第一个有关信息安全方面的标准以来到2004年底共制定、报批和发布有关信息安全技术、产品、测评和管理的国家标准76个，正在制定中的标准51个，为信息安全的开展奠定了基础。

信息安全标准化工作的发展趋势

- 国际化合作
- 商业化驱动
- 明确安全标准化研究方向

国际化合作

- 信息安全的国际标准大多数是在欧洲、美国等工业发达国家标准的基础上协调产生的，基本上代表了当今世界现代信息技术的发展水平。
- 信息安全标准化工作是一个国际性的工作，共性的问题多于个性，本着积极采用国际标准的原则，适时地转化了一些国际信息安全基础技术标准为我国信息化建设服务，会对中国的信息安全技术起到一个快速发展的作用。

国际化合作

- 我们不仅主动地采用国际标准，转化国际标准，更重要的是我们还有计划、有重点地参与国际标准的起草，主动承担国际标准的起草工作，包括标准试验验证和讨论的全过程。
- 我们应该采取积极的态度，对国际标准要花大力气，认真分析、研究，逐步使我国的信息安全标准化工作与国际标准化工作的计划、速度以及试验验证工作接轨。

商业化驱动

- 多年来，国家标准的制修订经费主要来源于政府财政拨款，经费的不足部分由项目承担单位自行解决。
- 随着改革开放的深入和信息化工作的开展，对信息安全标准化工作的要求越来越高。今后可以考虑采用国家加大投入，争取企业支持，标准出版物在发行工作中的改革，提高标准文本的出售价格等方法，使信息安全标准化工作逐步进入商业化运作模式，进入到一个良性发展的新局面。

明确安全标准化研究方向

- 扎扎实实地抓好基础性工作和基础设施建设，继续推进信息安全等级保护、信息安全风险评估、信息安全产品认证认可等基础性工作。
- 继续加快以密码技术为基础的信息保护和网络信任体系建设，进一步完善应急协调机制与灾难备份工作。
- 进一步加强互联网管理，创建安全、健康、有序的网络环境。
- 进一步创建产业发展环境支持信息安全产业发展，加快信息安全学科建设和人才培养，加强国际合作与交流，完善信息安全的管理体制和机制。

现有标准

- 国际上早在20世纪70年代就开始信息安全的标准工作。相继制定了很多安全标准，有代表性的标准有：
  - 信息技术安全评估标准ITSEC；
  - 可信计算机安全评估标准TCSEC的美国新联邦标准；
  - 加拿大可信计算机产品评估标准CTCPEC；
  - TCSEC的可信数据库解释TNI；
  - TCSEC的可信数据库解释TDI；
  - ISO-SC27-WG3安全评估标准；
  - ISO7498-2N安全体系结构标准；
  - Open Group 公司和Open Software Foundation公司组成的Open Group组织提供的X/Open Security安全标准；
  - Check Point公司提供的开放企业安全连接平台OPSEC（Open Platform for Secure Enterprise Connectivity）。

现有标准

- **我国互联网安全标准课题主要涉及：**
  - 分组过滤防火墙标准：防火墙系统安全技术要求；
  - 应用网关防火墙标准：网关安全技术标准；
  - 网络代理服务器：信息选择平台安全要求；
  - 鉴别机制标准；
  - 数字签名机制标准；
  - 安全电子交易：抵抗抵赖机制标准；
  - 网络安全服务标准：信息系统安全性评价准则和测试方法；

12.3 网络安全与法律法规

- 12.3.1 网络立法的内容
- 12.3.2 网络立法的形式
- 12.3.3 用户的行为规范
- 12.3.4 我国的相关法律法规

12.3.1 网络立法的内容

- 第一部分：公法内容
- 第二部分：私法内容
- 第三部分：网络利用的法律问题

公法内容

- 该部分内容是对网络进行管理的行政法内容，是对网络纠纷进行裁决的诉讼法内容和对网络犯罪行为进行规制和追究的刑法、刑事诉讼法内容。
- 它的作用，是使国家能够对网络依法进行管理，并对侵害网络权利、违背网络义务的行为进行制裁和处理，以维护社会的正常秩序、维护网络的正常秩序。当前正在制定的关于对网络进行规制的部门规章，就是属于这一部分的内容。

私法内容

- 这一部分的内容是从民法的角度，对网络主体、网络主体的权利义务关系（包括网站的权利义务）、网络行为、网络违法行为的民事责任作出的规定。
- 这种规定，是维护网络世界正常关系的必要条件，是网络主体正当行使网络权利、履行网络义务和依法实施网络行为的法律保障。
- 这一部分内容是维护网站和网民权利和义务的法律核心。网站和网民究竟有什么权利和义务、它们互相之间究竟有什么权利和义务，都是急需立法进行规定的。

网络利用的法律问题

- 其主要内容是对现实社会中的人们利用网络的便捷和迅速，进行网络以外的活动作出法律规定。规定人们怎样进行这种利用活动，并需要遵守哪些规则，若出现争议时应当依据怎样的规则进行处理等等。
- 网络利用形式，包括利用网络进行商务交易，利用网络进行文学创作，利用网络进行远程教学，利用网络进行研究（包括进行法律研究）等等。

12.3.2 网络立法的形式

- 网络立法的形式应当是：
  - 建立一部类似于《著作权法》、《商标法》或《专利法》的法律，用来全面规定网络的法律问题。其中既要有前面所说的三个方面的基本内容，还要有详细的行为规范和权利义务关系等规定；
  - 在一些基本法中补充一些有关网络内容的规定。例如，在诉讼法、刑法、行政法等法律中规定与网络相关的内容。在刑法中应当规定黑客犯罪的犯罪构成、刑罚幅度；在行政法中应当规定对网络违规行为的制裁和制裁程序等等；
  - 建立配套的行政法规和部门规章，对网络法还要作出实施细则，使之成为一个以网络法为核心的、由基本法的相关内容为配套的、由行政法规和行政规章做补充的、由最高司法机关的司法解释作为法律实施说明的一套完整的法律体系。

12.3.3 用户的行为规范

- **Internet**最初的教育科研背景对**Internet**文化的形成起到了重要的作用，这种文化已经规定了网络用户的行为规范，要求用户遵守某些行为规范。
- 随着其迅速发展和商业化，**Internet**的社会背景有了很大变化，但它所依托的技术和所施加的种种限制却依然存在。由于新出现的用户缺乏必要的相关技术背景知识，对于应有的网络文化缺乏了解，素质参差不齐，导致传统的**Internet**网络文化和行为规范并没有他们很好的遵守。
- 网络费用相对便宜、覆盖面广、使用方便的优点，也使得很多人出于好奇或商业活动的需要，对网络的有限带宽进行无制约的滥用，带来了一些不必要的负载重担。因此对用户网络行为的规范化是网络健康合理应用的关键问题之一。

12.3.4 我国的相关法律法规

- 2000年12月28日通过的《全国人大常委会关于维护互联网安全的决定》，成为我国针对信息网络安全制定的第一部法律性决定。
- 目前，我国针对信息网络安全的属于行政法规的有《电信条例》、《商用密码管理条例》、《计算机信息系统安全保护条例》、《计算机软件保护条例》等5个。
- 属于部门规章与地方性法规的则已经有上百件。
- 《中华人民共和国保守国家秘密法》、《中华人民共和国标准法》、《中华人民共和国国家安全法》、《中华人民共和国商标法》、《中华人民共和国刑法》、《中华人民共和国治安管理处罚条例》和《中华人民共和国专利法》等多个法律也增加了涉及到互联网管理和信息安全的条款。
- 最高人民法院、最高人民检察院出台的《关于办理利用互联网、移动通信终端、声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释》等司法解释。

12.4 小结

- 网络的开放性决定了网络的复杂性、多样性。任何安全的防范措施均不是单一存在的，任何网络入侵也并非单一技术或技术的简单组合。
- 随着技术的不断进步，各种新型网络攻击会不断出现。网络攻击事件并未随着网络安全技术的发展而减少。
- 网络安全问题本身具有动态性特点：今天的安全问题到明天也许不再称为问题；而今天不为人们关注的环节，明天可能称为严重的安全威胁。

小结(2)

- 网络安全人员需不断跟踪攻击行为和手法，研究网络和系统的安全漏洞；分析并掌握最新的网络安全技术；在原有安全系统的基础上及时调整网络安全策略；及时添加有针对性的网络安全产品、进行正确配置，基于网络安全强有力的保障。
- 网络安全管理人员在任何时候都不可掉以轻心，轻信目前网络的安全状态。要不断提高个人安全意识，及时跟进必要的防护手段对各种网络攻击予以坚决而有效的阻击。

Thank you for your attention!