《计算机安全》2006 年第 3 期 总第 61 期

信息泄漏防范何去何从

李军　清华大学信息技术研究院

众所周知，互联网是在缺乏安全性、可靠性设计和没有质量保障情况下迅速成为一个不可或缺的社会基础设施的。然而到今天，互联网的规模及其影响已经到了无法从头再来的程度。为了实现网络条件下的信息安全，从防火墙到入侵检测/防御系统，从防攻击、防病毒、防垃圾邮件到防蠕虫、防钓鱼（phishing）、防间谍软件，各类产品层出不穷，以致企业网络机房里的安全设备几乎快要比传输设备（路由器、交换机）还要多了。即便如此，安全漏洞依旧层出不穷，安全事件还是应接不暇，造成的损失也越来越大。现实迫使学界和业界不得不更全面地（holistically）分析信息安全问题，部署信息安全措施。

传统的安全防护最初是从面向静态网络连接的访问控制（access control）和信息过滤（content filtering）开始的。随着无线和移动网络的发展，信息安全新技术的热点又转移到了针对动态网络连接的准入控制（admission control）和端点安全（endpoint security）。近来较为引人注目的，还有全面管理端点各种物理连接的信息泄漏防范（information leakage prevention, ILP）技术和解决方案，又称防水墙或外泄检测（extrusion detection）。

信息泄漏防范的基本问题

信息安全的终极目标是保障信息在存储和传输时的安全。信息安全的漏洞既可以存在于有线或无线、固定或移动网络之中，也可以是通过 USB 等设备接口经由直接的物理接触构成。例如，利用 USB 盘窃取文件或安装“木马”是再容易不过的了；又如，只要从 CD 重启系统，通常就可以回避口令等各种检查，控制相关设备。

信息泄漏防范从广义上说包括防范被动失窃（信息被无权访问者获取）和防范主动透露（信息被授权访问者转移到受控范围之外）。

1. 防范被动失窃的主要手段是加强数据存储和网络传输的认证和加密机制。通过严格的认证，只有授权访问者才可以经由安全方式接触到相关信息，无权访问者既无法潜入，又因密码保护无法有效窃听，则被动失

窃的机会大大降低。

2. 防范主动透露就更加复杂了。因为这时信息泄漏的主体是被授权访问受控信息的，且具有相应网络操作的权限和信息解码的密钥，所以认证和加密就无法阻止这种情况了，需要通过信息过滤等手段来监控。

事实上，除了从备受关注的数据存储和网络传输的角度以安全服务器和安全网关部署防范被动失窃外，企业内部经过授权的主机和用户通常可以不通过安全网关直接取用服务器上的数据。当今的员工使用着越来越多可以连接到计算机设备上去的电子产品，包括装备 USB、蓝牙、红外、Wi-Fi 等各种接口的便携式存储和通讯设备。除传统的 CD-RW 和 DVD-RW 之外，这些设备的存储数据容量高达 300GB、通讯带宽也不断增长，造成了对信息泄露的严重恐慌。这些产品同样是黑客的最爱，可以穿过防火墙和杀毒软件在主机和网络中装入木马。

为了不让受保护的数据泄漏到受控范围之外，很多时候对企业内部用户使用的计算机的各种外设接口都要有所控制，其中包括 USB、打印机、CD/DVD 等。这种控制可以在几个不同层面上实施：

1. 设备层面：决定是否允许某类产品接入。这个产品类即可以是使用某个接口的所有产品（如各类 USB 产品），也可以是某个接口上的特定产品（如存储类 USB 产品，或带有某种特殊加密芯片的 USB 产品）。
2. 功能层面：决定是否允许某项功能使用。例如只允许对存储类 USB 产品进行“读”操作而不允许“写”操作。
3. 用户层面：决定是否允许某个用户进入。如果需要，可以对每次外设的使用都做用户认证。

上面描述的措施都是面向设备的，而防范被动失窃的另外一个方向就是面向数据的全程认证和加密。这种产品被统称为 ERM（Enterprise Rights Management），包括微软的 RMS（Rights Management Server），其方法类似于 DRM（数字版权管理，Digital Right Management），它使得受控数据（文件）总是以加密的形式存储，用户要通过中心服务器的认证并获取密钥才能读取。

相对而言，防范主动透露要复杂得多。除了网关上利用关键字词或文件特征进行匹配外，对于送往打印机、传真机等外设的数据都有可能需要扫描，这不但要求信息过滤方案可以解码各种文件格式和压缩格式，还要求较高的运算性能和

较大的缓存空间。

另外，一个统一的网关和代理（agent）的管理平台对于信息泄漏防范体系的运行也很重要。

信息泄漏防范的核心技术

网络设备的访问控制通常是由安全网关或“个人防火墙”完成的。而由安全网关或配置了准入控制的路由、交换设备，配合相关的认证和发布（补丁程序、特征文件等）服务器，以及主机上安装的端点安全代理，就构成了完整的网络准入控制系统，例如 TCG 的 TNC，Cisco 的 NAC 和微软的 NAP。

与此相比，网络设备之外的其它外设的接入则主要靠主机上的代理程序控制。这个代理程序可以是集成在端点安全代理之中的，也可以是独立的。它通过解剖操作系统内核中的驱动程序，获取唯一的设备号和接口协议，从而对其加以控制。例如，Safend Protector （即 Safend 信息安全卫士）是一种保护企业终端信息安全的软件解决方案，通过可视化的安全控件，可控的功能设置，在每一个用户主机上构建一套端口防护与管理体系，以防止信息的泄密，保护终端信息安全。它可以控制有线(USB、FireWire、PCMCIA、串口、并口)和无线(Bluetooth、WiFi、IrDA）以及存储（光驱、闪存、zip 驱动、软盘、磁带）等外设的接入。Safend Protector 对 USB、FireWire 和 PCMCIA 等设备的控制还可以细化到类型、厂商、型号以及设备编号等。

信息过滤技术涉及的问题就更复杂，解决方案的效果和性能也在很大程度上取决于其中模式识别方法的水平。受控的数据可以是有结构的，也可以是无结构的；可以是数据库中的具体数字，也可以是文件系统中的文档；可以是文本，也可以是多媒体。信息过滤技术在信息泄漏防范中的核心是从受控数据中抽取特征，用于信息分类，以决定外流的数据是否“涉密”。例如，PortAuthority 公司就用了 27 种专利算法来综合判定分类。又如，Vontu 公司使用了三种不同的技术，针对不同的应用需求：

1. 用标号文件匹配法（Indexed Document Matching，IDM）防止完整的、导出的或部分拷贝的源码、设计和媒体类文件被带出企业或加载到共享服务器。

2. 确切数据匹配法（Exact Data Matching，EDM)被用来保护价目表等通常存储在数据库中的信息。
3. 描述内容匹配法（Described Content Matching，DCM)按照包含关键字词或模式的特定文件类型、大小或名称、内容等对文件加以保护。

信息泄漏防范分为检测（Monitoring）和阻断（Blocking）两个阶段。目前市场上有些产品只是集中于检测信息泄漏有否发生，例如 Reconnex 公司的产品在对网络的监听（Sniffing）后进行内容分析和过滤就是其中的典型。这种监听的方案的好处是对网络本身的影响较少，但却无法实时阻断信息的泄漏，而只能进行事后处理。Vontu 公司的信息泄漏防范系统可以部署于网络出口干线（Data Path）上，从而可以在发现敏感信息泄漏时及时加以阻断。但是一般来讲，在网络出口对信息进行过滤分析有一定的局限性，因为这种方案只能识别明文，对加密的内容无法识别， 同时对端点处的信息泄漏如 USB 的拷贝无能为力。另外一些公司则是从端点着手，其中 DGate 公司的端点安全代理(Security Agent)和其专利智能信息过滤技术结合的解决方案就是一个例子，其解决方案在用端 (Point of Use)进行内容分析，并可以及时阻断信息泄漏，从而提供全面的信息泄漏防范解决方案，并可通过监控用户对敏感信息的操作来防止用户通过加密的方法泄漏信息。

信息泄漏防范还需要有统一的管理和维护系统，以集成相关局部统计和分析数据形成综合判断和全局管理。这就涉及到系统的建模、参数估计或学习，以及数据的关联性分析等技术。同时，集中的运行中心系统也为应急反应和事件处理提供了更丰富的操作和控制手段。

信息泄漏防范的市场前景

信息泄漏防范是一个新兴的产业。正因为它针对的是令企业头痛的首要内部安全问题，可以预料它的市场将随着产品的成熟而迅速扩大。据 IDC 的估计，全球信息泄漏防范市场（IDC 称之为 OCC，即 Outbound Content Compliance）的总值在 2006 年将接近 6 亿美元，并以每年约 50％的速度增长，到 2009 年将接近 19 亿美元。

信息泄漏防范的主要市场驱动力来源于以下几个方面的需求：

1. 企业对自身的知识产权、交易秘密（Trade Secret）和商业计划的保护。
2. 政府对企业的金融信息披露的规范管理，如美国的 Sarbanes-Oxley 法案对上市公司报表的严格管理。
3. 政府对私人信息的规范管理，如美国的 HIPAA 法案针对病人个人信息泄漏的管理。
4. 公众对越来越多的所谓个人身份信息盗用(Identity Theft)的不满。

以外设控制技术为主、经营信息泄漏防范产品的公司主要有 Safend、Safeboot 等。这些公司的产品与 SyGate（已被 Symantec 收购）等公司的端点安全产品结合在一起，可以构成较为完整的主机防御体系。日前，Safend 的产品已经通过其独家代理艾克斯特进入中国市场，并受到一些主流安全企业的关注和渠道、代理商的青睐。

以信息过滤技术为主、经营防范主动泄漏产品的公司主要有 Vontu、PortAuthority、Fidelis、Reconnex 和 Tablus 等，都是这几年新创的公司，且得到创投的追捧。留美华人团队创立的 DGate 公司也在其中一枝独秀。

国内以中软为代表的一些企业也较早推出了“防水墙”的概念和产品，但说法各不相同，概念不甚统一。中软和攀达防水墙的主要功能是包括网络接口在内的外设控制；山丽的防水墙则更象 ERM。目前国内自主开发的基于信息过滤的 ILP 产品还不多见。

信息泄漏防范技术目前还处在“各个击破”的阶段，从端点安全、外设管理、信息过滤、ERM 等各个方面提供防御手段、建立防护措施，根据需要集成各种手段、综合各项措施的努力才刚刚开始。

参考文献：

〔1〕李军，渐成热门的网络端点安全技术，《计算机安全》，2005 年第 1 期，总第 47 期。

〔2〕Lidror Troyansky，Information Identification: Critical Requirements for Effective Data Security，White Paper of PortAuthority Technologies，2005.

〔3〕Brian E. Burke, Worldwide Outbound Content Compliance 2005-2009

Forecast and Analysis: IT Security Turns Inside Out, Market Analysis of IDC, 2005.