防范网络内部威胁的动态安全模型的研究与设计

STUDAY OF DYNAMIC MODEL TO DEFEND INSIDE THREAT

陆　军　（哈尔滨工程大学计算机科学技术学院 150001）
（哈尔滨黑龙江大学计算机科学技术学院 150080）
刘大昕　（哈尔滨工程大学计算机科学技术学院 150001）
付立平　（哈尔滨黑龙江大学计算机科学技术学院 150080）

摘要：本文分析了外围安全环境、安全常规控制、技术控制和内部威胁之间的动态模型，揭示了内部信息安全各因素之间相互影响、相互制约的关系，并描述了内部信息安全控制的实现方法，对于防范内网威胁具有重要指导意义。

关键词：信息安全 信息泄漏 常规控制 内部威胁

1　引言

怎样防止内部信息泄漏和内部攻击日益成为信息安全的焦点，特别是对于来自内部人员的恶意攻击，不仅涉及到技术问题，还可能要考虑到整个组织范围内的政策、文化、惯例、手续流程、价值观念、雇员工作行为等，这些非技术性因素对于未来形成内部安全规则以及信息的安全评估具有重要意义。本文就是在讨论上述问题的动态关系基础上，分析各种不安全因素，探讨智能生成相应检测规则的可行性，从而最大限度地减少来自内部的恶意攻击。防范内部信息外泄以及内部攻击是当前信息安全领域一个新的重要分支，无论在理论还是在实际应用方面，都具有很大研究价值。

2　内部安全控制种类

USSS/CERT 标准研究中心采纳的内部威胁犯罪的定义为[1]，非法拥有或是经常拥有合法访问被攻击的网络/数据的权利，危及任何信息系统、网络或数据安全的行为。

潜在的造成信息泄漏的人员可能有：

2.1　安全意识淡薄的内部人员

由于他们安全意识淡漠，可能会造成内部资源信息滥用，如违反公司规定，私自绕过防火墙玩网络游戏，浏览网页等，不知不觉中为黑客开了后门，破坏了网络安全；随意将重要资料带回家处理；将公司网络拓扑图告知他人等。

2.2　对公司不满的职员

他们认为自己遭受不公平待遇，进而产生报复心理，该类人员可能对企业信息安全形成一定威胁。

2.3　公司临时雇员

对企业内部有一定了解，流动性较大，不宜管理。

2.4　公司前雇员

对企业内部了解较多，可能由于遭到公司解聘而怀恨在心。他们可能会对企业信息安全造成严重威胁。

2.5　与竞争对手有联系的内部人员

如间谍、试图跳槽的高级管理人员，他们可能将公司机密数据透露给竞争对手，从而给公司造成重大损失。

2.6　商业合作伙伴或承约人

由于同他们存在合作关系，如共同开发某个项目，因此存在必要的信息交流，但是需要对交流的信息范围进行控制，否则就会造成信息泄漏。

2.7　企业顾问

他们对企业了解较详细，特别是他们可能为多个企业充当顾问，因此需要加强管理。

2.8　客户

为了让客户更多了解企业，企业往往尽可能提供给客户大量信息，导致无意间泄漏了企业重要机密信

息，应当将客户所知信息限制在适当范围内，建立客户知情信息检查机制。

事实上，内部安全工作不只涉及人员和技术，它还有可能包括领导层与下属间关系、奖惩制度、工作环境等，因此为了有效保障信息系统安全，可以将安全控制分为以下三类[2]。

(1) 技术控制。为了保护系统免于攻击而采取的技术上的安全机制，通常包括配备反病毒软件和防火墙；使用系统漏洞检测软件定期对网络系统进行扫描分析，找出可能的安全隐患，及时安装系统补丁和安全补丁程序，做好安全配置，减少系统安全漏洞；对重要数据进行加密处理，还可以限定用户阅读范围，并保证这些数据离开内部网络后就失效；此外，还有权限与角色管理，对文件和目录的安全控制，反拷贝技术，蜜罐技术，硬盘加密与还原技术，保护内存中敏感数据，信息泄漏取证技术，备份与恢复以及审计功能等。

(2) 常规控制。安全的常规控制通常指公司结构、管理过程等，能保证公司正常运转并减少被攻击可能性，或者最大限度减少攻击造成的影响。例如，按照信息安全级别不同，对信息安全区域进行划分，集中管理机密信息；设立正确的存取权限或特权，建立详细的安全规则；设计和控制适当的雇员监管关系，加强对离职或辞职人员的管理，及时删除离、辞职人员的访问权限；由两个以上的人担任网络的管理员、没有人能不加限制地存取整个网络；常规的危险评估等。

(3) 环境因素。环境因素通常与公司的文化、价值观念和信任相关联。这些因素可能反映了管理的发展方向，对于增强员工对企业的归属感进而推动内部信息安全具有重要作用。环境因素是可以被创造的，例如，通过教育和培训计划增强员工的安全意识，遵守网络安全管理制度和国家信息网络安全法规，奖惩机制等，此外，还有其他一些反映公司信息安全方面的相关因素[3]，如信息技术投资占整个公司预算的百分比，信息安全方面的投资占整个信息技术投资的百分比，安全事件所造成的经济损失占整个公司预算的百分比，从事安全技术的工作人员占整个公司员工的百分比，每年发生的内部安全事件等，这些信息都可以作为相关规则为技术控制服务。

必须充分理解技术控制、安全常规控制和环境因素三者之间的动态链，需要一种方法学来捕获和研究三者之间的复杂关系，以便得到一个完整而有效的预防、检测和阻止内部威胁的管理方法。

3 内部信息安全的动态模型

首先我们来分析内部攻击形成过程。通常有一个直接动机引发内部攻击，如职员遭到解雇，工作未得到认可，未得到升迁，降职等都有可能使雇员心怀不满，进而形成攻击意识。除直接动机外，还有其他因素(内部系统技术弱点、常规管理漏洞、不利的环境因素等)的刺激使得攻击者铤而走险，最终引发内部攻击。当然，攻击可能不会突然发生，最开始可能仅仅是攻击者口头上表达不满，随着矛盾激化，逐步演变成实际攻击的前奏行为，如预留标记、故意出现一些错误、试探系统对安全威胁的反应、出现与工作不相干的问题或其他相互关联的行为等，此时若没有及时进行有效检测，或检测出的异常行为由于没有达到预定阈值而加以忽略，就会使攻击者得以进一步实施实际攻击行为，而对实际攻击行为没有相应的检测与反应措施，最终将可能造成严重危害，如系统崩溃，病毒扩散，重要文件被删除等。具体的攻击可能性以及实际攻击所能造成的危害程度还与攻击者本人知识和技术能力、风险承受能力、资源以及受惩罚的可能性有关[4]。图 1 显示了内部攻击形成过程。

为了及时预防、检测和阻止内部攻击和信息泄漏，需要捕获和研究技术控制、安全常规控制和环境因素三者与内部攻击之间的动态关系，通常是一种相互制约、相互促进的关系。例如某公司可能对公司内部信息安全不够重视，缺少相应的安全教育与培训计划，也没有专家咨询，对信息安全方面的投资较少，公司高层管理人员乃至广大员工对内部信息安全关注不多，相关安全法规不完善，执法效率低下，人们对法规和政策缺乏尊重，在这种不利的安全环境因素下，往往意味着公司内部只有低水平的安全常规控制，如不能进行定期的安全评估，没有对公司内部进行安全级别划分，缺乏对雇员适当的监控，对离、辞职人员更疏于处理等等，常规安全控制的管理混乱，致使当前仅有安全措施也不能有效发挥作用，例如对雇员缺乏适当监控，使得雇员可以随意进行违规操作或绕过相关检测，最终将导致重大安全隐患。因此有必要采用智能化技术手段加强安全控制管理，特别是加强权限与角色管理，将不

同人员分级，为不同部门制定不同策略以适应各自的工作情况，根据其权限对信息进行管理，例如适用于公司领导层转发邮件进行决策就不适用于普通员工；建立雇员档案与安全机制之间关联，使得雇员离开公司时就立刻清除其所有角色关系，进而保障内部系统安全。技术手段可以及早遏制、发现和防止内部隐患，从而进一步增强企业内部安全防范意识，形成良性循环的安全体系。图 2 显示了一个内部信息安全动态控制影响模型。

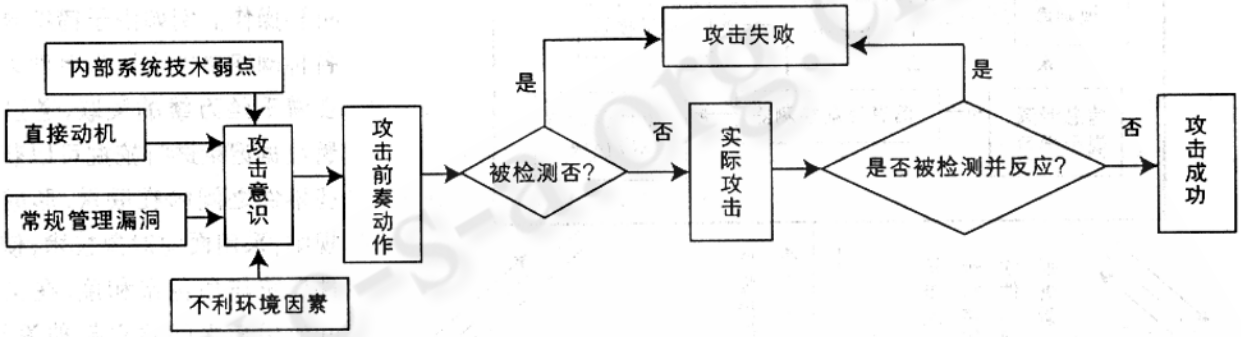

图 1　内部攻击过程

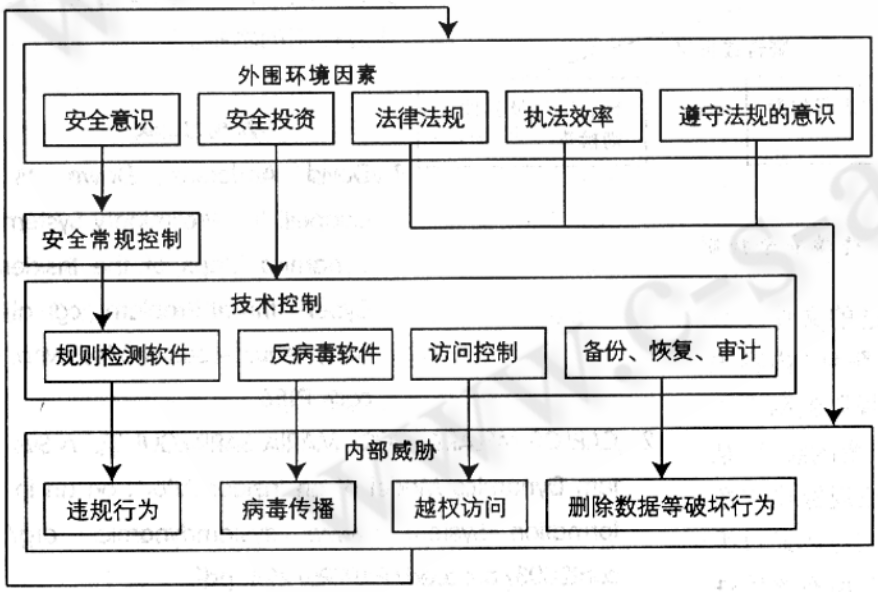

图 2　内部信息安全的动态模型

4　防信息泄漏体系的设计与实现

对于一个公司或企业，可以采用分布式手段，通过客户机——服务器模式实现内部信息安全的控制。终端（客户机）负责自身大部分安全监测工作以及信息收集，主控机负责保证各终端能正常运行监测程序，定期更新及分发安全规则，综合分析来自各终端的监测报告，这样大大减轻了主控机负担，其安全控制机制如图 3 所示。

由图中可见，每个客户终端机安装监测软件，并包括一个规则库，该规则库定期被主控机刷新，其信息包含有安全常规规则、技术规则，可以手动添加，也可以通过智能自动生成。我们用特定规则关键字分析文件名、进程名、消息头、内容及附件内容，根据最终的权重参数和同义词特征提供与所扫描内容更精确的匹配，进而阻塞、隔离用关键字进行标识的文件和进程，允许管理员或用户在通常信息后附加标准文字。可以在消息开始和末尾处添加拒绝文本，通过使用上述技术，管理员能限制不适当消息的交换。监测软件在本机起机后可以检查是否运行了一些必要程序，如反病毒软件，防火墙，规则检测软件等，否则将自动从主控机下载、安装并激活该程序，若不能激活该程序，则关闭本机；监测软件还监视本机是否运行了禁止运行软件，如游戏，一旦察觉就杀死该进程；此外，它还要监视日志异常信息，进行审计等工作。总之，监测软件负责检查并及时阻止违规行为，还要将该行为记录下来，写入监督报告，上报至主控机进行综合分析。

系统内部有一个主控机（服务器），主控机程序负

责监视各个终端是否运行了监测软件，若发现某终端未运行监测软件，则关闭该终端；主控机程序还负责综合分析各个终端传来的监督报告；对于内部攻击行为建立严格的取证体系，为内部人员建立档案，密切关注他们的行踪，采用数据挖掘等技术分析内部人员日常

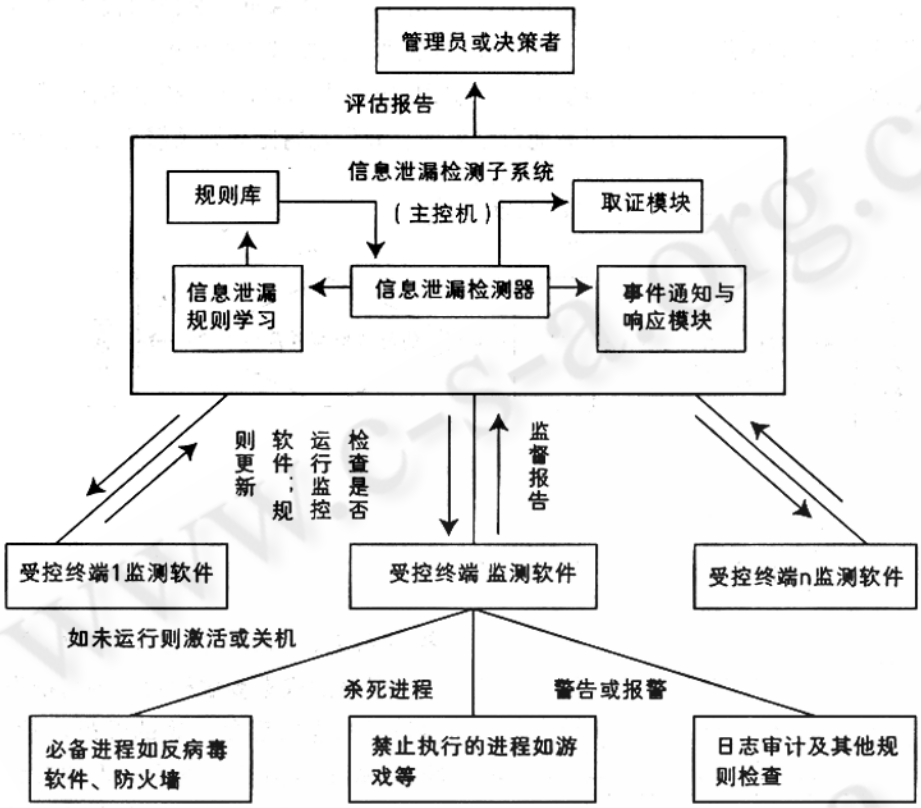

图 3　主控机—终端安全控制

行为，如其所访问的网站、拷贝或删除过的文件及数量，邮件（附件）的大小和个数，对邮件（附件）内容进行关键字检查，基于内容关键字对违反规则的网页进行回放，某时间段内所用各协议或端口流量的统计，某段时间内 cpu 或内存占用比率，越权或违规操作次数等，以便日后用于综合分析取证。此外，它可以通过手动或智能学习对规则进行更新，并定期向所有终端进行分发。主控机要根据各终端报告并结合内网安全环境因素进行智能分析，定期生成安全评估报告，交给管理员或决策者，进而调整安全策略，达到整体范围内的安全优化。

5　结论及研究展望

本文通过分析显示，外围安全环境、安全常规控制、技术控制与内部威胁之间存在动态制约关系，并阐述了采用分布式手段，通过客户机——服务器模式实现内部信息安全控制的基本方法。随着研究的深入，有必要进一步采用数据挖掘、人工神经网络等技术对各要素进行智能化分析和操作。例如由于错综复杂的各种网络事件或行为事件之间存在着千丝万缕的关联，通过对大量数据记录进行挖掘可以获得这些事件之间内在联系，形成关联规则；采用面向对象技术，使用文件血统与角色亲和度，在文件之间或用户之间建立某种关联，进而实现文件的安全控制；利用人工神经网络模拟内网各要素动态变化，使得整个内网安全达到自适应控制的水平。

参考文献

1 David Andersen, Dawn M. Cappelli 等. Preliminary System Dynamics Maps of the Insider Cyber – threat Problem. cgi. albany. edu/ ~ sdsweb/sdsweb. cgi? P186 .

2 CARLOS MELARA, JOSE MARIA SARRIEGUI 等. A System Dynamics Model of an Insider Attack on an Information System. www. systemdynamics. org/conf2003/proceed/PAPERS/294. pdf.

3 Chris Bateman, Dawn Cappelli, Casey Dunlevy 等. System Dynamics Modeling for Information Security . www. cert. org/research/sdmis/insider – threat – desc. pdf.

4 董良喜、王嘉祯、康广，计算机网络威胁发生可能性评价指标研究，计算机工程与应用，2004. 26，143 ~ 144。