具有预警功能的网络监管体系结构研究*)

张险峰 张 峰 秦志光 刘锦德
(电子科技大学计算机学院 成都610054)

Research on the Architecture of Network Monitoring Administration with Precaution

ZHANG Xian-Feng ZHNG Feng QIN Zhi-Guang LIU Jin-De
(College of Computer Science and Engineering, UESTC of China, Chengdu 610054)

Abstract The architecture of network monitoring administration with precaution is presented. Related technologies and approaches to realize the architecture are analyzed and provided. The architecture consists of a precaution subsystem and a monitoring administration subsystem. With building an adaptive abnormal detection model and taking abnormal assessment approach, the precaution subsystem can forewarn the intrusion attempts and send the precaution information to the monitoring administration subsystem in real time. Then the monitoring administration subsystem can take some countermeasures in advance. Moreover, based on intrusion tolerance technology, the monitoring administration subsystem can reconfigure the resources and the security policies when facing active intrusions, so as to provide the expected users with timely services and ensure the security of the protected services as well.

Keywords Network security, Precaution, Monitoring administration, Architecture, Intrusion tolerance

1 引言

目前,针对入侵检测系统(Intrusion Detection System, IDS)的研究方兴未艾,如 RealSecure、NetRanger、NIDES A.14、EMERALD A.19、Ripper A.21等。每一种都存在各自的缺点,比如较高的误警率或漏警率[1]。而且,IDSs 即使是能检测到入侵,入侵行为可能已经造成了严重的破坏。现代信息战的突然性空前增加,一个国家要保持常备不懈,有效地防御网络空间的突然袭击,应该通过运用预警技术监视识别大规模网络上的入侵企图和入侵行为,在入侵发生或入侵造成严重后果前,预先采取相应的监管措施来加强网络的安全。具有预警功能的网络监管技术主要涉及到入侵评估、预警信息的产生和处理、安全监管等技术。文[8]对入侵评估进行了研究,但对预警的策略没考虑。文[9]研究了入侵容忍系统的实现机制,本文借鉴了其入侵容忍的思想来实现安全监管功能。文[11]研究了网络管理模型,但对安全监管特别是具有预警功能的安全监管技术研究得很少。总的来说,目前国内外专门从事具有预警功能的网络监管技术的研究很少。

我们拟设计的具有预警功能的网络监管(Network Monitoring Administration with Precaution, NMAP)技术保护的对象是一些关键的、具有战略意义的网络服务,如:政府、国防和金融等部门的网络应用。要彻底杜绝网络入侵行为是不可能的,然而由于攻击者经过一个大规模网络进行入侵需要按一定步骤、花费一定时间来实施,我们就有可能通过对网络数据的实时收集、分析来对还未完全实施的入侵进行预警,进而做到主动防范。

本文中,我们对具有预警功能的网络监管体系结构进行了初步的研究。包括体系结构中各子系统的组成、各子系统间的关系、以及实现该体系结构所涉及的主要方法。

2 NMAP 的体系结构

为了对至关重要的网络服务进行分层次的保护,我们按安全可信程度对网络划分安全边界,形成不同的网络区域[7],并把要保护的服务放在安全可信度最高的区域。网络区域具体分为:内网,DMZ(Demilitarized Zone,非军事化区)和外网。内网的安全可信度最高,DMZ 次之,外网的安全可信度最低(可认为零,区域最广,攻击者也最多)。

NMAP 的体系结构由预警子系统(Precaution Subsystem, PS)和监管子系统(Monitoring Administration Subsystem, MAS)构成(见图1),两个子系统分别位于不同的网络区域。PS 基于分布式入侵检测系统原理来实现,主要包括两类部件:探测器代理(Sensor Agent, SA)和预警单元(Precaution Unit, PU)。SA 安装在外网的不同网络节点中,每个 SA 都是自治的 Agent。SA 应被分成不同的群。每个群负责收集特定区域的数据,且每个 SA 群对应一个自己的 PU,以方便管理,且可以在达到数据收集目的的情况下使整个系统经济、简洁。PU 安装在 DMZ 中,具有一定的安全性。每个 PU 均与 MAS 相连,各 PU 间有独立的通信链路,能相互交换预警结果,进行分布式协作处理。从 SA 到 PU 间的连结可以通过代理服务器也可通过直接连结。连结应支持不同的类型,在公共可访问的网络中,我们拟采用 SSL 来对 TCP 包加密。从 PU 到 MAS 的连结介质可以专用可以共享。在共享模式下,对被传送的数据应采取某种认证或加密的措施。MAS 安装在内网中,且处于被保护服务器的前端,这在一定程度减少了 MAS 和被保护服务器被攻击的机会。另外,安全管理员可在内网通过访问控制、认证等机制,增强其安全,同

*)国家863计划资助项目,项目编号:2002AA142040。张险峰 博士生,主要研究方向:网络安全技术。张 峰 博士生,主要研究方向:网络安全主动防御技术。秦志光 教授,博导,主要研究方向:网络安全、电子商务。刘锦德 教授,博导,主要研究方向:开放系统及其安全、中间件技术。

时减少被保护服务器需处理的服务请求，提高工作效率。

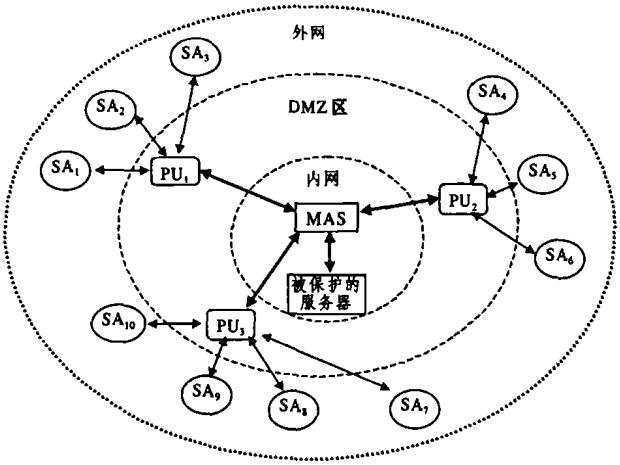

图1 NMAP体系结构示意图

当某个SA出了故障时，其状态可被其相连的PU检测出来并恢复到正常工作状态。如果某个PU出了故障，其工作状态可由其它PU或MAS检测出来并得到恢复。

在图1中，SA_1至SA_{10}为多个分布在外网的探测器代理，负责收集网络数据，由于我们只关心保护内网的服务，为了减少PU接收和处理的数据量，SA可对网络数据进行过滤，仅给PU传送那些目的IP属于DMZ和内网中的数据包，这样可以减少通信流量，提高效率。PU通过预警分析后产生预警信息发送到MAS，在MAS将根据预警信息的异常程度采取不同的防范措施。我们将在后面章节对PS和MAS进行更详细的讨论。

3 预警子系统(PS)的设计

PU是PS的核心组件，也是整个系统实现预警的关键，其主要功能是对各个SA发来的网络数据进行分析，实现预警。为了能够对已知和未知形式的攻击进行预警，我们拟在PU中采取误用检测和异常检测相结合的方法。

3.1 PS的结构设计

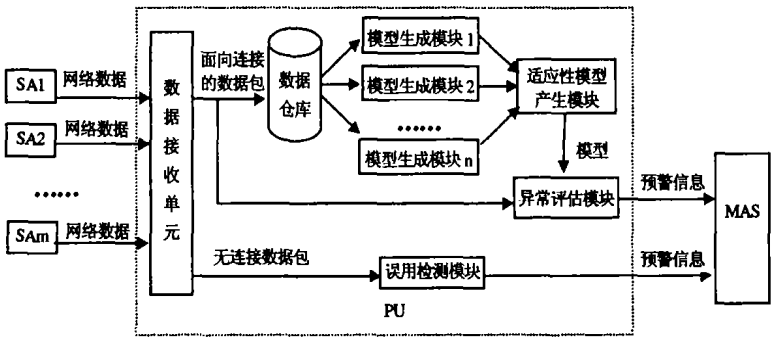

图2 预警单元(PU)的组成

在图2中，一个PU由虚框内的组件组成。数据接收单元从SA接收到的数据可以分为两类：面向连接的数据包和无连接的数据包。PU根据数据类型的不同进行不同的处理：(1)对于非连接数据包(如UDP包)，由于连续的若干个包可能是不同的SA发来的，PU很难对这些数据包进行关联，因此采取基于模式匹配的方法进行误用检测，如果检测到入侵企图，误用检测模块将产生预警消息并传之给MAS。此种方法对于未知形式的攻击无能为力，但对已知的攻击检测速度快，误警率低。(2)对于接收到的面向连接的数据包(如TCP包、ICMP包)，PU其格式化为预定的数据格式(如审计记录格式)后，同时传送到数据仓库和异常评估模块。数据仓库可根据模型生成模块的要求产生相应的训练数据，进而构建评估模型，并将生成的模型传送给异常评估模块，然后由异常评估模块对传来的审计数据进行异常评估(异常评估的方法将在3.3节中详细介绍)，进而可产生预警消息，并传送给MAS。由此可以看出，用于检测的模型是在现有模型的基础上，根据当前接收到的审计数据而对现有模型进行的修正，并把新产生的模型赋予异常评估模块，所有检测模型的产生具有自适应性。在图2中的1至N个模型生成模块，可根据要保护的服务类型(如telnet、ftp、http等)来区分。

3.2 自适应模型产生方法

通过对系统收集的大量审计数据集应用数据挖掘方法建立异常检测模型，从经验上证明是非常有效的[3~5]。然而，基于数据挖掘来建立异常检测模型要求产生用于训练的数据成本很高，并且从一个环境训练得到的模型往往不能很好地在其它环境里执行。因此，我们引入了在噪声数据背景下能够动态建立异常评估模型的方法[2]，该方法描述如下：

假设入侵事件相对正常行为而言是小概率事件。令一条审计记录 x_t 是入侵的概率为 p(因此 p 很小)，其产生符合的概率分布为 A；则 x_t 为正常数据的概率为(1−p)，相应的概率分布为 N。故此时整个数据产生所服从的分布满足 D=(1−p)N+pA 。设数据集 S 由分布 D 产生，并分为正常数据集 N 和异常数据集 A，这里 N 和 A 分别为分布 N 和分布 A 产生。假设处理完审计记录 x_t 后，正常数据集为 N_t，异常数据集为 A_t。初始时，由于还没检测任何异常数据，故：$N_0=S$，$A_0=\phi$。

检测某条审计记录 x_t 是否异常就等价于决定 x_t 是由分布 A 产生还是由分布 N 产生，A 产生的记录为异常数据，而 N 产生的记录为正常数据。定义分布 D 在接收到第 t 条记录的似然函数为：

$$L_t(D)=\prod_{i=1}^{|S|}P_D(x_i)$$

$$=((1-p)^{|N_t|}\prod_{x_j\in N_t}P_{N_t}(x_j))(p^{|A_t|}\prod_{x_j\in A_t}P_{A_t}(x_j))$$

这里 P_{N_t} 和 P_{A_t} 分别是正常数据和异常数据的概率分布。假设：

$N_t=N_{t-1}\backslash\{x_t\}$，$A_t=A_{t-1}\cup\{x_t\}$

如果比值(L_t/L_{t-1})大于某个值 t(t 为表征异常的敏感值)则判定记录 x_t 为异常，并将该数据由数据集 N_t 转移到异常集 A_t，否则该审计记录仍属于 N_t，即 $N_t=N_{t-1}$，$A_t=A_{t-1}$。

对每条审计记录重复此过程，最后我们从整个数据集中

可清除异常数据，得到适合于训练的正常数据集，此时我们就可以选择合适的建模方法来对数据集进行建模，如文[6]给出了一个基于系统调用的建模方法。

3.3 预警方法

每个 PU 从相应的 SA 接收到基于连接的数据包后，通过动态产生的模型可计算每个主体行为的偏移程度。我们以 POI(Probability Of Intrusion)来表示一个主体当前行为与其正常行为轮廓相比较的偏移程度，它也表示一个主体实施入侵行为的概率。这种对入侵概率的度量同文[8]的方法有些类似。每个 PU 可按以下步骤来计算某个主体的 POI：

(1)根据审计记录计算该主体的各个测量值。

(2)根据测量值的分布来计算每个测量值的偏移程度。

(3)综合所有测量值的偏移程度来形成一个偏移结果 D。

(4)计算 POI 值：$POI=\min(1, D/D_{Max})$，D_{Max}表示从历史审计记录中所得到的该主体的最大的偏移值。

在这里，我们定义两个阈值来评估入侵：下界 lb (lower boundary)和上界 ub (upper boundary)，其中 lb = average (POIs)，ub = [min(POIs), max(POIs)]/2，这里 POIs 为历史审计记录中所有主体全部的 POI 值。在一网络中，一般异常行为只占少部分，故正常行为的 POI 值很低(接近于0)，计算出的 lb 将高于正常行为的 POI 值，但低于 ub。

一开始要确定 lb 和 ub 是很困难的，我们可基于评估结果来调整这两个阈值：如果检测结果中有许多误警，我们可适当提高这两个值来降低误警率，这是因为 POI 大于 ub 的数据将被判定为入侵，因此增加 ub 值将减少被判为入侵的数量；如果检测结果中有许多漏警，我们可适当降低 lb 和 ub 值，以使异常的 POI 值达到应该预警的下限 lb，过高的 lb 将会漏掉一些本应被预警的数据。

确定适当的阈值后，我们可按以下方法对审计数据进行评估：

(1)如果某主体的 POI 大于等于 ub，则检测到了一个入侵，产生有入侵行为发生的预警信息给 MAS。

(2)如果某主体的 POI 大于等于 lb 但小于 ub，产生有异常行为(此时的异常行为不足以说明为入侵行为)发生的预警信息给 MAS。

(3)如果主体的 POI 值小于 lb，则继续执行。

如果网络数据被检测为入侵，则可将这些数据记录到数据库以做进一步分析或用于日后的法律取证。

4 监管子系统(MAS)的设计

MAS 安置在内网的受保护服务器的前端。其结构见图3。MAS 主要由以下组件组成：一组代理服务器、一组投票监控器、一组接收监控器、适应性重配置模块和审计控制模块。MAS 的设计借鉴了文[9]提出的入侵容忍系统的思想。

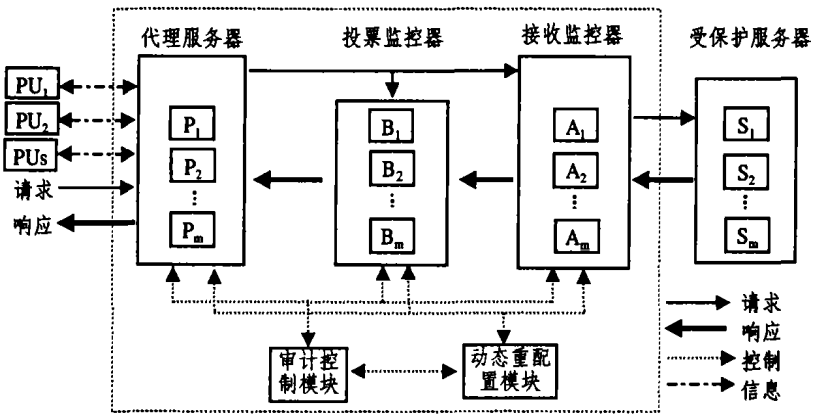

图3 监管子系统(MAS)的系统结构

代理服务器代表受保护服务器接收用户的服务请求，同时也作为 MAS 的数据接收部件接收 PU 发来的预警信息。由于某些攻击可能成功避开预警系统的检测，因此监管系统本身也应具有入侵检测的功能，其入侵检测技术应与预警子系统所采用的入侵检测技术不同，以便形成分层检测，相互补充。另外，代理服务器在性能上、在资源配置上可冗余，在平台(如操作系统)和执行方法上进行多样性设计，这样就可免除同种类型的攻击。

对于在内网里存在的对受保护服务器的攻击行为，本体系结构中没有设计对它们进行预警的机制，因为它们和受保护服务器处于相同的安全可信度的区域，MAS 很难有足够时间对它们进行预警，这些攻击主要依靠监管子系统中入侵检测功能来识别和阻止。

如果 MAS 接收到的是预警信息，在 MAS 应能关联接收到的预警信息，根据正常情况下的信息流量和特征等进行比较，推测入侵威胁的种类、发生地点等，对可能发生的入侵行为进行威胁程度预测，在遭受到攻击前动态调整安全策略，对软硬件资源进行重新配置来增强防御能力。具体的重配置措施包括改变对客户的访问控制(如限制访问某些关键的服务)，和/或暂时挂起不重要的服务直到系统从攻击状态恢复，和/或改变用于处理客户请求和增加审计等所需的冗余程度等。

如果 MAS 接收到的是用户服务请求，代理服务器根据入侵容忍策略来执行服务策略。该服务策略决定当前服务器形成的请求应转发到哪个受保护的服务器，同时决定如何对该请求判决来形成最后的响应。当受保护服务器产生响应时，首先送到接收监控器进行有效性检测，随后接收监控器把该响应和有效性检测结果传送到表决监控器。在接收监控器也可通过入侵检测技术来检测受保护服务器是否被入侵，并为适应性重配置模块提供入侵触发信息。表决监控器作为受保护服务器的代表，根据当前被检测的安全威胁级别，通过简单多数投票或拜占庭协商处理等方法来对最后的响应作出判决。最后的响应通过代理服务器传回给客户。适应性重配置模块可从系统其他所有模块接收入侵触发信息，然后对入侵威胁、容忍对象和代价/性能影响进行评估，进而对整个系统进行重新配置。由于任一单独组件都可能被入侵，因此适应性重配置模块应有备份，以免造成单点失效。审计控制模块的功能是对系统其他组件维护的审计记录进行审计，所有系统模块

可采取签名保护方法来维护审计日志，审计控制模块可对这些日志进行验证。审计控制模块里也可安装入侵触发器，它周期性地给其他组件发出合法或不合法的请求，然后通过验证这些组件的响应来识别异常行为，处理过的响应被传到适应性重配置模块来作进一步处理。

基于入侵容忍机制，系统在面对攻击的情况下，能够识别已被攻破的系统组件，评估破坏程度，进而动态地对软硬件资源和安全策略进行重配置来平滑地降低系统的功能和性能，保持尽量多的关键功能模块的正常运行，增强安全性，同时仍然持续地为预期的用户提供服务。

结束语 在本文中，我们提出了一个具有预警功能的网络监管体系结构，该体系结构并不改变网络用户和受保护服务器的应用，它对端用户和服务器应用都是透明的。该体系结构不仅能增强受保护服务的安全性和可用性，而且是一个具有可扩展性、开放性和通用性的合作框架。

然而，在该体系结构的实现上，尚有一些难题需要解决。一个高度可重配体系结构应具备多种入侵容忍策略并支持不同级别的安全需求。这就需要选择不同的入侵容忍技术、资源冗余程度等措施等来定义不同的策略，还涉及代价/性能比的折衷问题，非常复杂。而且，在运行时对安全策略的重配置可能导致以传统方式设计的软件(没有考虑到动态的安全)不同程度的出错，包括关键进程不期望的终止[10]。我们将在下一步工作中对这些难点进行研究。

参 考 文 献

1 Axelsson S. Intrusion detection systems: a survey and taxonomy. 14 March, 2000. Available at http: // citeseer. nj. nec. com/axelsson00intrusion. html

2 Mukherjee, Heberlein L T, Levitt K N. Network intrusion detection. IEEE Network, 1994, 8(3): 26 ~ 41

3 Eskin E, Miller M, et al. Adaptive Model Generation for Intrusion Detection Systems. Available at: http: // www. cs. columbia. edu/ids/publications/adaptive-ccsids00. pdf

4 Lee W, Stolfo S J, et al. Real Time Data Mining-based Intrusion Detection. Available at: http: // www. cs. columbia. edu/ids/concept/

5 Lee W, Stolfo S J, Mok K. Data mining in work flow environments: Experiences in intrusion detection. In: proc. of the 1999 conf. on Knowledge Discovery and Data Ming (KDD-99), 1999

6 Warrender C, Forrest S, Pearlmutter B. Detecting intrusions using system calls: alternative data models. IEEE Computer Society. In: Proc. of the 1999 IEEE Symposium on Security and Privacy, 1999. 133~145

7 King M, Dalton C E, Osmanoglu T E. Security architecture: design, deployment and operations. Sydney: Osborne/McGraw-Hill, 2001. 132

8 Yau S S, Zhang Xinyu. Computer network intrusion detection, assessment and prevention based on security dependency relation. Available at: http: // dlib. computer. org/conferen/compsac/0368/pdf/03680086. pdf

9 wang Feiyi, Gong Fengmin. SITAR: A scalable intrusion-tolerant architecture for distributed services. In: Proc. of the 2001 IEEE. Workshop on information Assurance and Security. United States Millitary Academy, West Point, NY, 2001 Available at: http: // panda. ece. utk. edu/~fwang2/papers/SITAR-norfolk-2001. pdf

10 Petkac M, Badger L. Security agility in response to intrusion detection. Proceeding of the Sixteenth Annual Computer Security Applications Conference (ACSAC'00). Available at: http: // www. acsac. org/2000/papers/43. pdf

11 Van Hemmen L J G T. Models supporting the network management organization. International Journal of Network Management, 2000, 10: 299~314

(上接第79页)

络连通的概率仍可保持在99%以上。

参 考 文 献

1 王国军，陈建二，陈松乔. 具有大量错误结点的超立方网络中的高效路由算法的设计与讨论. 计算机学报，2001，24(9)：909～916

2 Chen Jianer, Wang GuoJun, Chen SongQiao. Locally subcube-connected hypercube networks: Theoretical analysis and experimental results. IEEE Transactions on Computers, 2002, 51(5): 530～540

3 王高才，陈建二，张祖平. aMesh 网络容错概率上界及其证明. 卢正鼎主编. 2002全国开放式分布与并行计算学术会议论文集，武汉：华中科技大学出版社，2002. 295～298

4 Lillevik S L. The Touchstone 30 Gigaflop DELTA Prototype. In: Q. F. Stout, M. Wolfe, eds. IEEE Proceedings of the Sixth Distributed Memory Computing Conference. Portland, Oregon: IEEE Computer Society Press, 1991. 671～677

5 Lenosji D, Laudon J, Gharachorloo K, et al. The Stanford DASH Multiprocessor. IEEE Computer, 1992, 25(3): 63～79

6 Agarwal A, Bianchini R, Chaiken D, et al. The MIT Alewife Machine: Architecture and Performance. In: Santa Margherita, ed. IEEE/ACM Proceedings of the 22nd Annual Intl. Symposium on Computer Architecture, Ligure, Italy: ACM Press, 1995. 2～13

7 Cray Research Inc. Cray T3D System Architecture Overview. Technical report, HR-04033, March 1994.

8 Alverson R, Callahan D, Cummings D, et al. The Tera Computer System. In: Proc. of the1990 Intl. Conf. on Supercomputing. 1-6, 1990. http: //citeseer. nj. nec. com/alverson90tera. html

9 Allen F, Almasi G, Andreoni W, et al. Blue Gene: A vision for protein Science using a petaflop supercomputer. IBM Systems J., 2001, 40: 310～337

10 Boppana R V, Chalasani S. Fault-tolerant wormhole routing algorithms for mesh networks. IEEE Transactions on Computer, 1995, 44(7): 848～864

11 Almohammand B F A, Bose Bella. Fault-tolerant communication algorithms in toroidal networks. IEEE Trans. Parallel and Distributed Systems, 1999, 10(10): 976～983

12 Gaugha P T, et al. Distributed, deadlock-free routing in faulty, pipelined, direct interconnection networks. IEEE Transactions on Computers, 1996, 45(6): 651～665

13 Suh Y J, Yalmanchili S. All-to-All Communication with Minimum Start-up Costs in 2D/3D Tori and Meshes. IEEE Trans. Parallel and Distributed Systems, 1998, 9(5): 442～458

14 Chen C-L, Chiu G-M. A fault-tolerant routing scheme for meshes wth nonconvex faults. IEEE Trans. Parallel and Distributed Systems, 2001, 12(5): 467～475