一种基于 Switchware 的主动网络安全机制的研究

Study on the Security Mechanism of Active Network Based on Switchware

马 燕[1] 杨晓红[1] 李 波[2]

(重庆师范学院物理学与信息技术系 重庆400047)[1] (重庆工业管理学院计算机科学系 重庆400031)[2]

Abstract The problem of security is an emphasis of the research fields in Active Network, this paper discusses some of the characteristic of security such as the principle of attacks and protects in Active Network. Based on this, the paper studies emphatically the architecture and implementation of a Secure Active Network Environment (SANE), the mechanism of secure bootstrap AEGIS, and the mechanism of visiting resource ALINE and the mechanism of dynamic security. Finally the author brings forward a reformative project of dynamic security.

Keywords Security of Active Network, SANE, AEGIS, ALING

1 主动网络

主动网络(Active Network)的概念是在1995年由DARPA(Defense Advanced Research Projects Agency)研究协会提出来的。主动网络赋予网络"编程"的功能,即网络的行为是可控制的并且是与应用相关的。主动网络把更多的计算处理任务放在网络节点中,在不增加带宽的情况下,更加有效和智能地利用现有带宽,使资源得到充分使用。

与传统的网络相比,主动网络具有更大的优势。它可以为分布式系统更好地协调不同设备的工作、进行负荷的均衡处理、有效地避免单点故障;主动网络加速了网络结构的更新,由于主动网络中节点可编程控制,因此任何用户的程序都可以视为是对节点功能的扩充,这意味着网络结构和技术的更新工作都分配给了所有的用户,也不再需要为网络的每一种新功能制定新的标准,只需要制定主动网络语言的标准即可;主动网络还可以方便地实现网络的监控和事件过滤的智能化管理,主动网络中的交换设备之间以及交换设备与用户之间可以交换程序代码,有利于提高网络协议的适应性,因此它具有比传统网络更为强大的交换能力。因此,主动网络具有更为广阔的前景。

2 主动网络的安全问题

安全性是网络的一个非常重要的问题。主动网络的安全问题比以往更重要,因为数据包中携带了对网络节点资源进行访问的程序,它们在很大程度上可以对资源进行调用、修改等操作。因此,主动网络除了需要解决面临恶意攻击时系统的保密性、完整性和可用性等一般问题外,还要解决于信包中代码的出错和不期望的行为而导致的风险。在主动网络中,重要的通信元素有:信包、主动节点、网络资源,其中信包和主动节点可能会相互攻击,也可能会对网络中的资源进行攻击。因此,如何构建一个安全的主动网络环境,是当前研究的主要课题。

主动网络中的安全威胁主要有:破坏,主动信包与主动节点之间的相互攻击而使得信包或者是主动节点受到破坏;拒绝服务:主动节点由于被破坏或其它原因拒绝为主动信包服务;偷窃:主动信包非法获取主动节点的保密信息,节点非法获取主动信包中的用户信息;组合攻击:网络中用户非法向网络的一些中心路由器发送大量的主动信包,从而占用其所有带宽,使其瘫痪。

在主动网络中,为保证通信的安全,就必须同时对主动信包和主动节点进行保护。

(1)对主动节点的保护:对于主动网络中节点的保护措施一般有①代码认证:通过一个认证证书来实现,证书能够验证和识别代码发送者的数字签名和公钥,以确认主动代码的来源。②代码验证:在代码执行前首先运行代码验证程序,以确定在信包中是否有非法的代码,从而避免执行时造成对主动节点的破坏。③存取控制:控制代码对于主动节点的信息、网络资源等的访问。系统会根据主动代码的认证证书和系统的安全策略决定代码在主动节点上的访问权限。④限制技术:主要有时间限制(限制主动信包在主动节点上的执行时间),范围限制(限制主动信包能够经历的主动节点范围)等。通过这些手段从而有效地阻止主动信包对主动节点的攻击。

(2)对主动信包的保护:实现主动信包的保护一般有两种方式:加密和容错技术。加密是指对信包进行代码置换,使得在信包中不包含有明文代码和数据,这与传统的网络中信包的加密过程是相似的。而容错技术是实现对信包的备份、持续和重定向。备份是指在信包所经过的节点上对信包进行复制;持续是将信包临时存储以防止节点失效。对于这两种处理方式,均要消耗节点大量的存储资源和网络带宽,因此仅对重要的信包才这样处理。重定向是指在默认的路径失效时,信包重新建立一条通道,寻找另一路由。重定向主要消耗 CPU 的周期,它在信包保护方面有广泛的应用。

此外,精心设计主动网络的编程语言也是提高安全性的一条重要途径,通过语法和语句的精心选择可以限制一些不希望发生的动作,并提高其性能。

3 SANE—基于 Switchware 安全机制的研究

Switchware 是美国 Pennsylvania 大学的 SwitchWare 项目组研制出来的主动网络系统,它是基于可编程的 SwitchWare 交换机方案,主动节点由一个可编程元件来实现交换功能。在这种方案中,包的格式保留现有的不变,因此与现有的网络兼容性好,具有广阔的应用前景。在 Switchware 的系统

马 燕 副教授;杨晓红 讲师;李 波 教授,博士。

中采用了主动网络程序设计的语言 PLAN(Programming Language of Active Network),它用于在包中描述用户程序功能并可以调用节点低层功能模块。

3.1 SANE 的层次结构

为保证系统运行的安全性,Switchware 必须运行在一个安全的网络环境中,因此,SwitchWare 项目组提出了基于 Switchware 的层次结构:主动报文、交换点和安全主动路由器、安全主动网络环境 SANE(Secure Active Network Environment)。并将 SANE 作为结构中一个非常重要的组成部分。其层次结构如图1所示。

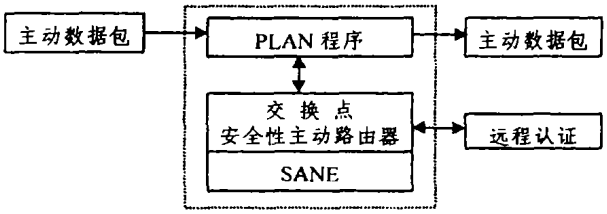

图1 Switchware 的层次结构

从图1中可以看出,主动报文在主动点上由 PLAN 提供相应的主动服务功能,PLAN 根据信包类型向交换点提请相应的服务功能,交换点提供网络服务的基本原语,并负责解释执行主动信包分组中的程序。整个系统建立在 SANE 基础之上,SANE 保证整个网络从自举到整个程序设计环境的安全一致性。

作为一种主动网络的安全机制,SANE 提供的安全性有静态和动态两类。静态检查的安全性很高,但是其代价也相应较高,因此这类检查不经常使用(如网络自举时使用)。动态检查是经常使用的,这类检查应在不降低安全性能的前提下简单使用,以降低系统的代价。

SANE 采用分层的体系结构,如图2所示。

在 SANE 系统中,体系的下层进行静态检查,它确保系统启动后进入到预期的状态。具体是通过一个 AEGIS 即安全启动机制来实现的。AEGIS 完成了启动之后,系统在运行过程中由动态检查来实现其安全性能。动态检查是对每个用户或是对每个数据包为单位进行的,它处于高层次端。主动网络中的元素处于运行状态时,其动态检查一般通过如下几种途径来实现:

1. 系统进行远程认证,如果需要还可进行节点到节点之间的认证;

2. 为所接收到的信包提供一种受限的运行环境;

3. 在各用户之间提供一种新的命名方式以区分节点服务名空间。

在上述体系中,有一个非常重要的要素,这就是公共密钥系统。它假定每个用户或用户组以及每一个主动信包都拥有一个公共或私有的密钥,用以鉴别或认证实体的身份。

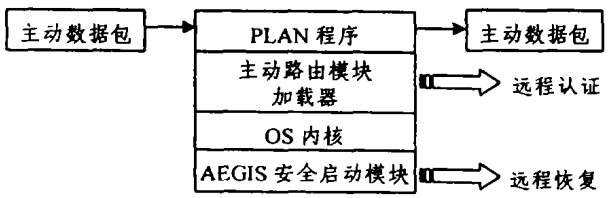

图2 SANE 的层次结构

3.2 安全启动机制 AEGIS

AEGIS 修改了 IBM PC 的进程处理的标准,以便所有的可执行代码(除了小部分可信任代码之外)在运行之前都通过数字验证。在 SANE 的结构中,AEGIS 假设系统的 BIOS 中的前32K 是不可修改的,这里存放着加以保护的密钥源。如期望系统具有自动恢复的能力,则此密钥源存放在一个可以恢复被损坏部分的位置。在上述假设前提下,安全启动进程便可以在用户进入每一级系统(如 BIOS 的初始化、Flash ROMS、Boot Block、OS 等)之前进行密码的认证。

如果认证失败,SANE 系统开始试图进行修复,由于安全启动是在网络中的节点实现的,因此需要远程启动。SANE 提供了一个远程恢复协议来实现被检查到错误部分的拷贝。如果信任源可用,系统就会为被损坏的部分提供一份正确的拷贝,系统重新安装后便可重新启动。SANE 的 AEGIS 将一种新技术 CLIC(Chained Layered Integrity Checks)应用于可修改的体系结构。

AEGIS 的控制机制如图3所示。

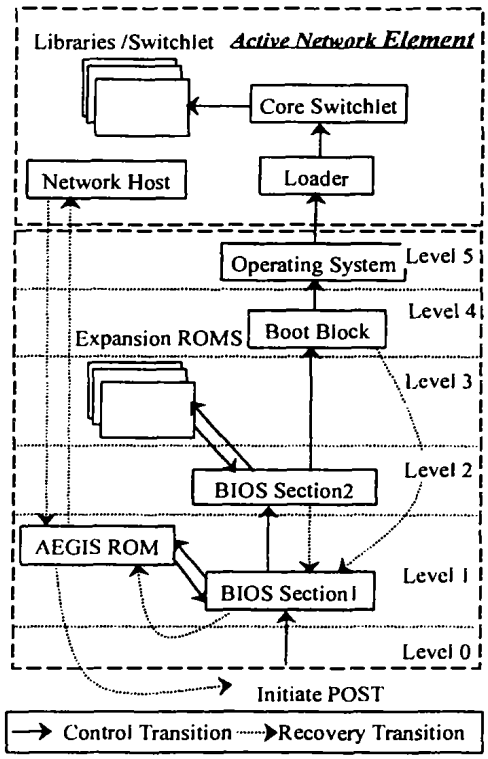

图3 AEGIS 启动控制流程

为了使结构更加清晰,将 AEGIS 的启动过程分层次来展示。层次越往上增加,则 AEGIS 所提供的功能也就越复杂。在最低层 Level 0,包含了很少的可信任代码、数字签名、公用密钥和恢复代码。系统假设该层是合法的,它主要是执行初始校验测试以识别 PROM 是否失效;在 Level 1层是包含有 BIOS 代码和 COMS 数据以及 AEGIS 的引导程序;Level 2层则包含有 BIOS 的剩余代码;Level 3包含所有扩展卡相关的 ROM 数据;Level 4层包含有操作系统引导块;Level 5是操作系统的核心模块。

传统的引导过程是通过调用指令由低层向高层进行,每一层的跃变不需要进行校验。而 AEGIS 系统则利用公用密码系统和加密的散列来保护从低层向高层的跃变的安全性。其恢复过程是通过信任源以确保在失败事件中下一个层次的完整性。

信任源可以存放在图3中的 Expansion ROM 之中，也可以存放在另一个节点上，它包含了验证拷贝所需要的软件。在第一种情况下，启动失败时通过内存中一个简单的拷贝就可以进行修复。如果它存放在网络中另一个节点上，当启动失败时就会通过远程请求另一个节点启动恢复程序，该程序由网络中可"信任"的主机通过安全恢复协议由远程实现错误部分的拷贝，这样即可以进行错误部分的修复，从而实现系统的重新启动。

AEGIN 机制通过改造 BIOS 系统、利用 FreeBSD UNIX 的思想而提升了 X86结构中的 OS 核心层次。AEGIN 的恢复算法还在发展中，但它将更多地吸收 OpenBSDR 中 IPSEC 协议的思路。

3.3 资源访问机制 ALIEN

ALIEN 的任务是控制信包对网络中资源的访问，确认一个应用程序（称为 Switchlet）不能超越其资源访问权限。ALIEN 包含了三个模块：Loader、Core Switchlet 和 Libraries /Switchlet。

Loader 模块是网络动态安全检查的基础，是 ALIEN 系统的核心部分。提供了系统所需要的最小化服务设置和操作系统的接口，并寻找和启动 Core Switchlet 模块。同时如果需要，Loader 还提供了策略和机制来改变 Core Switchlet 的执行状态。Loader 由三个基本模块组成：

1. Startup routines：系统的初始化；
2. Switchlet loading：按照安全策略动态加载 Switchlet；
3. System console：控制读循环。

Core Switchlet 是一个具有优先权的系统区域，它对用户是透明的。Core Switchlet 决定了系统的安全策略，通过添加或删减其功能，它能够确定 Core Switchlet 所工作的权限。由于 Core Switchlet 是可以加载的，因此在需要时，管理员可以改变或升级它的模块。它所提供的服务和功能由6个基本的模块组成：

1. Language primitives：提供访问语言基本功能的策略；
2. Operating system access：提供访问操作系统功能调用的策略；
3. Network access：提供访问网络的策略和机制；
4. Thread access：提供了访问线程的原语；
5. Loading support：支持 Switchlet 加载的策略和机制；
6. Message logging：提供增加记录文件中信息的策略和机制。

Libraries/Switchlet 是一组功能模块，它提供了一些有用的例行程序，这些例行程序不需要特权即可运行。

3.4 动态安全检查

主动节点在运行过程中，主要依靠动态安全性检查来确保按照网络管理员所制定的策略对节点和网络资源的访问。此外，节点也需要提供某种有关访问服务的许可（如用户之间的隔离）。这些许可部分是通过下层的操作系统和编程语言来提供，然而另外一些却要通过附加机制来实现。

主动网络的基本目标之一就是要允许用户在节点上安装自己的协议，可以动态地加载自己的模块。由于这些模块可能需要访问一些临界资源，因此对这些访问进行控制是非常必要的。此外还需要对某些具有"特别权限"的信包进行鉴别。因此，在主动网络的节点之间需要建立某些信任关系。

1. 直接在具有平等的节点之间建立信任。这就意味着可以在这些节点之间为授权者建立确认并可直接进行通信。

2. 采用"通道"方式。在这种方式下，需要通过一个探测信包来一步步地识别下一个节点并确认其信任关系。这样就可以从当前节点开始建立一条通信路径。

在一个主动节点上，如果一个授权者需要根据该节点的策略来请求一次特殊的动作（如使用某种授予特权的资源），节点就需要提供一个批准这种动作的授权证书。因此，就需要在授权者与节点之间建立某种安全的关联，节点可以利用这种关联来鉴别授权者的信包。同时在节点上保存这些关联的信息以便确定对后续的授权者的行为进行干预。

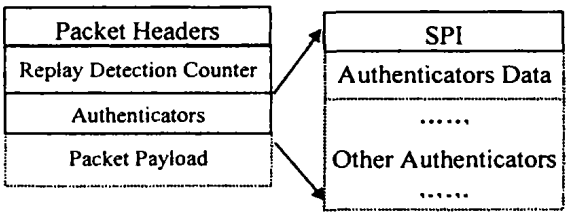

图4 Authenticators

图4显示的是建立了安全性关联之后的包格式（其中的论证（Authenticators）部分）。

在信包认证的部分包含了一个 SPI 域（the Security Parameters Index），它是一个数值，用以指示节点和授权者之间所建立的特别安全关联的标识。

在实际中，要实现这种方式需要付出的代价也是较昂贵的，因为：

（1）时间问题（CPU 的时钟主要耗费在加密的操作上）；

（2）更重要的是包头处理，因为在路径上的每一个节点都需要不同的认证（授权者与每一个节点之间的密钥都不相同）。

上述问题的产生与解决取决于主动节点在运行时的环境、受到攻击和采取防范的类型等。最简单的方法是进行优化处理。授权者可以利用公钥为路径上所有节点分配另外的密钥，由于公钥在信包中只需一种认证，这样信包在路径上所有节点都会被认证。

主动网络是网络体系发展中的一次质的变革，其前景十分诱人。它将成为21世纪网络体系的主流。但是目前很多问题还在研究中，特别是安全问题。因此，如何构建一个安全的主动网络体系，是当前研究的主要课题。SANE 系统由 AEGIS 和 ALIEN 构建而成，为主动网络提供了良好的安全服务。但是对于要求很高的实时系统（如需要提供 QOS 的系统），如果安全处理不及时，那么就无法保证传输质量。因此需要对认证和网络中资源访问的等级进行研究。目前，SANE 在小型实验网络中应用效果良好。在一个拥有数百万个节点的大型或全球网络中，要使 SANE 中的信任建立自动、迅速地实现，并且要使用人们更容易理解的安全策略，尚有很多工作要做。

参 考 文 献

1 Alexander D S，et al. Security in Active Networks. In Secure Internet Programming：Issues in Distributed and Mobile Object Systems，Springer-Verlag Lecture Notes in Computer Science State-of-the-Art Series，1999

2 Alexander D S，et al. A secure active network architecture：Realization in SwitchWare. IEEE Network，May/June，1998(12)：37～45

（下转第75页）

$X=R-(X)=X$，$\langle R^{-1}\rangle X=R^{-1}\cdot X=R^{-1-}(A)=X$

结论5 G是论域，子集$X\subseteq G$，$R\subseteq G\times G$是格。如果X是R的向前封闭集合或向前封闭集合的并集，则$[R]X=R\backslash X=R-(X)=X$，$\langle R^{-1}\rangle X=R^{-1}\cdot X=R^{-1-}(A)=X$

结论6 G是论域，子集$X\subseteq G$，$R\subseteq G\times G$是线性序。如果X是R的向前封闭集合或向前封闭集合的并集，则$[R]X=R\backslash X=R-(X)=X$，$\langle R^{-1}\rangle X=R^{-1}\cdot X=R^{-1-}(A)=X$

结论4、5、6的证明方法同结论3。

在事件结构逻辑(ESL)中，可达关系r_R是树(看作关系)，根据性质结论3，当集合X是R的向前封闭集合或向前封闭集合的并集，则可以得到$[R]X=R\backslash X=R-(X)=X$，$\langle R^{-1}\rangle X=R^{-1}\cdot X=R^{-1-}(A)=X$。

在非确定信息逻辑中(NIL)，可达关系r_R包括相容关系和格，根据结论4、5，如果集合X是半等价关系或半等价关系的并集，则可以得到$[R]X=R\backslash X=R-(X)=X$，$\langle R^{-1}\rangle X=R^{-1}\cdot X=R^{-1-}(A)=X$。

在时态信息逻辑中(TIL)，可达关系r_R是线性序，根据结论6，如果集合X是R的向前封闭集合或向前封闭集合的并集，则可以得到$[R]X=R\backslash X=R-(X)=X$，$\langle R^{-1}\rangle X=R^{-1}\cdot X=R^{-1-}(A)=X$

5.3 近似计算算法

根据结论2，我们可以得出基于关系R的上近似$R^-(A)$和下近似集$R_-(A)$可以通过$R\cdot A$和$R\backslash A$运算得到。

算法1

基于关系R的上近似$R^-(A)$：
设$E=\{x_1,x_2,\cdots,x_n\}$，$R\subseteq E\times E$，
$A=\{y_1,y_2,\cdots,y_m\}\subseteq E$

```
1. 设 R⁻(A)结果初始为 B
2. B=φ;
3. for i=1 to nfor j=1 to m
       if (xi,yj)∈R then
         B=B∪{xi};
4. return B
```

算法2

基于关系R的下近似$R_-(A)$：
设$E=\{x_1,x_2,\cdots,x_n\}$，$R\subseteq E\times E$，
$A=\{y_1,y_2,\cdots,y_m\}\subseteq E$

```
1. 设 R_(A)结果初始为 B
2. B =φ;
3. for i = 1 to n
Xi=φ
       for j = 1 to m
       if (xi,yj)∈R then
          Xi=Xi∪{yj};
       if Xi⊆A then
         B=B∪{xi};
4. return B
```

通过算法1和2我们可以对模态算子进行计算，并运用相应的Rough集精度概念，对不确定性进行描述。

在模态数据表示中，定义由关系R分类的近似精度为：

$d_R(X)=|[R]A|/|\langle R\rangle A|$

其中$|B|$，表示集合B元素的个数。

根据$d_R(X)$，定义粗糙度$P_R(X)=1-d_R(X)$。

同Rough集中对于知识的近似描述相同，X的R粗糙度与其精确度相反，精确度反映我们对于了解集合X的知识的完全程度，粗糙度表示的是集合X的知识的不完全程度。显然$0\leqslant d_R(X)\leqslant 1$，于是可用$d_R(X)$来定义Rough集[6]。

结束语 Rough集理论已被广泛地应用于知识分类和处理不完全信息，其上近似和下近似计算与模态逻辑中的必然算子[]和可能算子⟨⟩的语法性质相同，本文结合关系运算，证明其合成和右除运算与近似计算和模态算子的等价性，并从关系运算的角度给出了模态算子与近似集计算的算法。通过对模态逻辑中特定实例的研究，运用Rough集对其数据表示中特定的知识进行精确定义，并在一般情况下根据可达关系，对知识进行近似描述。

参考文献

1 陈世福，陈兆乾，等. 人工智能与知识工程. 南京：南京大学出版社，1997

2 [美]B. F 切莱士著，郑文辉，张宜生译. 模态逻辑导论. 广州：中山大学出版社，1989

3 Lin T Y, Liu Qing. First Order Rough Logic-revisited. In: Ning Zhong, Andrzej Skowron, Setsuo Ohsuga. eds. Lecture Notes in Artificial Intelligence 1711, Berlin: Springer-Verlag, 1999. 276～284

4 Liau Churn-Jung. An Overview of Rough Set Semantics for Modal and Quantifier Logics. International Journal of Uncertainty, Fuzziness and Knowledge-Based System, 2000, 8(1):93～118

5 Pawlak Z. Rough sets. International Journal of Computer and Information Sciences, 1982, 11(5):341～356

6 曾黄麟，等. 粗集理论及其应用. 重庆：重庆大学出版社，1996

7 Orlowska E. A Logic of Indiscernibility Relations. Bulletin of the Polish Academy of Sciences, Mathematics, 1987, 33:475～485

8 Hoare C A R, He Jifeng. The Weakest Prespecification I. Fundamenta Informaticae, 1986, 9(1):51～84; The weakest prespecification II. Fundamenta Informaticae, 1986, 9: 217～252

9 刘莉，李永礼，商琳. The Generation on Operation of Set and Pansystems Relation. In: Advances in Sysytems Science and Applications: Special Issue, 1996. 138～141

10 Fari～nas del Cerro Luis. A Simple Deduction Method for Modal Logic. Information Processing Letters, 1982, 14(2):49～51

11 Yao Y Y. Two views of the theory of rough sets in finite universes. International Journal of Approximate Reasoning, 1996, 15: 291～317

12 Fari～nas del Cerro Luis, Orlowska E. DAL-A logic for data analysis. Theoretical Computer Science, 1985, 36:251～264

13 李永礼，商琳，刘莉. Fixed Pansystems Theorems of Sub-binary Relation. In: Advances in Sysytems Science and Applications: Special Issue, 1996. 145～149

(上接第65页)

3 Alexander D S, et al. A Secure Active Network Environment Architecture: Realization in Switch-Ware. IEEE Network, 1998

4 Arbaugh W A, et al. A secure and reliable bootstrap architecture. In: IEEE Security and Privacy Conference, May1997. 65～71

5 Alexander D S. ALIEN: A Generalized Computing Model of Active Networks. PhD thesis, University of Pennsylvania, 1998

6 Tennenhouse D L, et al. A Survey of Active Network Research. IEEE Communications Magazine, January 1997. 80～86

7 van der Merwe J E, Leslie I M. Switchlets and dynamic virtual ATM networks. In: Proc. of the Fifth IFIP/IEEE Intl. Symp. on Integrated Network Management, San Diego, CA., May 1997