维普资讯 http://www.cqvip.com

安全组管理模型研究*)

尹 青 周 伟 王清贤
(信息工程学院计算机系 郑州 450002)

摘 要 形式化方法是研究复杂管理系统的有用工具。本文提出一个基于状态的安全组管理形式模型,采用 Z Notation 语言描述。安全组是共享组密钥的授权成员的集合,本文不是直接定义安全组而是定义组状态,组状态是某一时刻的组安全上下文,组的安全性和可靠性描述为某时刻组状态的性质。组管理过程是事件触发的组状态的变换过程,其终极目标是保证组在任一个稳定时刻都处于安全状态,但完全安全是不可能的。本文给出一个组策略框架,在此框架下提出安全组管理行为规则,并说明根据规则组状态转换过程满足安全策略约束。

关键词 安全组管理,组状态,形式模型,组策略,Z Notation 语言

Formal Model for Secure Group Management

YIN Qing ZHOU Wei WANG Qing-Xian
(Information Engineering University, Zhengzhou450002)

Abstract Formal method is useful and important for researching complicated management systems. A state-based model for sec-group management is presented in this paper. Using Z Notation language, group is defined as an association of group members and group keys. Group security and soundness are described as properties of group state at a time. The management system is modeled as a state transition system triggered by management events. The purpose of sec-group management is to maintain the group in a secure state at any stable time, but completely security is hardly possible. Given a group policy framework, we describe a suit of action rules and state that group is secure restricted in the framework under the rules.

Keywords Secure group management, Group state, Formal model, Group policy, Z Notation language

1 引言

安全多播越来越多地应用于大规模信息发布、分布式数据库更新、网络会议等应用领域。参与多播通信的实体采用对称密码机制来保护组通信安全,在密码意义下构成一个安全组,组成员共享一致的组密钥,实现组通信的机密性、完整性、认证、访问控制等。一对一通信的安全模式,即双方协商密钥建立安全信道,不能直接应用于多播,除了因为多播必须建立全组共享的安全信道外,还必须考虑组成员动态的加入或退出。本文研究多播安全组的管理,包括组成员的身份认证和授权、组成员加入/退出管理、组密钥的分配和更新、组安全状态的维护等,将从安全组建立到撤消的所有保证组安全的行为纳入安全组管理的范畴。

IETF 和 IRTF 的多播安全工作组提出多播安全参考框架,称为 SMuG 框架[1,2],将复杂的多播安全问题划分为三个主要的功能域:多播数据处理,组密钥管理和多播安全策略。SMuG 参考框架整合了多播安全相关的主要的实体和功能,并描述了其内在关系,对安全多播的设计具有指导意义。但框架没有专门定义安全组的管理,只是将安全组成员的身份认证、访问控制作为密钥管理功能域的一部分。

本文的研究是在 SMuG 参考框架范围内进行的,安全组角色模型及组策略空间符合文[3]中的定义。安全组管理广义上说包括从组建立到组撤消的整个过程中安全组行为的管理,本文主要讨论组成员管理和组密钥管理,建立一个形式化规范,定义相关的安全性质,并描述安全策略下的组管理行为规则。形式模型采用 Z Notation[4]语言描述,Z Notation 是牛津大学 Computing Laboratory 开发的一种基于类型集合论的规范描述语言[5],采用命题逻辑和谓词逻辑演算描述数学对象或构件之间的关系,结构化的机制 Schema 用来描述构件(包括属性和操作),能够用来定义状态空间以及动态特性。

2 安全组管理空间

安全组的管理遵循组生命周期(Group Live Cycle)模型。组生命周期的概念来自于 GSAKMP[6],由四个阶段组成:安全组定义、安全组建立、安全组维护、安全组撤销。

安全组建立之前应首先确定组安全策略[7,8],具体包括明确定义组成员的构成、规模和初始建立件,规定成员的身份及认证方式,规定组访问控制和密钥管理规则,定义组通信安全服务等等;另外,还需定义组中的角色,把一些特定角色委托给某些特殊实体,如指定某些实体作为组控制中心(GC)和密钥管理中心(KS),规定它们的授权和认证方式。安全组建立过程从 GC 正式接受委托、开始接受成员加入,直到满足安全组的初始条件进行组通信。安全组维护指组会话期间成员关系、组视图、组密钥的维护,包括一系列复杂的活动,其中最基本的是成员的动态管理,如会话期间成员加入/退出管理,违规成员处罚,以及由于成员动态变化和其它密钥更新事件引起的密钥更新。如果策略要求,还包括成员关系的维护、泄密恢复、失效恢复等。当安全组不再满足会话条件或需要强行结束组活动时,可以由 GC 向全体组成员发出组撤消通告,结束组生命周期。

安全组管理行为由组控制器 GC 和组密钥服务器 KS 共同实施,目标是保证安全组处于安全状态,即要求在任一稳定

*)本项目受到国家重点基础研究发展规划项目(973 项目,项目编号 G1999032700)资助。尹 青 博士研究生,主要研究领域为计算机软件与理论;周 伟 博士,主要研究领域为计算机软件与理论;王清贤 教授,主要研究领域为网络安全。

维普资讯 http://www.cqvip.com

时刻(比如密钥更新完毕),组安全上下文(Group Security Context)必须满足安全策略的约束。组安全上下文指任一时刻的组状态,是一组时变状态参量,包括组视图、密钥及状态等随时间、事件改变的状态参数。引起组安全上下文变化的事件有很多,如成员加入、成员退出、密钥生存周期结束等。根据安全策略,安全上下文的改变可能会引发一系列安全行为,如在向前保密安全策略下,新成员的加入导致密钥素材的更新。

安全组管理的核心是组密钥的访问控制,应考虑在组成员动态加入/退出的环境下,如何保证密钥的安全。安全组管理空间划分为三维,如图1。

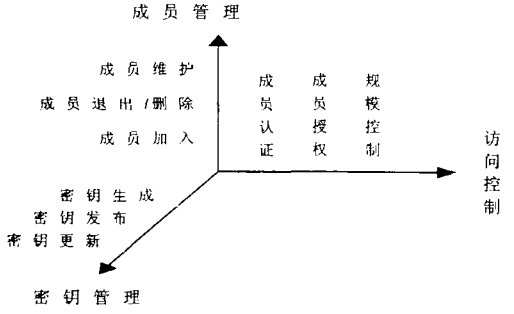

图1 安全组管理空间

访问控制:对拟加入会话的成员首先认证其身份,根据组策略验证其是否符合加入条件并授权,另外访问控制还包括组规模的控制,当成员数达到上限时阻止新成员的加入。

成员管理:在动态环境下组成员关系的管理维护,包括成员加入/退出事件的管理以及成员状态的维护。

密钥管理:保证密钥只为合法的成员掌握,包括密钥生成、发布和更新等。

本文讨论安全组的管理,假设组定义已经完成,组策略中明确定义了安全相关的行为、机制和参数,明确指定了组控制和密钥管理等服务实体。

3 模型基本定义

安全组是共享组机密的互作用实体的集合。只允许授权的实体参与会话是安全组的目标,而保证只有参与会话的实体才掌握组密钥是实现安全目标的手段。由于安全组允许成员自由地加入和退出,并且不可靠的网络环境也可以导致成员因泄密或失效而被删除,因而组成员集合是动态变化的,组密钥也要随之更新,才能保证组密钥只为当前合法的成员掌握。安全组是动态的,本文不是直接定义安全组,而是定义当前组状态的安全性。

首先定义基本类型:

$[ENTY]$:实体,网络中参与通信的单位,可以是进程、主机或用户。实体的集合是可数无穷的,实体之间是可区分的。

$[KEY]$:密钥素材,包括密钥、密钥状态及相关的参数。

$[Roles]$:组内角色,角色对应相应的权限和行为,由组策略定义。这里笼统地认为满足组访问控制策略的实体则分配角色参与组通信。

组预定的规模定义为一个外部常量:

$|GroupSize:N$

组访问控制规则抽象为实体与角色之间的关系,即规定哪些实体能够参与会话及分配的组角色。定义如下:

$|AcRule:ENTY \nrightarrow Roles$

组成员定义为访问控制策略允许并授权参与组通信的实体构成的集合,成员数目受组规模的限制。定义如下:

GroupMem

$$mems : ENTY \nrightarrow Roles$$
$$gsize : \mathbb{N}$$
$$mems \subseteq AcRule$$
$$gsize \leq GroupSize$$

组密钥定义为组使用过的和正在使用的密钥构成的序列,序列长度为#gkey,即当前组密钥的编号。该序列中密钥应满足独立性等安全特性,这里密钥之间的"≠"表示密钥之间是不相关的。

GroupKey

$$gkey : seq\ KEY$$
$$\forall i, j : dom\ gkey \bullet i \neq j \Rightarrow gkey(i) \neq gkey(j)$$

当前组密钥:

$currentkey == (\lambda GroupKey \bullet last\ gkey)$

组成员关系和组密钥是动态变化的,在某一时刻,安全组由当前时刻的成员集合、组密钥以及成员与组密钥之间的关系描述:

Group

$$GroupMem$$
$$GroupKey$$
$$hold : ENTY \leftrightarrow KEY$$
$$ran\ hold = ran\ gkey$$

定义1 某时刻组是安全的(secure),当且仅当只有授权的组成员才掌握当前密钥,即:

Secure_ : Group

$$s : Group \bullet Secure\ s \Leftrightarrow dom\ (s.hold \rhd \{last\ s.gkey\}) \subseteq dom\ s.mems$$

定义2 某时刻组是可靠的(sound),当且仅当授权的组成员都掌握当前密钥,即:

Sound_ : Group

$$s : Group \bullet Secure\ s \Leftrightarrow dom\ (s.hold \rhd \{last\ s.gkey\}) \supseteq dom\ s.mems$$

如果组在任意一个稳定的时刻都是安全且可靠的,则组是可信的(dependable)。

4 基于状态的组管理模型

4.1 目标和策略

安全组管理的终极目标是保证组是安全、可靠的,即保证组在每一个稳定时刻处于安全状态。显然,这个目标难以完全实现。应用根据具体的目标制定可行的策略,所谓安全即要求满足应用的安全策略,策略是执行组管理的依据。例如,

维普资讯 http://www.cqvip.com

实时新闻点播需要限制退出的成员不能访问其退出后的数据(即要求向前保密),而不必限制新加入的成员对其加入前的数据的访问(即不要求向后保密)。又如,机密性较高的会话需要限定密钥生命周期定时更新密钥,称为时间敏感的。

考虑以下策略项,分别代表向前保密(Forward Security)、向后保密(Backward Security)、时间敏感(Time Sensitive):

$Polices ::= FwSec \mid BwSec \mid Tisens$

组管理策略定义为:

$GroupPolices == \mathbb{P}\ polices$

4.2 组管理状态机模型

安全组管理可以视为事件触发的转换系统,由状态机描述。组状态指某一时刻的组安全上下文,包括组成员关系、组密钥及状态等。组管理是一个标记转换过程:

$$S_1 \xrightarrow{e1} S_2 \xrightarrow{e2} S_3 \cdots$$

引起组状态改变的事件称为组管理事件,有成员加入、退出、删除、失效、密钥更新等。本文将组管理事件简单定义为加入、退出和密钥更新:

$EVENT ::= JOIN \mid QUIT \mid TIMEOUT$

假设在某一个稳定状态 s_i,组是安全的。期望经过若干管理事件到达 s_j 状态仍是安全的。

组的初始状态的形成包括成员初始化和密钥初始化:

$GroupInit \triangleq GroupMemInit \wedge GroupKeyInit$

GroupMemInit

$GroupMem'$

$mems' = \varnothing$

$gsize' = 0$

GroupKeyInit

$GroupKey'$

$gkey' = \langle\rangle$

可以证明,初始状态是安全的。

4.3 组管理操作定义

组管理定义以下操作:

1) 加入:如果申请加入的成员符合访问控制条件并且组规模等条件允许,则加入成功。

GroupJoin

$\Delta GroupMem$

$m?: ENTY$

$gsize < GroupSize \wedge$

$m? \notin dom\ mems \wedge$

$\exists r \in Roles \bullet m? \mapsto r \in AcRule \Rightarrow$

$mems' = mems \cup \{m? \mapsto r\} \wedge$

$gsize' = gsize + 1$

2)退出:成员退出有主动和被动两种情况。主动指成员向服务器报告离开事件并销毁本地组密钥,被动指服务器将不安全或已掉线等情况的成员删除。两者都导致成员集合的改变。表示如下:

GroupQuit

$\Delta GroupMem$

$m?: ENTY$

$m? \in gms$

$mems' = \{m?\} \lhd mems$

$gsize' = gsize - 1$

注:$\lhd$ 表示定义域减少(Domain restriction)符号。

3)密钥更新:密钥更新是对全体组成员的操作,是密钥的"下推(push down)"动作。新密钥的产生应符合密钥生成原则,具有独立性。

Rekey

$\Delta Group$

$newkey?: KEY$

$\theta GroupMem' = \theta GroupMem$

$\theta GroupKey' = \theta GroupKey$

$\forall i: 1..num \bullet newkey? \neq gkey(i)$

$num' = num + 1$

$gkey' = gkey \oplus \{num' \mapsto newkey?\}$

$gms' = gms$

$hold' = hold \underset{e \in mems}{\cup} \{e \mapsto newkey?\}$

4.4 组管理行为规则

组安全管理要求组满足安全策略的约束,安全策略是组管理的行为指导。根据 4.1 节中规定的策略项,组管理行为规则定义如下:

1)只允许符合授权和访问控制策略的实体加入组,并分发密钥。

2)成员退出应向服务器申请并销毁本地密钥。

3)如果组策略规定向前保密(即退出的成员不能访问以后的数据),则发生成员退出事件后应启动密钥更新。

4)如果组策略规定向后保密(即加入的成员不能访问以前的数据),则发生成员加入事件后应启动密钥更新。

5)如果策略规定时间敏感,则超时应启动密钥更新。

简化的组管理行为规则形式化描述如下:

GroupMng

$Group$

$gpolicy: GroupPolicies$

$evt?: EVENT$

$FwSec \in gpolicy \Rightarrow (evt? = QUIT) \bullet$
$GroupQuit \wedge Rekey$

$BwSec \in gpolicy \Rightarrow (evt? = JOIN) \bullet$
$GroupJoin \wedge Rekey$

$Tisens \in gpolicy \Rightarrow (evt? = TIMEOUT) \bullet$
$Rekey$

(下转第 20 页)

维普资讯 http://www.cqvip.com

点数增多对性能带来的影响。

目前的流分析是以页框为单位的，但以字节为单位的流可能已经很早出现在页框内部，但我们只有在该流持续了3个页框时才发现，因此如果我们分析的粒度变得更小，比如对单个地址信息进行分析，就可以把流更早地检测出来，因此预取操作就可以被提前。这样对于页框流的元素个数比较少的应用，如SWIM，预取将带来更大的性能提高。但它要求检测/预取部件从更靠近CPU的地址相关部件获取页框基址信息，比如CACHE，如图2中虚线所示。相应地，页框流检测算法必须足够简单以便及时地处理大量的地址信息。因此，高效率的页框流检测算法也是我们下一步研究的对象。

我们目前的工作中没有区分读操作和写操作，如果将它们分开处理，页框数据的规则性能否进一步提高也是我们关心的方面。目前的预取是基于页框流的，既然我们的结构中有大量富足的网络带宽，我们考虑进一步开发非流的规则性，根据它们来预取更多的数据来提升性能。

总结 远程内存服务器结构可以带来高共享性和高可扩展性，但同时也加重了CPU和内存之间的速度不匹配问题。本论文采用模拟的方法来分析远程内存结构下典型应用的性能，验证了一些应用在远程内存结构下性能将明显下降的观点。同时我们也发现，由于本地内存不命中地址信息中以页对齐得到的页框基址有较好的规则性，所以我们考虑采用页框流预取机制来隐藏应用程序访问远程内存的数据传输时延，通过对不命中页框基址信息中的流的特征进行分析，发现采用页框流预取机制可以很好提高远程内存结构下程序的性能。最后我们利用模拟器进行实验，结果表明，通过使用页框流预取机制，在远程内存模式下应用程序的性能得到了不同幅度地提升。

参 考 文 献

1 樊建平，陈明宇. 网格化的动态自组织体系结构DSAG. 计算机研究与发展，2003. 12

2 Mohan T, Bronis R, de Supinski, et al. Identifying and Exploiting Spatial Regularity in Data Memory References. Supercomputing Conference 2003, Nov. 2003

3 Baer Jean-Loup, Chen Teen-Fu. An Effective On-chip Preloading Scheme to Reduce Data Access Penalty. Supercomputing Conference'91, Nov. 1991

4 Jouppi N P. Improving Direct-mapped Cache Performance by the Addition of a Small Fully associative Cache and Prefetch Buffers. In: Proc. 17th Intl. Symposium on Computer Architecture, May 1990

5 Savage N. Linking with light, IEEE Spectrum, Aug. 2002, 39

6 Hu Weiwu, Shi Weisong, Tang Zhimin. JIAJIA: A software DSM system based on a new cache coherence protocol. In: Proc. HPCN Europe 1999

7 Kodama Y, Sakane H, Sato M, Sakai S, Yamaguchi Y. In: Message-based efficient remote memory access on a highly parallel computer EM-X. International Symposium on Parallel Architectures, Algorithms and Networks'94, 1994

8 Renau J. Memory Hierarchies in Intelligent Memories: Energy/Performance Design. Master Thesis, Institution, Jan. 2000

9 Palacharla S, Kessler R E. Evaluating Stream Buffers as a Secondary Cache Replacement. In: Proc. 21st Intl. Symposium on Computer Architecture, April 1994

10 Zhong Yutao, Ding Cheng, Kennedy Ken. Reuse Distance Analysis for Scientific Programs. SC2003, 2003

11 Joseph H Earl C, Christopher G. Willard, et al. NUMAflex Modular Computing: New Model for Scalable Computing Infrastructure. report of IDC, 2000

12 Vander S P, Lilja W D J. Data Prefetch Mechanisms, ACM Computing Survey, June 2000

13 http://www.dgate.org/vmips/

14 http://www.tik.ee.ethz.ch/~topsy/

15 http://www.bitmover.com/lmbench/

（上接第14页）

可以证明，根据以上行为规则，在稳定状态（加入、退出、更新等操作完成后）下组满足安全策略的约束。

结束语 本文在给定的策略模型下给出了组管理规则的形式化描述。基于状态的组管理目标是保证组始终处于安全状态，但显然，完全安全代价太高因而几乎不可能实现。组策略表示应用对安全的限制条件，允许存在某些状态不满足安全性条件但符合组策略的约束，仍认为是安全的。

本文主要涉及组的安全性管理，对组的可靠性未作深入讨论。事实上，由于网络故障和密钥丢失等原因会导致隐性的成员状态改变，可靠性要求所有的合法成员都能参与通信，因而可靠性管理应包括成员状态的维护。在本文提出的模型框架下，成员状态的检测与维护及单个成员密钥的传送（即所谓密钥"下拉"）可以作为特殊行为添加到模型中。

参 考 文 献

1 Hardjono T, Canetti R, Baugher M, Dinsmore P. Secure Multicast: Problem Areas, Framework, and Building Blocks. Internet Engineering Task Force, Sept. 2000. draft-irtf-smug-framework-01.txt (Draft)

2 Hardjono T, Weis B. The Multicast Security Architecture. Internet Engineering Task Force, Nov. 2003. (draft-ietf-msec-arch-04.txt) (Draft)

3 周伟，尹青，郭金庚. 多播安全体系结构的研究与实现. 计算机工程与应用，2002.9

4 Spivey J M. The Z Notation: A Reference Manual. Second Edition, Prentice-Hall, 1992

5 Woodcock J C P, Davies J. Using Z: Specification, Refinement and Proof. Prentice-Hall, 1996

6 Harney H, Meth U, Colegrove A, Gross G. GSAKMP. Internet Engineering Task Force, Feb. 2004. draft-ietf-msec-gsakmp-sec-05.txt (Draft)

7 McDaniel P, Harney H, Dinsmore P, Prakash A. Multicast Security Policy. Internet Engineering Task Force, June 2000. (draft-irtf-smug-mcast-policy-00.txt) (draft)

8 McDaniel P, Harney H, Colegrove A, Prakash A, Dinsmore P. Multicast Security Policy Requirements and Building Blocks. Internet Research Task Force, Nov. 2000. (dra ft-irtf-smug-polreq-00.txt) (Draft)