基于安全局域网分级文件分发系统设计与实现

许肖威, 刘　雄, 戴一奇
(清华大学 计算机科学与技术系, 北京 100084)

摘　要: 通过分析安全局域网系统文件动态分级管理技术机制以及系统基于动态监控交换机的终端行为监控结构,提出了一种基于安全局域网分级文件分发系统的设计与实现方案。该系统解决了原有安全局域网系统监控结构的网络化扩展问题,实现了网络文件的分级可控管理,除了能够防范来自系统外部的普通网络攻击行为外,确保了对系统合法用户操作行为的控制,有效阻止了内部人员信息泄露的基本途径,能够提高各类共享数据的安全性。

关键词: 数据共享; 安全局域网系统; 文件分级; 安全网络存储系统; 网络文件分发系统
中图分类号: TP393.08　　**文献标志码**: A　　**文章编号**: 1001-3695(2012)11-4246-04
doi:10.3969/j.issn.1001-3695.2012.11.062

Gradable file distribution system design and implementation based on security LAN

XU Xiao-wei, LIU Xiong, DAI Yi-qi
(*Dept. of Computer Science & Technology, Tsinghua University, Beijing* 100084, *China*)

Abstract: By analyzing the technological mechanism of file dynamic grading management in security LAN system and the terminal behavior monitoring structure based on dynamic monitoring switches in the system, this paper introduced a gradable file distribution system design and implementation plan based on security LAN. This system could solve the problem of network extension of monitoring structure in current security LAN system, and achieved gradable and controllable management of network files. The system could not only prevent common network attacks from external system, but also achieved control of users' legal operations in the system, which effectively cut off the fundamental ways of internal users' information divulgence, and significantly enhanced the security of different types of sharing data.

Key words: data sharing; security LAN system; file grading; security network storage system; network file distribution system

随着互联网的持续发展,以网络技术为基础的分布式业务模式得到了日趋广泛的应用。网络所承载的信息量持续大规模增长,通过网络分发、共享重要敏感信息的需求进一步增强;同时,数据本身所包含的价值也在始终快速上升,任何针对数据内容的泄密事件都会对相关机构或者个人带来不可估量的损失。如何有效确保网络共享数据安全,防止机密敏感信息泄露成为了网络存储系统所面临的一个突出安全问题。网络存储系统自身的安全状况却始终不容乐观,遭受的安全风险还有进一步扩大的可能。系统面临的主要安全问题在于:除了需要继续应对来自系统外部网络攻击造成的威胁之外,来自系统内部合法用户造成的泄密事件数量逐年上升,危害性越来越大,内部用户泄密已经成为危害网络存储系统数据安全的又一个重要方面。

在现有网络存储解决方案中,内部用户不仅是系统服务的使用者,而且也是系统安全的维护者。因此,系统所具有的安全性不仅取决于所实现的安全防护技术,而且还受限于用户个人的网络安全防护意识、专业技术水平以及相关机构管理制度是否完备等人为因素。不可控成分相对较多,这就造成了已有网络存储系统面对用户泄密行为时常常无计可施,也就无法从根本上防范内部用户蓄意或者误操作造成的信息泄露,从而极大地降低和制约了该类存储系统的安全水平以及应用范围。从某种意义上来说,大量的网络存储系统用户无形中增加了多种网络攻击手段的"攻击表面",所以,开展对于"对外可防,对内可控"的新型安全网络存储方案的研究具有较强的理论和现实意义。

1　相关研究进展

1.1　网络存储系统

网络存储的概念一般是指用户通过网络从远程设备中获取所需数据的过程,而安全网络存储系统则是指那些实现了网络存储功能并且实现了某类能够确保数据安全机制的解决方案。根据各方案所提供安全性在系统结构中的不同层次,安全网络存储系统可以分为[1]安全网络文件系统、加密文件系统、可生存存储系统和基于存储的入侵检测系统四类,主流实现方案[2]包括 NASD、PASIS、S4、CFS[3]、SFS-RO[4]、SNAD、Plutus[5]和 SiRiUS[6]等。从数据机密性、完整性和可用性的角度,结合网络存储系统具体的安全需求及面临的主要安全性威胁,可以得出用于评价各类安全解决方案安全防护水平的网络存储系统基本威胁模型[7],如图 1 所示。

收稿日期: 2012-04-16; **修回日期**: 2012-05-29

作者简介: 许肖威(1982-),男,吉林洮南人,助理研究员,硕士,主要研究方向为网络与信息安全(presario_0625@yahoo.com.cn);刘雄(1978-),男,博士,主要研究方向为网络与信息安全;戴一奇(1946-),男,教授,博导,主要研究方向为网络与信息安全.

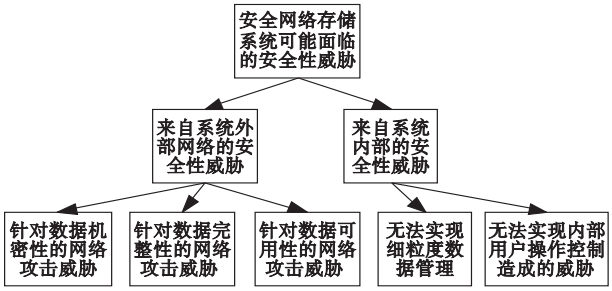

图1　网络存储系统基本威胁模型

根据各主流方案所实现安全机制在网络存储系统基本威胁模型中所发挥的作用进行归类,可得到目前安全网络存储系统在实现系统安全方面所采用的主要技术手段,如表 1 所示。

表 1　主流网络存储系统实现的安全机制

名称	机制
针对数据机密性的机制	磁盘加密、密钥分发服务器、自验证路径名、锁盒、门限、线上加密、积极密钥撤销等
针对数据完整性的机制	数字签名、数据校验和、密钥撤销、时间戳、门限、磁盘加密等
针对数据可用性的机制	文件组、密钥锁盒、自验证路径名、密钥分发服务器等
细粒度文件管理机制	CFS、SNAD、Plutus 实现了文件组、SiRiUs 实现了文件读写权限分离
系统内部用户行为控制机制	无具体技术机制

现有安全网络存储系统都是基于传统的“网络边界”思想设计的,比较重视来自系统外部网络攻击所造成的安全威胁,普遍缺乏较细粒度的文件管理机制,在限制系统用户操作行为方面存在严重不足。类似系统往往很难精确限定每份文件实际应该允许的可操作用户范围,采用文件级的控制访问控制方式往往会因为用户规模等问题而给系统性能增加相当大的额外开销,而文件组管理模式又会因为控制粒度较大而在实际应用中不能取得较好的效果。因此,一旦用户获得了某个文件的操作权限,系统将很难从技术的角度阻止用户对此文件可能的泄密行为,甚至用户可以在系统安全防护机制允许的情况下将文件信息泄露出去。从根本上说,缺乏对系统内部用户操作行为的限制机制是各主流方案存在的主要不足。

1.2　安全局域网系统

安全局域网系统[8]由清华大学网络安全实验室设计和研制,为国家自然科学基金、国家“863”计划以及“115”基金资助项目,是一种针对局域网数据管理、网络浏览、综合审计的一体化解决方案。该系统在文件管理方面具有动态分级的特点,能够实现系统内用户操作的行为控制,提高局域网共享数据的安全性。系统主要由功能服务器组、动态监控交换机[9]以及普通用户终端三部分组成,其基本结构如图 2 所示。

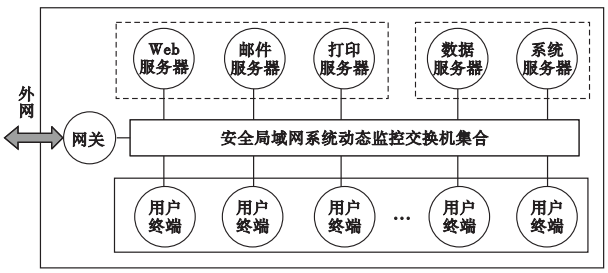

图2　安全局域网系统结构

基于普通 PC 的安全局域网系统根据 L-BLP 模型[10]的改进模型 EL-BLP 模型[11]设计和实现,具有较完善的状态转换规则和用户操作行为描述能力,并且系统状态转换规则安全性得到了理论证明。系统服务器、动态监控交换机以及部署于用户终端的监控器共同构成了安全局域网的终端行为监控结构。其中,系统服务器主要负责不同等级终端对不同级别文件访问规则动态的生成和审核;可编程的动态监控交换机主要负责访问规则的硬件化实现;终端行为监控器主要负责搜集和提取终端行为特征,系统实现了以“低等级用户无法接触高级别文件,高级别文件无法向低等级用户泄露”为特征的安全局域网文件共享,并且系统在结合多种入侵检测及安全防护技术的基础上,能够实现系统内部操作行为的审计追踪,满足了内网防护相关标准的要求。

2　基于安全局域网分级文件分发系统设计

基于安全局域网分级文件分发系统的设计思想为:以安全局域网文件动态分级管理的功能为核心,通过设计合理的文件访问控制与等级转换机制,解决安全局域网系统文件级别机制以及网络监控结构的网络化扩展问题,从而实现一种具有文件可分级特点的高安全性网络文件分发系统。

2.1　基于安全局域网分级网络文件分发系统概要

2.1.1　系统的基本结构

基于安全局域网分级文件分发系统的基本结构如图 3 所示,主要由网络传输服务器、等级转换服务器、安全局域网动态监控交换机、系统服务器以及普通用户终端组成。

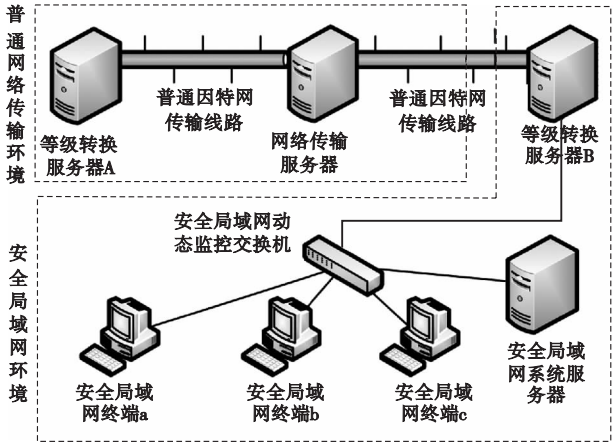

图3　基于安全局域网分级文件分发系统基本结构

根据设计方案的基本结构,系统典型的文件分发过程可描述为:a)等级转换服务器(RTS)A 对其存储的文件 f 的数据进行加密并为其设定相应的安全标签 T;b)具有安全标签 T 的加密文件 F 被发送至网络传输服务器(NTS),并在其控制下进一步发送至 RTS 服务器 B;c)RTS 服务器 B 将加密文件 F 所携带的安全标签 T 转换为安全局域网可识别的文件级别 r 并解密得到原始文件 f;d)终端用户在安全局域网动态监控交换机以及系统服务器的控制下对文件 f 进行系统访问规则所限定的各类操作,如用户终端 a 和 b 可以对文件 f 实施访问,而终端 c 的访问被禁止,此外,即使在用户终端 a 与 b 都能访问文件 f 的情况下,由于它们在系统安全策略中所具有的终端等级不同所能获得的操作权限也可能不同,可以假设终端 a 有权对文件 f 进行本地打印,而终端 b 则不能。

2.1.2　系统的总体设计

基于安全局域网分级文件分发系统的数据安全性主要由文件数据在系统各服务器中的存储安全、文件访问控制与系统等级转换的机制安全、数据网络传输过程中的传输机制安全几

个部分组成,系统的总体安全设计包含以下几方面:

a)系统的基本信任模型。根据网络存储系统基本威胁模型,针对基于安全局域网分级文件分发系统数据安全的潜在威胁主要来自以下两个方面:(a)存在于网络传输环境中的网络攻击;(b)分发系统内部用户不可控的操作行为。因此,在本设计方案中假设网络传输服务器为不可信,文件分发所依托的普通网链路为不可信网络环境,另外,系统内部用户由于其行为需要从系统的角度加以规范而也被假设为不可信实体。系统的基本信任模型如图 4 所示。

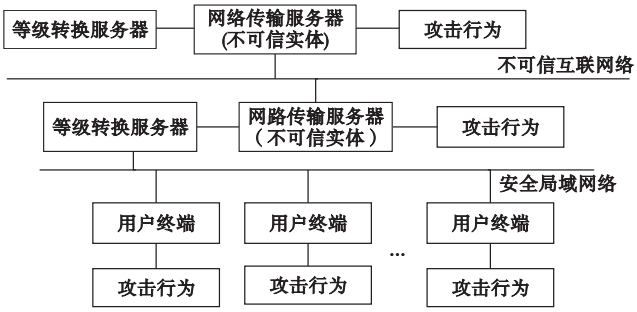

图4 系统的基本信任模型

b)关于密钥分发的基本假设。本系统设计方案中服务器规模相对固定,不存在某服务器加入或者退出系统的持续性动态变化过程,因此,系统设计中暂不考虑实现自动化的网络密钥分发机制。文中所涉及到的密钥交换过程都假设通过其他非系统自带的安全机制加以实现。

2.2 系统文件访问控制机制设计

基于安全局域网分级文件分发系统从系统的功能定位出发重点考虑了文件级的访问控制机制,其实现方式主要是通过为分发系统中的每份加密文件 *F* 建立相应的元数据文件 F-MD 并在其中添加相应的系统控制结构,而且在文件网络分发的过程中,文件 *F* 与对应的 F-MD 同时在系统各服务器间进行传送,以便在数据传输的各个阶段中能够连续地将系统网络安全控制机制作用于分发文件实体。

2.2.1 系统加密文件的基本结构

加密文件 *F* 主要由采用某对称加密算法加密的文件数据和带有持有文件的服务器数字签名的文件校验和组成,其基本结构如图 5 所示。

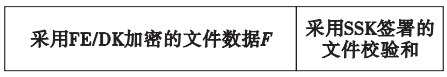

图5 系统加密文件*F*基本结构

其中,文件校验和采用数据散列算法实现,系统加密文件结构中所涉及的密钥概念如下:

a)文件加/解密密钥 FE/DK。由系统 RTS 服务器根据对称密码算法为每个文件单独生成。

b)服务器签署密钥 SSK。由系统 RTS/NTS 服务器根据非对称密码算法生成,为算法生成密钥对的私钥部分,用于实现服务器级的身份验证及访问控制。

c)服务器验证密钥 SAK。由系统 RTS/NTS 服务器根据非对称密码算法生成,为算法生成密钥对的公钥部分,用于实现服务器级的身份验证及访问控制。

2.2.2 系统元数据文件的基本结构

加密文件 *F* 所对应的文件元数据 F-MD 是系统实施访问控制的主要数据结构,主要由文件接收服务列表、文件传输信息基组以及相关校验部分组成,其结构如图 6 所示。

图6 系统F-MD文件结构

a)具有文件所有者标志的文件名。由采用系统 RTS 服务器 SSK 密钥签名的文件名实现,用于实现 *F* 与 F-MD 文件间的紧密关联,防范文件反转攻击(warp)的威胁。

b)接收文件的 RTS/NTS 服务器列表。主要由能够接收文件的服务器标志符组成,用于实现系统文件级的分发范围控制,出于效率考虑可采用明文方式实现。

c)文件传输信息基(FTIB)组。每个 FTIB 对应于接收文件服务器列表中的一个服务器,采用密钥锁箱(lockbox)原理实现,主要用于向各个服务器分发文件 FE/DK 密钥,指派文件安全标签(F-ST),实现文件网络分发阶段以 RTS/NTS 服务器为节点的系统内部行为控制。

d)元文件版本信息及 F-MD 校验机制。版本信息为使用 RTS 服务器 SSK 密钥签名的系统元文件版本编号,用于实现系统文件版本控制,确保 F-MD 能够防范来自文件回滚攻击(rollback)的威胁,而使用 RTS 服务器 SSK 密钥签署的元文件校验和则是为了防止针对元文件的数据窜改和伪造。

2.3 系统文件传输信息基的设计

文件传输信息基 FTIB 是元数据 F-MD 结构的一部分,主要用于实现系统对接收文件的 RTS/NTS 服务器文件操作权限的限制,其基本结构如图 7 所示。具体限制方式为:当 FTIB 中只具有 F-ST 标签部分时,对应服务器由于无法获取 FE/DK,无法实现文件数据解密而仅具有文件传输权限;如果 FTIB 同时包含 F-ST 和 FE/DK 部分,对应服务器则具有相应的文件处理权限。系统通过设置 FTIB 的方式实现了系统服务器文件传输权限与处理权限的有效分离。

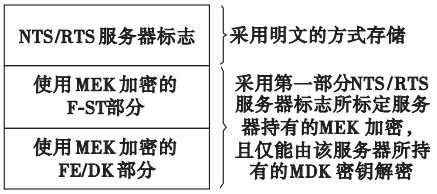

图7 文件传输信息基FTIB基本结构

文件传输信息基 FTIB 中所涉及的密钥概念如下:

a)文件传输信息基加密密钥 MEK。由系统 RTS/NTS 服务器根据非对称密码算法生成,为生成密钥对的公钥部分。

b)文件传输信息基解密密钥 MDK。由系统 RTS/NTS 服务器根据非对称密码算法生成,为生成密钥对的私钥部分。

2.4 系统文件安全标签的设计

文件安全标签 F-ST 是进行文件分发的 RTS 服务器为接收文件的每个服务器所设定的操作权限信息,主要用来实现安全局域网文件级别的远程设定,从系统设计的角度来说应该满足三方面的设计需要:a)文件安全标签应包含安全局域网系统服务器所制定的文件访问策略信息;b)F-ST 标签应具有可验证的设定服务器身份信息以防止标签伪造;c)F-ST 标签应该能够与文件数据紧密匹配,实现系统文件级的权限设定机制。综合以上设计需求的文件安全标签基本结构如图 8 所示。

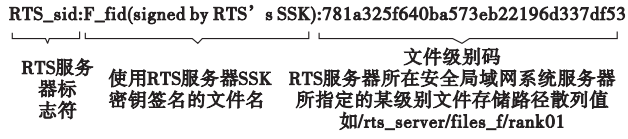

图8 文件安全标签结构

2.5　系统文件级别转换机制设计

系统文件等级转换机制主要用来实现系统文件安全标签的设定与识别,其功能主要是通过系统维护的文件级别转换表来实现。文件级别转换表的结构如图 9 所示,主要由安全局域网文件级别标志、文件级别码、安全局域网同级别文件 RTS 服务器本地存储路径信息组成。其中,文件存储路径信息是由安全局域网系统服务器根据安全局域网文件安全访问策略为 RTS 服务器中的同级别文件数据所指派的本地存储路径,而文件级别码是同级别文件 RTS 服务器的本地存储路径信息的散列值。安全局域网系统服务器通过对文件分发系统文件级别转换表的动态设定和维护,实现了对文件分发系统文件等级转换行为基于安全局域网系统安全策略的有效监控。

文件级别标志	文件级别码部分	存储路径信息部分
01	781a325f640ba5753eb22196d337df53	/rts_server/files_f/rank01
02	a166d4176d235ec6e15de330697169c4	/rts_server/files_f/rank02
03	043f5396a9a0926c5775e7444e2f858e	/rts_server/files_f/rank03
⋮	⋮	⋮

图9　系统文件级别转换表基本结构

3　基于安全局域网分级文件分发原型系统实现

根据基于安全局域网分级文件分发系统的基本结构以及所描述的系统功能机制设计方案,本文提出了文件分发原型系统的实现方案并在其基础上进行了系统实现,其中,系统实现方案的基本结构如图 10 所示。

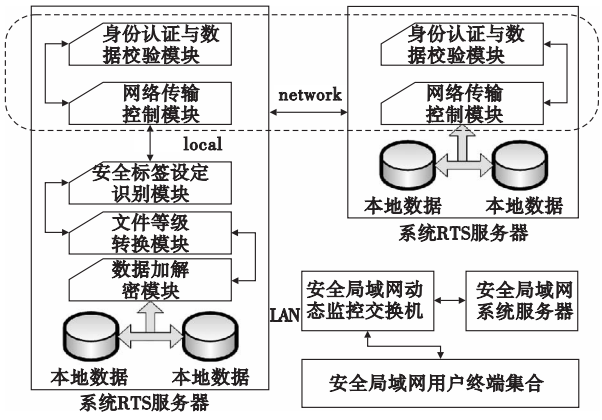

图10　原型系统实现方案

在系统实现方案中,NTS 服务器作为系统文件分发的中继节点实现并未考虑相关的文件处理功能,RTS 服务器作为整个系统文件分发的发起节点以及接收节点同时具有文件传输与处理的功能,系统功能机制主要实现五个系统功能模块。其中,网络传输控制模块、身份认证与数据校验模块主要实现系统设计方案中 2.2 节和 2.3 节所描述的文件访问控制机制;安全标签设定识别模块、文件等级转换模块以及数据加解密模块主要用于实现系统设计方案中 2.4 节和 2.5 节所描述的系统文件等级转换机制;并且,系统文件级别转换表由安全局域网系统服务器根据系统安全策略进行生成和维护。该实现方案对现有安全网络存储系统及安全局域网系统都进行了改进,主要体现在以下两个方面:

a)实现了安全局域网系统监控结构的网络化扩展。原有安全局域网系统中,系统监控主要由系统服务器、动态监控交换机以及部署在用户终端的终端行为监控器组成,依托局域网络实现本地配置本地管理。而在本文实现方案中,文件分发系统的文件等级转换机制处于安全局域网系统服务器的动态监控之下,通过文件安全标签的网络传递,实现了安全局域网系统服务器监控功能的网络化传递,确保了网络文件分发过程中系统安全策略的一致性以及连续性,对原有监控结构的本地化方案进行了改进,增加了原有系统的网络功能,提高了系统的适用范围。

b)实现了具有动态分级机制的安全网络存储方案。目前主流的安全网络存储系统实现方案中,并未涉及任何文件分级机制,对系统内用户行为缺乏控制。本文系统实现方案中的文件分级概念主要体现在两个方面:(a)通过在现有的安全局域网系统监控结构中添加网络化的文件等级转换机制,系统实现了系统共享文件的全网络化分级管理,远程用户终端对文件的访问行为同样需要受到系统安全策略的限制,而不仅仅局限于本地局域网用户终端;(b)在文件网络分发过程中,通过基于元数据 F-MD 结构的文件访问控制机制的设计,实现了系统以 RTS/NTS 服务器为节点的传输过程控制,系统可以对每份文件的分发范围以及接收文件服务器的相关权限进行动态设定,对系统服务器的网络传输权限以及文件处理权限进行了分离,能够有效提高系统的数据安全性。

4　结束语

本文提出了一种基于安全局域网的可分级网络文件分发系统的技术框架,并在此基础之上描述了该网络文件分发系统的原型设计方案。对具有文件分级管理特征的网络文件共享系统的安全性进行了研究,为系统后续的数据采集以及性能实验提供了相应的平台支撑,从而为今后开展相关的研究工作打下了一定的基础。

参考文献:

[1] 舒继武. 典型安全存储系统分类[J]. 中国教育网络,2007(11):70-72.

[2] STANTON P. Security data in storage:a review of current research, 0409034[R]. Urbana: University of Illinois at Urbana-Champaign, 2004.

[3] BLAZE M. A cryptographic file system for Unix[C]//Proc of ACM Conference on Computer and Communications Security. New York: ACM Press,1993:9-16.

[4] FU K, KAASHOEK M F, MAZIERES D. Fast and secure distributed read only file system[C]//Proc of the 4th USENIX Symposium on Operating Systems Design and Implementation. 2000:181-196.

[5] KALLAHALLA M, RIEDEL E, SWAMINATHAN R, *et al*. Plutus: scalable secure file sharing on untrusted storage[C]//Proc of the 2nd USENIX File and Storage Technologies. 2003:29-42.

[6] GOH E, SHACHAM H, MODADUGU N, *et al*. SiRiUS: securing remote untrusted storage[C]//Proc of the 10th Network and Distributed Systems Security Symposium. 2003:131-146.

[7] HASAN R, MYAGMAR S, LEE A J, *et al*. Toward a threat model for storage systems[C]//Proc of ACM Workshop on Storage Security and Survivability. New York: ACM Press, 2005:94-102.

[8] 程磊,司天歌,戴一奇. 基于动态监控器的安全局域网[J]. 计算机工程, 2008,34(6):158-160.

[9] 周麒麟,司天歌,戴一奇. 用于安全局域网络的动态监控器[J]. 清华大学学报:自然科学版,2009,49(1):123-126

[10] 司天歌,张尧学,戴一奇. 局域网络中的 L-BLP 安全模型[J]. 电子学报,2007,35(5):1005-1008.

[11] 薛海伟,徐长醒,林劼,等. 局域网中的 EL-BLP 安全模型[J]. 清华大学学报:自然科学版,2009,49(S2):2228-2232.