

民航网络自保护模型及其访问控制研究

杨宏宇¹, 白雪峰²

(1 中国民航大学 计算机学院, 天津 300300; 2 中国民航大学 空管学院, 天津 300300)

摘 要: 提出一种民航网络自保护系统模型, 设计其系统结构与分层响应框架, 在系统中设计了基于角色的访问控制策略和基于 Agent 的通信加密机制. 实验证明, 该系统模型的访问控制策略及通信机制能够有效保护网络自保护系统中的数据安全.

关键词: 自保护; 安全代理; 安全域; 通信; 访问控制

中图分类号: TP393

文献标识码: A

文章编号: 1000-7180(2010)11-0059-05

Research on Network Self-protection System Model of Civil Aviation and Its Access Control

YANG Hong-yu¹, BAI Xue-feng²

(1 School of Computer Science, Civil Aviation University of China, Tianjin 300300, China;

2 School of Air Traffic Management, Civil Aviation University of China, Tianjin 300300, China)

Abstract: This paper presents a civil aviation network self-protection model. The model's system structure and the layered response framework of this system model were designed. The role based access control policy and the agent based communication security mechanism of this system were proposed. Experimental results demonstrate that access control policy and communication mechanism of this system's model can effectively protect data security.

Key words: self-protection; intelligent agent; security domain; communications; access control

1 引言

近年来, 民航信息网络安全形势日益严峻, 民航重要信息系统和网络系统多次发生信息安全重大事故, 造成了严重的社会影响. 网络自保护系统是解决上述问题并提升民航重要信息网络系统安全性和生存性的一个重要途径.

针对当前民航信息网络的现状, 融合智能 Agent^[1]与网络安全技术, 设计了民航网络自保护系统模型结构, 给出该系统的访问控制策略与通信加密机制.

2 网络自保护系统模型

2.1 系统结构

基于安全域的思想^[2], 设计了民航网络自保护系统模型, 其系统结构如图 1 所示. 在该模型中, 将民航网络自保护系统划分为若干个安全域, 每个安全域内有若干主机, 每个主机上运行着多种软件和服务. 安全域中的主机上设置自治 Agent, 自治 Agent 分析主机系统和用户活动以及该主机接收的网络包, 实时分析检测针对该主机的入侵行为, 当发现入侵行为时, 做出合理的响应, 同时向安全域中的安

收稿日期: 2009-09-27; 修回日期: 2009-11-27

基金项目: 国家自然科学基金项目(60776807); 国家“八六三”计划重点课题(2006AA12A106); 天津市科技支撑计划重点项目(07ZCKFX01700); 中国民航科技基金项目(RKXZY0814); 中央高校基本科研业务费中国民航大学专项项目(ZXH2009A006)

全分析中心报告情况.

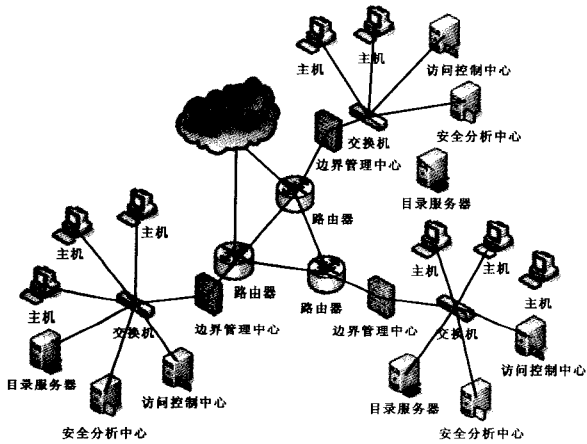


图 1 民航网络自保护系统结构

系统安全分析中心是自保护系统的决策分析中心,其他安全域中的信息提交到安全分析中心进行汇总、分析、融合,形成整个系统的安全趋势信息,进而提供安全域间攻击预警,以及安全域协同保护等功能.

在网络自保护系统中,网络中每一个安全域都对应一个域安全分析中心,它负责接收、汇集安全域中自治 Agent 的报告,分析在域层次上的入侵,做出响应,并向系统安全分析中心报告情况.系统安全分

析中心处于系统的顶层,根据域安全分析中心的报告,分析在整个网络层次上的入侵和安全态势^[3].

如果某个域安全分析中心发生故障或受攻击瘫痪,则系统安全分析中心发出指令,启动这个域中的后备域安全分析中心.如果系统安全分析中心发生故障,则系统内的域安全分析中心通过一定算法选举出新的系统安全分析中心.

2.2 分层响应框架

根据民航网络自保护系统的结构特点,采用基于分层响应的策略,设计了由系统层、安全域层和主机层组成的民航网络自保护系统分层逻辑架构(如图 2 所示).与之相对应,设计了由系统安全分析中心、安全域安全分析中心和主机自治 Agent 构成的网络自保护系统分层响应框架(如图 3 所示).

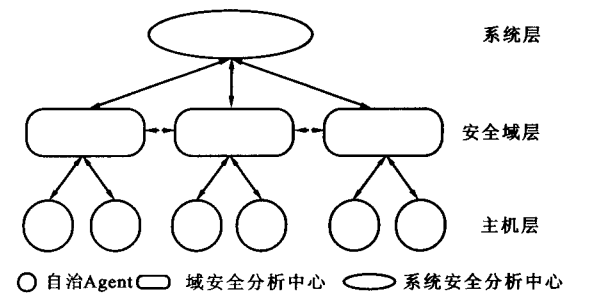


图 2 民航网络自保护系统逻辑架构

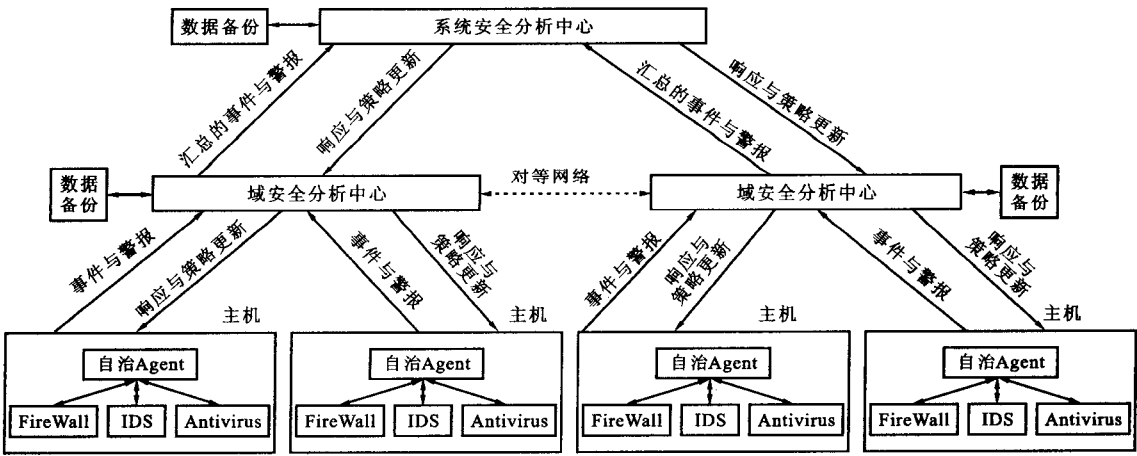


图 3 民航网络自保护系统三层响应框架

民航网络自保护系统三层响应框架由下向上分为主机层、安全域层和系统层.

在主机层,每个主机上都运行有自治 Agent 以及防火墙、IDS 和防病毒软件等安全防护系统.

在安全域层,每个安全域都有域安全分析中心负责安全域内的管理和控制,主要包括数据关联分析、域安全策略管理和响应恢复等部分.

在系统层,系统安全分析中心从全局角度对系

统安全进行管理和控制,主要包括关联分析、系统状态评估、响应恢复中心和系统安全策略管理等模块.网络自保护系统分层响应框架数据处理流程如图 4 所示,其中虚线表示节点主机发送数据方向.

3 系统访问控制策略

目前,传统的网络安全控制技术已经不适应开放式网络环境下安全访问控制的需要,因此出现了

安全域理论.安全域的基本思想就是建立一个逻辑上的域,对域中资源提供边界安全保护.网络自保护系统划分为多个安全域,如何对安全域资源进行访问

控制就成为网络自保护系统必需解决的问题^[5].本文提出的网络自保护系统模型采用基于角色的访问控制策略.

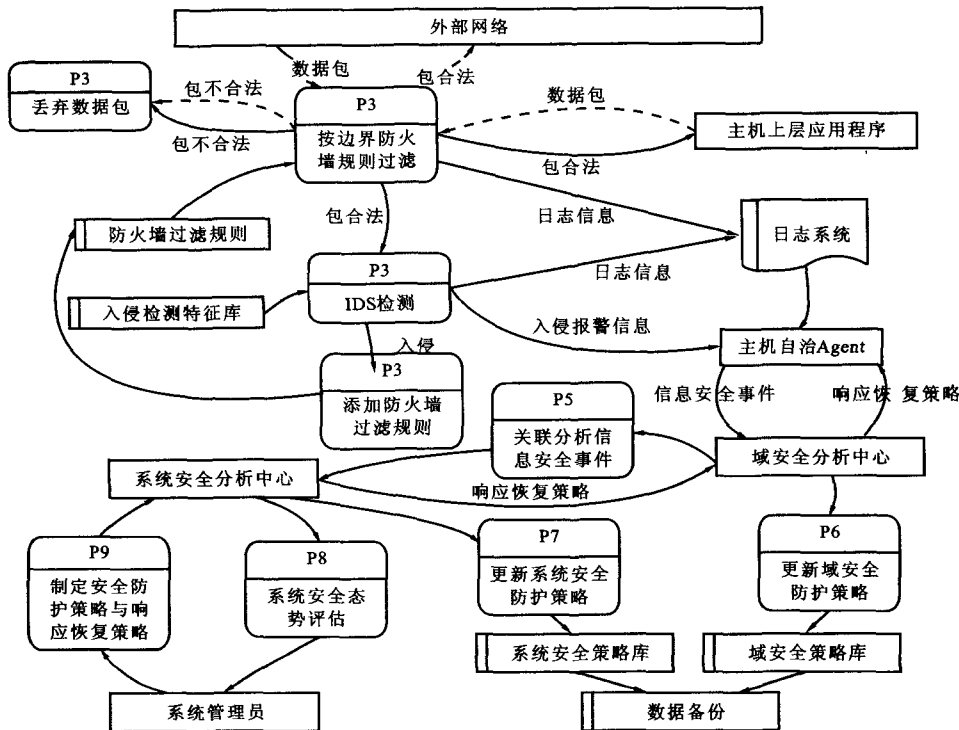


图4 网络自保护系统分层响应框架数据处理流程

3.1 基于角色的访问控制模型(RBAC)

基于角色的访问控制策略^[3]的基本思想是根据安全策略划分出不同的角色,资源访问许可权限被封装在角色中,系统管理员为用户分配合适的角色,用户通过角色间接地访问资源,实现了用户与权限的逻辑隔离.

随着 RBAC 模型^[4]的广泛应用,衍生出许多 RBAC 的扩展模型,其中以 Ravi Sandhu 等人提出的 RBAC96 模型^[5]最具代表性.本文网络自保护系统的访问控制采用 RBAC96 模型(如图 5 所示).

在 RBAC96 模型中,角色与权限、角色与用户之间均为多对多的关系,角色之间具有继承关系,而形成角色间的偏序关系和层次结构,易于反映系统组织结构和系统用户职权.

3.2 访问控制策略

将网络自保护系统划分为多个安全域,每个安全域均采用基于角色的访问控制.安全域的主体可通过各安全域的目录服务器查询安全域提供的资源与服务.对主体身份的认证及其访问权限的控制由各安全域内的访问控制中心实现.对于某个域内主体来说,可以访问的资源分为两种:域内资源和域外资源.

3.2.1 域内资源访问

如果主体访问本安全域资源,则主体发起请求,由域内访问控制中心对其身份和权限进行确认,如果用户合法,则可通过目录服务器查找所需资源或服务,而后主体可访问所请求的资源或接受服务.

3.2.2 域外资源访问

对某个安全域来说,外部安全域可根据信任关系分为信任安全域和不信任安全域.若安全域 A 与安全域 B 相互信任对方,则依靠两个安全域自身的

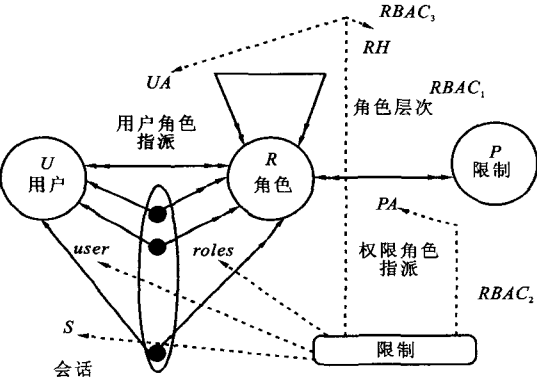


图5 RBAC96 模型框架

访问控制中心即可实现双方主体身份的认证. 如果安全域 A 为安全域 B 的不信任安全域, 则需引入权威的第三方认证中心, 为双方安全域的用户提供可靠的身份鉴别.

4 系统的通信安全机制

网络自保护系统模型的提出主要是为了加强民航网络自保护系统的安全防护性能力, 抵御恶意攻击、恶意代码加载、信息截取和对系统资源的非法访问. 因此保证网络自保护系统内 Agent 间信息传输的安全可靠、实现系统资源的访问控制是网络自保护系统构建和运行的基础.

4.1 Agent 通信

采用 JADE 作为网络自保护系统模型 Agent 的运行平台. JADE 平台采用命令 Agent 管理平台, 即 AMS、DF 和 ACC. 每台主机上运行一个容器, 一个平台可包含多个容器, 其中包括一个主容器. 每个容器中可运行一个或多个 Agent. JADE 根据通信双方 Agent 的位置不同, 采用不同的机制实现消息传递.

4.2 Diffie-Hellman 算法

Diffie-Hellman (DH) 算法是最著名的密钥共识协议^[6], 其用途是为通信双方建立一个共享密钥, 而且通信的任何一方都不需要事先知道对方信息.

假定通信双方为 A 和 B, 共同约定一个大素数 n 和底数 g . 这两整数不用保密, A 和 B 可公开约定. 为提高安全性, n 应较大. 该算法计算共享密钥的原理如下^[7]:

(1) A 选择一个大随机数 x (x 需保密), 并计算 $X = g^x \bmod n$.

(2) B 选择一个大随机数 y (y 需保密), 并计算 $Y = g^y \bmod n$.

(3) B 互换计算值 X 和 Y .

(4) A 计算 $K_A = Y^X \bmod n$, B 计算 $K_B = X^Y \bmod n$.

其中 $K_A = K_B = g^{XY} \bmod n$, 此即为 A 和 B 的共享密钥.

在网络自保护系统模型中, 依据 Internet 的简单密钥管理协议 (SKIP) 规定, g 取值为 2, n 的长度为 1024 位, 密钥取值如下:

F488FD584E49DBCD20B49DE49107366B336
C380D451D0F7C88B31C7C5B2D8EF6F3C923C043
F0A55B188D8EBB558CB85D38D334FD7C175743
A31D186CDE33212CB52AFF3CE1B1294018118
D7C84A70A72D686C40319C807297ACA950CD9969

FABD00A509B0246D3083D66A45D419F9C7CBD
894B221926BAABA25EC355E92F78C7.

4.3 自保护系统通信机制

网络自保护系统通信模型需要为系统中各 Agent 提供安全、可靠的通信服务, 防止传输的信息被窃听或篡改, 对系统资源进行访问控制, 防止非法用户对系统资源的非法访问. 为此, 设计并实现了安全通信流程 (如图 6 所示).

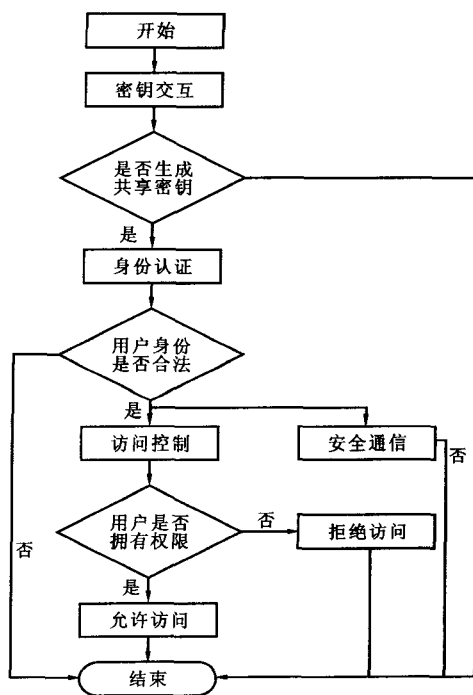


图 6 安全通信流程

4.3.1 密钥交互

两个互不信任的 Agent, 发送方 Agent A 与接收方 Agent B 进行通信, 建立会话, 使用 Diffie-Hellman 算法创建共享密钥, 该密钥用于后续通信数据的加密. 若某 Agent 不支持 DH 算法, 或 DH 共享密钥生成失败, 则中止当前连接, 会话建立失败.

4.3.2 身份认证

所有涉及信息安全的系统均须对用户进行身份认证, 这也是民航网络自保护性系统安全通信模型必须具有的安全防护措施, 本安全通信模型采用 X.509 证书进行用户的身份认证, 利用 Java 提供的 KEYTOOL 工具创建用户数字证书. 在身份认证阶段, 通信双方均需检验对方的数字证书是否有效, 是否被废除或到期. 若双方均确认对方身份合法, 则双方可进行数据的传输; 若某方数字证书不合法, 则中止连接.

4.3.3 对称加密

对于 Agent 间信息的加密传输有两种方法:一是采用对称密钥加密方法,二是采用非对称密钥加密手段.当网络信息安全事件发生时,网络自保护系统应及时地做出响应,如更新安全策略、事件汇总分析等,所以应尽量提高系统中各组成部分间通信的效率,而非对称加密运算量大,执行速度慢,故网络自保护系统中 Agent 间信息传输使用密钥交互生成的 Diffie-Hellman 共享密钥进行对称密钥加密.

5 结束语

本文针对当前民航网络所面临的安全防护问题,结合现有的网络安全理论模型和网络安全技术,设计民航网络自保护系统模型,给出系统的访问控制策略和安全通信机制,并采用 JADE 平台进行 Agent 安全性与抗重放攻击测试,测试结果证明本文提出的民航网络自保护系统模型具有较高的自主安全防护能力和生存能力.

参考文献:

- [1] Taraka Pedireddy. A prototype multi agent network security system[J]. AAMAS, 2003,29(5):14-18.
- [2] 段海新,吴建平. 计算机网络的一种实体安全体系结构[J]. 计算机学报,2001,24(8):854-859.
- [3] 张德银,刘连忠. 多安全域下访问控制模型研究[J]. 计算机应用,2008,28(3):633-636.
- [4] 杨柳,危初勇,陈传波. 一种扩展型基于角色权限管理模型(RBAC)的研究[J]. 计算机工程与科学,2006,28(9):126-128.
- [5] Ravi Sandhu, Edward Coyne. Role-based access control models[J]. IEEE Computer, 2005(15): 38-47.
- [6] 尹少平,董丹. Diffie-Hellman 密钥交换协议设计与实现[J]. 电力学报,2006,21(1):9-12.
- [7] 周小为,何斌. 基于角色的授权与访问控制的研究[J], 计算机与信息技术,2006(10):45-58.

作者简介:

杨宏宇 男,(1969-),博士,教授.研究方向为网络信息安全.

白雪峰 男,(1981-),硕士研究生.

(上接第 58 页)

- [3] Guo Qianjin, Yu Haibin, Xu Aidong. An online self-constructing wavelet fuzzy neural network for machine condition monitoring[C]// the fourth ICMLC. Guangzhou: 2005.
- [4] 彭刚,彭敏放,何怡刚. 基于聚类模糊神经网络的非线性电路故障诊断[J]. 微电子学与计算机,2006,23(8):1-3.
- [5] Kohonen T Teuvo. Self-organization and associative memory[M]. German: Springer Verlag, 1989.
- [6] Tian Jingwen, Gao Meijuan, Xiang Yujuan. The study of compost quality evaluation modeling method based on fuzzy neural network for sewage treatment[C]// ACIS. Queensland, Australia, 2007.

- [7] Saaty T L. Decision making with dependence and feedback: the analytic network process [M]. Pittsburgh: RWS, 2001.

作者简介:

黎谦 男,(1985-),硕士研究生.研究方向为实时软件工程.

杨红雨 女,(1967-),博士,教授,博士生导师.研究方向为图形图像处理、实时软件工程.

杨凯 男,(1981-),讲师.研究方向为空中交通管制技术.

门海艳 女,(1985-),硕士研究生.研究方向为席位气象显示.