文章编号:1001 - 9081(2005)08 - 1730 - 04

宽带无线 IP 网络安全体系结构模型

吴振强[1,2],马建峰[2]
(1. 陕西师范大学 计算机科学学院,陕西 西安 710062;
2. 西安电子科技大学 计算机网络与信息安全教育部重点实验室,陕西 西安 710071)
(zqiangwu@snnu.edu.cn)

摘 要:由于 BWIP 网络的非对称性特点,现有 ISO/IEC7498-2、IPsec、WAP、3GPP、CDSA 等安全体系结构框架都不能完全满足未来 BWIP 网络的安全需求。提出了一种适合未来 BWIP 网络的安全体系结构模型,该模型对 BWIP 网络所涉及的网络管理、安全操作、AAA、PKI、安全策略实施等技术进行了有机集成。给出了 BWIP 网络安全体系结构流入和流出的详细处理流程,并指出未来 BWIP 安全体系结构的研究方向。

关键词:宽带无线 IP 网络;安全体系结构;认证、授权和记账
中图分类号: TP393.08 **文献标识码**:A

Security architecture model for broadband wireless IP networks

WU Zhen-qiang[1,2], MA Jian-feng[2]
(1. *College of Computer Science, Shaanxi Normal University, Xi'an Shaanxi* 710062, *China*;
2. *The Key Laboratory of the Ministry of Education for Computer Networks and Information Security, Xidian University, Xi'an Shaanxi* 710071, *China*)

Abstract: Because of the asymmetry characteristic of BWIP networks, the existing security architecture frames can not completely satisfy the security requirement of the future BWIP networks, such as ISO/IEC7498-2, IPsec, WAP, 3GPP and CDSA. A kind of security architecture model which fits for the future BWIP networks was presented. The model integrated rationally with many technologies concerned in BWIP networks, for instance management, security Operation, AAA, PKI and the policy implement. Then a handling flow was described in detail of security architecture model for BWIP which flows out and in the model. Finally, some research directions of the security architecture for future BWIP were given.

Key words: BWIP networks; security architecture; AAA(Authentication, Authorization, and Accounting)

0 引言

宽带无线 IP(Broadband Wireless IP, BWIP) 网络中不同角色对安全的需求不同。移动用户关心的是如何获取 IP 地址、如何进行安全连接、如何获取网络中的安全服务等;而 ISP 提供商关心在提供服务的同时,如何对移动用户进行合理收费;企业管理者或网络内容提供商 ICP 关心如何确认用户的身份、如何保护信息的授权访问,即根据不同的角色提供不同的信息服务。所有这些需求都对目前的安全体系结构提出了挑战。同 BWIP 网络相关的安全体系结构规范有:ISO/IEC7498-2 通用安全体系结构框架[1]、IPsec 安全体系结构[2]、WAP 体系结构规范[3]、3G 安全体系结构[4]和通用数据安全体系结构 CDSA[5]。然而,这些安全体系结构都不能完全满足 BWIP 的安全需求[6],其存在的问题是:1) ISO 安全体系结构标准给出了安全服务与相关机制的一般描述,确定了在参考模型内部可以提供这些服务与机制的位置。这种安全框架只具有指导意义,按该框架提供的安全保障,会导致应用层数据重复加密和认证操作,密钥存贮和协商难以实现,系统效率低下,且无法满足 BWIP 网络的特殊安全需求[6],如窃听和流量分析等攻击。因此 ISO/IEC7498-2 不能适用于 BWIP 网络。2) IPsec 适用于有线网对称应用环境下的安全体系结构,不适合移动环境下低功耗、小内存、处理能力弱、带宽相对低和差错率高的特殊应用。因此 BWIP 网络应尽可能地采用非对称思想,以减轻移动设备处理能力弱的不足。3) WAP 安全协议栈是建立在新的安全体系结构基础上,其安全机制是通过 WAP1.X 协议栈中 WTLS 层来实现,由于 WTLS 的非标准性,存在同现有 TCP/IP 协议栈兼容性的问题,且 WTLS 存在许多安全漏洞。WAP2.X 将安全机制改用 SSL/TLS 方式,提出配合 WPKI 的方式来提供 WAP 协议的安全保障,这种解决方案主要是在传输层解决 WAP 的安全问题,不能解决网络层的安全问题。4)3GPP 安全体系结构是建立在第三代移动通信的基础上的,安全方面关注的是设备认证,技术重点放在接入上,通用性差,也不能满足未来 BWIP 下多种不同设备混合接入的全部安全需求,如 WLAN 设备通过 3G 网络漫游的计费问题等。5) Intel 体系结构实验室提出通用数据安全体系结构 CDSA,它是建立在固定网络上的软件开发体系,同样不适用于 BWIP 网络对安全性的要求。

本文针对 BWIP 网络存在的安全现状,提出了一个适合未来 BWIP 网络安全需求的安全体系结构模型框架,并给出了在该框架下的详细工作流程。

收稿日期:2005 - 02 - 27;**修订日期**:2005 - 04 - 22
基金项目:国家 863 计划资助项目(2002AA143021);国家自然科学基金资助项目(90204012)
作者简介:吴振强(1968 -),男,陕西商洛人,副教授,博士研究生,主要研究方向:计算机通信、网络安全; 马建峰(1963 -),男,陕西西安人,教授,博士生导师,主要研究方向:信息安全、密码学.

1　BWIP 网络的安全体系结构

从文献[6]可以看出,未来 BWIP 网络不仅要考虑数据的保密性、完整性,还要满足可认证性、可用性和不可抵赖性等。随着 BWIP 应用的深入,这些新的安全应用需求将会持续增长。本文认为 BWIP 安全体系结构应包含四个部分:BWIP 网络管理系统、BWIP 安全系统、BWIP 安全外围系统和外部安全支撑系统,具体模型见图 1。

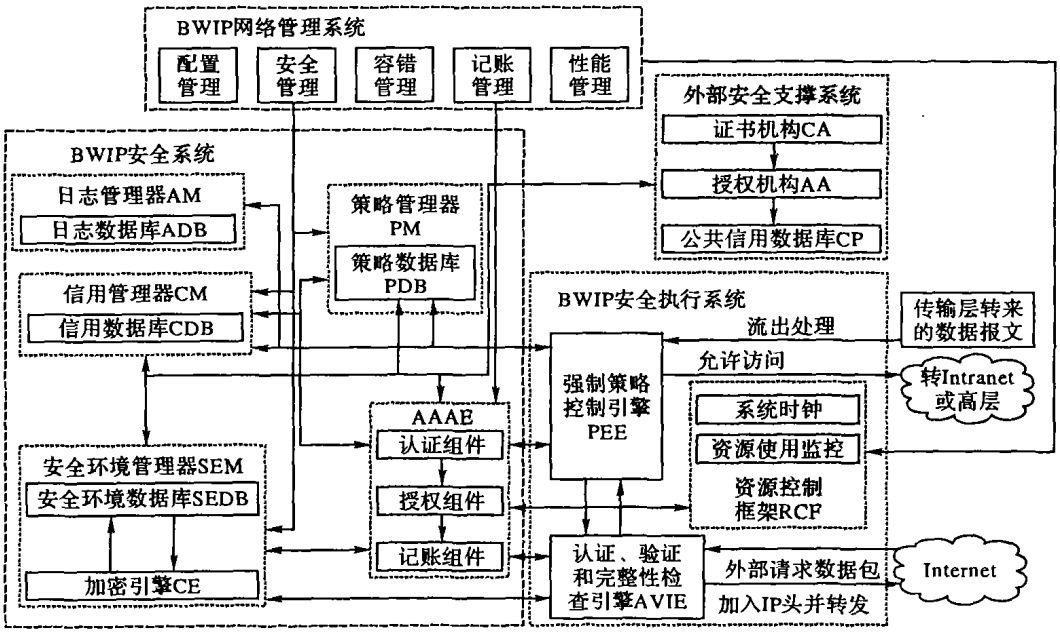

图 1　BWIP 网络安全体系结构模型

1.1　BWIP 网络管理系统

BWIP 网络安全体系结构的管理系统由配置管理、容错管理、安全管理、性能管理和记账管理五个部分。各个管理子系统的主要功能如下:①配置管理,管理 BWIP 网络中的网络设备,包括设备参数的配置与设备账目等;②容错管理,帮助 BWIP 网络管理人员进行故障定位,并进行故障恢复。同时还具有对 BWIP 体系结构中关键部件的冗余部分进行管理,以提高 BWIP 网络系统的服务能力和可生存性;③安全管理,对用户及其权限进行管理,同时也对网络安全策略进行管理,包括策略设定、策略配置等;④性能管理,对网络的资源进行监控和管理,根据网络的使用状况进行扩充、设置、规范等;⑤记账管理,记录移动用户使用网络资源的数量,调整用户使用网络资源的配额和记账收费。

1.2　安全系统

BWIP 安全体系结构中大部分安全操作都是由安全系统实现,同时安全系统也是重要安全数据的管理响应部件,如加密密钥、信任关系、安全策略等。安全系统是 BWIP 安全体系结构的核心内容,包括:

CE(Crypto Engine),实现真正的密码操作,如对称加/解密、非对称加/解密、哈希运算等。CE 提供不同的密码算法,为系统中的其他组件提供加/解密运算服务。

SEDB(Security Environment Database),在一个安全的环境中存贮有各种各样的加密密钥供 CE 使用。如 SEDB 中存放 MN(Mobile Node)的公私钥对,MN 与所有通信实体间通过 IKE 协商的密钥(MN-FA、MN-HA 等),以及不同节点协商的安全关联 SA 等。

SEM(Security Environment Manager),用于管理 SEDB 中的密钥,提供了手工配置加密密钥和自动管理密钥的功能,如启用 IKE 协商密钥和 SA,并保存在 SEDB 中。

AAAE (Authentication, Authorization, and Accounting Engine,认证、授权和记账引擎),实现 BWIP 网络中移动用户的身份认证,并根据其不同的角色进行授权访问,以及进行必要的记账操作,AAAE 依赖于 CE 和 SEDB 进行密码运算。由于 AAA 将会成为无线网络基础设施,BWIP 安全体系结构将 AAAE 作为一个引擎来实现,它相当一个代理部件,可以定期与 BWIP 网络中其他 AAA 进行交互,形成层次状的 AAA 管理体系,而非在线进行记账,这样有利用于减经 BWIP 网络负载,提高网络的效率。同时也将认证和授权放到 BWIP 安全体系结构中,便于进行认证和访问的细粒度控制,可以提高 BWIP 安全管理体系的灵活性。

PDB(Policy Database),其中存放的数据用来控制不同角色对 BWIP 网络的操作行为,如 IPsec 中的安全策略数据库(SPD)就可以用 PDB 来实现。

PM(Policy Manager),通过 AAAE 的授权模块在 PDB 中查询当前授权主体请求相关的策略。PM 也应向授权用户提供对 PDB 的编辑功能,可以是手工方式编辑,也可以是自动方式,如通过中心策略服务器下载策略数据等。

CDB(Credential Database),存放用户的信用数据,如公钥证书、属性证书等。

CM(Credential Manager),通过 AAAE 授权模块在 CDB 中查询当前授权主体请求相关的信用数据,返回其所有信用数据。CM 应向授权用户提供对 CDB 的编辑功能,有手工方式和自动方式,也可以从外部信用库中查找或下载信用数据。

ADB(Audit Database),存放安全相关活动的日志记录。

AM(Audit Manager),处理安全体系中安全功能子系统的日志,为管理者分析问题和决策提供依据。如入侵检测系统 IDS 通过日志数据识别和分析攻击行为。

1.3　BWIP 安全外围系统

BWIP 安全外围系统是 BWIP 安全体系结构的外围部分,包括强制策略控制引擎(Policy Enforcement Engine, PEE),认证、验证和完整性检查引擎(Authentication Verification Integrity Engine, AVIE),以及提供各种环境变量的系统,如资源监测框架 RCF 等。各种不同的无线设备通过无线访问点 AP/BS 接入 BWIP 网络,利用 BWIP 网络提供的安全服务。将 PEE 设置在 BWIP 中易受攻击的无线接点,此处的无线接入点 PEE 扮演着一个适配器层的角色,它根据授权决策对接

入系统的服务和实体进行管理。授权只是一个决策行为,而执行授权则是为了阻止非授权用户访问系统的服务与目标实体。当 AVIE 完成了认证、验证和完整性检查后,PEE 首先挂起通过接入点的用户请求,然后请求授权模块判断该请求是否允许,对该请求作出允许或拒绝的响应。如果授权通过,则移动用户可以通过 Internet 安全地访问内部网络 Intranet。

1.4 外部安全支撑设施系统

在 BWIP 安全体系结构中,需要外部安全支撑设施配合的有:①证书颁发机构(Certification Authority,CA);②授权机构(Authorization Authority,AA);③公共信用数据库(Credential Pository,CP)。当 MN 漫游到 BWIP 外部网络时,MN 必须出示他的公钥证书给认证模块,或者出示一个存放 MN 数字证书库的 URL 地址。

扩充性好的授权系统要求用户拥有一个或多个属性证书,属性证书是通过 AA 的可信第三方颁发,其多个属性证书并不要求是同一个 AA 颁发。当 MN 访问网络资源时,授权模块根据属性证书判断 MN 是否有所需的访问权限。信用库用于存放证明用户真实性的相关信息,如存放公钥证书、属性证书、证书撤销列表 CRL 等。

2 BWIP 安全体系结构的处理流程

2.1 流入数据的处理流程

BWIP 网络安全体系结构模型涉及 BWIP 网络中多个目标的特殊性,在移动节点 MN 上尽可能地分解任务,具体的加解密、认证和密钥协商等计算操作都尽可能地转移到固定网络完成。同时移动通信所需的外部代理(Foreign Agent,FA)、家乡代理(Home Agent,HA)等涉及到 IP 包的密码操作和认证,最复杂的是 Web Server 的处理过程,它涉及到密码操作、安全认证、审计、AAA 等多项功能。因此 BWIP 安全体系结构主要针对 BWIP Web 进行设计,其他 FA、HA 和 MN 等相关安全设施只选择相应的部分系统功能,并与安全体系整体协调一致。

BWIP 安全体系结构的功能主要集中在两点:1)数据包的安全保护过程,当数据包要访问服务器时,首先需要进行的操作是对数据包进行认证、用户角色验证和数据包的完整性检查;2)访问控制,用于审核 MN 要访问的资源是否授权,并进行相应的计费。流入数据的处理过程如图 2 所示。

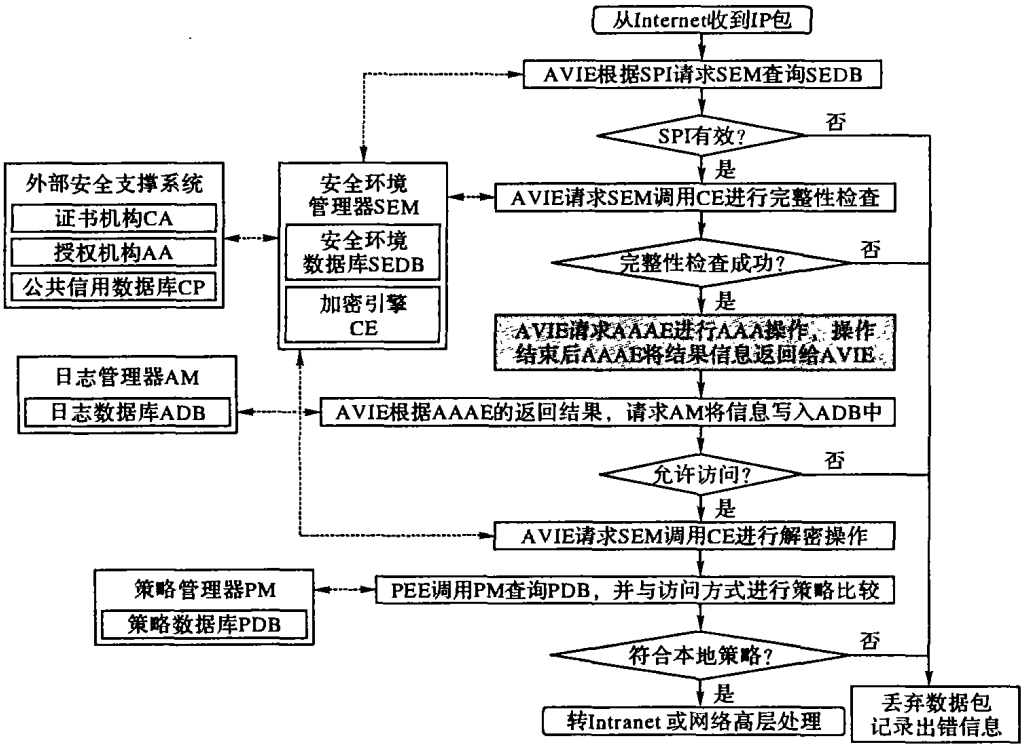

图 2 BWIP 安全体系结构流入数据的处理流程

BWIP 安全体系结构通过 AVIE 引擎实现数据包的有效性检查,它主要包括:①数字签名的验证,协助进行数据认证和完整性校验;②MAC 值验证,用于进行完整性保护;③公钥证书检查,用于检查数字签名;④属性证书检查,用于授权。

在对数据包成功进行完整性检查后,考虑不同用户间访问权限的差异(如 Web 服务器策略定义谁可以修改或维护服务器的数据库等),这就要求具有分角色保护 BWIP 网络的功能,防止用户误用或乱用安全策略。访问控制主要执行以下两步:①通过认证引擎分析每个请求数据包及其相应结点的安全策略;②PEE 根据认证引擎的肯定或否定响应,作出访问允许或拒绝响应。

在 BWIP 网络安全体系结构中,认证、授权和记账是紧密结合在一起的,简称 AAA。授权与记账是根据下列数据信息进行:①MN 对象名称,如 ID 号;②本地安全政策,这是对一些特殊对象进行控制;③MN 相关的信用程度;④MN 使用资源的时刻和资源的使用量。BWIP 安全体系结构中 AAA 的处理流程见图 3。

2.2 流出数据的处理流程

在网络层上执行加密和身份验证操作,对应用用户是透明的,应用程序只需对一个经过认证的端口与 IP 地址组合进行保护,这就需要定义一个过滤器来识别应用程序的数据流。BWIP 安全体系结构流出数据的处理流程见图 4。

当系统节点中的传输层或 Intranet 网络转交来的数据报文需向外网流出时,首先经过 PEE 中的过滤器进行过滤操作,即过滤器请求 PM 根据该数据包的 IP 地址和端口查询 PDB,得出相应的处理策略。若安全策略为丢弃,则 PEE 只简单地丢弃该数据包,并将处理信息传给日志管理器 AM,由 AM 记录到日志数据库 ADB 中;若安全策略为绕行,则表明这种类型的数据包是不需要进行安全处理,如部分 BWIP 网

络中的管理信令等,则 PEE 只需将该数据包直接交给 IP 层进行 IP 封装,并由 IP 层进行 IP 转发操作即可;若安全策略为封装处理,则 PEE 就将该数据包交给 AVIE,由 AVIE 进行相应的安全封装处理。

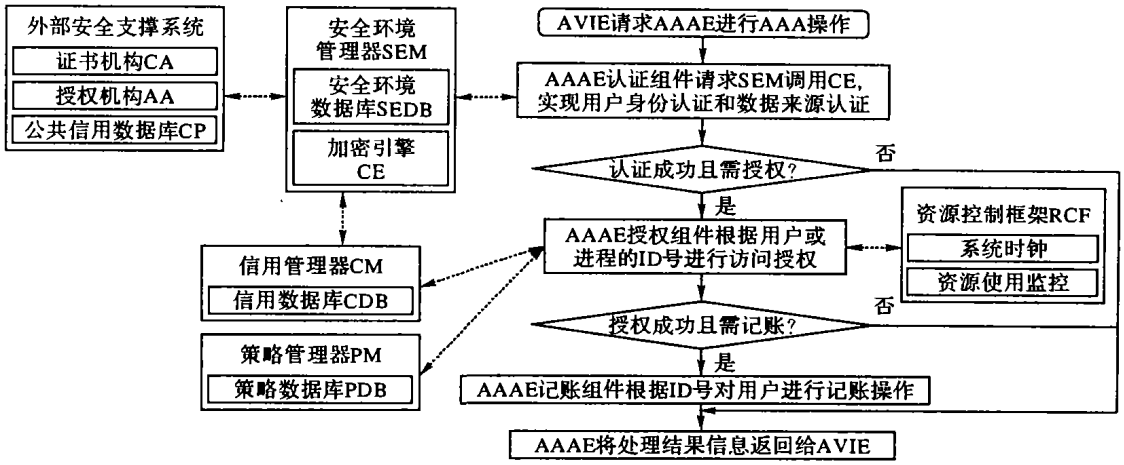

图 3　BWIP 安全体系结构中 AAA 的处理流程

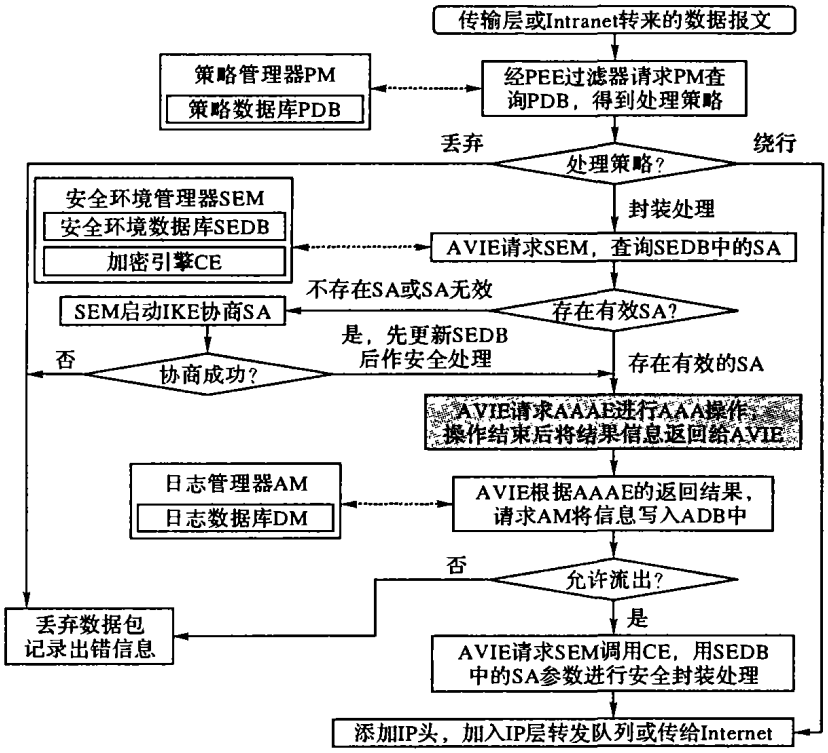

图 4　BWIP 安全体系结构流出数据的处理流程

流出数据的处理流程是:AVIE 先请求 SEM 查询 SEDB,查询该通信实体是否存在相应的 SA,若无 SA 存在或 SA 失效,通过 SEM 启用 IKE 进行 SA、加解密密钥、Hash 密钥、加密算法、认证算法等协商;若安全协商失败就丢弃数据包,并将协商结果信息传给日志管理器 AM,通过 AM 记录到日志数据库 ADB 中。当协商成功时,就首先保存这些协商的数据到 SEDB 中,并将处理结果返回给 AVIE,AVIE 请求 AAAE 进行相应的 AAA 操作。由于 AAA 操作是一个复杂的过程,在图 4 中用灰色框表示,其操作过程见图 3。AVIE 在收到 AAAE 的返回结果后,AVIE 不论处理结果如何,先将 AAAE 的返回结果传给日志管理器 AM,通过 AM 记录到日志数据库 ADB 中,以供系统安全管理人员查看日志,改进安全策略等。然后 AVIE 根据 AAAE 的返回结果进行处理,若是 AAA 操作失败(包括 AAAE 的认证或授权失败),则 AVIE 只需丢弃该数据包,并记录到 ADB 中;若 AAA 操作成功,表明系统允许该数据包流出网络,则 AVIE 请求 SEM 调用 CE,CE 根据 SEDB 中的 SA 参数进行相应的安全封装处理操作。

3　结语

BWIP 网络安全体系模型具有以下特点:①充分考虑到 BWIP 网络的安全需求与安全功能,如 AAA 技术;②采用集成的技术思想,将所有宽带无线接入链路安全技术进行透明处理,保持各自接入技术的特色,从网络层进行整体安全考虑,将现有及未来的 BWIP 技术都纳入到本安全体系之中,具有良好的扩展性和兼容性;③BWIP网络安全体系结构采用模块化设计思想,系统之间通过接口进行联系,系统灵活性强,便于扩充新技术和新算法等。

BWIP 网络融合移动通信和 Internet 技术,未来发展前景非常好,国际上有许多无线 Internet 组织都在致力于安全体系结构研究。未来 BWIP 安全体系结构研究将重点在以下几个方面进行:①结合密码学和容错技术,设计可生存的网络安全体系结构,在满足可靠性与安全性的同时,也在一定程度上满足信息保障和信息可生存性的要求;②研究硬件或软件容错技术在系统安全设计中的应用,以屏蔽入侵/攻击对系统功能的影响,保证系统关键功能的安全性和连续性;③基于可验证的加密技术,设计出满足系统安全需求、可以抵抗包括硬件故障在内的入侵/攻击行为、具有一定容忍入侵能力的可生存的网络安全体系结构。

参考文献:

[1] ISO/IEC7498-2, Security Architecture of OSI Reference Model, Part 2 security architecture[S]. 1989.

[2] Kent S, Atkinson R. Security Architecture for the Internet Protocol, RFC 2401[S]. November 1998.

[3] Wireless Application Protocol Architecture Specification[EB/OL]. WAP-100-WAPArch-19980430-a, WAP Forum, Http://www.wapforum.org, 2003.

[4] 3G Security Architecture(Release 5) technical specification[EB/OL]. Http://www.3gpp.org, 2002 - 12.

[5] Common Data Security Architecture(CDSA)[EB/OL]. Intel Architecture Lab, http://www.intel.com, 2005.

[6] 吴振强,朱建明. 宽带无线 IP 网络的安全需求分析[Z]. 西安电子科技大学计算机网络与信息安全教育部重点实验室, 863 课题组, 2003 - 10.