无线应用场景下基于 IPsec VPN 的研究与实现

张朝伟,李伟生

(北京交通大学 计算机与信息技术学院,北京 100044)

摘 要:随着无线局域网日益发展,无线网的安全问题倍受人们的关注。同时因特网的安全协议 IPsec 技术已相当成熟,将 IPsec 技术延伸到无线网络部分,以确保无线局域网的安全,这也是一种较好的解决方案。文中在扼要介绍虚拟专用网 VPN 安全机制的基础上,研究和分析了 IPsec 协议族的主要技术;在分析简化 IPsec 协议的基础上,结合具体常见的无线应用场景和 IKEv2 的密钥管理新技术来实现 IPsec VPN;同时重点分析了无线场景下 IPsec 安全隧道建立的过程和协议中对数据包的处理流程;最后,指出了无线网络技术的应用前景和未来 IPsec 的研究方向。

关键词:无线网络;IPsec;IKE;隧道;认证

中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2007)04-0104-04

Research and Implementation of IPsec VPN under Wireless Network Scenarios

ZHANG Chao-wei, LI Wei-sheng

(School of Computer and Information Technology, Beijing Jiaotong University, Beijing 100044, China)

Abstract: As the development of the wireless network, its security is focused by more and more people. At the same time, the security protocols of Internet IPsec technology has developed. It is a good method to guarantee the security of the wireless network by extending the protection of IPsec to wireless network. Briefly introduces the principle of IPsec in VPN and makes a detailed research and analysis on the main technology of IPsec serial protocols. Under the analysis and reduction of IPsec protocols, with the description of the wireless network scenarios, and with the Internet key exchange protocol version 2 to implement the IPsec VPN. Detail describe the establishing process of IPsec tunnel and its implementation. Finally, the application of the wireless network and the future research of IPsec are pointed.

Key words: wireless network; IP security; Internet key exchange; tunnel; authentication

0 引 言

随着因特网的普及和广泛应用,无线数据网络也迅速崛起,由于其有别于传统布线网络的优势,以及良好的移动特性吸引了广大用户和开发商关注。目前越来越多的移动设备(智能手机、PDA、笔记本等)通过无线网络接入因特网,这也正是下一代网络的重要组成部分。人们加大了对无线技术的深入研究,产生了更多的标准和规范。

目前 IEEE802.11 无线局域网已经支持高达 54Mbit/s 的数据传输速率,这可以满足语音、视频、文件传输等大多无线应用场景的要求。尽管无线局域网的抗干扰性强,但安全机制仍存在一些漏洞,比如 WEP 加密机制中密钥的重复使用和传输过程中消息容易被篡改等缺陷,无线局域网的安全机制仍不能有效保护用户的信息。

众所周知,虚拟专用网是在公网上,建立一个临时、安全的连接,通过采用各种技术保证网络数据的安全传输。IPsec 安全协议是 Internet 工程任务组织 IETF 制定的一组开放协议的总称,也是实现 VPN 功能的最佳选择,是目前提供网络间安全通信的主要手段。

VPN 技术有以下特点[1]:

(1)信息的安全性,采用隧道技术可为用户提供一个无缝的和端到端的连接服务;

(2)方便扩充性,用户可以方便地重构企业专用网,实现异地业务的安全访问,加强客户和合作伙伴之间的安全联系;

(3)方便的管理,可以将大量的管理工作放到网络服务提供者一端进行统一管理,从而减轻了企业内部

收稿日期:2006-07-30

作者简介:张朝伟(1979-),男,河南人,硕士研究生,主要研究方向为网络安全、移动 IP;李伟生,教授,主要研究方向为并行计算、网络安全、网络数据库等。

的管理负担;

(4)显著的成本效益,利用互联网构建企业内部的网络,可以节省了大量的投资成本和后期维护成本。

文中正是考虑到无线局域网的广泛应用和其目前仍存在的安全漏洞,以及 IPsec VPN 的众多优点,将 IPsec 技术应用到无线应用场景下,通过实现无线环境下的 IPsec VPN 来保证无线局域网环境下的信息的安全使用。

1　VPN 关键技术

VPN(Virtual Private Network)即:虚拟专用网,它是在公用网络上建立专用网的一种技术,通过采用隧道技术、加解密技术、认证技术、密钥管理技术以及访问控制技术在一条公网上,建立一个临时、安全的连接,从而实现移动用户同安全网关保护的局域网之间进行数据的安全传输。之所以称作虚拟网,主要是因为整个 VPN 网络的任意两节点之间的连接并不像传统的专用网那样建立端到端的物理链路,而是一条虚拟的连接。

1.1　隧道技术(Tunneling)

隧道技术是一种协议的封装技术。将一种协议(协议 X)封装在另一种协议(协议 Y)中传输,实现协议 X 在公网上传输的透明性。协议 X 被称为被封装协议,协议 Y 被称为封装协议。在公网上传输过程中只有协议 Y 所用到的 VPN 的端口号或安全网关的 IP 地址在公网上可见。隧道方式解决了专用网同公网之间的兼容问题,保护了发送端、接收端的 IP 地址和其他的协议信息,从而为用户提供无缝的、安全的、端到端的连接服务,确保信息资源的安全。

隧道是由隧道协议形成的,分为第二、第三层隧道协议,它们分别作用到 OSI 网络体系结构的第二层(数据链路层)和第三层(网络层)。这两种协议的主要区别在于,用户的数据包被封装到不同类型的数据包在隧道中传输。第二层隧道协议是以点对点的协议 PPP 为基础的,将网络协议封装到 PPP 帧中,在将整个数据包封装到隧道协议中,主要的协议有 L2TP、PPTP 等,主要用于远程访问虚拟专用网。而第三层隧道协议下是将网络协议直接封装到隧道中,形成数据包按照网络层协议进行传输,具有更好的扩展性、安全性和可靠性。主要的协议有 IPsec,GRE 等,主要用于端到端、端到安全网关或安全网关之间建立安全通道。

隧道技术是 IPsec 的核心技术,IPsec 采用的是第三层(网络层)的隧道封装技术,通过封装网络层协议来实现载荷的安全传输。

1.2　加解密和认证技术

加解密和认证技术是提供安全传输的重要技术,保证数据在传输过程中的安全性,不被非法用户窃取或篡改。加解密保证数据传输的安全性,即使数据丢失,真正的信息也将不会泄漏;认证技术是保证用户访问的合法性,只有通过认证的用户才能访问特定的资源。

以密钥为标准,可将密码体制分为单钥密码和双钥密码。单钥密码体制加密和解密时采用同一密钥,加解密速度快;双钥密码体制加密和解密密钥不同,加密采用公开密钥,解密采用不同的密钥,相对单钥密码体制,其密钥算法复杂、加解密速度慢。加解密算法主要有 DES,3DES 和 AES。现在的 VPN 一般采用混合的密码体系,加解密采用单钥,密钥传输的时候采用双密钥传输,这样既保证了速度,又保证了安全性。

证书技术保证用户的合法性,防止第三方恶意攻击,一般在传输数据之前先进行用户身份认证。一般的认证方法有:简单口令如质询握手认证协议和密码身份认证协议等;动态口令如 X.509 数字证书和动态令牌等;而按照 VPN 实施的环境的特殊性,IKEv2 中支持通过采用 EAP 载荷来支持不同环境下的认证方法。采用支持无线局域网(802.11 WLAN)场景下的 EAP－SIM 认证方法。采用认证方法需要认证服务器的支持,文中的实现中采用的认证服务器是部署在安全网关后面的 RADIUS 认证服务器。

1.3　密钥管理技术

密钥管理技术的主要任务就是保证在开放的网络环境下安全的传输密钥。目前密钥管理协议包括 ISAKMP, SKIP, MKMP 等。Internet 密钥交换协议 IKE 是 Internet 安全关联和密钥管理协议 ISAKMP 框架的实例化,已经成为主要的密钥管理标准。目前 IKE 有两个标准 IKEv1 和 IKEv2。IKEv2 是通过修改 IKEv1 消息的数目和消息的格式使协议更加安全和灵活。

1.4　访问控制技术

访问控制技术(Access Control Technology)就是 VPN 保证不同的用户对不同的信息资源访问权限的不同,以实现基于用户细粒度的访问控制,实现对信息资源最大限度的保护。

2　IPsec 协议族的研究

IPsec 是 IETF IPsec 工作组为了在 IP 层提供通信安全而制定的一套协议族,包括安全协议(AH 与 ESP)、密钥管理协议、安全关联以及加密认证算法等。IPsec 协议各组件之间的关系如图 1 所示。

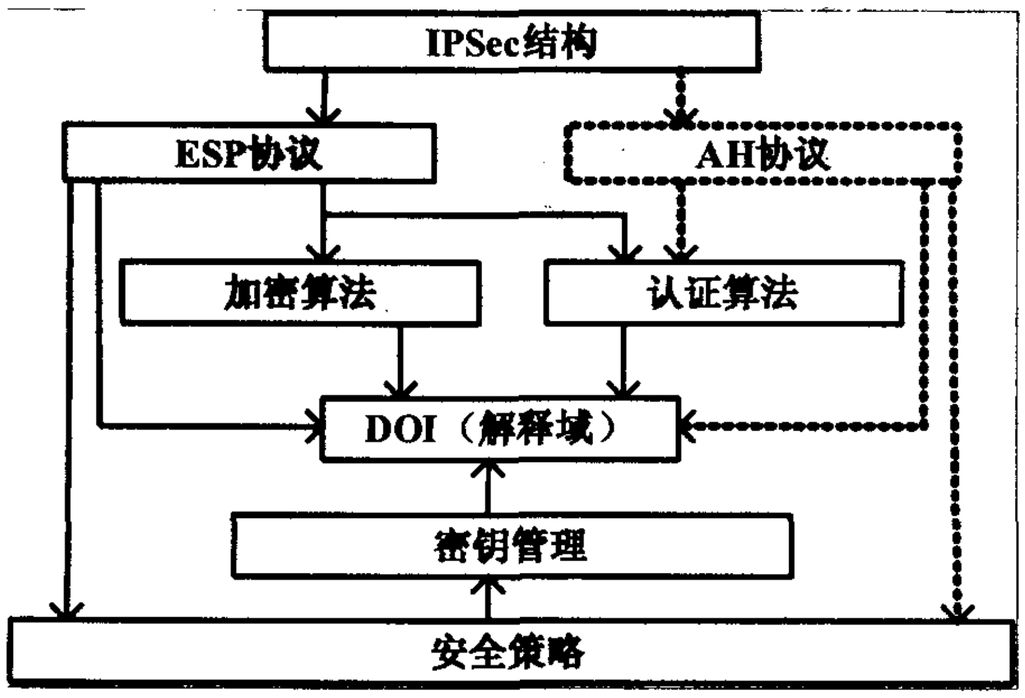


图 1 IPsec 体系结构

在 IPsec[2]体系结构中有一个重要的部分——解释域(Domains Of Interpretation,DOI)。安全协议涉及到密码学中的核心问题:加密和认证算法。为了使通信双方能正常通信,实现的 ESP 和 AH 必须遵从共同的解释规则,保持相同的解释域。当需要在 IPsec 中加入新的算法时,需要完成两个主要的工作:一是扩展 DOI,二是在协商过程中修改相应的算法字段。

2.1 安全协议和封装模式

IPsec 安全协议包括 AH(认证头)[3]和 ESP(封装安全载荷)[4],AH 和 ESP 都能够为 IP 层提供无连接的完整性、数据源认证和可选的、有限的抗重放(replay)保护。而 ESP 还能可选择性地保障数据的机密性,以及为数据流提供有限流量的保密性。

在实施 IPsec 时,AH 和 ESP 可以单独使用,也可以结合使用。IPsec 协议的制定者之所以对它们进行区分,主要是为了功能分配清楚,体现一定的灵活性。然而这种区别是完全没有必要,因为它们除了在认证范围上有所区别外,没有资料显示 AH 比 ESP 更安全,它们所用的认证算法和认证步骤都完全一样的,这种区别将使实际的操作更加复杂[5]。比如在 IKE 的协商中需要 SA 协商是使用 AH 或 ESP,或者两者都用,这显然造成了协议的复杂性。所以在 IKEv2 的协议规范中已经不再强制要求 AH 协议的实现支持。为了简化协议的实现,在图 1 中 AH 协议部分采用虚线表示,在协议实现中可以不用支持 AH。

IPsec 的封装模式有两种:隧道模式(Tunnel)和传输模式(Transport)。IPsec 通过这两种模式对 IP 及上层协议(TCP 和 UDP)进行封装提供安全保证服务。传输模式是本地方式,适合用于保护两台独立主机之间的通信,用于保护 IP 数据包内部的载荷;隧道模式则是封装加密整个 IP 包,适合于主机与安全网关之间和安全网关与安全网关之间的通信。两种模式的主要区别在于保护的范围和应用的场景不同。

不同的安全协议与不同的封装模式组合在一起,就形成了四种组合方式:AH 传输模式、AH 隧道模式、ESP 传输模式和 ESP 隧道模式。从前面 AH 和 ESP 的区别看,我们不去支持 AH 协议的实现,这样就减少了 AH 传输模式和 AH 隧道模式两种组合。从传输模式与隧道模式的区别来看,传输模式主要应用在端到端的主机之间的通信,隧道模式主要应用在主机同安全网关之间或网关与网关之间的安全通信。ESP 传输模式数据包的封装前后的格式如图 2(a)所示,处理后的数据包添加了 ESP 头、ESP 尾和认证数据,封装后的数据包 IP 头没有发生改变;ESP 隧道模式数据包的封装前后的格式如图 2(b)所示,在 ESP 隧道模式下除了添加了 ESP 头、ESP 尾和认证数据外,另外添加了新的 IP 头并且将新的 IP 头作为处理后的数据包的 IP 头。

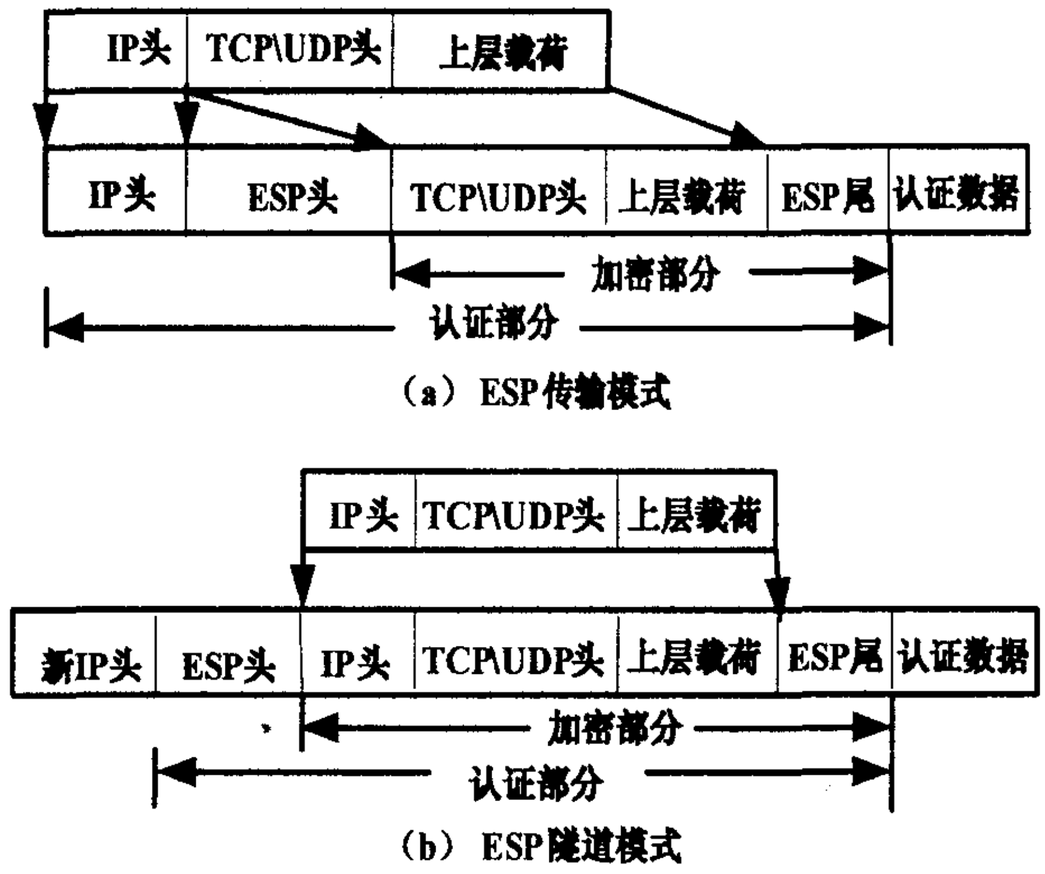


图 2 ESP 模式

2.2 安全联盟与安全策略

IPsec 有两个主要的数据库 SAD 和 SPD。SAD 中存放的是 SA 的记录,SA 是两个通信实体建立的协定,它决定了用来保护数据包安全的 IPsec 协议、转码方式、密钥及密钥的有效存活时间等。SA 是单向的,发送端的 SA 用来保护数据包,目的端的 SA 用来检查接收到的包的安全性。SA 是由三元组(安全参数索引 SPI, IP 目的地址, 安全协议)唯一表示的。

每条策略都定义了要保护什么通信、怎么保护以及和谁共享这种保护。

2.3 IKEv2

IKEv2[6]是在 IKEv1 的基础上,通过改变消息的格式和减少消息的数目简化 IKE。采用 IKE 一般包括两个阶段 IKE_SA_INIT 和 IKE_AUTH 两个阶段。IKE 所交互的消息都是以请求和响应的方式成对出现,在 IKE_SA_INIT 消息中协商了加密算法,交换 Nonce 和 Diffie－Hellman 交换。IKE_AUTH 阶段通过四对交互消息,并实现了 EAP－SIM 认证过程。

3　无线场景下 IPsec VPN 的实现

通过对具体应用场景的分析,详细描述了 IPsec 安全通道的建立过程和数据包交互的过程;并分别对数据包的进入和外出的处理过程进行描述。

3.1　无线场景下实现环境的构建

当移动终端要通过无线局域网[7],从外地网络访问安全服务的时候,比如 Web 服务、电子邮件服务、FTP 服务等网络服务,需要通过与安全网关之间建立 IPsec 安全通道,移动终端通过安全隧道访问网络服务,如图 3 所示。

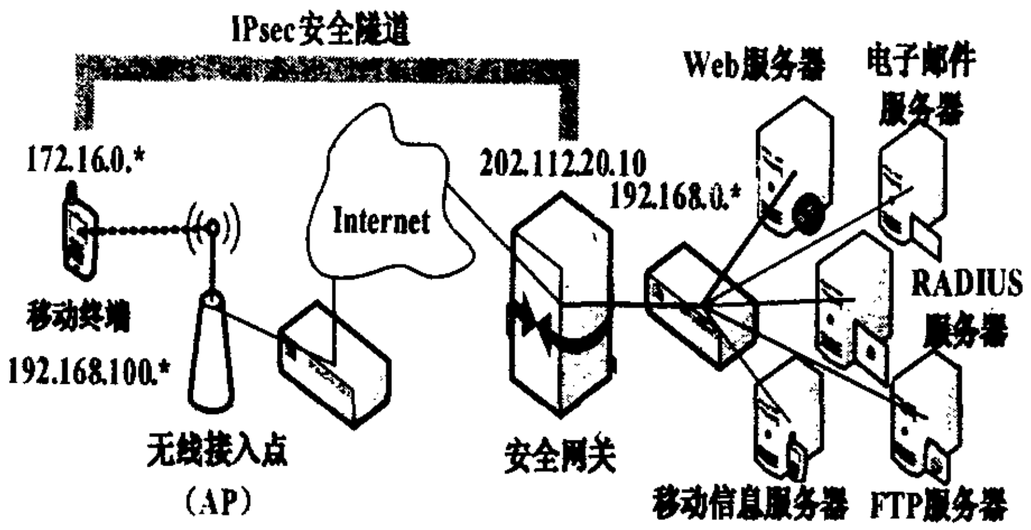


图 3　IPsec 无线应用场景

在无线局域网环境下建立 IPsec 安全隧道,建立的具体过程如下:

1) 移动终端首先与无线接入点 AP(Access Point)建立物理上的无线连接,移动终端必须按照 IEEE802.11 无线局域网协议的要求进行实现,当要建立无线连接的时候,首先应配置移动终端的 ESSID 应和所要连接的 AP 相同;该部分属于 WLAN 实现部分,不再详细讲述。

2) 当移动终端与 AP 建立无线连接候,AP 将通过 DHCP 方式动态地给移动终端分配 IP 地址,如:192.18.100.10,并且该 IP 地址将作为移动终端的实际要用的 IP 地址。在 IKE 协商的第一个阶段 IKE_SA_INIT 阶段,该地址将作为外出包的源地址和进入包的目的地址。

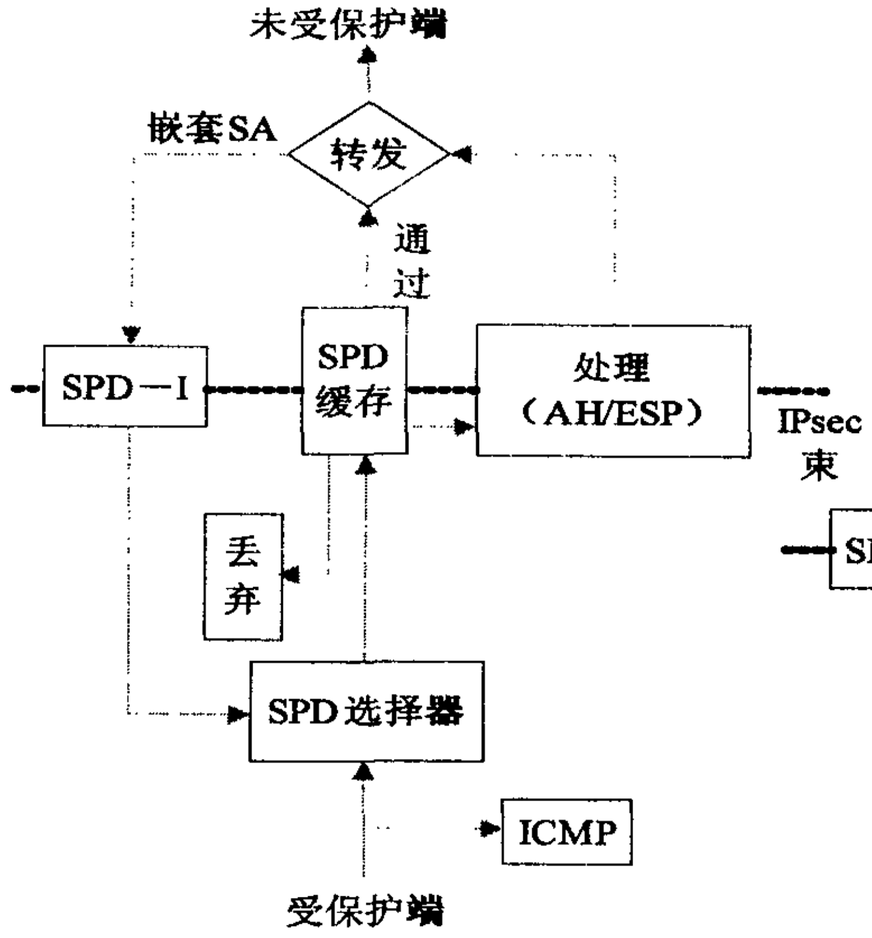
3) 当实际的物理链路建好以后,进行建立 SA 的过程。SA 建立包括两个阶段:第一阶段 SA 初始化 IKE_SA_INIT,该阶段中移动终端和网关之间只有一对交互包;第二阶段认证 IKE_AUTH,该阶段中包括四对数据包的交互。经过这两个阶段以后,IPsec 将建立安全遂道,进入和外出的数据包通过不同的 SPI 进行标识。

4) 当移动终端同安全网关建立好安全遂道以后,安全网关将会通过 DHCP 方法为移动终端分配一新 IP 地址,如:172.16.0.1;此时当移动终端需要访问安全网关所保护的服务的时候,需要加密的数据包将通过隧道方式传递。封装后的新的 IP 包则以网关分配的地址为新的 IP 头中的地址,而先前得到的 IP 地址则作为封装前的移动终端真实的 IP 地址;同样所有经过隧道发往移动终端的数据包也将以该地址为目的地址。

3.2　数据处理流程

IPsec 对数据包的处理主要分为外出和进入处理、AH 和 ESP 处理,如图 4 所示。协议处理可分为 SPD 处理、SA 处理、头和转码处理。对 AH 和 ESP 来说,SPD 和 SA 处理是相同的,只是转码和包头处理时不同。在新的 IPsec 体系结构[2]中,SPD 被分为三部分,SPD－S(安全载荷)、SPD－I(进入载荷)和 SPD－O(外出载荷)。

* 外出处理。



* 进入处理。

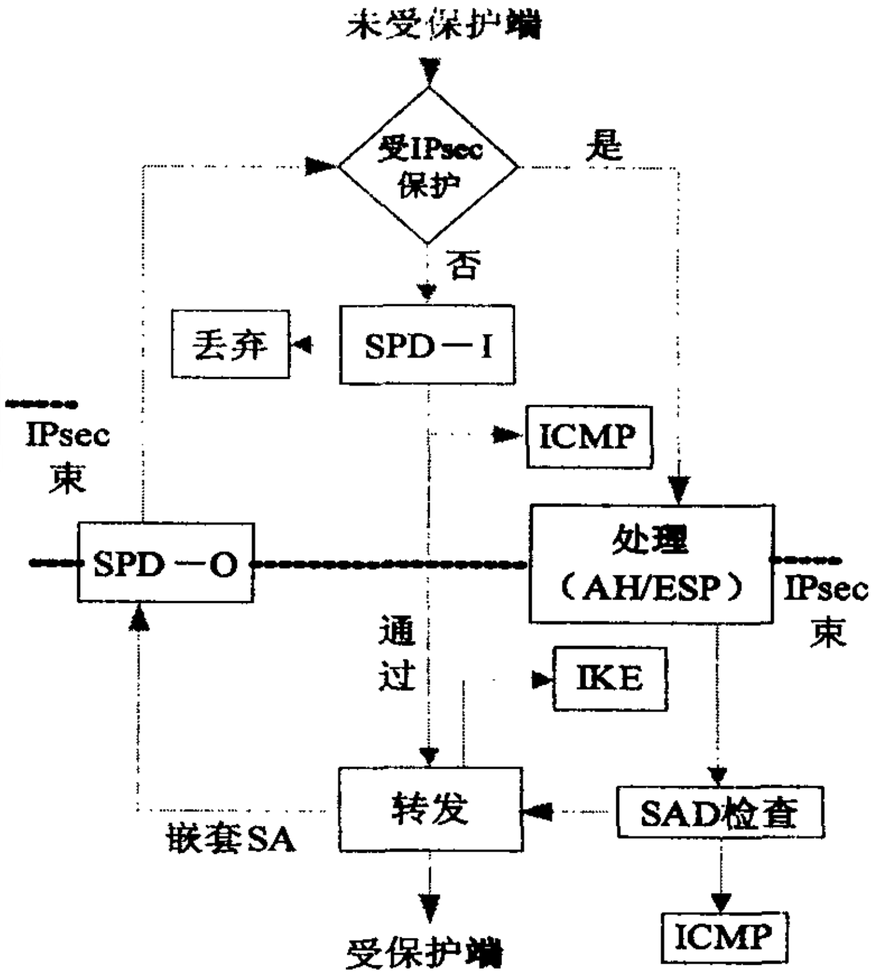


图 4　数据包的处理过程

每个外出的数据包首先查询 SPD 策略数据库,以决定下一步怎么处理。如果这个包要丢弃的话,则产生审计事件;如果 SPD 中致命这个包可以绕过 IPsec 处理,则和通常的数据包处理一样;如果需要应用 IPsec 处理的话,SPD 缓存实体将会映射到一个现存的 SA(束),或是一个新的 SA(束);按照协商好的协议进行 IPsec 处理。

(下转第 112 页)

MPP 收到检查消息后,会把 OrderB 发送给指定 ID 用户,此时用户能发现商家的冒充行为。

由此可见,方案具有抵制商家冒充行为的能力。

再次,若有用户冒充,则冒充攻击可能出现在方案的第(2)步或者第(3)步,有三种情况:

*用户 B 在购物完毕后使用用户 A 的 ID,这时 MPP 产生的 SessionKey 用用户 A 的 PIN 码加密后发给用户 A,此时用户 B 在不知道用户 A 的 PIN 码的情况下,无法进行下一步操作;

*用户 B 能够窃听或截取到消息 II 和 III,但无用户 A 的 PIN 码无法得到 SessionKey;

*用户 B 能够窃听或截取到消息 IV,但不能解密用 SessionKey 加密的内容,同时 Challenge 又抵制了重放攻击。因此只要用户的手持设备的 ID 不被窃取,用户就可不必担心自己被冒充。

由上面三种情况可知,方案能够抵制用户冒充的攻击,即能够认证用户。

5.4 不可否认性

不可否认性和认证性紧密相连。该方案每条消息摘要都经过了主体的数字签名,它们将作为不可否认的证据提供给对方,因此可以有效地防范客户和银行的事后抵赖行为。特别是商家和客户的电子收据能有效地抵制银行的抵赖行为。

5.5 可用性

综上所述,该方案较完备地考虑了移动支付系统的安全性需求,加之其可适应无线环境和手持设备的受限性,将大部分计算性功能从手持设备端转移到服务器端完成,另外 J2ME 平台提供了对 HTTPS 的支持,因此该方案是适用于构建实用的移动支付系统的。

6 进一步工作

实用的移动支付系统在技术上涉及到许多方面,文中所提出的方案着重考虑了无线环境下的安全性,但是有线环境下的安全性同样需要谨慎设计。另外,如何提高系统的吞吐量,使得当用户数量增加时,对用户的响应仍然相对及时,使用户不感觉到系统的延时仍需进一步研究。

参考文献:

[1] Mobile payment forum, Ltd. Mobile payment forum white paper[EB/OL]. 2002 - 12. http://www.mobilepaymentforum.org/info/mpf_docs/mpf_whitepaper.pdf.

[2] 冯登国. 密码学原理与实践[M]. 北京:电子工业出版社, 2003.

[3] Stallings W. 密码编码学与网络安全[M]. 杨 明,胥光辉等译. 北京:电子工业出版社,2002.

[4] Forum Nokia. MIDP 2.0 Introduction, Version 1.0[EB/OL]. 2003 - 03. http://forum.nokia.com.cn/sch/index.html.

[5] Daemen J, Rijmen V. AES Proposal: Rijndael, AES Algorithm Submission, National Institute of Standards and Technology (NIST) AES[EB/OL]. 1999. http://csrc.nist.gov/CryptoToolkit/aes/.

(上接第 107 页)

对进入的包进行检查看是否进行了 IPsec 保护,如果未受保护则查询 SPD - I 数据库决定是丢弃或是转发,同样如果丢弃则进行审计事件,如果通过就和普通数据包一样处理;如果受到 IPsec 保护,首先进行查找 SAD 数据库 ,查询有无与之相匹配的 SA 实体。如果没有丢弃该包,并进行审计事件;如果有与之匹配的 SA 实体,按照协商好的协议进行 IPsec 处理。进入和外出处理都考虑到嵌套 SA 的处理,如果需要则按上述流程处理。

4 结束语

主要讲述了 IPsec 在无线应用场景下的实现过程。而下一代网络将是一个混合异构网络,以高速固网为中间骨干网,边缘有多种有线和无线接入网络组成[8]。移动终端也将是下代网络的重要组成。如何保证这些设备在各种接入网络间安全自由切换,实现“无缝移动”,IETF 专门成立 MOBIKE 工作组,研究 IPsec 与移动 IP 之间的集成和互操作问题。IPsec 的发展目标将是保证未来各种网络之间的安全和平共处。

参考文献:

[1] 李成友,曹 伟. IPsec 研究与虚拟专用网技术[J]. 计算机工程,2002(2):246 - 248.

[2] Kent S, Seo K. RFC4301. Security Architecture for the Internet Protocol[S]. 2005.

[3] Kent S. RFC4302. IP Authentication Header[S]. 2005.

[4] Kent S. RFC4303. IP Encapsulating Security Payload(ESP) [S]. 2005.

[5] 龙艳彬,王丽军. IPsec 的分析与改进[J]. 计算机应用,2005(2):390 - 393.

[6] Kaufman. RFC4306. Internet Key Exchange (IKEv2) Protocol[S]. 2005.

[7] 徐 敏,罗汉文. 无线局域网安全问题研究[J]. 通信技术,2002(7):65 - 66.

[8] 叶润国,冯彦军. IPsec 在移动无线场景下的互操作问题[J]. 北京航空航天大学学报,2004(11):1057 - 1061.