WAP安全构架研究及WTLS的实现*

罗 蕾** 王 庆 谭罗丽

(电子科技大学计算机科学与工程学院 成都 610054)

【摘要】研究了基于无线应用协议安全构架的WTLS、WIM、WPKI、WMLScript 4个组成部分及安全构架体系的基本组成部分。分析了端到端的安全模型的三种实现方式，并比较其安全性。阐述了无线传输安全协议的服务类型、运行流程，采用消息事件机制设计WTLS状态机，并在移动终端上设计且实现了WTLS。

关 键 词 无线公共密钥系统; 无线传输安全协议; 安全构架; 移动商务

中图分类号 TP393

Research of M-Commerce Security Frame and Implement WTLS

Luo Lei Wang Qing Tan Luoli

(College of Computer Science and Engineering, UEST of China Chengdu 610054)

Abstract This paper studies wireless application protocol four components of security frame and base components of security frame architecture. Analyses three implement methods of End_to_End security frame and their securities. Service Levels and running flow of wireless transport layer security are described . WTLS state machine is designed by message event driven, design and implement WTLS of mobile terminal.

Key words wireless public KEY infrastructure; wireless transport layer security; security frame; m-commerce

移动商务(M-Commerce) 是利用移动通信手段来完成电子商务，它为电子商务的发展创造了更为广阔的发展空间。移动商务是通过手机、PDA(个人数字助理)等便携移动终端来完成商务活动。随着移动通信技术的发展，移动商务的条件日益成熟，安全问题作为移动商务发展的门槛，急需解决。目前，国外大公司纷纷推出以WAP(无线应用协议)为基础的移动商务安全构架，它具有开放性和使用的广泛性，主要以WPKI(无线公钥加密框架)为基础、WTLS(无线传输层安全协议)为安全传输协议；为移动终端厂商、移动运营商、增值服务商提供统一的移动安全构架模型。

1 WAP安全构架模型

WAP安全构架由WTLS、WIM(无线鉴别模块)、WPKI、WMLScript(无线标记语言脚本)四部分组成，各个部分在实现无线网络应用的安全中起着不同的作用，基于WAP的安全构架体系的组成部分如图1所示。其中，WPKI作为安全基础设施平台，是安全协议能有效实行的基础，一切基于身份验证的应用都需要WPKI的支持。它可与WTLS、TCP/IP、WMLScriptsign相互结合，实现身份认证、私钥签名等功能。基于数字证书和加密密钥，WPKI提供一个在分布式网络中高度规模化、可管理

2002年4月5日收稿
* 四川省科技攻关基金重点资助项目
** 女 35岁 工学硕士 副教授

的用户验证手段。

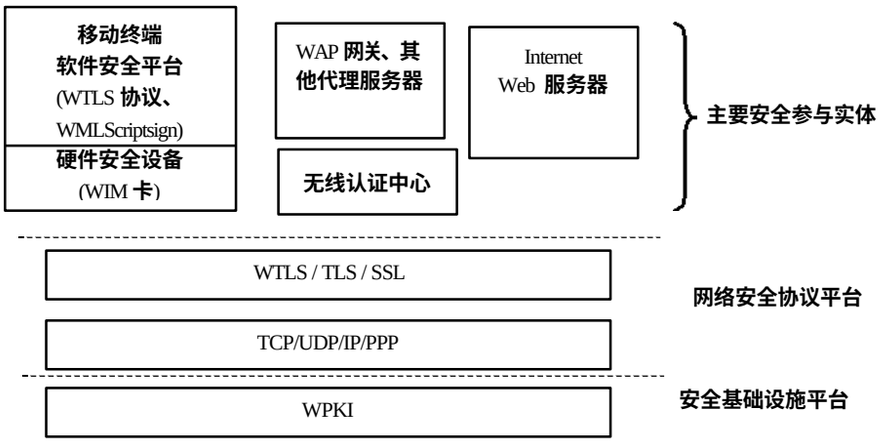

图1 基于WAP的安全构架模型

网络安全协议平台包括WTLS协议及有线环境下位于传输层上的安全协议TLS、SSL和TCP/IP协议。安全参与实体作为底层安全协议的实际应用者，相互之间的关系也由底层的安全协议决定。当该安全构架运用于实际移动电子商务，这些安全参与实体间的关系即体现为交易方(移动终端、Web 服务器)和其他受信任方(WAP网关、代理和无线认证中心)。

2 安全模型的实现及安全性分析

基于WAP的安全构架模型有不同的实现方式，虽然使用的基本安全协议是一样的，但不同的实现方式之间的安全级别却存在着较大的差异，下面对三种实现方式进行分析。

2.1 双区安全模式

双区安全模式是通过采用一个称为WAP网关的代理服务器来实现。WAP网关建在无线网的边缘，它像一座桥，把有线网和无线网联接起来，并把使用WTLS保护的数据转换成使用SSL保护的数据，双区安全模式如图2所示。图中，数据在无线环境下被封装在WTLS安全连接中，在有线环境下，则被SSL/TLS所保护，在这两个区域内数据是安全的。但在WAP网关中，数据在协议转换的过程中被提取出来，以明文的形式暴露在WAP的网关上。为了转移和发送数据，网关必须从WTLS解密，然后再加密进入SSL。这意味着WAP网关能"看见"通过它的数据，并进而可能泄露通过它的数据。双区安全模型是一个简便易行、成本较低的实现方式，在对WAP网关中的安全间隙能容忍的情况下可以解决一定的安全需要。

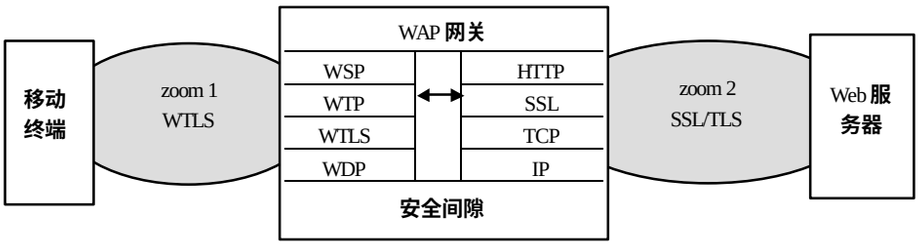

图 2 双区安全模式

2.2 端到端安全模型——WAP Server模式

相对于双区安全，端到端的安全在数据通道上不存在安全间隙，其安全数据通道建立在移动终端和最终要访问的服务器之间，数据在通道上传送的过程中一直处于加密状态。

端到端的安全模型有多种实现途径，图3是一种称作WAP Server的安全模型，它是通过建立一

个具有WAP网关的Web服务器来解决端到端的问题。因为数据在移动终端和WAP Server之间采用WTLS加密，数据通道上不存在协议转换，而WAP网关作为最终服务器的一部分，就不再是整个过程中的一个环节，数据解密出来直接提交给服务器操作，实现了端到端的安全。

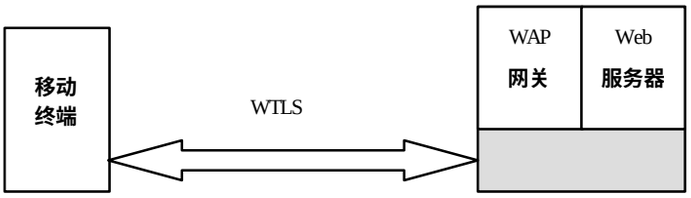

图 3　一种端到端安全模型—WAP Server

若采用WAP Server方式，用户必须重新配置WAP移动终端设备指向WAP Server，与之建立相应WAP会话。当用户想访问其他地方时，必须重新配置WAP设备来指向其他的网关。在移动终端设备一次只提供一种WAP网关配置的情况下，对用户来说比较麻烦。

2.3　端到端安全模型——透明网关模式

端到端安全的另一种解决途径是让WAP网关接收已经加密的WTLS数据流，并让其直接通到浏览器一方，可将问题的麻烦减到最少，如图4所示，更新网关比更新现有的移动终端要简单，而且代价也不大。第三方的网关(如移动提供商)依赖于数据流，其数据已由WAP Server使用WTLS来实现保护，当网关检测到 WTLS的数据流时，就简单地让其通过。在这种情况下，Web服务器必须具备解析WAP协议的功能，因此还需要更新Web服务器，由于无线接入的问题仍然由WAP网关解决，所做的改动远不如WAP Server模式大。还有一种实现端到端安全的途径是在其应用层级对数据进行再次加密(相对于WTLS层)，以便在用户和安全网关之间建立一个端到端的安全通道。这里存在一个安全网关，但并非WAP网关，而是在银行网络等系统网络内部的特殊网关，具有专门对应用数据解密的功能，从而使暴露在WAP网关中的应用数据仍被加密保护，不再被泄露。

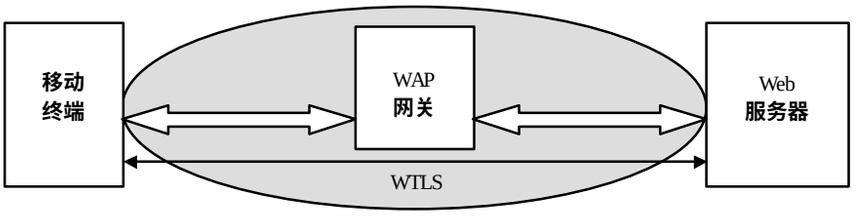

图 4　端到端安全模型的一种—透明网关模式

3　无线传输层安全WTLS

WTLS的作用是保证传输层的安全，作为WAP 协议栈的一个层次向上层提供安全传输服务接口。WTLS是以安全协议TLS1.0标准为基础发展而来的，提供通信双方数据的机密性、完整性和通信双方的鉴权机制。WTLS在TLS的基础上根据无线环境、长距离、低带宽自身的适用范围等增加了一些新的特性，如对数据报的支持、握手协议的优化和动态密钥刷新等。

3.1　WTLS的安全服务类别

WTLS能够提供下列三种类别的安全服务：

第一类服务能使用交换的公共密钥建立安全传输，使用对称算法加密解密数据，检查数据完整性，可以建立安全通信的通道，但没有对通信双方的身份进行鉴权；

第二类服务除完成第一类服务的功能外还可以交换服务器证书，完成对服务器的鉴别；

第三类服务除完成第二类服务的功能外还可以交换客户证书，在服务器鉴别的基础上，又增加

了客户鉴别，对恶意的用户冒充也能进行抗击。

从第一类服务到第三类服务安全级别逐级增高，可以根据应用对安全级别的要求选择性的实现某一级别的安全服务。通常应该对这三种类别的服务都能支持，在握手协商的过程中由客户端与服务端共同协商选定一个类别。

3.2 WTLS的运行流程

WTLS协议的安全连接建立过程大致分为以下几个步骤：1) 交换hello消息，以协商算法、交换随机数、检测恢复；2) 交换必要的加密参数供客户端和服务端使用，以协商premaster secret；3) 交换证书和必要的加密信息以实现双方认证；4) 从premaster secret和交换的随机数产生master secret，得到安全加密参数；5) 允许客户端和服务端检查对方是否产生了正确、相同的安全参数，以及确认握手过程没有受到攻击者的干扰；6) 协商完成后，双方可以在一个安全的通信连接上交换实际数据。

步骤1)～5)属于通信双方的握手协商过程，其流程如图5所示。通过握手协商建立好安全连接，并通过安全连接交换加密过的数据，握手协商过程是WTLS协议的主要内容。

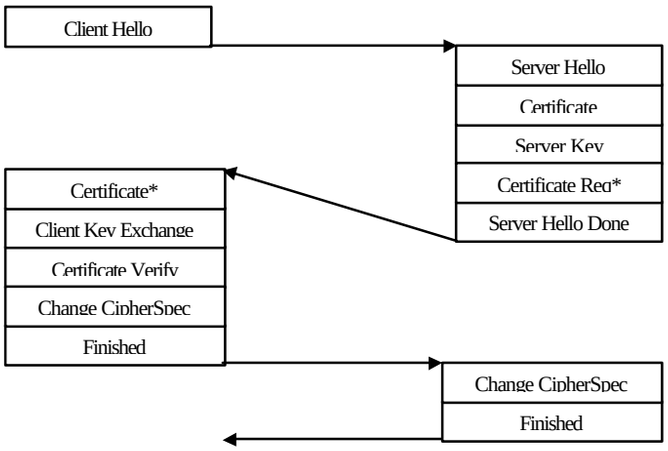

图 5 WTLS 完整握手流程图

3.3 WTLS协议结构

WTLS由功能协议层和记录协议层构成，其中功能协议层包含了握手协议、Change Chipher Spec、告警协议；记录协议层提供对握手协议层以及上层应用数据的封装结构，在客户端和服务端的WTLS对等层之间完成实际的数据传送任务，WTLS协议结构如图6所示。

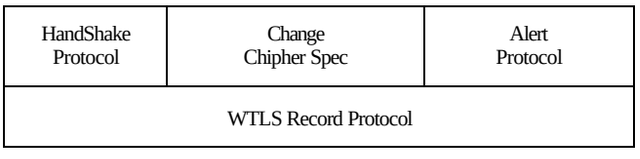

图6 WTLS协议结构

4 移动终端上WTLS的设计与实现

移动终端不同于普通PC，软件的设计和实现需要考虑这一环境的特点的软硬件特点。首先，移动终端(如PDA、手机)的硬件环境多为低处理能力的CPU，主频几十兆，多采用精简指令集，内存空间小。为此，程序需要采用高速度的数学运算库来提高加密速度，并确保对动态内存空间的基本要求尽量少。另外，不同厂家的移动终端采用的操作系统不同，这不仅是系统函数接口的不同和系统基本处理能力的不同，如有些系统本身不具有动态内存分配的能力和内存数据的大小端方式差

异。为了软件能适应不同的操作系统，尽量在设计和实现时做到采用标准C代码实现，无法避免的地方则通过代码中的宏来控制不同版本的编译。对特殊的系统缺陷必须有相应的机制来弥补，以确保软件具有较为广泛的适应性。

虽然移动终端的WTLS只需要实现WTLS状态机的客户端部分，但在设计和实现过程中考虑到软件适用程度的广泛性和作为一个协议软件研究的完整性，因此包含了关于服务端状态机的设计实现部分。另外，服务端的实现有助于建立一个良好的软件测试环境，可以模拟网络和服务器的非正常情况，测试现有网关不能支持的功能(如WTLS Class2/3 级别的安全功能)。

根据协议规范，WTLS客户端与服务端需要的基本数据结构以及对底层加密算法的要求相似，最大的区别在于状态机的不同：1) 状态机状态转换流程不同；2) 需要维护的状态机数目不同，客户端只需要维护一个状态机，服务端要同时维护多个状态机。因此软件实现的总体目标定位为完整的实现WTLS协议(包括客户端和服务端)，以客户端的实现为主要任务，在功能实现以外，充分考虑它的存储空间消耗、速度、稳定性、可移植性等性能要求，服务端软件只做功能实现，对性能要求暂不考虑。

4.1　软件结构设计

为了使WTLS软件具有良好的可维护性，设计时采用模块化的观点，根据对软件功能的分解，将划分为最顶层的状态处理机模块、支持状态处理机实现的基本数据结构处理模块和最底层的加密算法模块，每一模块又分为不同的小模块来实现。图7描述了WTLS软件模块的划分，以及各模块相互间的层次依赖关系。

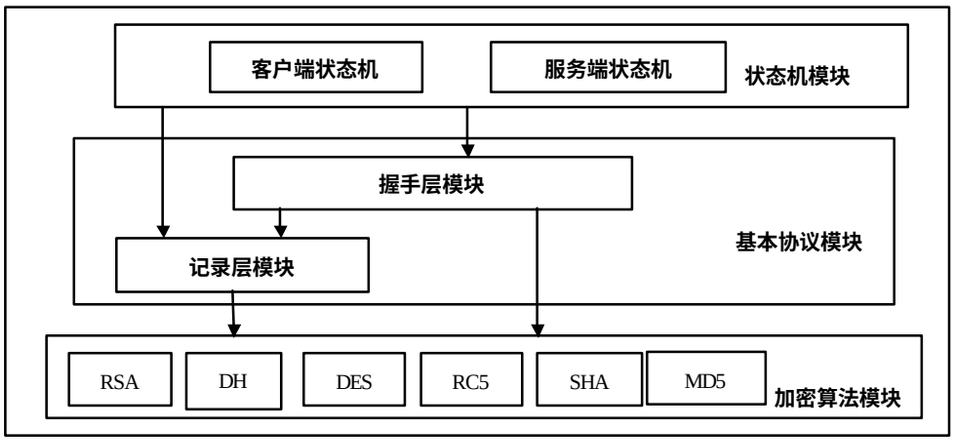

图7　WTLS软件的模块结构划分

1) 状态处理机模块是整个软件设计和实现的核心，该模块实现了WTLS协议规范中定义的状态机。协议中对状态机应该实现的能力进行了描述，设计中采用事件驱动的WTLS状态机模型，具体的实现包括该状态机的数据结构，以及各状态对应的事件处理函数。

2) 基本协议模块实现了WTLS协议规范中描述的数据结构，从最基本的向量类型到各阶段的握手结构、记录层的块结构，并且对每一个数据结构定义了必要的处理函数，如该结构类型的实体变量的创建、数据生成、撤消等，使程序具有良好的可读性。

3) 加密算法模块提供最基本的加密处理函数，如用于对称加密的RC5、DES，消息摘要函数SHA、MD5，证书有效性验证、签名、密钥交换所用的RSA，以及匿名密钥交换所用的DH算法。目前，由于受硬件条件的限制，没有可以利用的WIM卡这类方便的加密、认证手段，在实现WTLS软件的时候，使用软件方式来实现低层的加密函数库。在将来的实际商务应用中，可采用商用密码指定的算法库替换。

4.2 状态机模块的设计和实现

WTLS函数库采用状态机的方式实现，由状态机对象WTLS_machine保存每一个连接的当前状态，并根据发生的事件触发相应的操作。状态机的主要任务是通过握手建立安全连接，其握手过程比较繁杂，采用事件驱动的方式来实现状态机有利于程序设计和实现，WTLS状态转接如图8所示。整个握手过程可以分为以下三个阶段：

1) Create：客户方向服务器提出连接请求，服务器向客户方响应请求；

2) Exchange：双方交换密钥协商信息；

3) Commit：双方交换提交协商信息，通知对方协商的算法和密钥开始生效。

在每个阶段，在双方触发的事件包括请求(Request)、指示(Indication)、响应(Response)、确认(Confirm)。如Create阶段，首先客户方向服务器发请求Client Hello，由事件Create.req触发；服务器收到客户方的请求，触发Create.ind事件；服务器解析客户方的请求报文，设置事件Create.res，在这一事件触发下服务器生成并发送响应报文Server Hello 客户方收到这一报文后，触发事件Create.cnf。在每一次事件触发下，状态机状态转换，并同时执行相应操作。

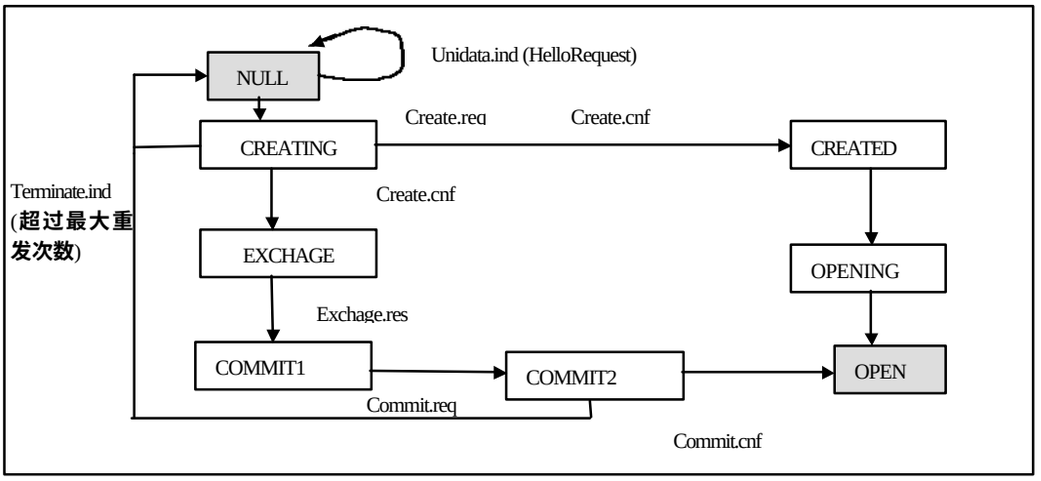

图 8 移动终端 WTLS 状态机状态转换示意

5 结 束 语

基于WAP的安全构架可实现端到端的安全解决方案，透明网关方式是一种简单实用的解决方式。设计与实现的移动终端上的WTLS已成功地移植到不同的移动终端上，并成功地与NOKIA、Phone.com等WAP网关互联。

参 考 文 献

1 WAP Forum. Wirless Transport Layer Security Specification(version 05-NOV-1999). WAP Forum, http: //www. wapforum. org. 1999

2 WAP Forum. WAP Transport Layer End-to-End Security. WAP Forum, http: //www. wapforum. org. 2001

3 WAP Forum. WML Script Specification. WAP Forum, http: //www. wapforum. org. 2001

4 WAP Forum. Public Key Infrastructure Definition. WAP Forum, http: //www. wapforum. org. 2001

5 WAP Forum. Wireless Identity Module. WAP Forum, http: //www. wapforum. org. 2001

6 WAP Forum. WAP Certificate and CRL Profiles Specification. WAP Forum, http: //www. wapforum. org. 2001

7 WAP Forum. Wireless Application Protocol Architecture Specification. WAP Forum, http: //www. wapforum. org. 2001

8 张惠媛. 移动互联网与WAP技术. 北京: 电子工业出版社, 2002