WTLS的研究与设计*)

Research and Design of WTLS

佘 堃[1] 周明天[1] 杨光志[2]

(电子科技大学计算机学院 成都610054)[1] (西南计算中心 绵阳621000)[2]

Abstract WAP is a standard protocol for mobile terminal accessing Internet, where WTLS is WAP's security foundation for E-commerce. In this paper, based on the newest WTLS specification, the WTLS information flow and states changing process are analyzed. Using DOT-based Modeling, the function library of WTLS is developed, and relevant psudo-codes are given.

Keywords WAP, TLS, WTLS, Wireless security, Mobile security

1 引论

当前电子信息领域内存在两大发展迅猛的技术:Internet技术和无线网络技术,它们已成为迈向信息社会的两大技术支柱。而WAP技术正是结合了以上两者的优势,日益显现出其蓬勃的生机与活力。

当前适合WAP的应用包括两个方面:一是即时信息的浏览和查询,包括新闻、天气预报、股票信息、航班信息、娱乐游戏、体育消息和健康常识等,这些信息是与移动终端设备的特性相适应的专有内容。目前,这方面的技术已经基本成熟,许多ICP(Internet内容提供商)都在开发这方面的应用;二是移动电子商务,WAP应用的长期目标就是使手机成为真正意义上的个人数字助理,可以将通信、支付、交易等功能集于一身,向用户提供如股票即时交易、手机银行等各种应用。不但要实现真正的移动电子商务,现有技术还不太成熟,特别是安全方面的问题亟需解决。为此,WAP论坛推出了无线PKI(WPKI)[1]和无线TLS(WTLS)[2]安全技术规范。本文只讨论WTLS。

2 WTLS

WTLS(Wireless Transport Layer Security)协议版本4-6-2001是从TLS1.0[3]协议演化而来的,其主题框架和握手流程模仿了TLS1.0协议中的内容,但又针对无线应用这一特殊领域的要求(如信道窄、处理能力低、内存小)做了相应的调整。

WTLS主要提供以下三方面的安全服务:客户方和服务器的合法性认证、对数据进行加密和保证数据的完整性。其流程如图1。

·WTLS客户发起会话,会话请求中包括密钥、支持的算法信息;

·WTLS网关根据这些信息选择合适的算法,并根据需要的算法和认证方式构造返回报文,包括选择的算法、证书、客户方证书请求等信息;

·WTLS网关发送该信息给客户;

·客户方根据算法验证网关身份、计算密钥参数和其他信息,构造响应包;

·客户方发送响应包;

·网关根据响应包信息验证客户身份、计算密钥参数;

·以后的数据全部加密后传输,但客户、网关使用的加密密钥不一样;

·最后,客户和网关任意一方都能主动发起连接终止。

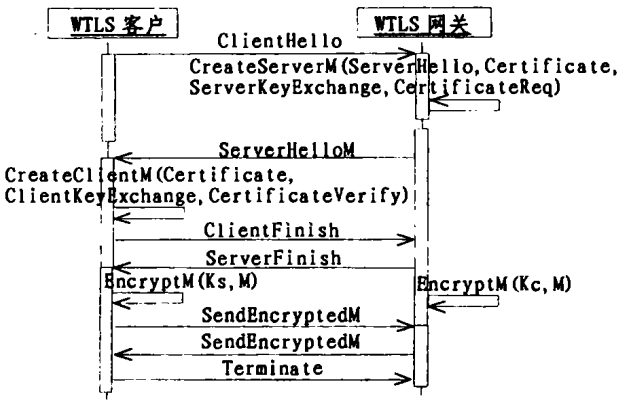

图1 WTLS完整流程图

3 WTLS系统(函数库)的分析与设计

3.1 WTLS系统(函数库)功能需求

本函数库用软件方式实现了WTLS协议,提供WTLS服务器和客户方的函数调用。向用户提供的调用接口函数主要有:

·WTLS_accept:服务器调用这个函数,等待客户方的Client Hello连接请求。当客户方连接请求到来时,本函数按照协议和客户方完成握手过程并最终按双方要求建立安全连接。

·WTLS_connect:客户方调用这个函数,向服务器请求建立安全的WTLS连接,并完成握手过程,直到双方建立安全连接。

·WTLS_read:客户方和服务器都可以调用这个函数,从当前的WTLS安全连接上读取数据。

·WTLS_write:客户方和服务器都可以调用这个函数,向当前的WTLS安全连接写入数据。

*)本文的工作得到国家八六三项目(863-301-7-9)的支持。佘 堃 副教授,研究方向:网络计算、安全计算、电子商务。周明天 博导,教授,研究方向:网络分布式计算,中间件计算。杨光志 高工,研究方向:网络计算、计算复杂性研究。

·WTLS_close：客户方和服务器都可以调用这个函数，向对方发出关闭通告，关闭 WTLS 连接。

·WTLS_resume：客户方调用这个函数，向服务器请求恢复以前的连接。如果服务器拒绝恢复，则和服务器进行完整握手过程。

这里给出这些需求的 Use Case 图，如图2。

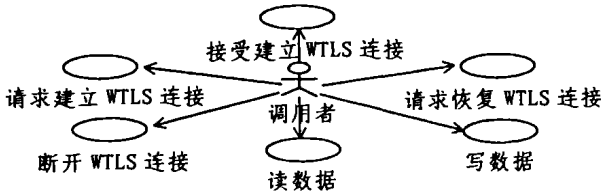

图2 WTLS 函数库 Use Case 图

3.1.1 *读数据(WTLS_read)流程* 以下以读数据为例，说明每一个功能模块的事件流和处理过程。

·调用者调用 WTLS_read。

·为保存一个 WTLS 连接的状态信息，引入一个 WTLS 状态机对象：WTLS_machine。用户需要调用的所有功能都通过这个 WTLS_machine 对象来实现。此时 WTLS_machine 从完成网络数据收发的网络协议实现对象 WTLS_transport 接收网络上传来的数据流。

·WTLS_machine 对象调用记录层协议的功能对数据流进行解码，因此这里需要引入一个完成记录层功能的记录层对象 WTLS_record。解码后得到 CipherText 结构。

·WTLS_record 在解码过程中调用加密算法的功能对 CipherText 进行解密。因此这里需要引入一个完成加密算法的对象 WTLS_cipher，而当前使用的加密算法标志和密钥都存储在 WTLS_machine 的连接状态中。

·WTLS_machine 把最后得到的数据返回给调用者。

3.2 WTLS 中的类对象

通过上面的分析可以看出，实现 WTLS 功能需要以下类或对象：

·WTLS_machine：状态机对象，保存当前状态，并提供最终面向用户的函数接口。它调用其他对象的功能，是整个函数库的核心对象。

·WTLS_transport：传输协议实现对象，实现网络传输协议 TCP 和 UDP，并封装 socket 函数，提供简单实用的函数接口。

·WTLS_certificate：证书管理对象，实现对 X.509个人证书和 WTLS 自定义证书的读、写、编码、解码、校验等功能。

·WTLS_config：配置模块，实现对 WTLS 配置文件的读写操作。

·WTLS_record：记录层协议模块，实现 WTLS 记录层协议定义的对明文、密文结构的编码解码。

·WTLS_handshake：实现 WTLS 握手协议定义的各种数据结构的编码、解码等操作。

·WTLS_cipher：实现 WTLS 协议中用到的加/解密算法。

另外，在我们的设计中进一步细化，还需要生成以下对象：

·WTLS_event：事件对象，存储 WTLS 事件类型和与该事件相关的参数。

·Symmetric_algor：对称加密算法对象，实现 WTLS 协议中用到的对称加密算法，这个对象是从 WTLS_cipher 对象派生出来的。

·Unsymmetric_algor：非对称加密算法，实现 WTLS 协议中用到的非对称加密算法，这个对象是从 WTLS_cipher 对象中派生出来的。

·DES[4]：DES 算法对象，实现 DES 算法，这个对象是从 Symmetric_algor 对象派生出来的。

·RC5[4]：RC5算法对象，实现 RC5算法，这个对象是从 Symmetric_algor 对象派生出来的。

·RSA[4]：RSA 算法对象，实现 RSA 算法，这个对象是从 Symmetric_algor 对象派生出来的。

·DH[4]：DH 算法对象，实现 DH 算法，这个对象是从 Unsymmetric_algor 对象派生出来的。

·ECDH[5]：ECDH 算法，实现 ECDH 算法，这个对象是从 Unsymmetric_algor 对象派生出来的。

·ECDSA[5]：ECDSA 算法，实现 ECDSA 算法，这个对象是从 Unsymmetric_algor 对象派生出来的。

以上对象构成 WTLS 函数库的类图，如图3所示。

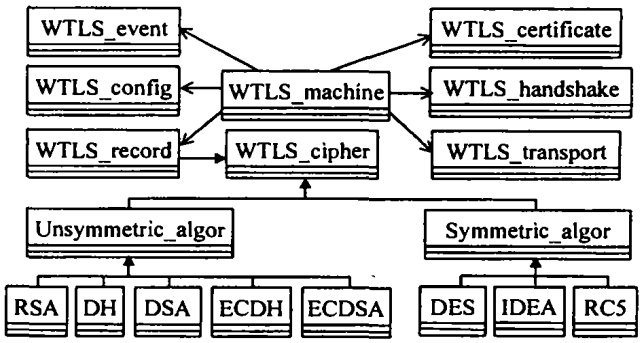

图3 WTLS 函数库类图

3.3 系统状态及事件定义

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。

本文以网关服务器的状态和事件为例进行描述。

3.3.1 *服务器的状态和事件* 整个握手过程可以分为三个阶段：①Create：客户方向服务器提出连接请求，服务器向客户方响应请求；②Exchange：双方交换密钥协商信息；③Commit：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，在双方触发的事件都包括请求(Request)、指示(Indication)、响应(Response)、确认(Confirm)，完全按照 OSI 模型[6]设计。例如在 Create 阶段，首先客户方向服务器发送请求 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。服务器状态定义如下：

·NULL 状态：服务器等待客户方的连接请求。

·CREATING 状态：服务器收到客户方的连接请求报文，进入算法选择阶段。

·CREATED 状态：服务器完成算法选择，进入密钥协商阶段。

·EXCHANGE 状态：服务器生成自己的密钥协商和证书报文，并发送给客户方端后，处于等待客户方密钥协商报文的阶段。

·OPENING 状态：服务器收到客户方密钥协商信息和证书，计算出安全连接所需的数据，处于等待本次协商得到确认的状态。

·OPEN 状态：服务器收到使用本次协商的算法及密钥加密的数据，协商得到确认，握手过程完成。

·COMMIT 状态：服务器收到客户方的连接请求后，如果是恢复以前的会话，则向客户方发送同意恢复的报文。

3.4 服务器状态机的实现

在 WTLS_accept 调用中，以 WTLS_machine 对象按照上节定义的状态和事件定义运转。当应用程序初始化 WTLS_machine 对象时，当前状态设置为 NULL，然后状态机启动。服务器实现状态机的伪程序如下：

```
while (machine->event_list)
{   switch(machine->state)
 {
case WTLSState_Server_NULL:
     machine->state = handle_server_null(machine);
     break;
case WTLSState_Server_CREATING:
     machine->state = handle_server_creating(machine);
     break;
case WTLSState_Server_CREATED:
     machine->state = handle_server_created(machine);
     break;
case WTLSState_Server_EXCHANGE:
     machine->state = handle_server_exchange(machine);
     break;
case WTLSState_Server_COMMIT:
     machine->state = handle_server_commit(machine);
     break;
case WTLSState_Server_OPENING:
     machine->state = handle_server_opening(machine);
     break;
case WTLSState_Server_OPEN:
     machine->state = handle_server_open(machine);
     break;
default:
     errno_abort("Critical Error; Undefined WTLSState");
     break;
 }
}
```

当 WTLS_machine 对象中的事件列表不为空时，就根据当前状态，调用相应的函数处理。在处理函数中，从状态机对象的事件列表中取出一个事件及其参数进行处理。处理结束后，根据协议的定义，设置下一事件或设置状态转换。

小结 本文以 WTLS 为基础探讨了无线安全方面的相关技术。利用对象技术和平台技术开发了 WTLS 的函数库。目前该平台已用于康佳 WAP 手机上，运行稳定可靠，有较好的性能价格比，打破了国外手机核心软件技术的垄断。

参 考 文 献

1 WAP Forum. Wireless Application Protocol, Public Key Infrastructure Definition. Apr. 2001

2 WAP Forum. Wireless Application Protocol , WAP-261-WTLS-20010406-a. Apr. 2001

3 Dierks T, et al. The TLS Protocol, Version 1.0. RFC 2246, Jan. 1999

4 Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd Ed. John Wiley&Sons, Inc, 1996

5 Institute of Electrical and Electronics Engineers. Standard Specification for Public Key Cryptography. IEEE P1363 working draft D13, March 2001

6 Tanebaum A S. Computer Networks 3rd Ed. NJ: Prentice Hall, Inc, 1996. 28～38

（上接第8页）

这样，基于统一的应用服务平台的公共支撑功能与服务来构建和实现各种应用系统，就能够有效避免重复建设和信息孤岛的形成，加强了数据共享，实现信息融合与共享，实现服务与应用、业务逻辑与流程的共享与互操作。在此基础上，将实现数据、信息、知识、服务、应用的价值链一体化，实现从信息生产到信息消费的信息流有序化，最终实现信息资源的动态管理、利用和优化配置。

数字城市的商业意义是整合各项资源，创建新型服务模式和市场模式，支持全球运筹管理，加强弹性调配各项产品及服务的能力。其社会意义是以信息流的优化促进社会资源优化配置、开发利用和增值，提升城市的综合竞争力。

结论与展望 数字城市的发展主线是：计算平台◇数据◇信息◇知识◇服务（应用），通过应用服务最终实现价值，其发展趋势是实现从数据、信息到知识的服务交换、共享和互操作。

数字城市应用服务平台是实现数据、信息和服务的交换、共享与互操作的支撑平台，是数字城市功能和作用的集中体现。建设数字城市，就是要创建一个智能服务平台，以通过信息流整合、有序化和优化其它资源流，从而形成城市信息服务市场空间和资源配置中心。因此，数字城市是社会资源的优化、整合、利用和增值的新型机制与模式，是政府（看得见的手）和市场（看不见的手）的虚拟延伸、连接与交汇。

本文针对数字北京的规划、设计和建设展开研究，所提出的框架模型和体系结构设计以及相关研究成果，已应用到数字北京示范工程的建设中，数字城市的关键技术研究和系统开发也正在深入展开。

参 考 文 献

1 Gore A. Digital Earth: Understanding Our Planet in the 21st Century[EB/OL], Given at the California Science Center, Los Angeles, California. http://www.digtial-earth.gov/speech.html, 1998

2 李琦，吴少岩. 数字地球——人类认识地球的第三次飞跃. [M]. 北京：北京大学出版社. 1999

3 承继成，李琦，易善桢. 国家空间信息基础设施与数字地球[M]. 北京：清华大学出版社. 1999. 173～185

4 王精业，王玉泉，等. 城市的可持续发展与数字城市研究[J]. 中国图像图形学报，1999，4(A 版)(4期增刊)：129～131

5 郝力. "数字城市"拉动城市产业信息化[J]. 中国图像图形学报，1999，4(A 版)(4期增刊)：137～139

6 http://www.digitalcity.com [EB/OL], 2001.7.

7 http://www.bristol.digitalcity.org [EB/OL], 2001.7.

8 http://www.virtuocity.com[EB/OL], 2001.7.

9 http://www.stedengids.net[EB/OL], 2001.7.

10 http://www.digitalcity.gr.jp[EB/OL], 2001.7.

11 董宝青，等. 数字北京工程总体框架及发展规划. 北京：北京市信息化工作办公室，2000年

12 http://e-speak.hp.com/product/overview.shtm [EB/OL], 2001.7

13 http://ip.opengis.org/mpp/[EB/OL], 2001.7

14 http://ip.opengis.org/ows/[EB/OL], 2001.7

15 http://www.openls.org/docs/4-OpenLS—Day—Architecture.ppt[EB/OL], 2001.8