基于WTLS的无线网关的实现

Realization of the Wireless Gateway Based on WTLS

代 坤 （中国科学院研究生院信息学院 100080）
鲁士文 （中国科学院计算技术研究所 100080）

摘 要：本文在阐述WAP、WAP网关基本概念和基本理论的基础上，引入了WTLS。从WTLS实现的角度，给出了WTLS应用系统的总体框架。提出了一个高效的基于WTLS的无线网关的实现方法。

关键词：WTLS WAP 网关

1 引言

20世纪90年代，通信领域出现了引人注目的两大增长——移动电话的迅猛发展和Internet接近爆炸式的普及。Internet与移动通信技术的融合，产生无线Internet应用。为了更适合于无线应用这一特殊领域，WAP（Wireless Application Protocol）技术产生了，它提供了一个业界技术规范，以便开发出用于各种无线通信网络的应用和业务。

无论是因特网还是无线网络，没有安全，就没有网络世界的繁荣。WAP中的安全层被称为无线传输层安全（Wirless Transport Layer Security，WTLS），被广泛应用于网上事务处理。WTLS为WAP提供了一个安全的传送服务接口，另外，WTLS还提供了一个管理安全连接的接口（包括建立和终止安全连接）。

2 WTLS在WAP网关中的实际应用

在WAP系统中，WAP网关与固定互联网中的服务器使用SSL进行通信，WAP网关和移动用户之间的安全通信使用WTLS协议。WAP网关提供了WTLS和SSL安全协议之间的转化桥梁，现有WTLS 1999-11-5版本主要来自于TLS1.0。

2.1 WTLS的构造

WTLS记录协议是一个四层分层协议，各协议共同实现了信息的安全传递。其中握手协议实现客户端与服务器的安全连接，协商安全参数，互相验证；报警协议用以实现互相通知出错信息；应用协议主要完成对数据的压缩、加解密以及向上层和下层传递信息；改变密码协议完成初始化安全参数。协议栈如图1所示：

2.2 WTLS安全的实现办法

2.2.1加密

WTLS的保密性依靠加密通信通道来实现，所使用的加密方法和计算共享密钥所需的值在握手时进行交换。当前常用的大批量加密算法有：RC5、DES、3DES和IDEA。

2.2.2密钥交换

WTLS的密钥交换机制提供了一种匿名交换密钥的方法。密钥交换算法可能是RSA、Diffie-Hellman或Elliptic Curve Diffie Hellman。

2.2.3鉴别

WTLS的身份鉴别依靠证书实现。在WTLS规范中，身份鉴别是可选的。

当前所支持的证书类型包括：X.509和WTLS证书。

2.2.4完整性

数据完整性通过使用消息鉴别编码(Message Authority Code, MAC)而得到保证，MAC算法同时也被认为是加密算法。WTLS支持通用的MAC算法，如SHA和MD5。

2.2.5安全状态

在安全协商后，会话通信双方将拥有同样的安全状态。当前状态通过安全参数产生，并持续更新。

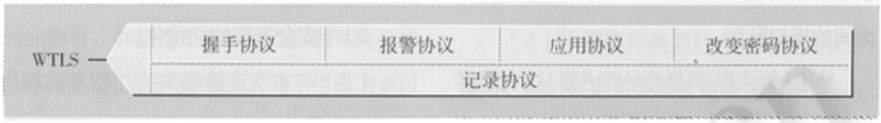

图1 WTLS的内部结构

3 基于WTLS的无线网关的实现

根据以上WAP和WTLS工作原理，我们建立了自己的无线安全网关。

3.1 系统接口

WTLS的技术实现是作为WAP网关实现中的一个重要组成，它不可避免地要与相邻层进行数据交换，在本文实现中，WTLS与相邻层所进行的数据交换均采用相同的消息结构，避免重复书写冗余代码，提高运行速度。

消息总是以消息长度作为第一个域，消息类型为第二个域。

在内存中，消息是以MSG结构来表现的，MSG结构中包含了一个变量（消息类型），一个独立的结构（分别代表每一类消息的结构）。

消息的名称和类型是在一个文件中声明

表1 安全连接中的安全参数列表

项目	描述
连接端	指出实体为客户端或服务器端
块加密算法	所使用的块加密算法
MAC 算法	用于保证消息的完整性校验的算法
压缩算法	在加密之前压缩数据的算法。
主密钥	一个20字节的密钥。
客户端随机数	由客户端提供的16字节的值
服务器端随机数	由服务器端提供的16字节的值
密钥刷新	连接状态的参数需要进行刷新的时间间隔（加秘密钥、MAC密钥以及初始化向量）
序列号模式	在安全连接中，用于产生序列号的方式。

的，以便修改及扩展。

3.1.1 WDP层数据接口

WTLS的下层为WDP（无线数据报协议）：WDP输入队列和WDP输出队列是它们之间的接口队列。

WDP输入队列是指WTLS要从WDP层接收输入的消息。所有提供给WTLS的消息均存储在WDP的输入队列中，每次WTLS从队列中读取一个消息。这些消息主要是客户端的请求（经过加密的）或握手信息。

WDP输出队列是指从内容服务器返回的内容经过WAP网关的应用层、会话层、事务层处理后，最后经WTLS对消息进行加密，将消息加入WDP输出队列（或者是WTLS将握手信息直接加入到WDP输出队列），等待WDP进行处理。

3.1.2 WTP层数据接口

WTLS的上层为WTP（无线事务协议）：WTP输入队列和WTP输出队列是它们之间的接口对列。

WTP输入队列是指WTLS要从WTP层接收输入消息，所有提供给WTLS的消息均存储在WTP的输入队列中，每次WTP从队列中读取一个消息。这些消息主要是内容服务器返回的内容经过WAP网关的应用层、会话层、事务层处理后送到WTLS中，等待WTLS的处理。

WTP输出队列是指经WTLS对消息（客户端的请求）进行解密后，将消息加入WTP输出队列，等待WTP进行处理。

3.2 系统设计及关键技术

安全层数据传输的一般过程为：

（1）安全连接的初始化。

（2）与本次连接相关的加密方式和压缩方式选择。

（3）通信双方的身份识别。

（4）本次安全连接传输密钥的确定。

（5）安全连接的建立。

（6）加密的数据传输。

（7）网络安全连接的关闭。

3.2.1握手协议

握手协议从密码学的角度实现了通信双方的密钥交换、身份鉴别、保密会话。在本文中，其安全性通过公开密钥的离散对数（Diffie—Hellman）得以实现。数据的加密则主要通过在密钥交换中生成的私有密钥，采用块加密的（CBC）模式利用对称算法（例如DES，RC5和IDEA等）实现。

本文所实现的WTLS的握手协议是在通信双方进行安全数据传输之前，确定本次安全连接的安全参数、数据加密密钥和算法。在通信方面，通过一次完整的握手在客户和服务器之间建立一个端对端的会话（Session）。一个会话可支持一个或多个并发的安全连接，会话参数可以被重新使用，从而减轻了网络负载。

事实上，握手协议的实现也是整个系统实现的要点所在。握手协议从最初的请求建立连接到最后的Finished消息的发送，其中包含了多种消息类型。而且在连接的建立过程中，不仅要求有安全连接的建立，更对握手过程完成的速度有更高的要求。

3.2.2密钥交换和生成

WTLS中的密钥交换算法可以根据客户和服务器双方的喜好在三类公开密钥算法中任意选择一种。在无公钥证书的情况下，由服务器端实时地生成随机公钥参数，利用握手的报文ServerKeyExchange传送给客户端。当客户端从ServerKeyExchange中获得服务器的公钥参数后，随机产生准密文pre masterkey（20bytes），用服务器的公钥进行保护，发送回服务器，服务器用相应的私钥获得客户端的准密文。

在客户和服务器端均生成了一致的准密文后，各自在本地根据其一次握手中达成的参数选择，生成数据加密的私有密钥。

密钥根据准密文、主密文、客户端随机数、服务器端随机数、报文序列号在握手的过程中动态生成。并遵循下列公式：

master_secret = PRF(pre_master_secret, "master secret",
ClientHello.random +erverHello.random) [0...19];

key_block = PRF(SecurityParameter.master_secret,
expansion_label, seq_num +
SecurityParameter.server_random +
SecurityParameter.client_random);

其中

PRF(secret, lable, seed) = P_hash(secret, label + seed);

P_hash(secret, seed) = HMAC_hash(secret, A(1) + seed) +
HMAC_hash(secret, A(2) + seed) +
HMAC_hash(secret, A(3) + seed) + ...

这里“+”表示连接。

A(0) = seed

A(i) = HMAC_hash(secret, A[i-1])

3.2.3公开密钥算法

利用DiffieHellman算法作为密钥加密是基于对离散问题的困难性。DH密钥交换协议如下所述：

（1）服务器选择一随机大数x，将P，g，gx mod P（P，g为两个大质数）发送给客户。

（2）客户也选择一随机数y，将gy mod P发送给服务器。

（3）两边各自用相应的私钥取得准密文pre masterkey = gxy mod n。

密钥交换安全的核心在于参数（P，g）生成，安全指数的生成是保证加密安全的关键。在实现中，我们采用预定义的Diffie-Hellman参数，P的长度为756位，g的长度为768位。

3.3 WTLS的总体实现结构

3.3.1系统环境

操作系统的选择是影响网关运行效率的关键因素之一。Linux支持多线程的操作，而且其安全性显著地高于WindowsNT等其他网络操作系统。

软件的安全性分析：

（1）解密算法在一个linux过程中实现，同时保证明文绝不在辅存中出现。算法就速度进行了优化，保证明文在内存中存在的时间非常短，当信息一旦传送到相邻层，明文立即从内存中清除。

（2）只有linux的根用户能够看到解密的信息。

（3）即使拥有根密码和有效linux工具的辅助，因为明文在内存中存留时间极短，对明文进行窃取也是非常难以实现的。

系统的实验环境采用WinWAP公司的模拟器作为客户端，服务器端采用通用的PC机。

3.3.2系统结构

对于WAP网关，同时访问网关的客户端可能会有多个。系统结构实现的总体目标是对于不同客户端的访问以最高的效率进行数据处理，并保证其安全正确性。

系统设计的难点在于如何将不同客户端的请求有机地组织起来。

这里，决定采用状态机队列的形式，先到先服务，使得系统的整体结构更加清晰。

WTLS需要与WTP及WDP层进行协议分组的交互。当WTLS与上层WTP通信时，采用端口号为9203的UDP Socket进行；有分组到达时，如果是来自上层WTP的数据报，则寻找或产生一个新的WTLS状态机，并把它加入状态机队列。对于状态队列中的状态采用宏调用的形式实现相应的动作，例如ROW(当前状态，条件，动作，下一状态)，并向下一状态转换，以减少函数的调用次数，从而增加程序的运行效率。。若有下层WDP的数据报到达，则产生一个新的WTLSEvent_SEC_UnitdataReq事件，并把这个事件加入到事件队列中去等待处理。队列机制的采用，使得消息以明文的形式仅能够存在于内存中，从而可以防止消息的泄漏，增加数据的安全性。

3.3.3编程语言选择

在我们的实现中选择GNU C编程环境。GNU C定义了由ANSI C所定义的所有库函数，并且附加了一些适用于Unix、Linux操作系统的其他的特性，如进程通信、信号处理等，特别适合于网络编程。

3.3.4主要数据结构和处理机制

WTLSMachine 和 WAPEvent是两个主要的数据结构，WTLS处理机包含对每一个请求的唯一标识，实现唯一索引。同时处理机中，将对于该请求进行处理的信息全部包括进来，减少了不必要的搜索，增加了运行速度。宏定义的采用，减少了不必要的函数调用，进一步提高了程序运行的效率。

3.3.5 WTLS事件类型

T_Unitdata:同传输层交换用户数据。

SEC_Terminate:用于终止连接，并标识告警描述及告警级别。

SEC_Exception:通知另一方警告的级别。

SEC_Creat:发起一个安全连接的建立过程。

SEC_Exchange:服务器希望与客户端惊醒公开密钥授权或密钥交换时。

SEC_Commit:握手结束，对等端任一方要求切换到协商好的连接状态时。

SEC_Unitdata:用于在同层体间交换用户数据。

SEC_Creat_Request:用于服务器要求客户端初始化一个新的握手过程。

3.4 WTLS的实现流程

3.4.1 WTLS向上传递请求

（1）WTLS从WDP的消息队列中取出一消息；

（2）对消息进行解包成WTLS记录；

（3）根据记录产生事件，并对产生的事件进行处理；

（4）根据事件类型对WTLS状态机进行读写，同时根据需要更新待决状态；

（5）对消息解密；

（6）将解密的消息加入WTP输出队列。

3.4.2 WTLS向下发送内容

（1）WTLS从WTP的消息队列中取出一消息；

（2）产生事件，并对产生的事件进行处理；

（3）根据事件类型对WTLS状态机进行读写；

（4）对消息加密，打包成WTLS记录；

（5）打包成消息结构，加入WDP输出队列。

3.4.3 WTLS事件产生及处理流程

（1）对WTLS记录或WTP的协议数据单元（udp）解包；

（2）根据包的内容产生事件；

（3）将事件加入事件队列；

（4）寻找或者创建状态机；

（5）WTLS根据状态集合事件类型，对事件进行处理；

（6）进行解密或加密后，传给相邻层。

3.5 实验数据分析

试验环境：在局域网内进行测试，以WinWAP 3.0作为模拟客户端，运行环境为PⅡ266的PC机、10M网卡；WAP网关运行环境为PⅢ的PC机、100M网卡。

实验所得数据：一个完全握手过程的完成时间为500ms—1000ms；一次简单握手过程的完成时间为50ms—100ms；WTLS从WDP接到一个数据包到将数据解密后传递到上一层，时间为50—100ms（不包含握手过程）。WTLS从WTP接到一个数据包到将数据加密后传递到下一层，时间为50—100ms（不包含握手过程）。

实验分析：根据以上实验数据和试验背景数据，在CDMA投入运行后，WAP手机从拨号完毕到接入互联网的整个过程在2秒内即可完成（网络通畅的情况下）。此接入速度以及几十K的网络传输速度，是手机用户绝对可以接受的，从而给WAP手机以及无线电子商务应用提供了一个更加广阔的市场。

4 总结

本文提出了一个高效的实现WTLS的方案。目前有关无线安全的WAP网关仍然是国际上网络研究领域的一个热点，相信随着研究的深入，会有更加优秀的算法和模型出现并得到比较普遍的应用。

参考文献

1 £¤^ £¤WAP FORUM，WAP-无线应用协议，机械工业出版社，2000年9月。

2（美）Bruce Schneier著，吴世忠等译，应用密码学，机械工业出版社，2000年。

3 Sami Jormalainen, Jouni Laine. Security in the WTLS. Computer Science and Engineering Helsinki University of Technology，1999.11。

4 Wireless Application Protocol Architecture Specification, Version 30-Apr-1998. WAP Forum。

5 § § ´ ±ß§L/TLS/WTLS原理，绿盟周刊，1999年。

6 Understanding Security on the Wireless Internet. PHONE.COM。

7 Wireless Application Protocol Service Indication, Version 08-Nov-1999. WAP Forum。