基于Kerberos协议的SyncML安全性改进

陈启安 陈永建
(厦门大学信息科学与技术学院 福建厦门 361005)

摘 要:本文分析SSL协议中握手协议的不安全性,在此基础上分析了SyncML同步传输过程中存在的安全风险。在对SyncML系统的安全风险分析的基础上,提出用Kerberos协议对SyncML数据同步进行身份认证,从而有效提高了系统的安全性。
关键词:SSL SyncML 认证服务器 TGS 密钥
中图分类号:G254 文献标识码:A 文章编号:1674-098X(2008)01(a)-0010-01

当代社会数据同步这个概念也被越来越多的人所认识。最典型就是PIM同步,设备管理信息同步以及push email的应用。许多著名的公司都加入到该领域的研究中。著名的移动开源软件公司Funambol就是典型的代表。该公司开发的同名产品funambol是一个移动设备软件的开发平台,它提供了用户端和服务器端的Java和C++的API。

1 SSL协议

1.1 协议简介

SSL是一种在客户端和服务器端之间建立安全通道的协议。SSL一经提出,就在Internet上得到广泛的应用。SSL常用来保护Web的安全,保护存有敏感信息Web的服务器的安全。

协议位于TCP层协议与应用层协议之间的一个可选层,任何在TCP/IP层以上的网络协议层SSL都可以支持,因此HTTP及SyncML等都在SSL的保护范围。协议在应用层通信之前就已经完成加密算法、密钥协商及服务器认证工作。此后,所有传送的数据都被加密。

1.2 SSL握手协议

SSL握手协议是在SSL应用程序数据传输前进行的。SSL握手过程流程如下:

(1)客户端发送Client_hello给服务器,并等待应答包Sever_hello。

(2)服务器发送数字证书,并确定加密算法。

(3)客户端检查服务器的数字证书正确性后,生成利用服务器的公钥加密的本次对话密钥发送给服务器。

(4)服务器用自己的私钥解密获取本次对话密钥。

(5)握手完成,开始进行数据传输。

1.3 SSL握手协议的密钥交换方式及存在的漏洞

SSL握手协议主要负责客户机和服务器之间的身份认证和协商会话的加密参数。Client_hello消息和Sever_hello消息中的密码组参数的第一个元素是密钥交换方法。SSL协议支持5种密钥交换方法:RSA;

匿名Diffie-Hellman;临时Diffie-Hellman;固定Diffie-Hellman;Fortezza。

2 SyncML协议

2.1 SyncML简介

SyncML是一种可扩展标记语言(XML)协议,它用于设备之间数据同步的开放标准,是开发第三代无线通信系统的最重要模块。协议通过定义并允许交换数据,以及确定如何解释这些数据,从而提供了客户端与服务器之间相互同步数据的结构。

2.2 SyncML同步过程中存在的安全隐患

为增强实用性,使SSL协议能够应用在通信双方都没有证书的情况下,SSL协议提供了匿名密钥交换方式,但这种方式却容易受到黑客攻击。黑客修改或转发数据。下面例子就说明这个问题。黑客(H)与在服务器(S)和客户端(C)中间,虽然H不能发现S与C已经交换的密码,但是他能够干扰他们的交谈。在同步开始前,H对握手数据并不进行修改,只是单纯转发握手数据。当S与C开始进行数据同步时,H在同步的数据上添加干扰消息,此时S与C并不知道他们接收到的消息被修改过。所以他们经过解密后的数据并不是对方发送过来的原始数据。H成功干扰了同步通信。

3 Kerberos认证方法

3.1 Kerberos简介

Kerberos协议主要用于计算机网络的身份认证。Kerberos服务器起可信仲裁者的作用,它可提供安全网络认证,允许客户端访问网络中不同的机器。协议基于对称密码技术。网络上每两个实体分别共享一个不同的密钥。其设计目标就是通过密钥系统为整个系统提供强大的认证服务。

客户端访问服务器需要进行六次通讯,即:

(1)客户端请求认证服务器(AS)发给接入TGS的票据。

(2)AS在数据库中查找用户实体,并产生一个会话密钥,并用用户秘密密钥对会话密钥加密。接着,AS把实体名、地址、TGS名、时间戳、时限及会话密钥打包成TGT(票据分配许可证),并用TGS的秘密密钥进行加密。然后将会话密钥和TGT发给客户端。

(3)客户端将第一个报文解密得到会话密钥,并生成一个认证单。然后向TGS申请接入目标服务器的票据。

(4)TGS用其秘密密钥对TGT进行解密,使用TGT的会话密钥对认证单进行解密,然后将认证单的信息与TGT的信息进行比较。此时,TGS产生新的会话密钥供双方使用,利用用户实体与TGS的会话密钥对新的会话密钥加密,并将新的会话密钥加入客户端提交给服务器的有效票据中,并用目标服务器的秘密密钥对此票据加密,最后将这两个报文提交给客户。

(5)客户端将收到的报文解密后,获得与目标服务器共同的会话密钥。然后客户端生成一个新的认证单,并用新会话密钥对其进行加密。最后将此认证单与从TGS收到的票据一并发给目标服务器。

(6)目标服务器对票据和认证单进行解密,并检查其地址、时间戳、时限等信息。如果一切都正确,服务器则知道用户实体的身份。此后的通信,客户端可以与目标服务器共享一个秘密密钥进行安全通信。

3.2 用Kerberos认证协议对SyncML服务器安全性的改进

SyncML服务器使用SSL协议对数据进行加密。但因为SSL的密钥交换方式支持匿名方式,所以如果客户端及服务器均无法提供身份认证,就容易导致同步数据受到黑客的转发和修改。

针对SSL协议的漏洞,我们用Kerberos协议来提高SyncML服务器的安全性。为了提供每个域中客户和服务器进行注册,每个域中都必须设一个Kerberos服务器。并当存在多个域时,Kerberos提供了一种支持域间认证的机制,每个相互操作的域的Kerberos服务器都应该共享一个密钥,双方服务器应该都能相互注册。

客户端为了发起请求必须先向本地Kerberos服务器的AS申请本地票据授权票据,然后向本地TGS申请远程TGS的票据授权票据,最后向远程TGS申请SyncML服务器的服务授权票据。取得服务授权票据后,客户端将自己的用户表示和服务授权票据发给SyncML服务器。服务器对票据解密后获得与用户共享的会话密钥,并认证了用户的合法性。同时,服务器发给客户端一个加密过的应答,客户端解密后可以确定服务器的身份。双方认证了对方身份并共享一个密钥后,使用这个密钥加密他们之间传输的消息,从而保证通讯的安全性。

接着客户端开始对SyncML服务器发出数据同步请求,并建立一个SSL会话。至此,我们用Kerberos协议解决了SSL协议握手过程中存在的身份认证漏洞的问题。系统在Kerberos协议身份认证结束后仍然用SSL协议加密数据同步。Kerberos协议的加入大大加强了同步协议的安全系数,从而保证了用户敏感数据不被外人所窃取。

4 结语

系统利用Kerberos协议加强了SyncML同步系统的安全性。假设Kerberos协议设计充分,则认证服务的安全性取决于Kerberos服务器的安全性。另外,还可以通过加强SSL协议的修订,增加身份的识别系统,加强身份认证的可信度,防止非法访问者进入。

参考文献

[1] SyncML Reference Toolkit [DB/OL]. http://sourceforge.net/projects/syncml-ctoolkit.
[2] 魏达,刘衍珩,李晓东. 基于Diffie-Hellman密钥交换的Web安全传输[J]. 吉林大学学报,2005.
[3] 陈云,彭春山,邓亚平. Kerberos认证协议的研究和改进[J].计算机技术,2006.
[4] 欧阳星明,舒之兵.对SSL握手协议密钥交换方式的改进与应用[J].计算机工程与科学,2006.