基于PKI体系的跨域密钥协商协议

魏振宇[1] 芦 翔[2] 史庭俊[1]
(扬州大学信息工程学院 扬州 225009)[1] (中国科学院信息工程研究所 北京 100000)[2]

摘 要 基于口令的跨域密钥协商协议和Kerberos协议无法抵抗口令猜测攻击,在金融、航天等通信安全需求高的场所,需要一种更有效的协议来保证通信安全。给出一种新的基于PKI体系的跨域密钥协商协议,采用公钥算法保证数据传输的安全,结合使用Diffie-Hellman协议生成会话密钥。协议有效地解决了利用预置共享密钥参与加/解密实施中间人攻击,以及Kerberos弱口令导致的攻击者可以实施口令猜测攻击的问题。跨域通信的公钥信息仅存储在各自域认证服务器,域内用户不需要配置跨域服务器的公钥信息,降低了配置复杂度、域内用户和域认证服务器之间密钥管理的复杂性,同时提高了域服务器鉴别身份的能力和信息机密性,使其免疫多种攻击,具有良好的前向安全性和扩展性。

关键词 密钥协商,共享密钥,Diffie-Hellman协议,机密性
中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2017.01.030

Cross-domain PKI-based Key Agreement Protocol

WEI Zhen-yu[1] LU Xiang[2] SHI Ting-jun[1]
(College of Information Engineering, Yangzhou University, Yangzhou 225009, China)[1]
(Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100000, China)[2]

Abstract It has been proven that security risks exist in most of the password-based cross-domain authentication and key agreement protocols or Kerberos protocol. It is necessary to propose a more effective protocol to ensure the communicating security in the area of finance and aerospace, which require high level communicating security. This paper proposed a cross-domain PKI-based key agreement protocol. This protocol can efficiently solve the key exposure problem in which the password guessing and man-in-the-middle attack is enabled. This problem is resulted from using share-key encryption and decryption to assure the security of data transmission or Kerberos weak passwords. To solve this problem, this protocol adopts the public key algorithm and uses the Diffie-Hellman protocol to create the session key. Meanwhile, this protocol makes users get rid of repetitive configuration of the cross-domain server public key information, which reduces the complexity of the configuration and the key management between users and servers. Besides, this protocol improves the ability to identify authenticity and the information confidentiality, and is immune to multiple attacking ways. This protocol also has forward security and good expansibility.

Keywords Key agreement, Share key, Diffie-Hellman protocol, Confidentiality

1 引言

随着互联网、移动互联网的快速发展,网络已经成为人们获取信息的主要方式,其中金融、传媒、教育等资源通过网络共享,使得人们可以直接通过网络获取需要的资源。但单一的运行模式使得各行各业之间信息交互性差、实时性低、重复性高,信息资源得不到有效利用,满足不了人们对行业之间的信息进行实时了解的需求。而行业之间进行的信息交互形成了一种以行业为个体的域间通信方式。同样,实时通信服务随着网络的普及得到了广泛的使用,信息交互和好友在线实时显示功能在实时通信服务中已经变得越来越流行。目前有许多免费的实时通信服务工具,如MSN Message, ICQ和YIM(Yahoo! Instant Message)等。然而不断出现的网络安全问题引发了人们对信息安全的关注,实时通信服务增强了加密功能来保障通信安全。Mannan和Van Oorschot[1]提出使用基于口令的三方认证和密钥交互协议,保证使用相同实时通信服务工具的通信双方在网络中进行信息传输时的安全。然而不是所有的用户都使用相同的实时通信服务工具,使用不用实时通信工具的用户之间进行信息交互,例如用户使用ICQ和YIM的人群,如何保证跨越不同实时通信服务之间的信息安全,目前没有有效地解决方式。相同通信实体之间信息交互为域内交互,基于口令的密钥协商协议可以有

到稿日期:2015-11-09 返修日期:2016-02-28 本文受国家高技术研究发展计划(2013AA011102),中国科学院战略性先导科技专项课题(Y2W0031102)资助。

魏振宇(1990—),男,硕士生,主要研究方向为信息安全,E-mail:weizhenyu@ciotc.org;芦 翔(1982—),男,博士,助理研究员,主要研究方向为智能电网、网络安全协议分析及性能评估、无线网络安全,E-mail:luxiang@iie.ac.cn;史庭俊(1963—),男,博士,副教授,主要研究方向为无线传感器、信息安全,E-mail:tjshi@yzu.edu.cn。

效地保障域内用户信息安全，而对于不同实时通信服务用户之间的交流，由于各自域的验证和密钥生成方式存在差异，因此无法使用各自域的密钥协议协商得到域间的共享会话密钥，域间信息交互若得不到密钥的保护，就会面临数据窃取、监听等各种威胁，造成企业机密和个人隐私信息的泄露，对企业经济和个人生活带来了影响。如何保证跨域用户信息交互安全成为研究者关注的重点，包括网格环境下基于身份的跨域认证[2]、基于 PKI 或 Kerberos 的跨域认证[3]、移动 IP 网络跨域认证[4]等。

2 相关工作

基于口令的跨域密钥交互（C2C-PAKE）协议首先由 Byun 等人[5]提出，其协议利用域内用户与域服务器之间预置的共享密钥，使得不同域之间依赖其预置的共享密钥协商得到跨域会话密钥，但其协议被证实无法抵抗字典攻击；Kim 等人[6]指出 Byun 协议存在内部攻击安全隐患，无法免疫字典攻击，并给出了改进后的协议；Yoon 和 Yoo[7]发现 Kim 给出的改进协议存在中间人攻击隐患，在 Kim 协议的基础上给出改进后的 C2C-PAKE 协议；然而 Liu[8]指出 Yoon 和 Yoo 的协议无法免疫服务器妥协和密钥妥协攻击，也给出改进协议，后来学者又提出了多种基于口令的 C2C-PAKE 协议[9-12]。基于口令的密钥交换协议被证明存在安全隐患[5-8]，新的协议在原协议的基础上进行修改，解决发现的问题，修改后的协议由于引入了新的方式进行鉴别或加解密等操作，在某些方面考虑得不完全而引入了新的安全隐患。文献[13]给出了一种基于现有安全的 PAKE（Password-based Authenticated Key Exchange）和 AAKE（Asymmetric-key Authenticated Key Exchange）协议作为黑盒的跨域密钥协商协议，通过使用现有的安全的 PAKE 协议，域服务器验证域内用户身份的合法性，随后合法的域间用户使用 AAKE 协议进行跨域用户之间的密钥协商。但是协议中 PAKE 或 AAKE 协议被证实存在安全隐患后，使用其它现有安全的 PAKE 或 AAKE 协议重新部署不仅增加了工作量，而且在协议使用安全的 AAKE 协议和 PAKE 协议的替换过程中，协议的流程可能存在差异，由此带来了额外的人力开销和资源浪费。在文献[10,14]中，域之间通过域服务器交互实现会话密钥协商，其协议在域数量较少的环境中便于部署。随着域数量的增加，考虑所有的域服务器之间的通信情形，域服务器之间需要构成一张全连通图，在最坏的情形下保证各域之间的连通性。随着域数量增加，协议配置和维护就变得更加复杂，在大规模部署中，域的离开和加入等操作会导致域间信息修改非常大，协议的扩展性差，无法满足我们对域的频繁加入和离开的需求。基于口令的跨域密钥交换协议中，大多数用户设置的口令便于记忆，容易遭受字典攻击，对于安全性需求较高的场所，如银行、公安、机场等，基于口令的跨域密钥协商协议很难保证传输信息的安全。目前在各个平台广泛使用的 Kerberos 协议实现了跨域密钥协商，域间用户需要进行多次跨域连接，开销较大，所依赖的时间戳实现时间同步也比较困难。而且 Kerberos 无法免疫口令猜测攻击，要求用户使用强口令提高协议安全，而且通信过程中的会话密钥由 Kerberos 产生，导致 Kerberos 可以窃听会话而不被举证。

本文提出了一种新的基于 PKI 体系的跨域密钥协商协议，协议使用公钥算法和 Diffie-Hellman 协议相结合来生成安全会话密钥，利用数字签名保证信息的完整性。协议解决了 Kerberos 跨域协议和基于口令的跨域密钥协议用户使用弱密钥导致密码猜测攻击和中间人攻击引起密钥泄露的问题，域服务器不需要维护域内用户和服务器之间共享密钥的安全，减少了服务器对预置共享密钥的安全性管理。使用 Diffie-Hellman 协议协商得到的安全会话密钥提升了系统对抗（包括字典攻击、重放攻击、中间人攻击等）多种攻击方式的能力，解决了 Kerberos 产生密钥导致窃听会话而不被举证的问题，并且它具有前向安全性和良好的扩展性。

3 协议模型

基于 PKI 体系的跨域密钥协商协议采用公钥算法和 Diffie-Hellman 协议实现域内用户身份鉴别和域间用户会话密钥协商的功能。域服务器首先对域内用户身份进行验证，用户和服务器之间的共享密钥作为服务器鉴别用户身份的一种方式，而且共享密钥不参与域内用户和服务器交互信息的加解密操作，有效地解决了口令猜测攻击带来的威胁，数字签名保证了传输信息的完整性。域间通信信息使用公钥算法进行加密，保证了域内信息交互的机密性。会话密钥使用 Diffie-Hellman 协议协商得到，保障了域间用户信息交互的安全性。每个域服务器拥有其它域服务器的有效公钥，该公钥用于加密域间用户在密钥协商阶段的通信信息，仅仅拥有公私钥对的域服务器才可以解密出跨域用户发送的密钥因子，实现域间会话密钥协商。下文描述文中出现的符号并介绍本协议流程。

3.1 符号

表 1 列出了相关符号的具体含义。

表 1 文中符号含义

符合	文中表达的含义
A,B	表示协议中不同域内的实体
A→B:M	A 发送消息 M 至 B
x,y	随机数
g	生成元
ID	用户身份标志
S_A,S_B	域认证服务器 A 和 B
h()	单向函数
PW_i	用户 i 与域服务器之间的共享密钥
sk	会话密钥 $sk=g^{xy}$
$\{\}Pub_i$	使用 i 的公钥加密数据
$\{\}Pri_i$	使用 i 的私钥对数据进行签名

3.2 协议描述

假设域服务器 S_i 和域内用户 i 通过安全信道预置口令 PW_i，服务器 S_i 通过安全信道得到其它域服务器的有效公钥，本文协议的流程如图 1 所示。

(1) $A \rightarrow S_A:\{ID_A,ID_B,u,M_1\}Pri_A$

客户端 A 选取一个随机数 r_a，使用单向函数计算得到 u，用于服务器验证客户端的合法性，选择需要进行跨域通信的客户端 ID，使用客户端口令加密随机数 r_a 得到 M_1，同时使用私钥对发送的信息签名，发送信息至域服务器。

(2) $S_A \rightarrow A:ID_A,ID_B,u',M_2,M_3,Ticket$

域服务器 S_A 接收到客户端发送的信息后，得到客户端的 ID 信息，获取该 ID 客户端的公钥并对发送的信息验证签名，查看数据是否被篡改。在验证 u 是否相同前需要使用口令解密得到用户生成随机数 r_a。验证完成后，服务器选取一

个随机数 r_a'，通过发送的信息得到需要通信的域服务器公钥信息，利用跨域服务器公钥对数据加密并利用自身私钥对数据签名得到 M_2，同时计算得到 *Ticket* 信息，其中 L 为 *Ticket* 信息的有效期。计算得到 u'，并使用口令加密服务器生成的随机数和跨域服务器公钥信息得到 M_3。

(3)$A \rightarrow B$: $ID_A, M_2, M_4, Ticket$

客户端 A 得到域服务器发送的信息，使用预置口令解密得到随机数 r_a'，验证 u' 是否一致。随后选择一个随机数 x 并计算得到 g^x。使用域服务器发送的公钥信息加密 g^x 得到 M_4。将得到的 M_2 和 *Ticket* 一并发送至客户端 B，进行跨域密钥协商。

(4)$B \rightarrow S_B$: $\{ID_A, ID_B, v, M_5\}Pri_B, M_2, M_4, Ticket$

客户端 B 接收 A 发送的信息后，选取一个随机数 r_b 并计算得到 v，使用客户端与域服务器的共享口令加密随机数 r_b 得到 M_5，随后使用客户端私钥签名发送的信息，并与接收 A 的信息一起发送至域服务器。

(5)$S_B \rightarrow B$: ID_A, ID_B, M_6

域服务器 S_B 接收客户端 B 发送的信息后，使用公钥验证签名。服务器通过 ID 得到跨域服务器的公钥，验证 M_2 信息的合法性，使用自身私钥解密得到随机数 r_a, r_a' 与 *Ticket* 的有效期为 L，验证当前时间是否合法，随后验证 *Ticket* 是否一致。最后通过私钥解密得到 A 的密钥因子 g^x，使用 B 的公钥加密 A 的密钥因子与随机数 r_a 和 r_a'，随后使用私钥对加密后的信息签名得到 M_6。

(6)$B \rightarrow A$: $\{r_a+1\}_{SK}, g^y$

客户端 B 得到域服务器发送的信息，使用公钥验证签名，验证完成后利用私钥解密得到 A 发送的密钥因子，选取随机数 y 并计算得到会话密钥 sk，发送信息至客户端 A。

至此，不同域之间实体 A 和 B 的密钥协商完成，双方使用协商后的会话密钥通信。

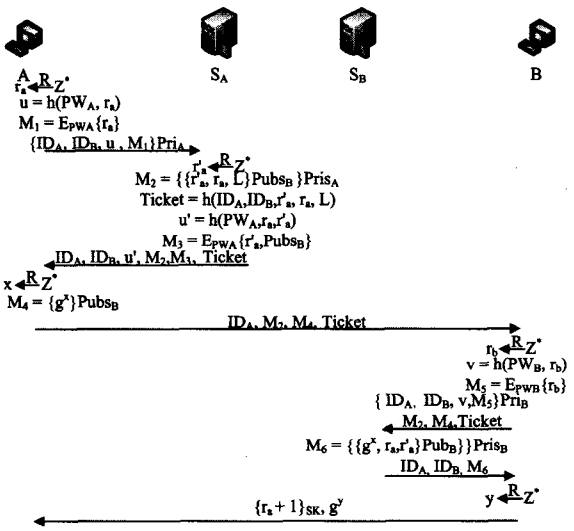

图 1　跨域密钥协商

图 2 给出了多个域之间通信的方式，其中虚线内表示一个域，包括域服务器与域内用户。其中给出 3 个域 A、B 和 C，当 C 域离开时，需要销毁现有域内 C 域服务器的有效公钥信息，同时也销毁 C 服务器中保存的其它现有域的有效公钥信息。当加入新域时，仅仅需要将新域服务器的有效公钥分发到现有域服务器即可完成配置。

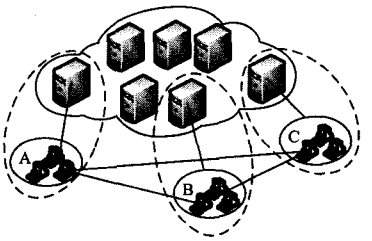

图 2　域间通信

4　安全性分析

(1)前向安全：攻击者不可以利用泄露的密钥信息计算得到过去或将来的会话密钥信息。

假设攻击者已经获取到用户和域服务器之间预置的共享密钥和泄露的会话密钥，攻击者通过分析历史截获的数据，尝试利用该共享密钥解密出原始数据。在本协议中，域服务器和用户之间预置的共享密钥并没有参与加解密操作，只是在消息 1 和消息 4 中作为用于服务器验证用户身份的一种辅助信息。如果攻击者使用离线密码猜测解密消息 1 和消息 4 中的数据，u 与 v 使用单向函数计算得到，攻击者无法逆向推导出口令信息。而消息 1 在流程 $\{ID_A, ID_B, u, M_1\}Pri_A$ 中使用客户端的私钥对信息签名，在未得到客户端私钥时，攻击者无法对消息 1 的数据内容进行篡改。消息 2 中的信息 M_2 使用域服务器私钥签名，攻击者即使重放消息 1 的信息，由于 r_a' 随机选取，每次的签名值也不同，攻击者无法得到有用的信息，时间戳 L 可以检测当前信息是否合法以有效预防重放攻击。虽然攻击者可以使用泄露的会话密钥解密出本次会话的信息，但是协议每次会话密钥 $sk=g^{xy}$，系数 x 和 y 每次都随机得到，攻击者即使得到当前会话密钥也不能解密出历史数据以及重构后的会话数据。因此本协议具有前向安全性。

(2)密码猜测攻击包括离线密码攻击和在线密码攻击两种方式。

离线密码猜测攻击：本文协议能安全免疫离线密码猜测攻击。攻击者在已知口令 PW 的情况下，通过离线密码猜测解密消息 1 的信息：

$A \rightarrow S_A$: $\{ID_A, ID_B, u, M_1\}Pri_A$

通过消息 1 的信息可以发现，攻击者在得到口令 PW 后，可以解密得到 r_a 随机数，但消息 1 使用 A 的私钥签名，攻击者无法得到私钥从而不能篡改和伪造消息 1。攻击者在未得到对应的私钥时也不能重构伪造的消息 1 的内容，尝试解密不会得到有效私钥 Pri_A，例如使用 RSA 加解密数据时，基于现有的计算资源，2048 位需要数十年才可以被破解。而且口令 PW 仅仅作为验证用户 A 身份的一种标识，并没有参与加解密操作，如果尝试使用 PW 解密数据，攻击者将得不到任何有用的信息。因此，攻击者即使得到预置口令 PW 也无法得到任何有用的信息以推导出会话密钥，因此本协议免疫离线密码猜测攻击。

在线密码猜测攻击：用户与域服务器预置口令 PW 用于验证用户身份的一种方式，并没有参与加解密操作，而且该类攻击方式容易通过监测客户端发送的连续错误请求检测出来，如果检测到一个用户连续的错误请求信息，将通知用户受到攻击威胁，通过提醒用户更改密码或者在超出有效的请求次数后关闭用户请求等方式免疫该类攻击。

(3)重放攻击:在本文协议流程中,攻击者可以重放消息1的信息:

$A \rightarrow S_A:\{ID_A, ID_B, u, M_1\}Pri_A$

由于域服务器在接收到消息1的信息后无法判断消息1的新鲜性,因此该重放数据是有效的。域服务器收到消息1并验证消息1的信息是否被篡改。域服务器发送消息2至攻击者:

$S_A \rightarrow A: ID_A, ID_B, u', M_2, M_3, Ticket$

服务器选取随机数 r_a' 计算得到 $Ticket = h(ID_A, ID_B, r_a', r_a, L)$,并使用跨域服务器公钥加密 $Ticket$ 生成所需的敏感信息,同时使用域服务器私钥签名加密信息。由于 r_a' 的选取具有随机性,因此每次生成的签名值也不相同,用户每次重放得到的消息2的内容也各不相同。攻击者重放的消息1的信息无法帮助其得到任何有用信息,而且在未知用户私钥时无法伪造任何信息,时间戳 L 可以有效地预防历史信息的重放。攻击者在有效时间内重放消息3的内容,可以完成与客户端 B 的密钥协商过程。由于重放的数据是合法时间内的有效密钥协商信息,因此客户端 B 将与攻击者协商得到 sk 会话密钥。sk 的协商过程中,B 的随机数 y 通过随机获取,即使每次重放成功,得到的会话密钥 sk 也各不相同,而且会话密钥由 Diffie-Hellman 计算得到,每次都由客户端 A 与 B 协商生成,攻击者在无法解决离散对数难题的情况下无法计算得到会话密钥 sk。因此攻击者得不到解密会话密钥的任何有用信息,故本协议免疫重放攻击。

(4)已知密钥攻击:本协议能安全对抗已知密钥攻击,攻击者得到会话密钥 sk 后想利用已知会话密钥推导未知密钥。从协议交互流程可以得到,会话密钥重构需要得到随机数 x 和 y,且随机数之间相互没有依赖关系。随机数 x 和 y 分别由各自的用户在用户 A 发送至用户 B 的消息3中以及用户 B 发送至用户 A 的消息6内随机选取。攻击者需要得到 S_B 域服务器私钥才可以获取到 g^r 的值攻击者需要得到 $sk = g^{ry}$,即使得到 g^y 的值,攻击者也需要进一步计算出 x 或 y 的值才可以进一步推算出 sk,由于 Diffie-Hellman 协议依赖于离散对数难题,攻击者需要解决离散对数问题才可以得到需要的密钥有效信息,但是使用现有的计算资源无法解决离散对数问题。攻击者重放的信息不能帮助推导出任何关于密钥计算的信息,也无法实现后续通信流程,从而无法完成密钥协商整个流程。

(5)中间人攻击:如果攻击者伪装为 $A(B)$,使用域服务器的公钥加密发送消息1:

$A \rightarrow S_A:\{ID_A, ID_B, u, M_1\}Pri_A$

对于服务器 S_A,服务器验证消息1的完整性后,根据用户的 ID,选取需要跨域通信的域服务器公钥发送至攻击者。由于信息传输过程使用各自用户或域服务器的私钥签名,保证了数据的完整性,因此攻击者在未知用户私钥时无法对数据内容进行篡改,单一的重放功能无法计算协商得到有效会话密钥 sk,基于时间戳的签名信息可以有效地预防利用历史信息重构会话,而且会话密钥 sk 由 Diffie-Hellman 协议计算得到,攻击者使用现有计算资源无法计算出 Diffie-Hellman 系数,因此协议免疫中间人攻击。

攻击者伪装为域服务器 $S_A'(S_B')$,用户使用私钥签名消息1的内容发送至 S_A',由于公钥信息是对外公开可获取的,攻击者可以验证消息1的内容。响应消息2的内容需要使用域服务器的有效私钥对消息2中的 M_2 进行签名,攻击者在未得到域服务器私钥时无法伪造出合法的签名值,因此无法做出合法的消息2响应,就不能继续实现后期的信息交互,进而用户和域服务器之间无法完成双方认证,攻击者得不到后期密钥交互信息,更无法得到会话密钥。因此本协议免疫中间人攻击。

5 性能分析

信息交互数量如表2所列。

表2 信息交互数量

Protocol	C↔S	C↔C	S↔S	Total
Byun-Lee-Lim[15]	6	2	0	8
Yin-Bao[14]	4	0	2	6
Feng-Xu[9]	5	3	0	8
Yoneyama[10]	4	0	2	6
Chen L[13]	4	4	0	8
Our	4	2	0	6

从表2可以看出,在文献[9,13,15]的密钥协商过程中,域服务器之间没有直接进行通信,密钥协商通过域间用户协商得到,本协议也是通过域间用户使用 Diffie-Hellman 协议协商得到安全会话密钥。与对比协议相比,本文协议的交互次数明显减少,在固定通信带宽的前提下,本协议的服务器可以容纳更多的客户端,而且域间客户端交互流程明显简化,减少了密钥协商的时间开销,在大规模网络部署中,有利于新域的加入和已存在域的离开操作,具有良好的扩展性。其中文献[10,14]与本协议相比,虽然交互次数没有明显的差异,但该类协议是通过域服务器之间的信息交互完成密钥协商,在上述分析过程中可以发现,域间服务器通信在实现大规模网络部署中,域的加入和离开等操作需要花费大量的时间和精力去实时维护域服务器之间的连通性,保证现有域之间密钥协商的安全性。密钥协商由跨域认证服务器之间的协商得到,例如 Kerberos 协议中,会话密钥由 Kerberos 产生,导致窃听会话而不被举证。而本协议弥补了域服务器之间的通信实现跨域密钥协商的缺陷,在域服务器之间的通信进行密钥协商的过程中导致域的加入和离开操作产生巨大的人力和资源消耗,本协议采用域间用户信息交互取代域间服务器通信方式,域服务器完成域内用户的认证,并通知跨域服务器。域的加入和离开操作需要维护域服务器之间的公钥信息,然而公钥数据本身对外公开可见,因此可降低域间通信网络的维护和人力资源的成本。

表3数据给出了 Chen L 协议[13]与本协议的加解密和 Diffie-Hellman 系数的出现次数。对比数据发现,协议使用公私钥加解密次数为3,但是签名和验证签名的次数有明显的升高,在签名和验证签名方面增加了4次计算量,对称加密次数减少了1次。对比协议在加解密计算开销方面存在明显的不足,因为这样可以保证密钥协商过程中数据的机密性与完整性,确保协商得到的会话密钥是安全的。但是本协议在交互流程中要比其他协议少两次跨域用户之间的信息交互,在时间开销方面,跨域通信次数减少,大大降低了整个协议的时间开销。虽然在计算量方面增加了时间开销,但是通过减少的跨域交互流程弥补了计算性能上的额外开销。而 Diffie-Hellman 系数比其协议减少了一半以上,Chen L 协议中系数个数为12,而本协议中随机数个数只为5,因此本协议降低了

(下转第 182 页)

平台构建[J]. 质量技术监督研究,2015(4):55-57.

[25] WU Kai. The design and implementation of bar code scanning software based on Android platform[J]. Information Safety, 2013(10):223-231. (in Chinese)
吴凯. 基于 Android 平台的条码扫描软件的设计与实现[J]. 信息安全,2013(10):223-231.

[26] XU Jie-min, XIAO Yun. The present situation and development prospect of two dimensional bar code technology [J]. Computer and Modernization, 2004(12):141-142. (in Chinese)
徐杰民,肖云. 二维条码技术现状及发展前景[J]. 计算机与现代化,2004(12):141-142.

[27] ZHANG Xiao. Research and implementation of software protection strategy based on Android platform[D]. Beijing: Beijing University of Posts and Telecommunications, 2015. (in Chinese)
张晓. 基于 Android 平台的软件保护策略的研究与实现[D]. 北京:北京邮电大学,2015.

[28] LIU Zhi. Application of three weight DES, RSA, SHA-1 algorithm design data encryption system[J]. Software Guide, 2015 (5):165-167. (in Chinese)
刘志. 应用三重 DES、RSA、SHA-1 算法设计数据加密系统[J]. 软件导刊,2015(5):165-167.

[29] CHENG Xiao-rong, MA Li, HE Zhuang-zhuang. Analysis and improvement of public key RSA encryption algorithm[J]. Network Security, 2015(8):44-45. (in Chinese)
程晓荣,马力,何壮壮. 公钥 RSA 加密算法的分析与改进[J]. 网络安全,2015(8):44-45.

(上接第 158 页)

对存储资源的需求,提高了协议的扩展性。

表 3 加密操作对比

	Protocol	2C	2S	Total
Our	Signing/private key decryption	3	4	7
	Verifying/public key encryption	3	4	7
	Symmetric key encryption/ decryption	2	1	3
Chen L[13]	Signing/public key decryption	0	2	2
	Verifying/public key encryption	2	0	2
	Symmetric key encryption/ decryption	2	2	4

结束语 本文提出了一种新的基于 PKI 体系的跨域密钥协商协议,采用公钥算法与 Diffie-Hellman 协议协商得到安全会话密钥,解决了基于口令的跨域密钥协商协议和 Kerberos 协议存在的弱口令的安全问题。本协议共享密钥仅仅作为鉴别用户身份的一种方式,用户和域服务器之间的共享密钥泄露不会影响协议的安全性,降低了服务器密钥管理的复杂性。域间用户信息交互使用另一个域服务器的公钥加密,拥有私钥域服务器才能解密跨域信息,保证了域间信息交互的机密性。安全性分析表明本协议具有对抗包括字典攻击、重放攻击、中间人攻击等多种攻击方式的能力,并且具有前向安全性和良好的扩展性。

参 考 文 献

[1] MANNAN M, OORSCHOT P C V. A Protocol for Secure Public Instant Messaging [M]. Financial Cryptography and Data Security, 2006:20-35.

[2] CAO T, QUAN T, ZHANG B, et al. Crypt analysis of Some Client-to-Client Password-Authenticated Key Exchange Protocols[C]// 2010 3rd IEEE International Conference on Proceedings of the Broadband Network and Multimedia Technology (IC-BNMT). 2010:654-658.

[3] YAO Y, WANG X, SUN X. A Cross Heterogeneous Domain Authentication Model Based on PKI[C]// International Symposium on Proceedings of the Parallel Architectures, Algorithms and Programming. 2011:325-329.

[4] ZHANG Jiao, ZHANG Yu-jun, ZHANG Han-wen, et al. A Fast Inter-Domain Authentication Method Combining Trust Mechanism in Mobil IPv6 Networks[J]. Journal of Computer Research and Development, 2008:45(6):951-959. (in Chinese)
张娇,张玉军,张瀚文,等. 结合信任机制的移动 IPv6 网络快速跨域认证方法[J]. 计算机研究与发展,2008,45(6):951-959.

[5] BYUN J W, JEONG I R, LEE D H, et al. Password-Authenticated Key Exchange between Clients with Different Passwords [C]// Information and Communications Security, International Conference, ICICS 2002. Singapore, 2002:134-146

[6] KIM J, KIM S, KWAK J, et al. Cryptanalysis and Improvement of Password Authenticated Key Exchange Scheme between Clients with Different Passwords[C]// Computational Science and Its Applications, ICCSA 2004. Springer Berlin Heidelberg, 2004: 895-902.

[7] YOON E J, YOO K Y, et al. A secure password-authenticated key exchange between clients with different passwords[C]// Proceedings of the 2006 International Conference on Advanced Web and Network Technologies, and Applications. Springer-Verlag, 2006:659-663.

[8] LIU Xiu-mei, ZHOU Fu-cai, CHANG Gui-ran. A Verifier-Based Key Exchange Protocol in Cross-Realm Setting[C]// International Conference on Networks Security, Wireless Communications and Trusted Computing. 2009:5560-5563.

[9] FENG D G, XU J. A New Client-to-Client Password-Authenticated Key Agreement Protocol[C]// Coding and Cryptology, Second International Workshop, IWCC 2009. 2009:63-76

[10] YONEYAMA K. Cross-Realm Password-Based Server Aided Key Exchange [C]// Proceedings of the 11th International Conference on Information Security Applications. 2010:322-336.

[11] XU J, ZHU W T, JIN W T. A Generic Framework For Constructing Cross-Realm C2c-Paka Protocols Based on The Smart Card [J]. Concurrency and Computation: Practice and Experience, 2010, 23(12):1386-1398.

[12] CHUANG P J, LIAO Y P. Efficient and Secure Cross-Realm Client-to-Client Password-Authenticated Key Exchange [C]// Proceedings of the 2014 IEEE 28th International Conference on Advanced Information Networking and Applications. 2012:701-708.

[13] CHEN L, LIM H W, YANG G. Cross-domain password-based authenticated key exchange revisited[C]// Proceedings of the INFOCOM, 2013 Proceedings IEEE. 2012:1052-1060.

[14] YIN Yin, BAO L. Secure Cross-Realm C2C-PAKE Protocol [M]. Information Security and Privacy, 2006:392-406.

[15] BYUN J W, LEE D H, LIM J I. EC2C-PAKA: An efficient client-to-client password-authenticated key agreement [J]. Information Sciences: an International Journal, 2007, 177(19): 3995-3401.