基于D-H公钥系统前向保密的密码协议

李 闵,卢建朱,黄益栓
(暨南大学 计算机系,广东 广州 510632)

摘 要:Diffie-Hellman(D-H)算法可以实现密码系统的密钥交换,其安全性依赖于计算离散对数的难度,并且Diffie-Hellman密钥交换协议能够提供前向保密性。文中通过分析Diffie-Hellman密钥交换协议,给出了一个可以应用于任何非对称密码体制的具有前向保密的密码协议。

关键词:前向保密;密码协议;单向函数;密钥交换
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2006)10-0153-02

A Forward Secrecy Protocol Based on D-H PKE System

LI Min, LU Jian-zhu, HUANG Yi-shuan
(Computer Department, Jinan University, Guangzhou 510632, China)

Abstract: Diffie-Hellman(D-H) algorithm can exchange the key in a crypto system, the security of which is based on the discrete algorithm. And Diffie-Hellman key-exchange protocol can provide a crypto system with the forward secrecy. Analyze Diffie-Hellman key-exchange protocol, and present a crypto graphical protocol with forward secrecy which can be applied to any asymmetric crypto systems.

Key words: forward secrecy; crypto graphical protocol; one-way function; key exchange

0 前 言

公钥加密系统中,算法对用户和攻击者都是公开的,系统的安全性依赖于密钥的安全性。密钥的泄露直接威胁密码系统,使得所有保护系统的安全措施失效。如何减少密钥泄露所造成的损失是目前信息安全领域研究的一个热点。

目前已经提出许多方法(包括秘密共享[1]、短时加密[2]和事先加密[3])试图解决这个问题。一般关注的是前向安全(forward secure)。前向安全的主要思想是:将整个系统的生存时间化分成若干个时期,利用密钥更新算法在每个时期开始产生自己对应的密钥,而公钥保持不变。同时在每个时期开始时,将上一时期的密钥删除,产生并保存新密钥。这样,即使某个时期的密钥泄露了,也不会威胁到该时期之前的其他密钥,从而提高了系统的安全性和有效性。前向安全密钥交换概念最先由Günther[4]和Diffie等人提出的。一个前向安全的密钥交换协议,即使长期密钥泄漏也不会危及以前产生的会话密钥[5]。后来,Anderson[6]提出非交互式的前向安全,Bellare和Yee[7]研究了非交互式对称加密。

基于Diffie-Hellman的公钥系统可以实现安全的前向保密性。张喆等[8]给出了一种使用Diffie-Hellman建立的密码协议,在协议中使用了双方的身份标识,需要第三方的PKI(公钥基础设施)的支持。王滨等[9]提出一种无第三方PKI身份认证的密码协议,但是计算要复杂,在加密时,同时使用公钥私钥加密一个信息造成计算增加,不利于小型设备的使用。

文中通过研究Deffie-Hellman的密码协议,提出一种交互式无需身份认证的具有前向保密的密钥协议,可用于任何非对称密码系统,但是需要PKI的支持。该协议在计算量上也要比文献[8]的计算量小,特别适用于小型设备的通讯,如移动设备或智能卡之间通讯。

1 Diffie-Hellman密钥建立协议

A、B作为通信的双方,现在要进行密钥的交换。

(1)$A -> B: A, g^{r_A} \pmod p$

(2)$B -> A: g^{r_B} \pmod p, H_1(g^{r_B} \bmod p, K_{AB})$

(3)$A -> B: H_2(K_{AB})$

A: $K_{AB} = (g^{r_A})^{r_B} \bmod p$

B: $K_{AB} = (g^{r_B})^{r_A} \bmod p$

说明:

(1)A选择随机数r_A,并发送给B:

A, $g^{r_A} \pmod p$

(2)B选择随机数r_B,计算:

$K_{AB} = (g^{r_A})^{r_B} \pmod p$

并将$g^{r_B} \pmod p$, $H_1(g^{r_B} \bmod p, K_{AB})$传给$A$。

收稿日期:2005-12-25

作者简介:李 闵(1979-),女,安徽六安人,硕士研究生,研究方向网络技术及安全;卢建朱,博士,副教授,研究方向为计算机网络与信息安全。

(3)A 接收到后计算:

$K_{AB} = (g^{r_A})^{r_B} \bmod p$

并计算 $H_2(K_{AB})$,传给 B,证实 A 已经得到 K_{AB},A,B 分别已经计算出 K_{AB} 的值,K_{AB} 就作为会话密钥开始通信。

符号说明:

g 和 p 是大素数,g 是模 p 的本原元,r_A 是由 A 产生的随机数,r_B 是由 B 产生的随机数,分别作为 A 和 B 的私钥。K_{AB} 代表通过协议建立的会话密钥,$H_1(\cdots)$ 和 $H_2(\cdots)$ 是两个散列函数,进行散列运算。

2 一种新型具有前向保密性密码协议

2.1 提出新模型

这里将上文所示协议改为如下形式:

(1) $A -> B$: $g^{r_A} \bmod p$

(2) $B -> A$: $g^{r_B} \bmod p, b$

A: $K_{AB} = H(g^{br_B} \bmod p, r_A)$

B: $K_{AB} = H(g^{br_A} \bmod p, r_B)$

这里要求散列函数 $H(\cdots)$ 具有下列性质:

$H(g^{br_B} \bmod p, r_A) = H(g^{br_A} \bmod p, r_B)$,在数学可以找到满足这一性质的散列函数。所以 Diffie - Hellman 密钥建立协议能具有前向保密安全性就是因为它成功地应用了离散对数求解这个数学上的 NP 问题[10]。

2.2 实现前向保密性密码协议的详细设计

2.2.1 初始 T_0 时刻的协议

初始化,构造双方公共参数 g,p 以及散列函数 H,H_1,H_2。A 产生 A 的长期私钥是 r_A,B 产生 B 的长期私钥是 r_B。

2.2.2 T_i 时刻到 T_{i+1} 时刻的协议

(1)$A -> B$: $Q_i, g^{r_A} \bmod p$

(2)$B -> A$: $g^{r_B b_i} \bmod p, H_1(g^{r_B b_i} \bmod p, K_{AB_i})$

(3)$A -> B$: $H_2(K_{AB_i})$

说明:

(1)A:产生一个请求 Q_i,并将其传给 B 表示 A 要求生成第 i 阶段会话的密钥 K_{AB_i}。

(2)B:接收 Q_i 后,产生一个随机数 b_i,并计算密钥

$K_{AB_i} = H(g^{r_B b_i} \bmod p, r_B)$

以及散列值 $H_1(g^{r_B b_i} \bmod p, K_{AB_i})$,将 $g^{r_B b_i} \bmod p$,$H_1(g^{r_B b_i} \bmod p, K_{AB_i})$ 传给 A。

(3)A:计算

$K_{AB_i} = H(g^{r_B b_i} \bmod p, r_A)$

以及散列值 $H_1(g^{r_B b_i} \bmod p, K_{AB_i})$,验证消息来自 B,并传 $H_2(K_{AB_i})$ 给 B,证实得出密钥。B 收到后进行验证,证实 A 获得了密钥 K_{AB_i}。

A 和 B 的第 i 次会话的密钥 $K_{AB_i} = H(g^{r_A b_i} \bmod p, r_B) = H(g^{r_B b_i} \bmod p, r_A)$。

3 安全性分析

3.1 选择密文攻击

在协议中,由 PKI 负责公布 g,p,H,H_1,H_2 等参数,要计算 $g^{r_A b_i}$,这是个离散对数问题[10],无法在有效的多项式时间内计算。故协议可以防止密文攻击。

3.2 中间人攻击

假设中间人为 E,其通过 PKI 获得私钥为 r_E,可以获得 g,p,H,H_1,H_2 等公共参数,又假设 E 可以截获并修改 A,B 的通讯内容。

(1) $A -> E$: $Q_i, g^{r_A} \bmod p$

$E -> B$: $Q_i, g^{r_E} \bmod p$

B 用自己的私钥替换了 A 的私钥,送给 B。

(2) $B -> E$: $g^{r_B b_i} \bmod p, H_1(g^{r_B b_i} \bmod p, K_{BE_i})$

$E -> A$: $g^{r_E e_i} \bmod p, H_1(g^{r_E e_i} \bmod p, K_{EA_i})$

E 产生随机数 e_i,替换了 B 的 b_i 和其私钥,这样 E 可以同时和 A,B 通讯,而 A,B 却认为是和对方通讯。

(3) $A -> E$: $H_2(K_{EA_i})$

$E -> B$: $H_2(K_{BE_i})$

在这种攻击模式中,E 可以通过实时截获和修改 A,B 的通讯内容,而达到知晓其信息的目的,这在通讯设备上要求很高,而且性能要好,况且成本很高,在安全性要求不是特别高的通信中,特别是小型设备,我们的协议具有很大的优势。

3.3 会话密钥的泄漏

如果第 i 阶段建立的会话密钥 K_{AB_i} 泄漏,那么根据协议只会暴露当前的会话内容,而不会暴露第 i 阶段以前的会话内容,所以实现了前向安全。并且,也不会暴露第 i 阶段以后建立的会话内容,因为不能推出第 $i+1$ 阶段的会话密钥,所以具有较好的安全性。

3.4 A,B 长期私钥的泄漏

如果 A,B 的长期私钥泄漏,根据协议并不能得到当前会话的密钥 K_{AB_i},所以系统仍然是安全的。而且可以通过重新执行 Diffie - Hellman 协议,建立新的私钥来更换 A,B 的长期私钥。

4 小 结

文中提出基于 Diffie - Hellman 密码协议,并实现了密码系统的前向安全性,而且无需身份认证,提高了系统的效率,特别适用于安全性要求不高的小型设备使用。

参考文献:

[1] Ostrovsky R, Yung M. How to withstand mobile virus attacks [A]. PODC '91[C]. [s.l.]: ACM, 1991. 51 - 59.

[2] Damg'ard I B, Nielsen J B. Improved non - committing encryption schemes based on a general complexity assumption [A]. Crypto '00[C]. LNCS 1880. [s.l.]: Springer - Verlag, 2000. 432 - 450.

(下转第 166 页)

如果发布服务的所有输入都被匹配,带有最低匹配等级的输入将决定最终的匹配结果。比如表 1 中,匹配等级 5 代表所有输入对的属性匹配都是等价,类型匹配要么是等价要么是包含,但只要有一个输入对的类型匹配是包含,将决定了匹配等级低于所有类型匹配都是等价的等级。

输入参数匹配的步骤如下:对于发布服务的每一个输入,都试图找到和其具有最高匹配等级的请求服务输入。最高的匹配等级大于 0 则找到了一个匹配。发布服务的输入和具有大于 0 的最高匹配等级的请求服务的输入形成一个输入对。

当发布服务的输入列表为空时,输入参数匹配等级返回为 6,因为此时发布服务不需要任何输入参数,没有必要进行输入的匹配。

输出参数的匹配与输入一样,这里不再赘述,但值得注意的是匹配顺序的颠倒,对于请求服务的每个输出,系统都试图在发布服务输出中找到一个匹配。

在 OWL - S 中,可以使用 OWL 本体中描述的某种分层方法来对服务进行分级。在这个本体中,每个具体的服务或者是类 Profile 的实例或者是类 Profile 某个子类的实例。在进行服务 Profile 分级的匹配时,系统试图在发布服务中找到最匹配请求服务需求的服务。假设 reqServiceHie 表示请求服务分级,advServiceHie 表示发布服务分级。reqServiceHie 和 advServiceHie 均为某个服务分层本体中定义的概念。两者进行类型匹配的结果见表 2。

表 2 服务分级匹配结果

等级	匹配结果	注释
0	失败	两者彼此没有任何关系
1	未分类	两者中只要有一个未分类,即直接是 Profile 类本身的实例
2	包含	advServiceHie 被 reqServiceHie 所包含。即 advServiceHie 代表一个比 reqServiceHie 更具体的概念。既然发布服务的分级是请求服务分级的一个子类,意味着发布服务提供比请求服务需求更具体的功能
3	匹配	reqServiceHie 和 advServiceHie 是等价的。这是对请求服务分级的最好匹配

最后一个匹配阶段是服务质量的匹配,服务请求者提出的服务质量和发布服务的服务质量进行语义匹配以检验服务质量要求是否满足。

4 总结和展望

文中介绍了语义 Web 服务的描述语言 OWL - S,设计并实现了一个基于 OWL - S 的 Web 服务发现系统。针对 OWL - S 描述的 Web 服务的发布和查询过程进行了介绍,重点介绍了 Web 服务的 OWL - S 信息在数据库中的存储结构以及服务匹配算法。文中只是实现语义 Web 服务发现的一个初步模型,存在一些不足之处,如系统并没有考虑与现有 UDDI 注册中心的结合,另外文中所介绍的 OWL - S 本体到数据库的映射完全取决于系统采用的推理机,推理机的局限性会导致信息存储的不完整,这些问题将在进一步研究工作中予以解决。

参考文献:

[1] Berners - Lee T, Hendler J, Lassila O. The Semantic Web[J]. Scientific American, 2001, 284(5): 34 - 43.

[2] OWL Web Ontology Language Guide[R/OL]. W3C Candidate Recommendation 18 August 2003. http://www.w3.org/TR/2003/CR - owl - guide - 20030818/, 2003.

[3] Martin D. OWL - S: Semantic Markup for Web Services[R/OL]. Technical report, Daml consortium, http://www.daml.org/services/owl - s/1.0/owl - s.pdf, WRSP Primer Working Draft 0.3., 2004 - 02.

[4] Paolucci M, Kawamura T, Payne T R, et al. Importing the Semantic Web in UDDI[A]. In Proc of Web Services, E - Business and Semantic Web Workshop, CAiSE 2002[C]. [s.l.]: [s.n.], 2002.225 - 236.

[5] Kopena J, Regli W. DAMLJessKB: A tool for reasoning with the semantic web[J]. In IEEE Intelligent Systems, 2003, 18: 74 - 77.

[6] Paolucci M, Kawamura T, Payne T, et al. Semantic matching of web service capabilities[A]. In Proceedings of 1st International Semantic Web Conference (ISWC2002)[C]. Berlin: Springer - Verlag, 2002.333 - 347.

(上接第 154 页)

[3] Lindell Y. A simpler construction of CCA2 - secure public - key encryption under general assumptions[A]. Eurocrypt 2003[C]. LNCS 2656. [s.l.]: Springer - Verlag, 2003.241 - 254.

[4] Fujisaki E, Okamoto T. Secure integration of asymmetric and symmetric encryption schemes[A]. Crypto'99[C]. LNCS 1666. [s.l.]: Springer - Verlag, 1999.537 - 554.

[5] Desmedt Y, Frankel Y. Threshold cryptosystems[A]. Crypto'89[C]. LNCS 435. [s.l.]: Springer - Verlag, 1989.307 - 315.

[6] Anderson R. Two remarks on public key cryptology[EB/OL]. Invited Lecture, ACM - CCS '97. http://www.cl.cam.ac.uk/ftp/users/rja14/forwardsecure.pdf, 1997.

[7] Bellare M, Yee B. Forward security in private - key cryptography[A]. CT - RSA 2003[C]. LNCS 2612. [s.l.]: Springer - Verlag, 2003.1 - 18.

[8] 王 滨,汪和松. Diffie - Hellma 密钥建立协议的前向保密性研究[J]. 长沙电力学院学报(自然科学版),2004,19(3): 15 - 17.

[9] 王 滨,张少武,杨 飚. 密码协议的前向保密性研究[J]. 计算机工程与应用,2004,40(25): 157 - 160.

[10] Cheon J H, Lee D H. Diffie - Hellman Problems and Bilinear Maps[EB/OL]. http://eprint.iacr.org/2002/117/, 2002.