基于 ECDLP 的 SIP 认证密钥协商协议①

曹 阳

(陕西理工学院 数学与计算机科学学院, 汉中 723000)

摘 要: SIP 协议是应用层控制协议, 为了提高 SIP 协议的安全性, 文中基于椭圆曲线离散对数问题的难解性, 结合用户身份、用户口令及单向陷门函数 F(), 提出了一种基于 ECDLP 的 SIP 认证密钥协商协议. 协议过程主要由初始化、注册、登录认证、口令修改四部分组成. 安全分析表明, 该协议实现了双向认证、提供了安全会话密钥, 能抵抗口令猜测攻击、中间人攻击、重放攻击、冒充攻击、Denning-Sacco 攻击等. 与相关协议比较, 本文所提出的基于 ECDLP 的 SIP 认证密钥协议具有更高的安全性, 能更好的满足应用需求.

关键词: 椭圆曲线离散对数问题; 认证; 密钥协商; SIP; 单向陷门函数 F()

SIP Authentication Key Agreement Protocol Based on ECDLP

CAO Yang

(School of Mathematics and Computer Science, Shaanxi University of Technology, Hanzhong 723000, China)

Abstract: The SIP protocol is a controlling protocol of the application layer. In order to improve the security of SIP protocol, based on the intractability of the elliptic curve discrete logarithm problem, combining with the user's identity, password and one-way trapdoor function F(), this paper proposes an SIP authentication key agreement protocol with the basis of ECDLP. The agreement process consists of four parts: initialization, registration, login authentication, and changing password. The safety analysis shows that the proposed protocol not only provides two-way authentication and a safe session key, but also resists the password-guessing attack, man-in-the-middle attack, replay attack, masquerade attack, and Denning-Sacco attack. Compared with other protocols, the proposed SIP authentication key agreement based on ECDLP has higher security and can better meet the application demands.

Key words: elliptic curve discrete logarithm problem; certification; key agreement; session initiation protocol; one-way trapdoor function F()

SIP[1-2]协议是基于文本的一种点对点协议, 是应用层控制协议, 它可以建立多媒体会议会话. 用户需要使用 SIP 服务的时候, 需要进行身份验证, 因此认证已经成为 SIP 安全问题中的重要问题. 近十年, 大量的作者对 SIP 的安全问题提出了多种认证协议[3-6], 但一系列协议存在最大的问题仍然是口令猜测、Denning-Sacco 攻击等问题. 如: 文献[7]在离散对数难题之上, 基于 Diffie-Hellman 密钥交换算法提出了一种认证协议以克服 SIP 存在的安全问题, 但该协议仍然存在离线口令猜测攻击和 Denning-Sacco 攻击; 文献[8]针对文献[7]存在的问题, 提出一种基于椭圆曲线 Diffie-Hellman 密钥交换算法的高效认证协议, 虽然协议减少了内存需求量和执行时间, 但该协议仍然存在口令猜测攻击和 Denning-Sacco 攻击; 文献[9]结合单向哈希函数和异域运算提出了基于随机新鲜数的高效认证协议, 但协议无密钥协商, 会话密钥无安全性, 遭受离线口令猜测攻击和 Denning-Sacco 攻击; 文献[10]结合智能卡、口令、生物特征三要素提出基于 ECC 的三因子 SIP 认证协议, 但协议仍然存在口令猜测攻击, 且无双向认证. 文献[11], 基于离散对数问题, 为

① 基金项目:国家自然科学基金(21373132);陕西省教育厅资助项目(15JK1139);陕西理工学院科研计划(SLGKY14-09)
收稿时间:2015-06-02;收到修改稿时间:2015-09-06

© 中国科学院软件研究所 http://www.c-s-a.org.cn

SIP 提出一种基于 ECC 的改进认证及密钥协商协议, 但该协议仍然存在离线口令猜测攻击. 基于上述问题, 本文结合用户身份、用户口令及单向陷门函数 F(), 基于椭圆曲线离散对数问题的难解性, 为 SIP 提出了一种认证密钥协商协议.

1 椭圆曲线离散对数问题

椭圆曲线密码[12](Elliptic Curve Cryptosystem, ECC)中用到的椭圆曲线定义在有限域上, 有限域 F_p 上的椭圆曲线 $E(F_p)$ 定义为: $y^2=x^3+ax+b$, 其中, $a,b\in F_p, 4a^3+27b^2\neq 0(\mathrm{mod}\ p)$, p 是大于3的素数, G 为 $E(F_p)$ 上的基点, q 为 G 的阶(q 为一个安全大素数).

如果存在整数 l $(0<l<q-1)$, $Q=lG$, 则称 l 为 Q 的以 G 为基的离散对数. 对于 $E(F_p)$ 上的一点 G, 对任意的 Q, 求整数 l, 使得 $Q=lG$ 的问题称为椭圆曲线上的离散对数问题(elliptic curve discrete logarithm problem, ECDLP)[12], 椭圆曲线密码体制正是利用这个困难问题设计而来, 并以较短的密钥提供更高的安全性.

2 认证密钥协商协议

本协议过程主要由系统初始化、注册、登录认证、口令修改四个部分组成, 协议中用到的主要参数含义描述如下:

S: 服务器;

U_A: 通信方;

$E(F_p)$: 有限域上椭圆曲线;

$E_x()$: 用密钥对消息进行加密;

$D_x()$: 用密钥对消息进行解密;

$F_s()$: 服务器的单向陷门函数, 只有S才能对函数求逆;

$H()$: 安全无碰撞哈希函数;

PW_A: 用户口令;

ID_A: 用户身份;

$\oplus$: 异或运算.

2.1 系统初始化

服务器S和用户共同选取一条椭圆曲线 $E(F_p)$, 服务器S选取一个随机数 $r\in[1,q-1]$ 作为自己的私钥, 计算 $R_S=rG$ 作为自己的公钥, 公开参数q, a, b, G, p, $H()$, R_S, $F_s()$.

2.2 注册

用户通过安全信道和服务器之间进行通信, 协议过程为:

(1)用户U_A选取随机数ID_A作为自己的身份, 选取随机数 PW_A 作为自己的口令, 并将 $E_{R_S}(ID_A,PW_A)$ 传送给S.

(2)服务器S收到用户U_A发送的 $E_{R_S}(ID_A,PW_A)$ 后, 计算 $D_r(E_{R_S}(ID_A,PW_A))$, $X_A=H(ID_A\|R)\oplus PW_A$, 并将 (ID_A,PW_A) 存储于服务器安全用户数据库.

2.3 登录认证

(1) $U_A\rightarrow S:(F_s(ID_A),E_{R_S}(R_1))$

用户U_A选取随机数 $r_a\in[1,q-1]$, 计算 $R=r_aG$, $R_1=R\oplus H(ID_A\|PW_A)$, 公布自己的公钥R, 并将 $(F_s(ID_A),E_{R_S}(R_1))$ 发送给S.

(2) $S\rightarrow U_A:(E_R(R_2,X_1))$

S收到用户发送的消息 $(F_s(ID_A),E_{R_S}(R_1))$ 后, 求解单向陷门函数得ID_A, 并检验ID_A是否在数据库内. 如果ID_A不在数据库内, 则服务器S停止执行协议, 拒绝登录. 否则, 服务器S计算 $PW_A=X_A\oplus H(ID_A\|r)$, $D_r(E_{R_s}(R_1))$ 得 R_1, 同进计算 $R'=R_1\oplus H(ID_A\|PW_A)$, 服务器生成一随机数 r_s, 计算 $R_2=r_sG$, $SK_S=r_sR'=r_ar_sG$, $X_1=H(S\|ID_A\|R'\|R_2\|SK_S)$, 将 $(E_R(R_2,X_1))$ 发送给U_A, 并计算共享密钥 $SK=H(ID_A\|S\|R'\|R_2\|SK_S\|PW_A)$.

(3) $U_A\rightarrow S:(F_S(ID_A),E_{R_S}(X_2))$

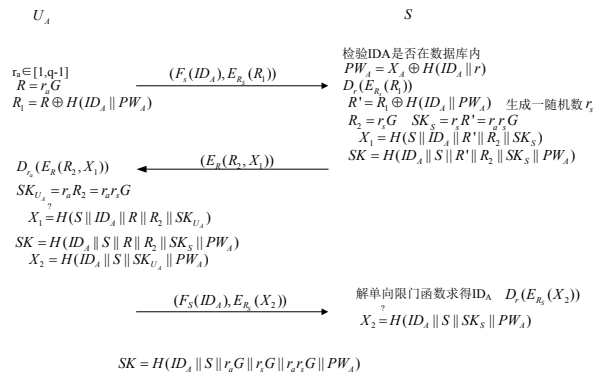
用户U_A收到服务发送的消息 $(E_R(R_2,X_1))$ 后, 计算 $D_{r_a}(E_R(R_2,X_1))$, 得 R_2, X_1, 计算 $SK_{U_A}=r_aR_2=r_ar_sG$, 计算 $X_1=H(S\|ID_A\|R\|R_2\|SK_{U_A})$, 并判断 X_1 是否与发送来的 X_1 相等, 若不相等, 用户U_A终止会话, 否则, U_A认证了服务器S. 用户U_A计算共享密钥 $SK=H(ID_A\|S\|R\|R_2\|SK_S\|PW_A)$, $X_2=H(ID_A\|S\|SK_{U_A}\|PW_A)$, 并将 $(F_S(ID_A),E_{R_S}(X_2))$ 发送给服务器S.

(4)S认证U_A, 实现双向认证

服务器S收到用户U_A发送的消息 $(F_S(ID_A),E_{R_S}(X_2))$ 后, 求解单向陷门函数 $F_S(ID_A)$ 得ID_A, 认证用户U_A, 若U_A合法, 计算 $D_r(E_{R_S}(X_2))$ 得X_2, 计算 $X_2=H(ID_A\|S\|SK_S\|PW_A)$, 并判断 X_2 是否与发送来的 X_2 相等, 若不等, 则服务器终止会话, 否则, 服务器认证了用户U_A的身份, 接受共享会话密钥.

如果以上步骤执行都正确, 则用户U_A和服务器S实现了相互认证, 完成了密钥协商, 双方会话密钥 $SK=H(ID_A\|S\|r_aG\|r_sG\|r_ar_sG\|PW_A)$, 登录认证协商过

© 中国科学院软件研究所 http://www.c-s-a.org.cn



程如图 1 所示.

图 1 登录认证协商过程

2.4 口令修改

当用户U_A怀疑自己的口令被盗或定期想修改自己的口令时, 则可以通过以下协议过程修改口令.

(1)用户U_A执行登录认证服务请求, 收到服务器S发来的认证通过消息后, 输入自己的新口令值 PW_A', 计算 $PW_B = H(SK \| SK_{U_A}) \oplus PW_A'$, $X = H(SK \| SK_{U_A} \| PW_A')$, 并将 $(F_S(PW_B), E_R(X))$ 发送给服务器S.

(2)服务器S收到消息 $(F_S(PW_B), E_R(X))$ 后, 利用单向陷门函数求得 PW_B, 用私钥解密消息得 X, 计算 $PW_A' = PW_B \oplus H(SK \| SK_{U_A})$, $X \stackrel{?}{=} H(SK \| SK_S \| PW_A')$. 如果相等, 服务器同意修改口令, 计算 $Y_1 = H(SK_S \| SK \| "ACCESS")$, 并将 $("ACCESS", E_R(Y_1))$ 发送给用户, 服务器计算 $X_A' = H(ID_A \| r) \oplus PW_A'$,并用 X_A' 代替 X_A 存储在数据库中. 如果不相等, 则服务器拒绝修改口令, 计算 $Y_2 = H(SK_S \| SK \| "FAILURE")$, 并将 $("FAILURE"), E_R(Y_2))$ 发送给用户U_A.

3 方案分析

3.1 安全性分析

(1) 抵抗口令猜测攻击

因为在线口令猜测攻击很容易被检测, 通过阈值限制锁定账户的办法得到有效遏制, 所以, 在此只考虑离线口令猜测攻击.

情形1, 假如攻击者E从服务器上数据库内获取了用户的验证值 X_A, 要想从 X_A 中计算出口令 PW_A 是不可能的.

假设攻击者E猜测出一个口令并计算出 $H(ID_A \| r_s) = X_A \oplus PW_A$, 但E无法验证 $H(ID_A \| r_s)$ 的正确性, 因为 r_s 为S的私钥, 用户 ID_A传送过程中通过单向陷门函数保护起来了.

情形2, 攻击者E可能做如下的字典攻击.

E 选取随机数 r_1 计算 $R_1 = r_1 G$, 并将 $(F_S(ID_A), E_{R_S}(R_1))$ 发送给服务器S, 服务器S收到用户发来的登录请求消息后, 求解陷门函数得ID_A, 解密 $E_{R_S}(R_1)$ 得 R_1, 计算 $PW_A = X_A \oplus H(ID_A \| r_s)$, $R' = R_1 \oplus H(ID_A \| PW_A) = r_1 G \oplus H(ID_A \| PW_A)$, $R_2 = r_s G$, $SK_S = r_s R' = r_1 r_s G \oplus H(ID_A \| PW_A)$, $X_1 = H(S \| ID_A \| R' \| R_2 \| SK_S)$.并将消息 $(E_R(R_2, X_1))$ 发送给用户U_A. 当攻击者E获取了消息 $(E_R(R_2, X_1))$ 后, 试图作离线口令攻击, 必须对($(E_R(R_2, X_1))$ 进行解密, 计算出 $SK_{U_A} = SK_S$, 即必须计算出 $SK_{U_A} = r_1 r_s G \oplus H(ID_A \| PW_A)$. 即使攻击者得到了 R_2, X_1, 但他也无法验证 X_1 的正确性, 要验证 X_1 的正确性必须知道 SK_S, r_s, r, 而攻击者E想通过公开的 R, R_s 得到 r_a, r_s, 则面临ECDLP问题, 因此本协议能抵抗口令猜测攻击.

(2) 抵抗中间人攻击

攻击者E想要构造消息 X_1, X_2, 需要用户的PW_A及服务器的私钥 r_s, 而攻击者不可能知道 PW_A 及 r_s. 因为 PW_A' 和 r_s 是两个秘密信息, 所以攻击者无法对本协议做中间人攻击.

(3) 抵抗Denning-Sacco攻击

假设攻击者由于某种原因获得了某一轮的会话密钥, 在此基础上获得会话双方密钥, 用户口令或服务器私钥, 则协议存在Denning-Sacco攻击. 本协议中, 假设攻击者E获得了某一轮的会话密钥 SK, 且事先记下了会话双方在网络上发布的信息, 则他必须在有效的时间 T' 内计算出 $r_a r_s G$ 才能计算出 $S_K' = H(ID_A \| S \| r_a G \| r_s G \| r_a r_s G | PW_A)$ 与获得的会话密钥 SK 进行比较, 而E要从 $r_a G$, $r_s G$ 计算出 $r_a r_s G$ 则面临ECDHP(Elliptic curve Diffie-Hellman)问题和ECDLP问题.

(4) 抵抗重放攻击

协议中, 只有服务器能对 R 进行应答, 且服务器也只对合法用户进行应答. 因为消息传送过程中采用了单向陷门函数对用户 U_A 的身份进行保护, 且 R_1 通过对方公钥进行加密, 要得到 R 必须知道用户的身份 ID_A 和私钥 r_a, 困难性仍然基于 ECDLP 问题. 因此, 能抵抗重放攻击.

© 中国科学院软件研究所 http://www.c-s-a.org.cn

(5) 抵抗冒充攻击

攻击者无法冒充用户欺骗服务器S, 因为他不知道用户的口令, 也就无法构造出正确的登录请求消息 R_2 和 X_2, 同样攻击者E无法冒充服务器欺骗用户, 因为他不知道服务器的私钥 r_s, 也无法求解单向陷门函数 $F_s(ID_A)$ 得出用户ID_A, 从而无法计算 R_1, 也就无法计算出挑战信息 X_1, R_2. 因为登录请求和服务器发送的挑战信息在传递过程中采用对方公钥进行加密, 攻击者要想获得信息必须知道用户或服务器的私钥, 问题困难性基于ECDLP问题, 所以协议能够抵抗冒充攻击.

(6) 提供双向认证

协议中, 用户和服务器之间提供了双向认证. 协议执行过程中, 只有合法的服务器才能对用户的请求作出正确响应, 服务器收到用户请求消息后, 首先解密相关消息判断用户是否合法, 如果合法, 生成随机数计算 X_1, 并将 X_1 加密后发送给用户, 用户解密 X_1 验证服务器的身份. 同样服务器通过用户发送给服务器的 X_2 验证用户的身份, 因为只有合法用户才能拥有正确的私钥和口令, 从而实现了双向认证.

(7) 提供安全会话密钥

攻击者E要想从 SK_{U_A}, SK_S, R_1, R_2 中解出 r_s, r_a, 进而计算出共享会话密钥, 问题的难解性基于 ECDLP 和ECDHP 问题, 因此攻击者E无法计算出共享会话密钥. 假若攻击者 E 获得了用户 U_A 和服务器 S 之间的某一轮会话密钥 SK, 由 Diffie-Hellman 密钥交换知, 他也无法推导出用户 U_A 和服务器 S 之间下一轮的会话密钥 SK', 因为生成每一轮会话密钥都使用了不同的随机数, 因此, 协议提供了会话密钥的安全性.

3.2 相关协议比较

本协议从冒充攻击、口令猜测攻击、Denning-Sacco攻击、双向认证、安全会话密钥五方面与引言中提到的文献[7-11]进行比较, 如表 1 所示. 其中 S 表示安全, NS 表示不安全, P 表示提供, NP 表示不提供.

表 1 相关协议比较

	文献[7]	文献[8]	文献[9]	文献[10]	文献[11]	本协议
冒充攻击	NS	NS	NS	S	S	S
口令猜测攻击	NS	NS	NS	NS	NS	S
Denning Sacco 攻击	NS	NS	NS	S	S	S
双向认证	P	P	P	P	P	P
安全会话密钥	NP	P	P	P	P	P

3 结语

本文针对 SIP 协议的安全性问题, 基于椭圆曲线离散对数问题的难解性, 结合用户身份、用户口令及单向陷门函数 F(), 提出了 SIP 认证密钥协商协议. 协议主要由系统初始化、注册、登录认证、口令修改四部分组成. 文中从口令猜测攻击、中间人攻击、重放攻击、双向认证、会话密钥安全性等方面对所提出的协议进行分析, 分析表明, 所提出的 SIP 认证密钥协议具有更高的安全性, 实际应用更加安全.

参考文献

1 Rosenberg J, Schulzrinne H, Camarillo G. SIP: Session initiation protocol. RFC 3261, 2002.

2 Geneiatakis D, Dagiuklas T, Kambourakis G, et al. Survey of security vulnerabilities in session initiation protocol. IEEE Communication Surveys and Tutorials, 2006, 8(3): 68–81.

3 Lee CC. On security of an efficient nonce based authentication scheme for SIP. Int. J. Netw. Secur, 2009, 9(3): 201–203.

4 Xie Q. A new authenticated key agreement for session initiation protocol. International Journal of Communication Systems, 2012, 25(1): 47–54.

5 Liu FW, Koenig H. Cryptanalysis of a SIP authentication scheme. Communications and Multimedia Security, Springer Berlin, Heidelberg, 2011: 134–143.

6 He DB, Chen JH, Zhang R. A more secure authentication scheme for telecare medicine information systems. Journal of Medical Systems, 2012, 36(3): 1989–1995.

7 Yang CC, Wang RC, Liu WT. Secure authentication scheme for session initiation protocol.Computers and Security, 2005, 24: 381–386.

8 Durlanik A, Sogukpinar I. SIP authentication scheme using ECDH. World Enformatika Socity Trans. on Engineering Computing and Technology, 2005, 8: 350–353.

9 Tsai JL. Efficient nonce-based authentication scheme for session initiation protocol. International Journal of Network Security, 2009, 8(3): 312–316.

10 Yoon EJ, Yoo KY. A three-factor authenticated key agreement scheme for SIP on elliptic curves. Proc. of the 2010 Fourth International Conference on Network and System Security, 2010: 334–339.

11 Arshad R, Ikram N. Elliptic curve cryptography based mutual authentication scheme for session initiation protocol. Multimedia Tools and Applications, 2011, 10(11): 787–789.

12 曹阳,郝玉洁,洪歧.一种基于ECDLP有身份认证的ECDH密钥协商方案.重庆邮电大学学报,2012,24(1):118–120.

© 中国科学院软件研究所 http://www.c-s-a.org.cn