基于自验证公钥的跨域口令认证密钥协商协议*

张 青
(天津财经大学 商学院, 天津 300222)

摘 要: 结合自验证公钥密码学和口令构造了一个用户可以直接通信的跨域口令认证密钥协商协议。域服务器通过口令认证实现对域内用户的认证,并与对方域服务器一起协助用户完成认证和密钥协商。该过程中,域服务器不能获取关于会话密钥的任何信息,且各参与方之间能够实现相互认证。与同类协议相比,该协议需要较小的计算和通信代价,并能抵抗字典攻击和未知会话密钥共享攻击。

关键词: 密钥协商; 跨域; 口令; 字典攻击
中图分类号: TP393.08 **文献标志码**: A **文章编号**: 1001-3695(2013)12-3790-04
doi:10.3969/j.issn.1001-3695.2013.12.070

Cross-realm password-authenticated key agreement protocol based on self-certified cryptography

ZHANG Qing
(*School of Business*, *Tianjin University of Finance & Economics*, *Tianjin* 300222, *China*)

Abstract: Combining self-certified cryptosystem and password, this paper firstly proposed a cross-realm password-authenticated key agreement protocol in direct communication model. The protocol was consist of two parts. Servers could authenticate each other and negotiate session key with the help of the self-certificated public key. Clients could be authenticated by the password pre-shared with corresponding server. The honest but curious servers could not obtain the session key in the protocol. Compared with similar protocols, the protocol need lower communication and computation cost, and can resist dictionary attacks and unknown-key share attack.

Key words: key agreement; cross-realm; password; dictionary attack

0 引言

随着网络规模和云计算技术的发展,一些企业和机构逐步建立起了自己的计算资源。为了保护这些资源的安全,这些企业和机构会构建本地的认证服务器,保证非授权用户不能访问资源。由此,各个相对独立的安全域随之形成。当位于不同安全域里的用户需要与对端进行通信时,就必须进行跨域认证和会话密钥建立。

跨域认证和会话密钥建立的通信方式通常有直接通信和间接通信两类。直接通信是指发起通信的用户从其所处安全域中的服务器处获取与对端用户通信的相关认证信息,然后将此发送给对端用户,而对端用户需要借助于其自身所处安全域中服务器的协助,完成对发起用户的认证并独立产生与发起用户通信所需的会话密钥。间接通信方式是指发起通信用户只需要与其所在安全域中的服务器会话,相应地,对端用户也只需要与其所处安全域中的服务器进行通信。用户间的认证和会话密钥建立完全依赖于各自安全域中的服务器间的通信来实现。

直接通信与间接通信相比,直接通信中的用户和所在安全域中的服务器,以及通信用户之间较易实现两两认证和密钥确认等问题。另外,直接通信还能避免间接通信中随着两个域中需要进行通信的用户数量增加,这两个域中的服务器易成为通信瓶颈的问题。因此,本文将主要研究如何在直接通信框架下实现跨域端到端认证和会话密钥建立的问题。

口令由于具有易于选取、容易记忆、使用方便、节省存储空间等特点成为最实用的认证和协助密钥建立的方法。口令认证密钥协商的思想是用户与服务器之间预先共享口令,处于同一个域之间的用户需要进行通信时借助于域服务器的协助来完成认证和密钥协商。而对于处于不同域之间的用户需要借助各自域中的服务器以及域服务器之间的交互来完成认证和密钥协商。口令使用有很多的优点,当然也存在着不可避免的缺点。常见的是字典攻击问题。字典攻击主要分为离线字典攻击、在线可测字典攻击和在线不可测字典攻击三类。

跨域口令认证密钥协商协议为处于不同安全域中的用户建立安全通信信道提供了很好的途径和方法。Byun 等人[1]于 2002 年构造了第一个直接通信的跨域端到端口令认证密钥协商协议。但文献[2]发现他们的协议不能够抵抗字典攻击。文献[3~5]中对文献[1]的协议进行其他攻击,改进协议并提高了协议工作效率。文献[6]提出了一个具有安全性证明的跨域端到端口令认证和密钥协商协议。然而文献[7]发现如果域服务器之间预共享的对称密钥一旦泄露,文献[6]中的协

收稿日期: 2013-03-08; **修回日期**: 2013-04-28 **基金项目**: 陕西省科技厅自然科学基础研究计划项目(2010JM2016)
作者简介:张青(1969-),女,湖北荆州人,博士,主要研究方向为信息安全、密码学(zhangqing_bupt@sina.com).

议则不能抵抗中间人攻击。此外,文献[8]指出文献[6]中的协议不能抵抗在线不可测字典攻击。文献[9]在文献[6]的基础上,改进了其安全模型的缺点,设计了新的安全模型,并在其中证明了自己构造协议的安全性。但是文献[9]中采用的公钥加密算法导致协议的计算消耗过大,参与方负载偏重。另外,协议在通信消耗方面也没有达到较优,协议交互的次数较多。近两年来文献[10~13]在跨域认证和密钥协商问题上作出了较好的成果。其中,文献[13]给出的是一般性构造,文献[10,11]使用了较为复杂的对运算,文献[12]采用了模幂运算和数字签名,同样不能在效率上达到较优。

本文结合自验证公钥密码学和口令信息,构造了一个直接通信的跨域口令认证密钥协商协议。协议中的每个域服务器持有一个基于自验证公钥产生的公私钥对,服务器间通信所使用的对称会话密钥是由服务器利用各自的公私钥对协商产生,该对称密钥可定期进行更新。用户间的跨域通信借助于各自服务器的协助完成,域服务器通过对口令的验证实现对域内用户的认证,用户间的认证借助于对服务器提供的认证信息实现并最终建立会话密钥,诚实且狡猾的域服务器不能获取关于会话密钥的任何信息。

1　预备知识

p 是有限域 F_p 的元素个数,其中 p 是大素数(长度大于 160,或 $p=2m$,m 为正整数)。定义 F_p 上的椭圆曲线 E:当 $p>3$,$y^2=x^3+ax+b$;或当 $p=2$,$y^2+xy=x^3+ax^2+b$。P 是 $E(F_p)$ 中阶为 q 的一个基点,q 为大素数。

1.1　椭圆曲线上离散对数问题(DLP)

G 是由点 P 生成的循环加群,给定 Q,找到正整数 n,使得 $Q=nP$。

1.2　椭圆曲线 Diffie-Hellman 密钥交换协议(ECDH)

A 选择随机数 $a\in F_q$ 并计算 $P_A=aP$ 发送给 B;B 选择随机数 $b\in F_q$ 并计算 $P_B=bP$ 发送给 A。A 和 B 分别计算 aP_B、bP_A,从而得到共同的会话密钥 $K=(ab)P$。

1.3　自验证公钥密码学

自验证公钥结合了基于证书和基于身份的密码学的优点,提供了认证用户公钥的机制[14~16]。用户的公钥可由系统权威 SA 对用户身份的签名直接计算。下面是一个简单的自验证公钥机制。

1)系统建立　SA 选择一个非奇异的定义在有限域 F_q 上的椭圆曲线 E,生成元 P 的阶为 n。SA 选择密钥对(s_s,Pk_s),这里 $Pk_s=s_sP$。相关参数 E、P、n、Pk_s 是公开的,s_s 是秘密值。

2)私钥生成　用户 U 选择随机数 k_u,计算 $K_u=H_1(\mathrm{ID}_u,k_u)P$,将 ID_u、K_u 通过安全信道发送给 SA。SA 收到消息后,选取随机数 r_u,计算用户 U 的公钥证据 $R_u=K_u+r_uP$ 和部分私钥 $x_u=H_2(\mathrm{ID}_u,R_u)s_s+r_u$。然后 SA 将 R_u、x_u 返回给用户 U,用户 U 计算私钥 $s_u=x_u+H_1(\mathrm{ID}_u,k_u)$。

3)公钥生成　基于预操作,用户 U 收到公钥证据 R_u 后,计算相应的公钥 $Pk_u=H_2(\mathrm{ID}_u,R_u)Pk_s+R_u$。

4)正确性　公钥能够被正确计算:

$$PK_u=s_uP=x_uP+H_1(\mathrm{ID}_u,k_u)P=H_2(\mathrm{ID}_u,R_u)s_sP+r_uP+H_1(\mathrm{ID}_u,k_u)P=H_2(\mathrm{ID}_u,R_u)Pk_s+R_u$$

2　协议描述

基于自验证公钥的跨域口令认证密钥协商协议具体内容包含系统参数选择、系统初始化、认证和密钥协商以及密钥更新四部分。

2.1　系统参数选择

系统存在一个持有公私钥对(s_s,Pk_s)的系统权威 SA,负责选取系统的安全参数,同时与各安全域服务器线下交互,产生域服务器的自验证公私钥对以及公钥证据。S_A 和 S_B 分别是安全域 A 和 B 的域服务器。U_i 是来自安全域 A 的用户,U_j 是来自安全域 B 的用户。pw_i 和 pw_j 分别是用户 U_i 和 U_j 与各自域服务器共享的口令信息。域服务器 S_A 和 S_B 分别持有公私钥对和公钥证据(s_A,PK_A,R_A)和(s_B,PK_B,R_B)。P 是 q 阶循环群 Z_q^* 的生成元,$H:\{0,1\}^*\rightarrow\{0,1\}^l$ 是哈希函数。

2.2　初始化过程

首先,SA 利用自验证公钥密码学为域 A 中的服务器 S_A 产生公私钥和公钥证据(s_A,PK_A,R_A)。其次,各安全域中的用户 U_i 和 U_j 分别与相应的域服务器 S_A 和 S_B 共享口令 pw_i 和 pw_j。此外,SA 同时在初始化阶段还定义了一系列系统运行所需的密码学函数和参数,如 hash 函数的选取,公开系统参数 Z_q^*、P、PK_s、H 等。

2.3　协议运行

当处于 S_A 的安全域中的用户 U_i 需要与处于 S_B 的安全域中的用户 U_j 建立安全信道时,U_i 发起会话。协议的具体描述如下:

a)U_i 选取随机值 $x_i\in Z_q^*$,计算 $K_{iA}=(x_i+H(\mathrm{ID}_i,pw_i))PK_A$ 和 $X_i=x_iP$。随后,A 利用 X_i 和 K_{iA} 计算验证信息 V_i,$V_i=H(\mathrm{ID}_i,\mathrm{ID}_j,\mathrm{ID}_A,\mathrm{ID}_B,X_i,K_{iA})$。然后将 X_i 和 V_i 发送给服务器 S_A。

b)收到消息后,S_A 首先利用 X_i 计算 $K_{Ai}=s_A(X_i+H(\mathrm{ID}_i,pw_i)P)$,再计算验证信息 $V'_i=H(\mathrm{ID}_i,\mathrm{ID}_j,\mathrm{ID}_A,\mathrm{ID}_B,X_i,K_{Ai})$,通过验证 $V_i\overset{?}{=}V'_i$ 是否相等,以此判断用户 U_i 的通信请求是否合法。如果不相等,则终止协议;如果相等,则 S_A 选取 s_i 计算 $k=s_iX_i$ 作为用户 U_i 与 U_j 间的认证密钥。然后利用自己的私钥 s_A 和 U_j 所在安全域的服务器 S_B 的公钥 PK_B 计算域间安全会话的密钥 $K_{AB}=s_APK_B$。此后,S_A 分别计算 $E_i=E_{K_{Ai}}(\mathrm{ID}_i,\mathrm{ID}_j,S_i)$ 和 $\mathrm{Ticket}_{ij}=[\mathrm{ID}_i,\mathrm{ID}_j,k,L]_{K_{AB}}$,并将 E_i 和 Ticket_{ij} 发送给 U_i。

c)U_i 收到消息后,用 K_{Ai} 解密消息 E_i 获取 ID_i、ID_j、S_i,并检查前两者是否是正确的信息。如果不是,则终止协议;如果是,则选取 $a_i\in Z_q^*$ 计算 $k=x_iS_i$ 和 $b_i=H(\mathrm{ID}_i,\mathrm{ID}_j,a_iP,k)$。然后将$\{\mathrm{ID}_i,\mathrm{ID}_j,a_iP,b_i,\mathrm{Ticket}_{ij}\}$发送给 U_j。

d)U_j 收到信息后,执行与 U_i 在第一步中类似的操作,生成 X_j、V_j,并将$\{\mathrm{ID}_i,\mathrm{ID}_j,X_j,V_j,\mathrm{Ticket}_{ij}\}$发送给 S_B。

e)S_B 收到 U_j 的消息后,首先利用私钥 s_B 和接收到的消息 X_j 计算密钥 $K_{Bj}=s_B(X_j+H(\mathrm{ID}_j,pw_j)P)$ 和 $V'_j=H(\mathrm{ID}_i,\mathrm{ID}_j,\mathrm{ID}_A,\mathrm{ID}_B,X_j,K_{Bj})$,通过验证 $V_j\overset{?}{=}V'_j$ 是否相等来判断通信请求是否合法。如果不等,则协议终止;如果相等,则进行下一步操作。其次,S_B 用自己的私钥和 U_i 所在的安全服务器 S_A 的公钥

计算对称加密密钥 $K_{BA}=s_BPK_A$。S_B 用密钥 K_{BA} 解密 Ticket_{ij} 获取[ID_i,ID_j,k,L];再次,S_B 通过检查时间戳 L 和身份信息 ID_i 来验证 Ticket_{ij} 的有效性。最后,S_B 用对称密钥 K_{Bj} 加密消息 ID_i、ID_j、k,并将加密结果返回给 U_j。

f) U_j 解密收到的消息获取 ID_i、ID_j、k 之后,检查身份信息是否合法。如果不合法,协议终止;否则,用密钥 k 验证从 U_i 处接收到的认证信息的合法性。如果验证没有通过,则终止协议;否则,U_j 随机选取 $a_j\in Z_q^*$ 并计算 a_jP,$sk_{ji}=H(\mathrm{ID}_i,\mathrm{ID}_j,a_ja_iP,k)$ 和验证信息 $b_j=H(\mathrm{ID}_i,\mathrm{ID}_j,a_jP,k,sk)$。然后将 a_jP 和 b_j 发送给 U_i。

g) 收到消息 a_jP 和 b_j 后,U_i 分别计算 $sk_{ij}=H(\mathrm{ID}_i,\mathrm{ID}_j,a_ia_jP,k)$ 以及相应的验证信息 $b'_j=H(\mathrm{ID}_i,\mathrm{ID}_j,a_jP,k,sk)$,然后验证 b'_j 与 b_j 是否相等。如果不等,U_i 终止会话;否则,U_i 计算 $c_i=H(\mathrm{ID}_j,\mathrm{ID}_i,a_iP,a_jP,k,sk)$,并将其发送给 U_j 确认。

h) U_j 通过验证收到的消息 c_i 来验证 U_i 的合法性。如果不合法,U_j 终止会话;否则,生成会话密钥 sk。

3 协议分析

对协议的分析主要从协议的效率和安全性两个方面展开。协议效率主要考虑了协议的计算代价和通信代价。协议安全性主要考虑协议能否抵抗字典攻击和未知密钥共享攻击以及协议是否能够实现会话密钥的公平性、新鲜性、前向安全性和已知会话密钥安全等属性。

3.1 效率分析

以下将比较本文新协议和文献[6,9,12]中的协议。为了更好地刻画协议的计算代价,采用了下列符号表示各种不同运算所需的时间以及相应的对比关系[17]:T_S 表示一次对称加密所需时间;T_{Mul} 表示一次乘法运算所需时间;T_{Exp} 表示一次模幂运算所需时间,且 $1T_{\mathrm{Exp}}\simeq 240T_{\mathrm{Mul}}$;$T_{\mathrm{EC_{Mul}}}$ 表示一次椭圆曲线上的点乘运算所需的时间,$1T_{\mathrm{EC_{Mul}}}\simeq 29T_{\mathrm{Mul}}$;$T_{\mathrm{Sig}}$ 表示一次签名或验证签名所需要的时间;T_{PE} 表示一次公钥加密或解密所需时间。由于哈希运算所需时间较少,在此将忽略这部分时间。与相关协议相比,新协议避免了消耗较高的模幂运算和对运算。表 1 分别分析了各协议中各个参与方的计算代价,然后求和并按照转换关系进行转换,对计算消耗总量加以比较。由表 1 可以发现,新协议在单个参与方的计算量和总计算量上均占优势。此外,表 1 中还展示了各个协议所需要的通信代价,新协议比文献[6,9]中的协议至少少了一步。因此,与同类协议相比,新协议在通信消耗和计算消耗方面均较优。

表 1 几种协议的效率比较

		文献[6]	文献[9]	文献[12]	新协议
计算消耗	U_i	$3T_S+3T_{\mathrm{Exp}}$	$2T_S+4T_{\mathrm{Exp}}+1T_{\mathrm{Sig}}$	$1T_S+2T_{\mathrm{Exp}}+1T_{\mathrm{Sig}}$	$1T_S+3T_{\mathrm{EC_{Mul}}}$
	U_j	$3T_S+3T_{\mathrm{Exp}}$	$1T_S+3T_{\mathrm{Exp}}+1T_{\mathrm{Sig}}$	$1T_S+3T_{\mathrm{Exp}}+1T_{\mathrm{Sig}}$	$1T_S+3T_{\mathrm{EC_{Mul}}}$
	S_A	$4T_S+1T_{\mathrm{Exp}}$	$3T_S+1T_{\mathrm{Exp}}+2T_{\mathrm{Sig}}+1T_{PE}$	$3T_S+1T_{\mathrm{Exp}}+1T_{\mathrm{Sig}}$	$2T_S+3T_{\mathrm{EC_{Mul}}}$
	S_B	$4T_S+1T_{\mathrm{Exp}}$	$4T_S+1T_{\mathrm{Exp}}+2T_{\mathrm{Sig}}+1T_{PE}$	$3T_S+4T_{\mathrm{Exp}}+1T_{\mathrm{Sig}}$	$2T_S+2T_{\mathrm{EC_{Mul}}}$
	总计	$14T_S+1920T_{\mathrm{Mul}}$	$10T_S+2160T_{\mathrm{Mul}}+6T_{\mathrm{Sig}}+2T_{PE}$	$8T_S+4T_{\mathrm{Sig}}+2400T_{\mathrm{Mul}}$	$6T_S+11T_{\mathrm{EC_{Mul}}}$
轮数		8	9	7	7

3.2 安全性分析

1) 抵抗字典攻击 在三类字典攻击中,离线字典攻击是指攻击者不参与协议,只利用窃听到的信息验证猜测的口令是否正确;在线字典攻击是指攻击者参与协议,利用截获或者窃听到的信息伪造新的与口令相关的信息发送至协议的某参与方,结合该参与方的输出判断自己的猜测是否正确。此外,又依据攻击者猜测到错误的口令信息能否被该参与方察觉分为在线可测和在线不可测两类。首先,对于离线字典攻击,以用户 U_i 为例,协议中传递的与口令相关的信息仅有利用信息 $K_{iA}=(x_i+H(\mathrm{ID}_i,pw_i))PK_A$ 计算的 $V_i=H(\mathrm{ID}_i,\mathrm{ID}_j,\mathrm{ID}_A,\mathrm{ID}_B,X_i,K_{iA})$,而计算 K_{iA} 所需的信息除口令 pw_i 外,还需要用户 U_i 选取的随机值 x_i,x_i 是以其离散对数的形式传递的。这导致敌手缺乏足够的信息验证其猜测的口令是否正确。因此,离线字典攻击可以避免。其次,协议中的域服务器在解密消息后均会验证被加密的信息是否与自己掌握的信息一致,以此来确定发送该信息的用户是否掌握正确的口令信息。也就是说,攻击者的错误猜测能够被参与方察觉。因此,在线不可测字典攻击可以抵抗。再次,一旦某用户提交的信息验证失败的次数超过预定的门限值,该域服务器就会意识到该用户口令已经成为在线字典攻击的目标。然后域服务器将通知该用户停止使用该口令并启用新的口令。因此,协议可以抵抗在线可测字典攻击。

2) 抵抗口令泄露模仿攻击 口令泄露模仿攻击是指如果一个用户的口令泄露,攻击者可以伪装成其他用户来与该用户进行交互协商会话密钥,以达到其攻击目的。新协议中,即使用户 U_i 的口令信息泄露,攻击者能够计算 $H(\mathrm{ID}_i,pw_i)P$,但由于攻击者没有获取域服务器 S_A 的私钥信息 s_A,所以仍然无法计算正确的密钥信息 $K_{Ai}=s_A(X_i+H(\mathrm{ID}_i,pw_i)P)$,无法产生合法的加密信息返回给用户 U_i。因此,新协议能够抵抗口令泄露模仿攻击。

3) 抵抗未知会话密钥共享攻击 未知会话密钥共享攻击是指攻击者能够使得致使用户 U_i 认为自己与用户 U_j 共享了一个会话密钥,实际上这个会话密钥由用户 U_i 与攻击者共享。协议运行时参与方不能发现其他参与方的身份信息被替换是产生此类攻击的根本原因。新协议中,协议所有参与方的身份信息均与协议运行的其他信息一起经过只有通信双方才能产生的密钥加密或者产生相应的 hash 值同步传递,接收方可以验证发送方的消息是否被窜改。因此,新协议从根本上避免了此类问题的发生,协议能够抵抗未知会话密钥共享攻击。

4) 前向安全性 各参与方单独选取的随机数构成了协议的最终会话密钥,并且协议传递的信息是随机数所对应的离散对数形式。由于椭圆曲线上离散对数问题的困难性,攻击者获得用户的口令信息或者域服务器的长期私钥无助于其获取参与方选择的随机数。因此,攻击者仍然不能计算正确的会话密钥。所以,协议能够实现会话密钥的前向安全性。

5) 会话密钥公平性 协议使用 Diffie-Hellman 密钥协商的思想产生最终的会话密钥,同时随机数 a_i 是由用户 U_i 随机选取的,随机数 a_j 是由用户 U_j 随机选取的。因此,任何一方不能单独控制会话密钥的选择,实现了会话密钥的公平性。

6) 已知会话密钥安全 攻击者获取一次通信的会话密钥,仍然不能获取其他次通信的会话密钥。这是因为通信双方最终获取的会话密钥是由随机数构成的,而这些随机数是由参与方在每次通信时随机选取的。随机数的不相关性使得攻击

者即使获取了一次通信的会话密钥也无法利用该信息去获取另一次通信的会话密钥,以此实现了已知密钥安全。

4　结束语

本文结合自验证公钥密码学和口令信息,提出了一个用户直接通信的跨域口令认证密钥协商协议。域服务器间通过自验证公钥密码学实现相互认证和密钥协商。域服务器通过口令认证实现对域内用户的认证,并协助用户完成认证和生成密钥,但不能获取最终的会话密钥。分析结果表明,与同类协议相比,新协议计算代价和通信代价均较低,且能抵抗字典攻击和未知会话密钥共享攻击。协议同时保证了会话密钥的公平性、前向安全和已知会话密钥安全等属性的实现。

参考文献:

[1] BYUN J W, JEONG I R, LEE D H, *et al*. Password-authenticated key exchange between clients with different passwords[C]//LNCS, vol 2513. 2002:134-146.

[2] CHEN L. ISO/IEC JTC 1/SC27 N3716, A weakness of the password-authenticated key agreement between clients with different passwords scheme[S]. 2003.

[3] KIM J, KIM S, KWAK J, *et al*. Cryptanalysis and improvement of password-authenticated key exchange scheme between clients with different passwords[C]//LNCS, vol 3043. 2004:895-902.

[4] PHAN R C W, GOI B M. Cryptanalysis of an improved client-to-client password-authenticated key exchange (C2C-PAKE) scheme [C]//LNCS, vol 3531. 2005:33-39.

[5] WANG Shu-hong, WANG Jie, XU Mao-zhi. Weaknesses of a password-authenticated key exchange protocol between clients with different password[C]//LNCS, vol 3089. 2004:414-425.

[6] BYUN J W, LEE D H, LIM J I. EC2C-PAKA: an efficient client-to-client password-authenticated key agreement [J]. Information Science, 2007, 177(19):3995-4013.

[7] WANG Feng-jiao, ZHANG Yu-qing. Cryptanalysis of a client-to-client password-authenticated key agreement protocol, Report 2008/248[R/OL]. (2008). http://eprint. iacr. org/.

[8] PHAN R C W, GOI B M. Cryptanalysis of two provably secure cross-realm C2C-PAKE protocols[C]//Proc of INDOCRYPT. 2006:104-117.

[9] FENG Deng-guo, XU Jing. A new client-to-client password-authenticated key agreement protocol[C]//Proc of IWCC. 2009:63-76.

[10] 陈安林,潘进,郭超,等. 移动自组网中跨域两方认证密钥协商协议研究[J]. 计算机应用研究,2011,28(7):2734-2737.

[11] 刘小琼,潘进,李国朋. 基于无证书的两方跨域认证密钥协商协议[J]. 计算机应用研究,2012,29(2):646-649.

[12] 王涛. 跨域客户间口令认证的密钥交换协议[J]. 计算机工程与设计,2012,33(7):2546-2549.

[13] CHEN Li-qun, HOON W L, YANG Guo-min. Cross-domain password-based authenticated key exchange revisited[C]//Proc of the 32nd IEEE International Conference on Computer Communications. 2013:1052-1062.

[14] GIRAULT M. Self-certified public keys[C]//Proc of EUROCRYPT. 1991:490-497.

[15] PETERSEN H, HORSTER P. Self-certified keys—concepts and applications[C]//Proc of Communications and Multimedia Security. Boca Raton: Chapman and Hall. 1997:102-116.

[16] SAEEDNIA S. Identity-based and self-certified key-exchange protocols[C]//Proc of ACISP. 1997:303-313.

[17] KOBLITZ N, MENEZES A, VANSTONE S. The state of elliptic curve cryptography[J]. Journal of Design, Codes and Cryptography, 2000, 19(2-3):173-193.

(上接第 3789 页)

[3] AI-MAMORY S O, ZHANG Hong-li. Intrusion detection alarm reduction using root cause analysis and clustering[J]. Journal of Computer Communication, 2009, 32(2):419-430.

[4] GADDAM S R, PHOHA V V, BALAGANI K S. K-means + ID3: a novel method for supervised anomaly detection by cascading K-means clustering and ID3 decision tree learning methods[J]. IEEE Trans on Knowledge and Data Engineering, 2007, 19(3):345-354.

[5] 韩占柱. 改进 K-means 算法的网络数据库入侵检测[J]. 微电子学与计算机,2012,29(3):144-150.

[6] PIETRASZEK T. Using adaptive alert classification to reduce false positives in intrusion detection [C]//Lecture Hotes in Computer Science, vol 3224. 2004:102-124.

[7] 李金凤,王怀彬. 基于关联规则的网络故障告警相关性分析[J]. 计算机工程,2012,38(5):44-46.

[8] VIINIKKA J, DEBAR H. Processing instrusion detection alert aggregate with time series moding[J]. Information Fusion, 2009, 10(2):312-324.

[9] 梅海彬,龚俭. 多 IDS 环境中基于可信度的警报关联方法研究[J]. 通信学报,2011,32(4):138-145.

[10] 张亚普,孟相如,张立,等. 基于 SVM 和模糊逻辑的告警相关性分析[J]. 计算机应用研究,2011,28(2):685-688.

[11] 闫生超,唐云善,张春平,等. 基于网络和时间关联关系的告警相关性分析[J]. 电力系统自动化,2011,35(9):78-87.

[12] KIM D S, SHINBO H, YOKOTA H. An alarm correlation algorithm for network management based on root cause analysis[J]. International Journal of Computer Science and Network Security, 2011, 9(12):1233-1238.

[13] YASAMI Y, MOZAFFARI S P. A novel unsupervised classification approach for network anomaly detection by K-means clustering and ID3 decision tree learning methods[J]. Journal of Supercomputing, 2010, 53(1):231-245.

[14] HARIRI A, RASTEGAR R, NAVI K, *et al*. Cellular learning automata based evolutionary computing for intrinsic hardware evolution [C]//Proc of NASA/DoD Conference on Evolvable Hardware. 2005:294-297.

[15] MITCHELL T. Machine learning[M]. New York: McGraw-Hill, 2004.

[16] CHEN Yan, LEE J. Autonomous mining for alarm correlation patterns based on time-shift similarity clustering in manufacturing system [C]//Proc of IEEE Internation Conference on Prognostics and Health Management. 2011: 365-371.

[17] HAN Jia-wei, KAMBER M. Data mining: concepts and techniques [M]. San Mateo: Morgan Kaufmann, 2006.

[18] IMANAZARI M, NOORHOSSEINI S M, AKBARI F. Dynamic alarm correlation based on cellular learning automata in telecommunication networks[J]. Internation Journal of Computer Science and Network Security, 2009, 9(12):168-173.

[19] WALLIN S. Chasing a definition of "alarm"[J]. Journal of Network and Systems Management, 2009, 17(4):457-481.