一种可证安全的基于浏览器的联合身份管理双向认证协议*

王 凯[1]，祝跃飞[1]，林 敏[2]
（1. 解放军信息工程大学，郑州 450002；2. 河南工业大学，郑州 450000）

摘 要：提出了一种基于浏览器的联合身份管理双向认证协议，在 TLS 会话中采用人类可感知认证码验证身份权威服务器，通过绑定客户端证书结合加强同源策略达到双向保护令牌的目的。最后用形式化模型分析了其安全性，证明了协议能够提供安全的认证。

关键词：联合身份管理；基于浏览器的身份认证；人类可感知认证码；安全令牌
中图分类号：TP309 **文献标志码**：A **文章编号**：1001-3695(2013)06-1843-04
doi:10.3969/j.issn.1001-3695.2013.06.063

Provably secure browser-based mutual authentication protocol for federated identity management

WANG Kai[1], ZHU Yue-fei[1], LIN Min[2]
(1. *Information Engineering University of PLA*, *Zhengzhou* 450002, *China*; 2. *Henan University of Technology*, *Zhengzhou* 450000, *China*)

Abstract: This paper proposed a browser-based mutual authentication for federated identity management, which identified the identity authority based on human perceptible authenticators in a TLS session and protected the token mutually by binding the client certificate and using stronger same origin protocol. The paper analysed the security of the protocol in the formal model, and proved that the protocol could provide secure authentication.

Key words: federated identity management(FIM); browser-based authentication; human perceptible authenticators; security token

0 引言

联合身份管理(FIM)是指让用户用同样的身份标志数据来获得所有参与联合服务的进入许可。该技术能够有效地降低服务提供商(service provider)身份管理的难度，并减少用户管理身份的成本和风险。在 FIM 协议框架中，用户使用浏览器等作为用户代理(user agent)与服务提供方、身份权威(identity authority)交互。当用户访问服务需要进行认证授权，服务提供方将认证交给信任的身份权威。身份权威验证用户并产生一个安全令牌给用户，用户交予服务提供方验证授权。主要的 FIM 产品包括微软的 Passport 及其后续产品 CardSpace 和 CardSpace 2.0(更名为 U-Prove)、Athens 及其替代者 Shibboleth、基于安全断言标记语言(security assertion markup language，SAML)的自由联盟框架(liberty alliance project)。目前这些 FIM 方法的安全性并没有得到足够的保证，大量文章研究报道了 FIM 可能遭受的多种攻击，尤其在基于浏览器的实现中存在一些问题：

a)相关研究表明，普通的网络用户并不能理解服务器证书，也不能很好地识别浏览器的安全指示。

b)所有通过浏览器发送的数据都被保存在浏览器的文档对象模型(document object model，DOM)中，DOM 仅受同源策略(same origin policy，SOP)保护，而 SOP 可以很容易被针对域名解析的相关攻击所欺骗，包括跨站攻击和域欺骗攻击等，使得所有的数据都可能被恶意的脚本访问。

c)浏览器只能通过身份权威产生令牌和通过 TLS 加密保护传输数据，所以这些令牌都不能与合法的客户端通过加密方式结合，从而可以很轻易地被使用上述攻击方法偷取令牌的攻击者所使用。

本文提出一种基于浏览器的联合身份管理双向认证协议(BBFIM)，其内容包括：

a)用户感知的与身份权威的双向认证。考虑到减少用户对固定浏览器和外接设备的依赖性以及静态密码的不安全性，用户验证方法为一次性密码(one time password，OTP)(可选与静态密码结合)，身份权威的验证则需要提供一个用户预留的人类可感知认证码(human perceptible authenticator，HPA)，如文字、声音、图像等。

b)通过加强 SOP 对服务器进行认证。身份权威除了产生一个令牌外，还为浏览器提供联盟内所有服务提供方的(服务器，公钥)对，以此作为 SOP 的源因子，加强对服务器的验证。

c)将令牌和合法的客户端绑定。身份权威为浏览器生成一个客户端证书，并将令牌与公钥证书进行绑定。考虑到攻击者并不能访问证书的私钥，从而即使攻击者获得了令牌，也由于不能证明自己对客户端证书的合法拥有而无法正常使用令牌。

收稿日期：2012-09-14；**修回日期**：2012-10-30 **基金项目**：郑州市科技创新团队基金资助项目(10CXTD150)

作者简介：王凯(1989-)，男，安徽滁州人，硕士研究生，主要研究方向为网络安全、密码(quanjiaokk@gmail.com)；祝跃飞(1962-)，男，教授，博导，主要研究方向为密码理论及信息安全；林敏(1981-)，男，湖南汉寿人，硕士研究生，主要研究方向为车载网络安全.

1 相关研究

Kormann 等人[1]表明了 Passport 系统容易被攻击者从 cookie 中窃取票据,Slemko 随后公布了一个对微软 Passport 系统的攻击。Groβ[2]分析了 SAML 容易被攻击者拦截攻击获得 URL 中的认证令牌。Gajek 等人[3,4]研究了一种可以应用于 CardSpace 以及 SAML 框架的攻击。

针对以上攻击,Bruegger 等人[5]提出一种安全方法 TLS-Federation,使用 X.509 客户端证书扩展包含令牌作为身份信息,从而加强对客户端的验证。事实上,这也可以利用 SAML v2.0 方法,通过将公钥置于 Holder-of-Key 断言中完成对 SAML 令牌的加密[6]。Gajek 等人[7]提出一种基于浏览器的 Kerberos 认证方法,将客户端证书与令牌进行绑定,从而保证令牌的合法使用。然而基于用户弱安全性假定,还应该考虑对服务器欺骗进行防护。基于 Karlof 等人[8]提出的 SLSO(strong locked same origin policy)(使用服务器的公钥作为 SOP 的源因子,而不是不安全的 DNS),Gajek 等人[9]针对 LA 和 LBP 框架提出了一种加强的约束方法。本文在对用户弱安全能力的假定下,提出了一种普适的基于浏览器的联合身份管理认证协议,用不同的方法分别对两种服务器进行验证,将安全令牌与合法用户进行有效的绑定,并通过形式化模型对协议进行描述和安全分析。

2 基于浏览器的认证协议的形式化安全模型

2.1 协议参与者及相应的能力和密钥

协议的参与者包括身份权威服务器 I,服务提供方 S,客户端 $C:=(U,B)$,其中 B 为浏览器,U 为用户。U 的模型是一个计算能力有限的概率机器,可以识别 HPA,并能利用某种带外手段(如短信或口令卡)获得一次性密码。定义 U 的密钥为长期密钥 $LL_U:=(\text{uname},\text{OTP}(k),w\in W)$,包括与 I 通过某种带外机制进行注册的用户名、HPA 以及 OTP 获取方法,其中 $k\in\mathbf{N}$ 是协议的安全参数,W 为 HPA 空间。B 是一个与服务器交换协议消息的概率多项式时间(probabilistic polynomial time, PPT)机器。浏览器负责对收到的一个消息 $m\in M$,根据浏览器的状态 $\psi\in\{0,1\}^{\lambda_1(k)}$ 进行相应的处理,包括将 HPA 展示给用户以及存储令牌信息,其中 $M\in\{0,1\}^{\lambda_2(k)}$ 是指所有 Web 对象的消息空间,$\lambda_i:\mathbf{N}\to\mathbf{N},i\in[1,2]$ 是一个多项式,ψ 表示浏览器对于消息处理的配置,可以被浏览器的 DOM 模型更改。另外浏览器 B 可以利用不同的设备接口接收用户输入,如鼠标、键盘等。定义其密钥为短期密钥 $SL_B^{\text{Aftaut}}:=(\text{cert}_B,\text{sk}_B,\text{token}^*,\{(S,pk_S)\mid S\in FS\})$,包括用户被 I 认证后生成的证书、加密令牌以及所有联盟内 S 的(域名,公钥)对,用户退出时删除(可选),存在一定有效期。身份权威服务器 I 是一般的 PPT 机器,定义其密钥为长期密钥 $LL_I:=(\text{cert}_I,sk_I,(\text{uname},\text{OTP}(k),w),\{(S,pk_S\mid S\in FS)\})$,包括其证书及相应的私钥、与用户共享的长期密钥、联盟 FS 内所有 S 的(域名,公钥)对。服务提供方 S 是一般的 PPT 机器,定义其密钥为长期密钥 $LL_S:=(\text{cert}_S,sk_S,\text{cert}_I)$,包括其证书及相应的私钥、$I$ 的公钥证书。

2.2 攻击者能力

对手 A 能够控制所有的通信过程,并且可以通过控制域名解析使得伪造的服务器证书被用户接受,从而使得 A 能够访问浏览器的 DOM 模型。考虑到对操作系统的恶意软件攻击可以破坏几乎所有加密协议的安全性(进一步地,安全协议可以通过结合可信平台计算对恶意软件攻击进行防护),本文不考虑对手 A 对浏览器 B 以及服务器 I 和 S 所在平台的恶意软件攻击,因此 A 不能窃取平台内存储的秘密信息,如证书私钥。同样地不考虑对手通过物理手段获得用户的密钥。

定义 A 通过以下请求参与协议的执行:

a) $\text{Execute}(C,P)(P\in\{I,S\})$。窃听协议会话的执行,并获得相应的会话副本。

b) $\text{Invoke}(C,P)(P\in\{I,S\})$。执行一个新的协议实例,并通过 B 获得第一条协议消息。

c) $\text{Send}(P,m)(P\in\{C,I,S\})$。向某协议参与方发送一个消息,并收到相应的响应。

d) $\text{RevealDOM}(C)$。窃取浏览器 DOM 中存储的信息。

2.3 攻击游戏

为了区别不同的实例,每个协议参与者用一个 $\text{cid}\in\mathbf{N}$ 表示通信标志符。当 $\text{cid}_C=\text{cid}_S$ 或者 $\text{cid}_C=\text{cid}_I$ 时认为两个实例属于同一个会话,称两个实例配对。如果在执行中,双方认证成功,则互相接受,否则实例中止。由此给出定义:

定义 1 当每一个 $\text{Execute}(C,P)(P\in\{I,S\})$ 请求结果产生两个配对的实例,并互相接受,称 BBFIM 协议 Π 正确。

定义 2 假设 BBFIM 协议 Π 正确,$\text{Game}_{\Pi}^{\text{BBFIM}}(A,k)$ 是 C、I、S 的实例和符合上述能力假设的对手 A 之间的交互过程。交互中下列情况出现,称 A 赢得攻击游戏。

a) 一个实例 $[C,\text{cid}_C]$ 接受,但是没有配对的实例 $[S,\text{cid}_S]$,或者反之;

b) 一个实例 $[C,\text{cid}_C]$ 接受,但是没有配对的实例 $[I,\text{cid}_I]$,或者反之。

对于所有以安全参数 k 运行的 PPT 对手,赢得攻击游戏的最大可能性定义为

$$\text{Succ}_{\Pi}(A,k)=\max_A\mid Pr[A.\text{ wins. in. Game}_{\Pi}^{\text{BBFIM}}(A,k)]\mid$$

当该函数为 k 的可忽略函数,协议 Π 可以提供安全的认证。

3 安全协议

3.1 加密模块

BBFIM 的主要组成部分是 TLS 协议,在其密钥协商之后完成认证,本文使用协议规范中最常见的基于 RSA 的加密组件,包括如下(为了构造 k 的可忽略函数,协议将以下加密模块形式化为运行在 k 的多项式时间上的概率图灵机,即对不同参数的不同长度用多项式 $p_i:\mathbf{N}\to\mathbf{N},i\in[1,5]$ 构造):

a) 伪随机函数 $\text{PRF}_i:\{0,1\}^{p_1(k)}\times\{0,1\}^*\to\{0,1\}^*,i\in[1,4]$,该函数用来派生不同长度的密钥。用 $\text{Adv}_{\text{PRF}}^{\text{prf}}(k)$ 定义所有 PPT 对手辨别 PRF 输出的最大优势。

b) 提供 CUF-CPA 安全的函数 MAC-Enc 和相应的验证函数 Dec-MAC,该函数先计算消息验证码再对称加密,定义其中对称加密算法为 $(s\text{Enc},s\text{Dec})$,消息验证码函数为 MAC,则 $\text{Dec-MAC}_{k_1,k_2}(m^*,m):=(S\text{Dec}_{k_1}(m^*)==m\mid\text{MAC}_{k_2}(m))$,$\text{MAC-Enc}_{k_1,k_2}(m):=s\text{Enc}_{k_1}(m\mid\text{MAC}_{k_2}(m))$,其中 m 为传输的消息。用 $\text{Adv}_{\text{MAC-Enc}}^{\text{cuf-cpa}}(k)$ 定义所有 PPT 对手破坏 CUF-CPA 安全性的最大优势。这里在文献[6]的基础上将消息验证码函数和对称加密函数结合视为一个函数,因为消息传输总是先计算

消息验证码再加密,其安全性由两者共同决定[13]。

c)提供 IND-CPA 安全的非对称加密算法(asEnc,asDec)。用 $\mathrm{Adv}^{\text{ind-cpa}}_{(\text{asEnc},\text{asDec})}(k)$ 定义所有 PPT 对手破坏(asEnc,asDec)的 IND-CPA 安全性的最大优势。

d)抗冲突的哈希函数 hash:$\{0,1\}^{*}\rightarrow\{0,1\}^{p_2(k)}$。用 $\mathrm{Succ}^{\text{coll}}_{\text{hash}}(k)$ 定义所有 PPT 对手成功找到一个哈希冲突的最大可能。

e)提供 EUF-CMA 安全的数字签名函数 Sig 和相应的验证函数 Ver。用 $\mathrm{Succ}^{\text{euf-cma}}_{(\text{Sig},\text{Ver})}(k)$ 定义所有具有签名谕示的 PPT 对手成功找到一个伪造签名的最大可能。

3.2　协议描述

3.2.1　初始化阶段

在协议执行之前,需要一些注册过程,完成以下内容的交互或注册(这些交互过程一般是某些带外机制,或者通过其他途径保证网络通道的安全,如监测软件等):

a)C 向 I 注册用户名、HPA,并获得带外的一次性密码获得方法 $\mathrm{OTP}(k)\in\{0,1\}^{p_4(k)}$,如口令卡或注册手机号。为了简化协议,这里假设使用口令卡直接获得。

b)C 和 S 注册各自的私钥和证书对,这里假设相应的公钥可以从证书中获得。

c)C 和 S 之间交互(S,pk_S)对以及 cert_I。

3.2.2　C 和 I 之间的交互

当 C 通过 URL 向 S 请求服务时,如果 B 存在 SL_B^{Aftaut},则协议直接进入 3.2.3 节,否则 S 通过重定向码先让 C 与 I 交互。

在请求阶段,双方交互各自产生的随机数,并计算得到通信标志符 $\mathrm{cid}_C=r_C|r_I$,同时 I 将证书发送给 C。在密钥协商阶段,会话密钥(包括对称密钥 k_1 和 MAC 密钥 k_2)通过主密钥 k_m 产生,k_m 由预主密钥 k_p 产生,k_p 由 C 随机选择,并通过 pk_I 加密传送给 I。C 和 I 从所有之前处理的消息(这里简写为 prev)出发,先哈希,再计算 PRF,通过会话密钥加密完成双方会话密钥的确认,如图 1 所示。

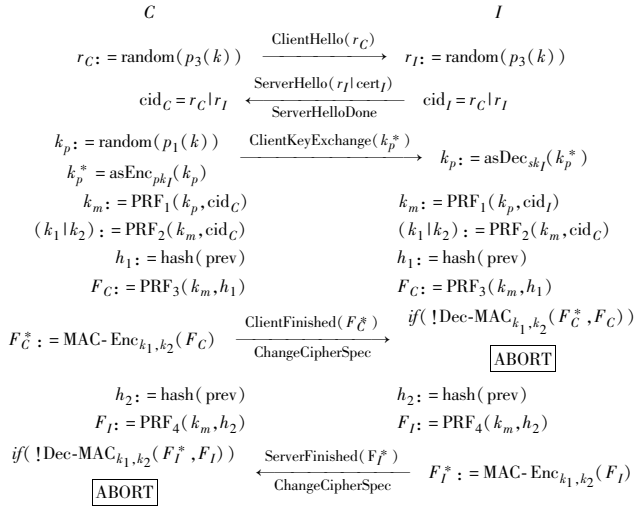

图 1　C 和 I 之间的密钥协商

加密传输阶段,C 将用户名和一次性密码发送给 I 进行验证,验证成功后 I 将相应的 w 发送给 C。I 与 C 互相验证后,I 为客户端生成令牌和证书,将它们与(S,pk_S)对发送给 C,其中需将令牌与证书公钥绑定并通过 I 私钥签名,C 将其存储在浏览器中,即 SL_B^{Aftaut}。如图 2 所示,其中省略 Dec-MAC$_{k_1,k_2}$ 的默认验证。

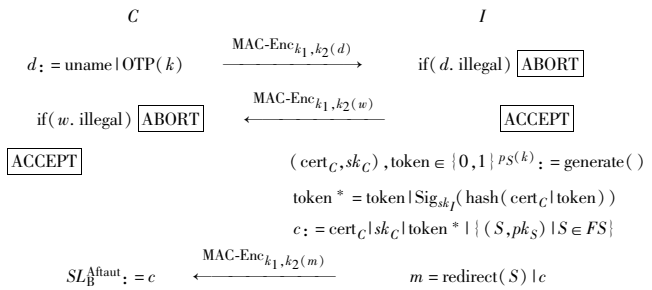

图 2　C 和 I 之间的相互认证

3.2.3　C 和 S 之间的交互

请求阶段与密钥协商阶段与 3.2.2 节完全相同,仅增加对客户端证书的认证,通过用证书私钥签名实现,签名内容为所有之前处理的消息的哈希,如图 3 所示。

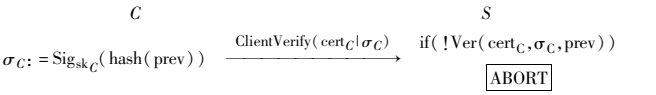

图 3　C 和 S 之间的客户端证书认证

加密传输阶段,C 判断(S,pk_S)对是否在 SL_B^{Aftaut} 中,对于合法的 S,C 将含 token^{*} 的 cookie 发送给 S,否则发送一个空的 cookie,S 用 I 证书验证上述签名。如图 4 所示,其中省略 Dec-MAC$_{k_1,k_2}$ 的默认验证。

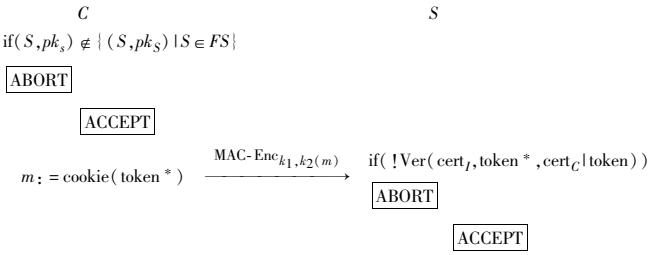

图 4　C 和 S 之间的相互认证

3.3　安全分析

下面分析 BBFIM 协议的安全性,令 q 为对手 A 参与 $\mathrm{Game}^{\text{BBFM}}_{\Pi}(A,k)$ 执行的协议会话的最大数目。

3.3.1　针对 C/I 交互的攻击

a)当 A 注入一个伪造的服务器证书时,协议的安全性依赖于协议中双方的认证方法。这里包括对一次性密码和 HPA 的猜解,假设 OTP 的获取方法对于 A 是随机的,且 A 不能伪造出非用户注册的 HPA 而不被用户发现,可以得到其被 A 破坏的概率上限为 $\mathrm{Succ}^{\text{InjCert}}_{CI}(A,k)\leqslant\dfrac{q}{2^{p4(k)}}+\dfrac{q}{|W|}$。

b)否则协议的安全性依赖于 TLS 协议是否被 A 破坏。针对协议中 TLS 的每一次秘密计算(包括随机数和加密模块)的破坏,构造一系列攻击游戏(本文不一一列举),应用文献[10]中的同时证明方法,从而可以获得 TLS 协议被 A 破坏的概率上限为

$$\mathrm{Succ}^{\text{NoInj}}_{CI}(A,k)\leqslant\frac{2q^2}{2^{p3(k)}}+\frac{q^2}{2^{p1(k)}}+4q\mathrm{Adv}^{\text{prf}}_{\text{PRF}}(k)+$$

$$4q\mathrm{Adv}^{\text{cuf-cpa}}_{\text{MAC-Enc}}(k)+q\mathrm{Adv}^{\text{ind-cpa}}_{(\text{asEnc},\text{asDec})}(k)+2q\mathrm{Succ}^{\text{coll}}_{\text{hash}}(k)$$

3.3.2　针对 C/S 交互的攻击

a)当 A 注入一个伪造的服务器证书时,协议的安全性依赖于协议中双方的认证方法。这里包括对令牌的猜解和(S,pk_s)对的伪造,可以得到其被 A 破坏的概率上限为

$$\mathrm{Succ}^{\text{InjCert}}_{CS}(A,k)\leqslant\frac{q}{2^{ps(k)}}+q\mathrm{Adv}^{\text{ind-cpa}}_{(\text{sEnc},\text{sDec})}(k)+q^{\text{NaInj}}_{CI}+q^{\text{InjCert}}_{CI}$$

b) 否则协议的安全性依赖于 TLS 协议是否被 A 破坏。同样地可以获得 TLS 协议被 A 破坏的概率上限为

$$\mathrm{Succ}_{CS}^{\mathrm{NoInj}}(A,k) \leqslant \frac{2q^2}{2^{p3(k)}} + \frac{q^2}{2^{p1(k)}} + 4q\mathrm{Adv}_{\mathrm{PRF}}^{\mathrm{prf}}(k) + 3q\mathrm{Adv}_{\mathrm{MAC\text{-}Enc}}^{\mathrm{cuf\text{-}cpa}}(k) + q\mathrm{Adv}_{(\mathrm{asEnc},\mathrm{asDec})}^{\mathrm{ind\text{-}cpa}}(k) + 3q\mathrm{Succ}_{\mathrm{hash}}^{\mathrm{coll}}(k) + q\mathrm{Succ}_{(\mathrm{Sig},\mathrm{Ver})}^{\mathrm{euf\text{-}cma}}(k)$$

最终可以得到以下结论：如果 PRF 是标准伪随机函数，(MAC-Enc，Dec-MAC) 具有 CUF-CPA 安全性，(asEnc，asDec) 具有 IND-CPA 安全性，hash 抗冲突，(Sig，Ver) 具有 EUF-CMA 安全性，那么协议 Π 提供定义 2 中所述安全的认证。事实上这些安全性假设在 TLS 协议规范下是有效的，因为协议规定的 RSA 加密 (PKC#1 或 RSA-OAEP) 已证在 ROM 下具有 IND-CPA 安全性[11]，协议规定的 RSA 签名 (PKCS#1 或 RSA-PSS) 已证在 ROM 下具有 EUF-CMA 安全性[12]；另外 Krawczyk[13] 已证明了 TLS 中的先 MAC 再加密结构具有 CUF-CPA 安全性。

4 结束语

基于浏览器的认证由于其广泛性和脆弱性成为了多种攻击的目标。本文介绍和分析了一种基于浏览器的联合身份管理的认证协议，对用户作最弱的安全性假设：不能理解服务器证书，仅通过容易识别的指示来评估网页，但是能够识别人类可感知认证码，并能够使用某种线下安全认证方法，包括动态密码令牌、外接安全证书等。协议加强浏览器的安全模型，通过实现 SLSO 策略加强对服务器端的认证，同时将安全令牌与客户端公钥证书进行绑定，确保客户端的合法性。最后分析了协议的安全性，证明了协议在 DOM 攻击下能够提供安全的认证。

参考文献：

[1] KORMANN D，RUBIN A. Risks of the passport single sign on protocol [J]. Computer Networks，2000，33(6)：51-58.

[2] GROβ T. Security analysis of the SAML single sign on browser/artifact profile[C]//Proc of the 19th Annual Computer Security Applications Conference. Washington DC：IEEE Computer Society，2003：298.

[3] GAJEK S，SCHWENK J，STEINER M，*et al*. Risks of the CardSpace protocol[C]//Proc of the 12th International Conference on Information Security. Berlin：Springer-Verlag，2009：278-293.

[4] CHEN X，GAJEK S，SCHWENK J. On the insecurity of Microsoft's identity metasystem CardSpace，Horst Görtz Institute for IT Security technical report HGI TR-2008-003 [R]. Bochum：Ruhr-Universität，2008.

[5] BRUEGGER B P，HUHNLEIN D，SCHWENK J. TLS-Federation：a secure and relying-party-friendly approach for federated identity mana-gement[C]//Proc of Special Interest Group on Biometrics and Electronic Signatures. 2008：93-104.

[6] KOHLAR F，SCHWENK J，JENSEN M，*et al*. On cryptographically strong bindings of SAML assertions to transport layer security[J]. International Journal of Mobile Computing and Multimedia Communications，2011，3(4)：20-35.

[7] GAJEK S，JAGER T，MANULIS M，*et al*. A browser-based Kerberos authentication scheme[C]//Proc of the 13th European Symposium on Research in Computer Security. Berlin：Springer-Verlag，2008：115-129.

[8] KARLOF C，SHANKAR U，TYGAR J D，*et al*. Dynamic pharming attacks and locked same-origin policies for Web browsers[C]//Proc of the 14th ACM Conference on Computer and Communications Security. New York：ACM Press，2007：58-71.

[9] GAJEK S，LIAO Li-jun，SCHWENK J. Stronger TLS bindings for SAML assertions and SAML artifacts[C]//Proc of ACM Workshop on Secure Web Services. New York：ACM Press，2008：11-20.

[10] SHOUP V. Sequences of games：a tool for taming complexity in security proofs[EB/OL]. (2004-10-20). http：/eprint. iacr. olrg/2004/332. pdf.

[11] SHOUP V. OAEP reconsidered[J]. Journal of Cryptology，2002，15(4)：223-249.

[12] JONSSON J. Security proofs for the RSA-PSS signature scheme and its variants [EB/OL]. (2001-11-23). http：//eprint. iacr. org/2001/053. pdf.

[13] KRAWCZYK H. The order of encryption and authentication for protecting communications (or：how secure is SSL?)[C]//Proc of the 21st Annual International Cryptology Conference on Advances in Cryptology. London：Springer-Verlag，2001：310-331.

(上接第 1842 页)

[2] BERGAMO P，D'ARCO P，SANTIS A，*et al*. Security of public key cryptosystems based on Chebyshev polynomials[J]. IEEE Trans on Circuits and Systems-I：Regular Papers，2005，52(7)：1382-1393.

[3] XIAO Di，LIAO Xiao-feng，DENG Shao-jiang. A novel key agreement protocol based on chaotic maps[J]. Information Science，2007，177(3)：1136-1142.

[4] HAN S. Security of a key agreement protocol based on chaotic maps [J]. Chaos，Solitons，and Fractals，2008，38(3)：764-768.

[5] XIANG Tao，WONG K W，LIAO Xiao-feng. On the security of a novel key agreement protocol based on chaotic maps[J]. Chaos，Solitons，and Fractals，2009，40(2)：672-675.

[6] WANG Da-hu，HU Zhi-guo，TONG Zao-jing，*et al*. An identity authentication system based on Chebyshev polynomials[C]//Proc of the 1st International Conference on Information Science and Engineering. 2009：26-28.

[7] ZHAO Geng，LU Fang-fang. Security of several public key algorithms chaos-based proposed recently[C]//Proc of International Conference on Communication. [S. l]：IEEE Press，2006：1573-1576.

[8] 刘亮，刘云，宁红宙. 公钥体系中 Chebyshev 多项式的改进[J]. 北京交通大学学报，2005，29(5)：56-60.

[9] KOCAREV L，MAKRADULI J，AMATO P. Public-key encryption based on Chebyshev polynomials[J]. Circuits，Systems，and Signal Processing，2005，24(5)：497-517.

[10] WANG Xing-yuan，ZHAO Jian-feng. An improved key agreement protocol based on chaos[J]. Communications in Nonlinear Science and Numerical Simulation，2010，15(12)：4052-4057.

[11] 赵耿，闫慧，童宗科. 基于 Chebyshev 多项式的公钥密码算法的研究[J]. 计算机工程，2008，34(24)：137-139.

[12] 郝舒欣，赵耿，徐刚，等. 基于 Chebyshev 多项式的身份认证方案的研究[J]. 计算机应用与软件，2012，29(1)：70-73.