第41卷 第6期 西 安 交 通 大 学 学 报 Vol.41 №6
2007年6月 JOURNAL OF XI′AN JIAOTONG UNIVERSITY Jun. 2007

基于SWIM卡公钥认证的二阶段握手加密套接层协议

常朝稳[1,2]，覃征[1]，司志刚[2]，韩培胜[2]
(1.西安交通大学电子商务研究所，710049，西安；2.信息工程大学电子技术学院，450004，郑州)

摘要：根据普通智能手机移动接入时端端加密的安全需求，提出了一个基于SWIM卡公钥认证的二阶段握手加密套接层(SSL)改进协议.在握手的第1阶段，该协议由SWIM卡完成终端与网关之间基于公钥证书的身份认证，并产生、分发密钥材料.利用第1阶段的认证结果替代标准SSL握手协议的认证部分，利用第1阶段产生的共享密钥、随机数按照标准SSL密钥生成方法生成移动通信双方的会话密钥、初始化向量，进而完成第2阶段的握手SSL改进协议.所提协议的安全性通过了BAN的逻辑推理、证明，其适用性分析结果表明，在端端安全性、通信带宽效率变化、密码运算量和移动终端普适性等方面，它要比无线应用协议更适于移动应用的安全性需要，在相同的实验环境下，移动终端安全接入的时间也从3.5 s缩短到1.5 s.

关键词：移动通信；二阶段握手；加密套接层协议
中图分类号：TN915 **文献标识码**：A **文章编号**：0253-987X(2007)06-0669-05

Protocol of Two-Phase Handshaking Security Socket Layer Based on SWIM Card Public-Key Authentication

Chang Chaowen[1,2], Qin Zheng[1], Si Zhigang[2], Han Peisheng[2]
(1. Institute of Electronic Commerce, Xi′an Jiaotong University, Xi′an 710049, China; 2. School of Electronic Technology, Information Engineering University, Zhengzhou 450004, China)

Abstract: To solve the problem of end-to-end encipherment in smart-phone mobile access, an improved two-phase handshaking SSL protocol based on SWIM card public-key authentication is proposed. It accomplishes identity authentication and shared-key agreement between mobile telephone and gateway in the first phase. Then, the information produced in the forepart is used to replace the certification part of standard SSL handshaking protocols in the second phase. The shared-key and random number created in the first phase are used to produce session key and initialization vector for the encryption communication between mobile telephone and gateway by creating standard SSL keys. The security of improved two-phase handshaking SSL protocol is proved by BAN-logic reasoning, and the improved protocol is more adaptive for security needs of mobile applications than WAP protocols in four aspects: end-to-end security, efficient bandwidth change, the key calculation intensity and the universality of mobile terminal. In the same experiment environment, the time for a security connection established between mobile telephone and gateway is shortened from 3.5 s to 1.5 s.

Keywords: mobile communication; two-phase handshake; security socket layer protocol

---

收稿日期：2006-10-09. 作者简介：常朝稳(1966～)，男，在职博士生，副教授；覃征(联系人)，男，教授，博士生导师.
基金项目：金盾工程资助项目(J1GAB23WO13).

随着移动电子商务的发展，敏感信息的安全传输问题变得越来越突出. 典型的应用场景采用了3部件安全体系结构(终端、网关和认证鉴别节点). 在该体系结构中，认证鉴别节点实现了接入网关和移动终端的认证、鉴别工作，移动终端与安全网关之间实现了端到端安全通信. 由于移动终端的多样、复杂和不开放性，所以采用加密套接层(SSL)安全协议是一种较为理想的接入方式.

在不安全的网络条件下，SSL协议可以解决通信双方的安全信息交换问题[1]，但在一些嵌入式操作系统中，SSL协议的应用受到了限制和制约[1-2].

在移动通信中，基于无线应用协议(WAP)栈的安全传输协议(WTLS)与无线识别模块(WIM)相结合是解决移动通信安全的技术手段之一，而WAP1.x协议在WAP网关下经WTLS与SSL的协议转换[3]，不再适于端端加密的安全通信要求.

本文在分析SSL协议工作原理的基础上，结合移动终端的特殊性，提出了一种基于SWIM卡的二阶段握手安全通讯协议.

1 SSL协议及SWIM卡

SSL握手协议是整个SSL的核心，它的安全能力是通过Client Hello和Server Hello建立的，服务器与客户之间是通过可选择的认证步骤，同时基于数字证书的公钥认证机制完成相互认证的. 一种通用的方法是将证书和私钥放置在一个令牌中，这样SWIM卡就可以承担这一角色.

SWIM卡是在普通用户识别模块(SIM)卡中实现WIM模块的功能. WIM是一种无法篡改的装置，类似于全球移动通讯系统标准里的SIM模组，它支持WTLS协定，提供应用层面的安全功能，存放和处理使用者的身份认证信息，生成、加密、脱密、嵌入WTLS交换信息所需的密码及算法.

SWIM卡的安全服务可以设计为扩充的应用协议数据单元(APDU)命令集，在一般的手机中，移动设备通过标准的$T=0$协议，利用扩展的APDU安全命令就可以访问SWIM卡，从而获得相应的安全服务. 遗憾的是，一般的智能手机操作系统的应用层不支持访问这种扩展的APDU命令，这就无法在SSL层获得SWIM卡提供的安全服务.

2 基于二阶段握手的SSL协议

2.1 第1阶段

在第1阶段，终端和网关之间基于SIM卡开发工具包(STK)完成基于公钥证书的身份认证和共享密钥的产生、分发.

由于手机等移动终端的功能受限，所以在应用层无法直接访问SWIM卡，但是可以利用STK技术实现第1阶段的认证工作，并生成共享密钥. STK允许SWIM卡运行自己的应用软件，而SWIM卡通过宿主其上的应用程序来提供卡内的安全服务，基于移动终端的短信息通道或通用无线分组业务(GPRS)通道，在卡与接入端(安全接入网关)之间完成基于公钥证书的认证，认证过程如图1所示.

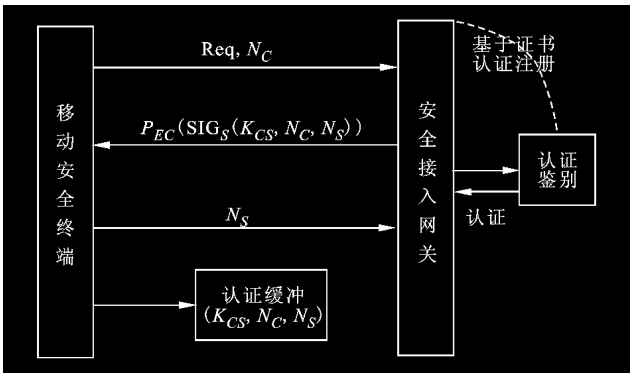

图1 基于SWIM卡的认证过程

认证协议所发送的消息包括$C\rightarrow S: N_C$、$S\rightarrow C: P_{EC}(\mathrm{SIG}_S(K_{CS}, N_C, N_S))$、$C\rightarrow S: N_S$，其中$C$表示客户端，$S$表示安全接入网关，$P_{EC}$表示用于客户端的公钥加密，$\mathrm{SIG}_S$表示用于网关的私钥签名，$K_{CS}$表示共享密钥，$N_C$表示终端产生的验证因子，$N_S$表示接入网关产生的验证因子.

认证协议的执行步骤描述如下.

步骤1：SWIM卡向安全接入网关发出明文认证请求，请求内容包括N_C、数字证书或证书索引号(一般是手机号码).

步骤2：安全接入网关将SWIM卡的相关信息(如证书索引)经签名后送给认证鉴别服务器，以验证移动终端证书的合法性，并返回终端公钥证书. 若移动终端证书是合法的，安全接入网关将产生K_{CS}和N_S，同时利用自己的私钥和SWIM卡的加密公钥对K_{CS}、N_S和N_C进行签名和加密，然后传给SWIM卡.

步骤3：SWIM卡对安全接入网关发送来的密文信息进行脱密(先用预存的安全接入网关的公钥验签，再由自身的私钥脱密)，检查N_C的一致性，并将N_S以明文传给安全接入网关. 如果安全接入网关核对、通过，说明安全接入网关和移动终端都是自身证书的合法持有者.

步骤 4：SWIM 卡将协商认证结果用保护密钥加密，之后放入 SWIM 卡和移动设备(ME)可共享的认证缓存区.

2.2　第 2 阶段

第 2 阶段利用第 1 阶段的认证结果，替代了标准 SSL 握手协议的认证部分，第 1 阶段产生的 K_{CS}、N_C 及网关随机数 N_S 按照标准的 SSL 密钥生成方法生成移动终端和网关的会话密钥、初始化向量，利用 Client Hello 消息、Server Hello 消息，协商出协议版本、会话 ID、密码组、压缩方法等信息，完成加密通信. 改进的 SSL 协议如图 2 所示.

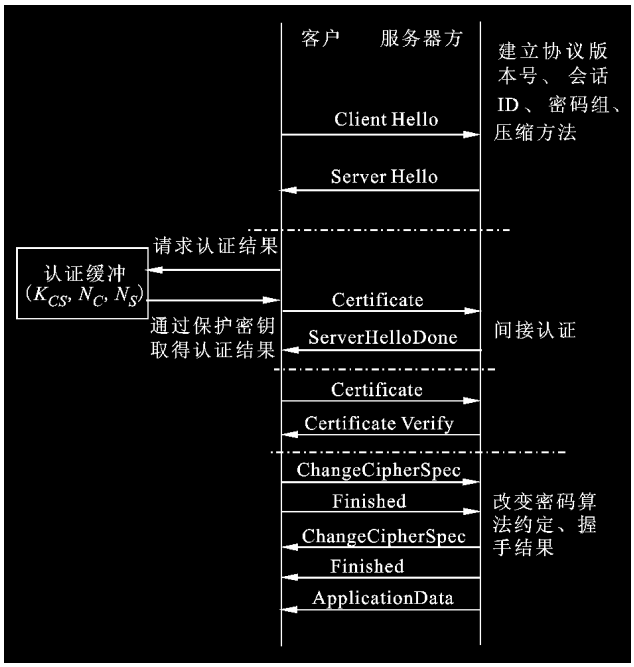

图 2　改进的 SSL 握手协议

在改进的协议中，SSL 握手协议的 Client Hello、Server Hello 消息的内容、格式保持不变，其变化是在握手协议的认证阶段不再进行基于数字证书的双方认证，而是由 ME 访问认证缓存区，用保护密钥脱密认证缓存区的数据获得第 1 阶段的认证结果(K_{CS}，N_C，N_S)，并将 K_{CS} 作为共享密钥，N_C 和 N_S 作为随机数按标准 SSL 协议进行后续处理，完成加密通信. 只有通过第 1 阶段认证的双方，才可能拥有相同的认证结果(分别存储在自己的认证缓存区)，这样在改进的 SSL 握手协议中，隐含实现了通信双方基于数字证书的公钥认证.

3　协议安全性分析

3.1　推理规则

BAN 逻辑是常用的协议形式化分析工具[4-5]，其逻辑符号说明如下.

$P|\equiv X$：P 相信 X，或 P 有权相信 X；

$\xrightarrow{K}P$：K 是 P 的公开密钥；

$\#(X)$：X 是新的；

$P|\Rightarrow X$：P 对 X 有仲裁权；

$P \xleftrightarrow{K} Q$：P、Q 之间共享 K；

$P \lhd X$：P 看到过 X；$P|\sim X$：P 曾说过 X.

推理规则描述如下.

(1)消息含义规则.

对于共享密钥，如果有

$P|\equiv Q \xleftrightarrow{K} P$，$P \lhd \{X\}_K$，则 $P|\equiv Q|\sim X$.

对于公钥，如果有

$P|\equiv \xrightarrow{K} Q$，$P \lhd \{X\}_{K^{-1}}$，则 $P|\equiv Q|\sim X$.

(2)临时值验证规则.

如果有

$P|\equiv \#(X)$，$P|\equiv Q|\sim X$，则 $P|\equiv Q|\equiv X$.

(3)仲裁规则.

如果有 $P|\equiv Q|\Rightarrow X$，$P|\equiv Q|\equiv X$，则 $P|\equiv X$.

(4)信仰规则.

如果有 $P|\equiv X$，$P|\equiv Y$，则 $P|\equiv (X,Y)$；如果有 $P|\equiv (X,Y)$，则 $P|\equiv X$；如果有 $P|\equiv Q|\equiv (X,Y)$，则 $P|\equiv Q|\equiv X$.

(5)传送规则.

如果有 $P|\equiv Q|\sim (X,Y)$，则 $P|\equiv Q|\sim X$.

(6)接收规则.

如果有 $P \lhd (X,Y)$，则 $P \lhd X$；

如果有 $P \lhd \langle X \rangle_Y$，则 $P \lhd X$；

如果有 $P|\equiv Q \xleftrightarrow{K} P$，$P \lhd \{X\}_K$，则 $P \lhd X$；

如果有 $P|\equiv \xrightarrow{K} P$，$P \lhd \{X\}_K$，则 $P \lhd X$；

如果有 $P|\equiv \xrightarrow{K} Q$，$P \lhd \{X\}_{K^{-1}}$，则 $P \lhd X$.

(7)新鲜性规则.

如果有 $P|\equiv \#(X)$，则 $P|\equiv \#(X,Y)$.

(8)共享密钥规则.

如果有 $P|\equiv R \xleftrightarrow{X} R'$，则 $P|\equiv R' \xleftrightarrow{X} R$；如果有 $P|\equiv Q|\equiv R \xleftrightarrow{X} R'$，则 $P|\equiv Q|\equiv R' \xleftrightarrow{X} R$.

(9)共享秘密规则.

如果有 $P|\equiv R \overset{X}{\longleftrightarrow} R'$，则 $P|\equiv R' \overset{X}{\longleftrightarrow} R$；如果有 $P|\equiv Q|\equiv R \overset{X}{\longleftrightarrow} R'$，则 $P|\equiv Q|\equiv R' \overset{X}{\longleftrightarrow} R$.

3.2　协议第 1 阶段安全性证明

利用 3.1 节所述 BAN 逻辑推理规则对基于二

阶段握手的改进SSL协议的安全性证明如下.

初始化假设:①$C|\equiv\xrightarrow{K_C}C$($C$当然相信$K_C$是自己的公开密钥);②$C|\equiv\xrightarrow{K_S}S$(对$C$来说,网关$S$是可确定的,$C$知道$K_S$是$S$的公开密钥);③$C|\equiv\#N_C$($C$相信$N_C$是新鲜的,因为$N_C$是由$C$自己生成的);④$C|\equiv S|\Rightarrow C\xleftrightarrow{K_{CS}}S$(本协议规定,共享密钥由网关产生,所以$C$相信$S$对共享密钥$K_{CS}$有仲裁权);⑤$S|\equiv C\xleftrightarrow{K_{CS}}S$($S$相信共享密钥$K_{CS}$,因为$K_{CS}$是由$S$自己生成的).

根据3.1节的第1阶段的协议描述,协议可理想化,描述如下.

(1)$C\rightarrow S:N_C$ from C

(2)$S\rightarrow C:\{\{C\xleftrightarrow{K_{CS}}S,N_C,N_S\}_{K_S^{-1}}\}_{K_C}$ from S

(3)$C\rightarrow S:N_S$ from C

证明过程描述如下.

由理想化协议(2)得知C看到过S向C发送的消息内容,即

$$C\lhd\{\{C\xleftrightarrow{K_{CS}}S,N_C,N_S\}_{K_S^{-1}}\}_{K_C}\tag{1}$$

根据BEN逻辑的接收规则(6),由式(1)和初始化假设(1)可推理C看到K_S签署的K_{CS}、N_C和N_S,即

$$C\lhd\{C\xleftrightarrow{K_{CS}}S,N_C,N_S\}_{K_S^{-1}}\tag{2}$$

根据消息含义规则(1),由式(2)和初始化假设②可得

$$C|\equiv S|\sim\{C\xleftrightarrow{K_{CS}}S,N_C,N_S\}\tag{3}$$

由初始化假设③和新鲜性规则(7)可得

$$C|\equiv\#\{C\xleftrightarrow{K_{CS}}S,N_C,N_S\}\tag{4}$$

根据临时值验证规则(2),由式(2)和式(4)可得

$$C|\equiv S|\equiv\{C\xleftrightarrow{K_{CS}}S,N_C,N_S\}\tag{5}$$

根据信仰规则(4),由式(5)可得

$$C|\equiv S|\equiv C\xleftrightarrow{K_{CS}}S\tag{6}$$

即C相信S相信共享密钥K_{CS}.

根据仲裁规则(3),由式(6)及初始化假设④得

$$C|\equiv C\xleftrightarrow{K_{CS}}S\tag{7}$$

即C相信共享密钥K_{CS}.

由理想化规则(3)可得

$$S\lhd N_S\tag{8}$$

由初始化假设⑤知

$$S|\equiv C\xleftrightarrow{K_{CS}}S\tag{9}$$

即S相信共享密钥K_{CS}.

由于N_S只有C利用自己的私钥解开消息(初始化假设②)后才能获得,所以

$$S|\equiv C|\equiv C\xleftrightarrow{K_{CS}}S\tag{10}$$

即S相信C相信共享密钥K_{CS}.

由以上步骤,成功得到了一级信仰(式(7)、式(9)及二级信仰(式(6)、式(10)),即C相信共享密钥K_{CS},S相信共享密钥K_{CS},C相信S相信共享密钥K_{CS},S相信C相信共享密钥K_{CS}.第1阶段协议安全性得证.

3.3 协议第2阶段安全性分析

对于标准的SSL握手协议来说,移动终端C向网关S发送Client Hello请求(包括移动终端随机数N_i),网关处理Client Hello消息,发送Server Hello消息(包括N_r),响应移动终端,同时双方就SSL的协议版本号、会话ID、密码组和压缩方法达成一致,交换随机数N_i与N_r.接下来,网关发送Certificate Request消息,请求验证移动终端的合法性,而移动终端接收到Certificate Request请求,发送Client Certificate消息,并将移动终端证书发送到网关,由网关验证此证书的有效性.移动终端发送Client Key Exchange,包含用网关证书公钥加密的预共享密钥M_p,而网关接收到此信息后,用网关的私钥解密得到M_p.网关与移动终端之间利用预共享密钥M_p、N_i、N_r,按SSL标准协议可以产生双方的共享密钥M,进而利用M、N_i、N_r产生双方的会话密钥、初始化向量.

由此可以看出,标准的SSL握手协议的证书请求、交换和认证的最终目的是确认双方的身份,并协商找出双方的共享密钥M、N_i和N_r,而在基于二阶段握手改进SSL协议的第2阶段,是用第1阶段的结果替代了标准SSL握手协议的这一部分(其他的未变化),第1阶段完成的也恰恰是双方身份的确认,并产生K_{CS}、N_C及N_S(它们分别对应M、N_i和N_r),而第1阶段的K_{CS}作为一个可信的共享密钥,与N_C及N_S一起按照标准的SSL密钥生成方法生成移动终端和网关的会话密钥、初始化向量,再通过SSL纪录层协议完成双方的安全通信.因为第1阶段握手的作用与标准SSL握手协议的证书请求、交换和认证的最终目的是相同的,并得到性质相同的共享密钥和随机数,可以推论:只要第1阶段握手是安全的,改进的SSL协议就是安全的.

根据3.2节,经BAN逻辑证明,该协议在第1阶段是安全的,共享密钥K_{CS}也是安全、可信的,所以基于二阶段握手的改进SSL协议是安全的.

4　协议适用性分析

(1)端端安全性. 本文基于二阶段改进的 SSL 协议，利用 STK 技术直接在第 1 阶段 SWIM 卡上实现了终端与网关之间基于公钥证书的身份认证，并产生、分发了共享密钥，手机终端在 SSL 握手时无需再进行身份认证，既保证了协议的安全性，又克服了 SSL 协议受到的制约，解决了 WAP 协议、SSL 协议面临的应用难题.

(2)通信带宽效率的变化. 在标准的 SSL 握手协议中，ME 与网关要交换证书(每张证书大小在 800 B 左右)和大量的密钥材料，仅认证协商就需交换 2 kB 的信息，而在改进的二阶段握手协议中，ME 与网关交换的信息仅包括 K_{CS}、N_C 及 N_S，大大减少了信息的交换量.

ME 通过与 SWIM 卡交互，获得密码服务，ME 通过标准的 $T=0$ 协议，利用扩展的 APDU 安全命令就可以访问 SWIM 卡. 根据 GSM 11.11、GSM 11.14 标准规定，这种通信的速率一般在 9 600 B/s (很低)，而在一次握手协商中，ME 要进行签名、验签和证书有效性检查，这些信息都要 ME 传送给 SWIM 卡，由 SWIM 卡完成后再传给 ME，ME 与 SWIM 卡交换次数为 3×2，信息量比较大. 在改进的协议中，认证协商的整个操作全部在 SWIM 卡上完成，认证协商中 ME 不需要与 SWIM 卡交互，仅需在第 2 阶段将认证结果(K_{CS}、N_C 及 N_S)取走，这种信息交互次数和信息交互量将降至最小.

由于减少了 ME 与网关的信息交换量，减少了 ME 与 SWIM 卡之间的交换次数，在相同的实验环境下(GPRS 通信、Dopod 830 手机)，移动终端安全接入的时间可从 3.5 s 缩短到 1.5 s 左右.

(3)密码运算量. 对于标准的 SSL 握手协议来说，终端和网关双方需要相互的身份确认，需要双方分别进行签名、验签等密码运算，双方需要根据预共享密钥 M_p、N_i、N_r 产生双方的共享密钥 M. 改进的 SSL 协议仅需要网关做一次级联的签名和加密运算，终端做相应的验签、解密运算，就可获得共享密钥 K_{CS}(即标准 SSL 协议中的 M)，省去了标准 SSL 协议中的中间预共享密钥 M_p 的分发和 M 的计算，减少了协议的密码运算量.

(4)终端普适性. 普通手机 ME 无法在应用层直接获得 SWIM 卡的安全服务，而改进的 SSL 协议通过将 SSL 握手协议分成 2 个阶段，利用 STK 技术经第 1 阶段直接在 SWIM 卡上实现了终端与网关之间基于公钥证书的身份认证，并产生、分发了共享密钥，ME 也只需要通过普通的文件访问方式获得认证协商的结果，从而绕开了一般移动终端的技术限制，所以说改进的 SSL 协议具有适用性.

5　结束语

移动安全是移动计算的关键问题之一，在目前的应用环境下，已有的安全协议在端端加密、终端适用性以及效率等方面还不尽完善. 本文所提协议在 SSL 协议基础上进行了改进，协议安全性通过了 BAN 逻辑推理、证明. 适用性分析结果表明，在端端安全性、通信带宽效率变化、密码运算量和移动终端普适性等方面，改进协议比无线应用协议更适于移动应用的安全性需要，在相同实验环境下，移动终端安全接入的时间也从 3.5 s 缩短到 1.5 s.

本协议在金盾工程资助项目(J1GAB23W013)中得到了具体验证，实际应用表明：该协议适用于大多数手机等移动终端，并能有效地解决现有移动终端数据传输的安全保密性问题.

参考文献：

[1] 徐永强. 基于 SSL 的安全数据通道的理论与实践[J]. 电子科技，2004(6)：40-42.
Xu Yongqiang. The theory and practice of the SSL based safe data channel [J]. Electron Science and Technology, 2004(6):40-42.

[2] 樊时凯，王敏. SSL 通信的中间人攻击与防范 [J]. 信息网络安全，2004(9)：57-58.
Fan Shikai, Wang Min. The man in the middle attack in SSL communication [J]. Netinfo Security, 2004(9):57-58.

[3] WAP Forum. Wireless application protocol architecture specification [EB/OL]. (1998-04-30) [2006-01-01]. http://www.wapforumorg/wap.

[4] 钱勇. 认证协议设计与分析方法的研究 [D]. 上海：上海交通大学计算机科学与技术系，2001.

[5] Meadows C. Analysis of the Internet key exchange protocol using the NRL protocol analyzer [C]// Proceedings of the IEEE Symposium on Security and Privacy. Los Alamitos, USA: IEEE Computer Society, 1999: 84-89.

(编辑　苗凌)