认证协议中数据同步的分析

邓淼磊[1,3] 黄照鹤[2] 杨录山[1] 周利华[3]
(解放军信息工程大学理学院 郑州 450001)[1] (南阳理工学院网络中心 南阳 473004)[2]
(西安电子科技大学计算机学院 西安 710071)[3]

摘 要 认证双方数据的同步是认证协议以及认证密钥交换协议的基本要求,但是在协议设计过程中难以把握且经常被忽视。对近年来可证明安全的一个RFID认证协议和一个RFID认证密钥交换协议以及可证明安全的一个移动卫星通信系统认证密钥交换协议进行了仔细分析,分别发现了针对这些协议的数据同步攻击,这些攻击破坏了协议的可用性。最后分别给出了改进方案,以克服存在的安全隐患。

关键词 认证协议,数据同步,攻击,安全
中图法分类号 TP393.08 **文献标识码** A

Data Synchronization of Authentication Protocols

DENG Miao-lei[1,3] HUANG Zhao-he[2] YANG Lu-shan[1] ZHOU Li-hua[3]
(Institute of Science, PLA Information Engineering University, Zhengzhou 450001, China)[1]
(Network Information Center, Nanyang Institute of Technology, Nanyang 473004, China)[2]
(School of Computer, Xidian University, Xi'an 710071, China)[3]

Abstract Data synchronization is a basic requirement for authentication protocols and authenticated key exchange protocols, but it is much trickier and many times overlooked. By carefully analyzing an RFID authentication protocol, an RFID anthenticated key exchange protocol, and an authenticated key exchange protocol for mobile satellite communication systems which were found to be provably secure at present, attacks of data synchronization to these protocols were found respectively. These attacks destroy the availability of protocols. Furthermore, improvements to overcome the security vulnerabilities of these protocols were proposed.

Keywords Authentication protocol, Data synchronization, Attack, Security

认证协议工作在不可靠或者敌意的通信环境下,攻击者对于协议可以有各种各样的攻击手段,包括窃听、篡改、截断协议的通信,甚至加入任何可能的消息,把协议的消息转到其他接收者等等。因此,对于协议的攻击隐晦而多样[1]。其中数据同步攻击,导致认证双方的数据不能同步更新,破坏了协议的可用性。尤其是在认证双方计算能力和存储能力不对称的环境,如RFID协议中,攻击者更容易进行数据同步攻击。例如,Lee提出的LCAP协议[2],它每次执行之后都要动态刷新标签的ID。在协议流程中,标签是在接收到最后一条消息且验证通过之后才更新其ID的,而在此之前,后端数据库已经成功完成相关ID的更新。因此,存在数据同步的潜在安全隐患。类似地,Henrici提出的基于杂凑的ID变化协议[3],其中标签也是在接收到最后一条消息且验证通过之后才更新其ID和LST信息的,而在此之前,后端数据库已经成功完成相关信息的更新。因此,如果此时攻击者进行攻击(攻击者可以伪造一个假消息),就会在后端数据库和标签之间出现严重的数据不同步的问题。另外,人们还发现在OTYT06[4],SLK06[5],HMNB07[6]等协议中,存在对数据同步的攻击[7]。

可证明安全是近年来比较可信的认证协议形式化设计与分析方法,其中的通用可组合(UC)模型[8]更是受到了广泛的推崇。基于UC模型,Le设计了前向安全的RFID认证协议和认证密钥交换协议[9],冯涛设计了移动卫星通信系统认证密钥交换协议[10]。他们分别证明了协议是UC安全的。本文通过分析发现,以上证明存在问题,设计的协议并不是UC安全的,攻击者可以进行数据同步攻击。而后对他们的协议进行了修改,以克服存在的安全隐患。

1 RFID认证协议和认证密钥交换协议的安全分析

在文献[9]中,Le分别设计了前向安全的RFID认证协议O-FRAP和认证密钥交换协议O-FRAKE。

1.1 对O-FRAP的分析

O-FRAP协议的描述如图1所示。

Le在文献[9]中证明了O-FRAP能够UC安全实现匿名认证理想函数 F_{anauth}。但是证明过程存在问题。在理想攻击

到稿日期:2009-04-03 返修日期:2009-07-01 本文受国防科技预研项目资助。
邓淼磊(1977-),男,博士生,主要研究方向为安全协议设计和分析,E-mail:dmlei2003@163.com;黄照鹤(1979-),女,讲师,主要研究方向为计算机应用和网络信息安全;杨录山(1963-),男,副教授,主要研究方向为信息与计算科学;周利华(1942-),男,教授,博士生导师,主要研究方向为计算机网络安全等。

者(也称仿真者)S的仿真操作中,作为标签(TAG)临时身份的随机数 r 和标签与服务器(SERVER)共享的密钥 k^a 总是绑定在一起的,即(r,k^a)是同步生成和更新的。而在现实协议 O-FRAP 中,标签在接收到服务器的挑战 r_{sys} 后,就开始用 v_1 更新随机数 r_{tag}。但是直到协议的最后一步,标签才用 v_4 更新密钥 k^a_{tag}。即在现实协议 O-FRAP 中,标签的随机数和密钥并不是同步更新的。因此仿真操作存在问题,理想过程和现实过程是可区分的,协议不是 UC 安全的。

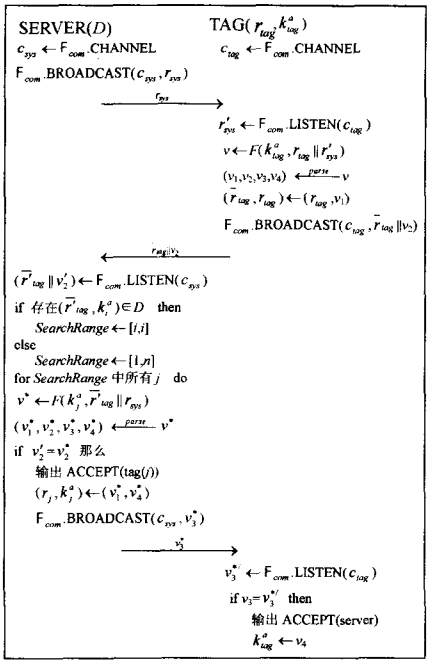

图 1 O-FRAP 协议

攻击者可以进行数据同步攻击。攻击者可以在最后一步伪造一个假消息,或者截断最后的消息,那么协议结束后,标签中用作临时身份的随机数进行了更新,密钥没有更新,而服务器中存储的相应随机数和密钥都进行了更新。这样,标签中的数据和服务器中的数据是不同步的,标签将不能再通过服务器的认证,协议的可用性遭到了破坏。

1.2 对 O-FRAKE 的分析

O-FRAKE 协议是 O-FRAP 协议的直接扩展,增加了密钥交换的功能。O-FRAKE 协议中,在服务器端,生成的用于安全通信的会话密钥 k^b_{tag} 和标签的随机数 r_{tag}、标签的密钥 k^a_{tag} 是同时进行更新的;在标签端,r_{tag} 在标签接收到服务器的挑战 r_{sys} 后就进行了更新,而 k^b_{tag} 和 k^a_{tag} 是在标签成功认证服务器后才进行更新。因此存在数据同步的安全隐患,攻击者可以按照对 O-FRAP 的攻击方法,对 O-FRAKE 进行数据同步攻击。

2 移动卫星通信系统认证密钥交换协议分析

冯涛[10]设计了一个用于移动卫星通信系统的认证密钥交换协议 MSCS-AKE。协议的具体描述如下:

1)$P_{NCC}\rightarrow P_{Ui}$:$P_{NCC}$ 向 P_{Ui} 发送认证请求(sid,r_{NCC})。

2)$P_{Ui}\rightarrow P_{NCC}$:$P_{Ui}$ 接收到 r_{NCC} 后,计算 V←$F(k_i,r_{NCC}\|r_{ui})$,将 V 分离为 $V=v_1\|v_2\|v_3\|v_4$,其中 r_{ui} 是 P_{Ui} 的临时身份,F 是伪随机函数,计算 $v_4\oplus f_u$,$v_4\oplus H(f_u)$。其中 $f_u=g^a \bmod p$。并更改记录(ID_{ui},r_{ui})为(ID_{ui},v_1),然后向 P_{NCC} 发送$(sid,r_{ui}\|v_2,v_4\oplus f_u,v_4\oplus H(f_u))$。

3)$P_{NCC}\rightarrow P_{Ui}$:$P_{NCC}$ 接收到$(sid,r_{ui}\|v_2,v_4\oplus f_u,v_4\oplus H(f_u))$,首先利用 r_{ui} 查找数据库获得相应的秘密信息(ID_{ui},r_{ui},k_i),然后计算 V^*←$F(k_i,r_{NCC}\|r_{ui})$。将 V^* 分离为 $V^*=v_1^*\|v_2^*\|v_3^*\|v_4^*$,假如 $v_2=v_2^*$,则 P_{NCC} 对 P_{Ui} 的认证成功并更改记录(ID_{ui},r_{ui})为(ID_{ui},v_1^*)。然后,P_{NCC} 计算 $f_u=v_4^*\oplus(v_4\oplus f_u)$,$H(f_u)=v_4^*\oplus(v_4\oplus H(f_u))$。接着,$P_{NCC}$ 检查计算出的 $H(f_u)$ 是否正确。如果正确,P_{NCC} 开始计算 $f_c=g^b \bmod p$,新的会话密钥 $k_i^*=f_u^b \bmod p=g^{ab} \bmod p$,并计算 $v_4^*\oplus f_c$,$H(f_u\|k_i^*\|v_1^*)$。这里,v_1^* 是一个 P_{Ui} 新的临时身份。然后,P_{NCC} 把(ID_{ui},r_{ui},k_i)更新成(ID_{ui},v_1^*,k_i^*)。P_{NCC} 向 P_{Ui} 发送$(v_4^*\oplus f_c,H(f_u\|k_i^*\|v_1^*),v_3^*)$。

4)P_{Ui} 接收到消息$(v_4^*\oplus f_c,H(f_u\|k_i^*\|v_1^*),v_3^*)$后,计算 $f_c=v_4\oplus(v_4^*\oplus f_c)$,$k_i^*=f_c^a \bmod p=g^{ab} \bmod p$。然后,$P_{Ui}$ 检查是否 $H(f_u\|k_i^*\|v_1^*)=H(f_u\|k_i^*\|v_1)$,$v_3^*=v_3$。如果相等,$P_{Ui}$ 相信 P_{NCC} 是合法的,并且 k_i^* 是有效的。然后 P_{Ui} 保留秘密消息(ID_{ui},v_1,k_i^*)。

在 MSCS-AKE 中,临时身份 r_{ui} 在 1)中就进行了更新,即由 r_{ui} 更新为 v_1,而密钥 k_i 到 4)才进行更新。因此一旦 P_{Ui} 没有正确接收到最后一条消息,r_{ui} 和 k_i 就不能同步更新。当再次运行协议时,P_{NCC} 利用接收到的 v_1 查找数据库获得的秘密信息是(ID_{ui},v_1,k_i^*),这样在 3)中,P_{NCC} 就不能成功认证 P_{Ui}。

3 协议改进

通过前面的分析可以看到,造成攻击的原因是协议中本该绑定在一起的秘密数据没有同时更新,这样攻击者就可以导致认证双方的数据不同步。下面对上述协议给出改进方案,以弥补现有的安全缺陷。

3.1 对 O-FRAP 和 O-FRAKE 的改进

对 O-FRAP 协议的修改是:让标签在成功认证服务器后,同时更新秘密的随机数和密钥。即在标签接收到服务器的挑战 r_{sys} 后,先不更新 r_{tag},到协议的最后一步,标签再同时更新 r_{tag} 和 k^a_{tag}:(r_{tag},k^a_{tag})←(v_1,v_4)。这样,把标签的秘密随机数和密钥绑定在了一起,同时进行更新。可以证明,协议修改后,理想过程和现实过程是不可区分的,协议是 UC 安全的。证明过程与文献[9]中的相同。

对 O-FRAKE 协议的修改与此类似,即在标签接收到服务器的挑战 r_{sys} 后,先不更新秘密的随机数 r_{tag}。在标签成功认证服务器后,同步更新随机数、标签密钥和会话密钥:$(r_{tag},k^a_{tag},k^b_{tag})$←$(v_1,v_4,v_5)$。同样可以证明,修改后的协议是 UC 安全的。

3.2 对 MSCS-AKE 的改进

对 MSCS-AKE 的修改是:a)让 P_{Ui} 对临时身份 r_{ui} 和密钥 k_i 同步进行更新;b)当 P_{NCC} 在数据库中查找不到相应的秘密信息(ID_{ui},r_{ui},k_i)时,利用数据库中存储的更新前的密钥逐个进行计算。修改后的协议描述如下:

1)$P_{NCC}\rightarrow P_{Ui}$:$P_{NCC}$ 向 P_{Ui} 发送认证请求(sid,r_{NCC})。

2)$P_{Ui}\rightarrow P_{NCC}$:$P_{Ui}$ 接收到 r_{NCC} 后,计算 V←$F(k_i,r_{NCC}\|r_{ui})$,将 V 分离为 $V=v_1\|v_2\|v_3\|v_4$,其中 r_{ui} 是 P_{Ui} 的临时身份,F 是伪随机函数,计算 $v_4\oplus f_u$,$v_4\oplus H(f_u)$。其中 $f_u=g^a \bmod p$。然后向 P_{NCC} 发送$(sid,r_{ui}\|v_2,v_4\oplus f_u,v_4\oplus H$

(f_u))。

3) $P_{NCC} \rightarrow P_{Ui}$: P_{NCC} 接收到 $(sid, r_{ui} \| v_2, v_4 \oplus f_u, v_4 \oplus H(f_u))$，利用 r_{ui} 查找数据库获得相应的秘密信息 (ID_{ui}, r_{ui}, k_i)，然后计算：$V^* \leftarrow F(k_i, r_{NCC} \| r_{ui})$；如果查找不到相应的信息，那么根据数据库中记录的所有更新前的三元组中的密钥 k_i' 逐个计算 $V^* \leftarrow F(k_i', r_{NCC} \| r_{ui})$。将 V^* 分离为 $V^* = v_1^* \| v_2^* \| v_3^* \| v_4^*$，假如 $v_2 = v_2^*$，则 P_{NCC} 对 P_{Ui} 的认证成功并更改记录 (ID_{ui}, r_{ui}) 为 (ID_{ui}, v_1^*)。然后，P_{NCC} 计算：$f_u = v_4^* \oplus (v_4 \oplus f_u)$，$H(f_u) = v_4^* \oplus (v_4 \oplus H(f_u))$。接着，$P_{NCC}$ 检查计算出的 $H(f_u)$ 是否正确。如果正确，P_{NCC} 开始计算：$f_c = g^b \bmod p$，新的会话密钥 $k_i^* = f_u^b \bmod p = g^{ab} \bmod p$，并计算 $v_4^* \oplus f_c, H(f_u \| k_i^* \| v_1^*)$。这里，$v_1^*$ 是一个 P_{Ui} 新的临时身份。然后，P_{NCC} 把 (ID_{ui}, r_{ui}, k_i) 更新成 (ID_{ui}, v_1^*, k_i^*)。P_{NCC} 向 P_{Ui} 发送 $(v_4^* \oplus f_c, H(f_u \| k_i^* \| v_1^*), v_3^*)$。

4) P_{Ui} 接收到消息 $(v_4^* \oplus f_c, H(f_u \| k_i^* \| v_1^*), v_3^*)$ 后，计算 $f_c = v_4 \oplus (v_4^* \oplus f_c)$，$k_i^* = f_c^a \bmod p = g^{ab} \bmod p$。然后，$P_{Ui}$ 检查是否 $H(f_u \| k_i^* \| v_1^*) = H(f_u \| k_i^* \| v_1)$，$v_3^* = v_3$。如果相等，$P_{Ui}$ 相信 P_{NCC} 是合法的，并且 k_i^* 是有效的。然后 P_{Ui} 更改记录 (ID_{ui}, r_{ui}, k_i) 为 (ID_{ui}, v_1, k_i^*)。

可以证明，修改后的协议是 UC 安全的，证明过程与文献[10]中的相同。

结束语 在认证协议设计过程中，认证双方数据同步问题难于把握，往往被忽视。对近来证明是 UC 安全的几个认证协议进行了分析，指出了安全证明中存在的问题以及这些协议在数据同步方面的缺陷，并给出了相应的修改，以弥补存在的安全隐患。修改后的协议可以证明是 UC 安全的。

参 考 文 献

[1] 邓淼磊，邱罡，周利华. 基于串空间和状态转换的认证协议分析方法[J]. 计算机科学，2007，34(10)：96-98

[2] Lee S M, Hwang Y J, Lee D H. Efficient authentication for low-cost RFID systems[C]// International Conference on Computational Science and its Applications. IEEE Computer Society, 2005：619-627

[3] Henrici D, Muller P. Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers [C]// 2nd IEEE Annual Conference on Pervasive Computing and Communications Workshops. IEEE Computer Society, 2005：149-153

[4] Osaka K, Takagi T, Yamazaki K, et al. An efficient and secure RFID security method with ownership transfer[C]// CIS. 2006：778-787

[5] Seo Y, Lee H, Kim K. A scalable and untraceable authentication protocol for RFID[C]// EUC Workshops. 2006：252-261

[6] Ha J, Moon S, Nieto J M G, et al. Low-cost and strong-security RFID authentication protocol[C]// EUC Workshops. 2007：795-807

[7] Deursen T, Radomirovic S. Attacks on RFID protocols [EB/OL]. http://eprint.iacr.org/2008/310.pdf

[8] Canetti R. Universally composable security：A new paradigm for cryptographic protocols[C]// 42th IEEE Annual Symposium on Foundations of Computer Science. IEEE Computer Society, 2001：136-145

[9] Le T, Burmester M, Medeiros B. Universally composable and forward secure RFID authentication and authenticated key exchange[C]// 2nd ACM Symposium on Information, Computer and Communications Security. ACM Press, 2007：242-252

[10] 冯涛，马建峰. UC 安全的移动卫星通信系统认证密钥交换协议[J]. 宇航学报，2008，29(6)：1959-1964

(上接第 75 页)

安全的多身份单密钥解密方案。在判定性 q-TBDHE 假设下，证明了所提方案在适应性选择密文和身份攻击下是不可区分的。同时直接获得 CCA 的安全性，因此方案更加有效。

参 考 文 献

[1] Shamir A. Identity-based cryptosystems and signature schemes [C]// Advances in Cryptology-Crypto'84. Santa Barbara, California, USA, LNCS 0196, Berlin：Springer-Verlag, 1984：47-53

[2] Boneh D, Franklin M. Identity-based encryption from the weil pairing [C]// Advances in Cryptology-Crypto'01. Santa Barbara, California, USA, LNCS 2139, Berlin：Springer-Verlag, 2001：213-229

[3] Boneh D, Boyen X. Efficient selective-ID secure identity based encryption without random oracles[C]// Advances in Cryptology-Eurocrypt'04. Interlaken, Switzerland, LNCS 3027, Berlin：Springer-Verlag, 2004：223-238

[4] Boneh D, Boyen X. Secure identity based encryption without random oracles[C]// Advances in Cryptology-Crypto'04. Santa Barbara, California, USA, LNCS 3152, Berlin：Springer-Verlag, 2004：443-459

[5] Waters B. Efficient identity-based encryption without random oracles[C]// Advances in Cryptology-Eurocrypt'05. Aarhus, Denmark, LNCS 3494, Berlin：Springer-Verlag, 2005：114-127

[6] Gentry C. Practical Identity-based encryption without random oracles[C]// Advances in Cryptology-Eurocrypt'06. Saint Petersburg, Russia, LNCS 4004, Berlin：Springer-Verlag, 2006：445-464

[7] Guo Fuchun, Mu Yi, Chen Zhide. Identity-based encryption：how to decrypt multiple ciphertexts using a single decryption key[C]// Pairing-based Cryptography-Pairing'07. Dublin, Ireland, LNCS 4575, Berlin：Springer-Verlag, 2007：392-406

[8] Guo Fuchun, Mu Yi, Chen Zhide, et al. Multi-identity single-key decryption without random oracles[C]// Inscrypt' 07. Xining, China, LNCS 4990, Berlin：Springer-Verlag, 2007：384-398

[9] Canetti R, Halevi S, Kate J. A forward-secure public key encryption scheme[C]// Advances in Cryptology-Eurocrypt'03. Warsaw, Poland, LNCS 2656, Berlin：Springer-Verlag, 2003：255-271

[10] Ren Yanli, Gu Dawu. Secure Hierarchical Identity Based Encryption Scheme in the Standard Model[C]// INDOCRYPT 2008. Kharagpur, India, LNCS 5365, Berlin：Springer-Verlag, 2008：104-115