基于缩减到 53(20-72)步的 SHA-1 的 H^2-MAC 的等价密钥恢复攻击

张　丽[1]，　王　沛[2]

(1. 山东大学计算机科学与技术学院，山东济南，250101；
2. 国防科技大学信息系统与管理学院，湖南长沙，410073)

摘要　H^2-MAC 是 Kan Yasuda 在 ISC 2009 上提出的一种新型的 MAC 结构，与 HMAC 的不同之处仅在于 H^2-MAC 用固定的常数 IV 代替 HMAC 的外部密钥，计算 MAC 值时只访问一次种子密钥，在保持 HMAC 优势的基础上简化密钥管理。文中首次给出基于缩减到 53 (20-72)步的 SHA-1 的 H^2-MAC 的等价密钥恢复攻击，并进行一般性伪造攻击(Universal Forgery)，证明取消外部密钥导致安全性降低。首先构造基于 53 (20-72)步 SHA-1 的 H^2-MAC 的区分器，达成区分攻击，在区分攻击的基础上利用比特探测技术，恢复中间链接变量，即等价密钥，最后进行一般性伪造攻击。即在不知道密钥的前提下，攻击者可伪造任意消息 M 的合法 MAC 值，攻击的复杂度为 2^{99} 次 MAC 查询，远低于一般性伪造攻击的理想复杂度。

关键词　密码分析；H^2-MAC-SHA-1；等价密钥恢复攻击；一般性伪造攻击

DOI　10.3969/j.issn.1009-3516.2013.04.020

中图分类号　TN918　　**文献标志码**　A　　**文章编号**　1009-3516(2013)04-0084-04

Equivalent Key Recovery Attack on H^2-MAC Instantiated with SHA-1 Reduced to 53 (20-72) Steps

ZHANG Li[1], WANG Pei[2]

(1. School of Computer Science and Technology, Shandong University, Jinan 250101, China;
2. College of Information System and Management, Nation University of Defense Technology, Changsha 410073, China)

Abstract: H^2-MAC, which was proposed by Kan Yasuda in Information Security Conference (ISC) 2009, is a new type of MAC construction. Compared with HMAC, H^2-MAC is much easier for algorithm implementation and key management, for it gets access to the key only once. This paper first presents an equivalent key recovery attack H^2-MAC-SHA-1 reduced to 53 (20-72) steps, which conduces to a universal forgery attack directly. Firstly, an H^2-MAC-SHA-1 distinguisher is constructed. Then, the intermediate chaining variable, i.e., the equivalent key is recovered by using the distinguisher and bit flipping technology. Consequently, the universal forgery attack is processed. The adversary unknowing the secret key can process the universal forgery attack by computing the valid MAC value of M, which can be an arbitrary message. The complexity of the attack is about 2^{99} queries, which is much lower than the ideal complexity of the universal forgery.

收稿日期：2013-03-28
基金项目：高等学校博士学科点专项科研基金资助项目(20100131120015)
作者简介：张　丽(1983-)，女，安徽临泉人，博士生，主要从事密码学与信息安全研究.
E-mail：lizhang@mail.sdu.edu.cn

Key words: crypt analysis; H^2-MAC-SHA-1; equivalent key recovery attack; universal forgery

消息认证码(Message Authentication Code, MAC)是带密钥的杂凑函数,输入密钥 K 和任意长度的消息 M,输出固定长度的摘要值。消息认证码常用于保证数据完整性和进行消息源认证,被广泛应用于各类 Internet 协议,如 SSL/TLS、SSH、IPsec 等。

*H*MAC 是国际通用的 MAC 标准之一[1]。HMAC 用到 2 个密钥——内部密钥与外部密钥,故在计算 MAC 值时需 2 次访问种子密钥,为密钥管理带来不便。

H^2-MAC 是 Kan Yasuda 在 ISC 2009 上提出的一种新型密钥前缀 MAC 结构[2]。H^2-MAC 与 *H*MAC 非常类似,不同之处仅在于 H^2-MAC 用固定的常数 IV 代替 *H*MAC 的外部密钥,因此计算出 MAC 值时只访问一次种子密钥,在保持 *H*MAC 优势的基础上简化密钥管理。但是,需深入考察外部密钥对 MAC 安全性的影响。2010 年,Wang 提出对 H^2-MAC-MD5 的选择性伪造攻击,复杂度为 2^{97} MAC[3]。2011 年,Liu 等提出对 H^2-MAC 的基于生日攻击的选择性伪造攻击,复杂度为 $2^{n/2}$ 次 MAC 查询(n 为 MAC 码长度)[4]。这二者都是选择性伪造攻击,即攻击者在不知道密钥的前提下,可计算形如$(M_0||M^*)$的消息的合法 MAC 值,其中 M_0 为一个完整的消息分组,M^* 为任意消息。而本文给出的是一般性伪造攻击,即在不知道密钥的情况下,攻击者可以伪造任意消息 M 的合法 MAC 值。

本文考察 *H*MAC 结构和 H^2-MAC 结构使用 SHA-1 算法进行实例化后的安全性。由二者的结构定义易知,H^2-MAC 的密钥相当于 *H*MAC 的内部密钥,对 *H*MAC 安全性分析均适用于 H^2-MAC 结构。对基于 SHA-0 的 *H*MAC 算法,存在内部密钥恢复攻击[5]。对基于 SHA-1 的 *H*MAC 算法,由于没有高概率的差分路线,目前最好的分析结果是基于缩减到 53(20-72)步 SHA-1 的 *H*MAC 算法的内部密钥恢复攻击[6]。这些攻击均可直接转换为 H^2-MAC-SHA-0/1 的密钥恢复攻击。本文在此基础上,提出了基于缩减到 53(20-72)步的 H^2-MAC-SHA-1 的等价密钥恢复攻击和一般性伪造攻击。

1　背景知识

1.1　符号定义

首先,定义本文出现的符号。H:杂凑函数;h:压缩函数;IV:杂凑函数的初始值;ICV_k:第 k 次迭代得到的中间链接变量;M_i:分组长度为 1 的消息;$\widetilde{K}$:等价密钥;$x||y$:比特串 x 和 y 的级联;$>>>s$:循环左移 s bit。

1.2　*H*MAC 和 H^2-MAC 算法

*H*MAC 是目前国际通用的 MAC 标准之一。计算消息 *M* 的 MAC 值如下:$HMAC(K,M)=H(IV,(K_0\oplus opad)\parallel H(IV,(K_0\oplus ipad)\parallel M))$. 其中,$K_0$ 是在密钥 K 填充足够多的"0"构成的一个消息分组,$opad$ 和 $ipad$ 分别是长度为一个消息分组的固定常数。*H*MAC 在计算 MAC 值时需 2 次访问密钥 K_0,为密钥管理带来不便。

为解决 *H*MAC 密钥管理方面的不便,在第 12 届信息安全国际会议上,Kan Yasuda 提出 H^2-MAC 结构[2]。H^2-MAC 计算如下(见图 1):

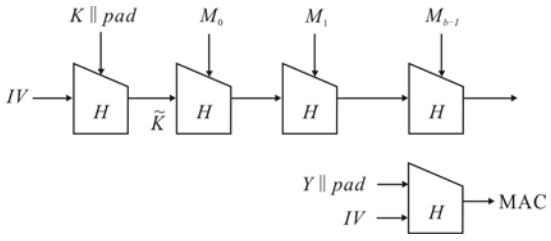

图 1　H^2-MAC 算法

Fig. 1　Graph one Method of H^2-MAC

H^2-MAC$(K,M)=H(IV,H(IV,K\parallel pad\parallel M))$,其中,$pad$ 是由 H 决定的常数,保证 $K\parallel pad$ 的长度为一个消息分组。根据采用的具体杂凑函数,将消息分成 b bit 大小的消息分组,在最后一个消息分组里进行填充并加入消息的长度。

可见,H^2-MAC 是外部密钥用初始 IV 代替的特殊的 *H*MAC。在软硬件实现时,与 *H*MAC 结构一样,H 可直接套用现有的杂凑函数,如 SHA-1。由于只访问一次密钥,更易于算法实现及密钥管理。但是只采用内部密钥为算法安全性带来了负面影响,攻击者一旦恢复中间链接变量的值,就可以进行一般性伪造,所以中间链接变量可看作等价密钥。

将用 SHA-1 算法代替 H 得到的 H^2-MAC 算法记为 H^2-MAC-SHA-1。不失一般性,定义 $\widetilde{K}=h(IV,K\parallel pad)$,见图 1。

2　基于 53(20-72)SHA-1 的 H^2-MAC 的等价密钥恢复攻击

首先,给出 H^2-MAC-SHA-1 的区分攻击,将 H^2-MAC-SHA-1 算法与基于随机函数(RF)的 H^2-

MAC 算法区分开。由于 SHA-1 的结构特性,没有高概率的差分路线,我们对基于缩减到 53(20-72)步 SHA-1 的 H^2-MAC 进行分析。然后,基于该区分器,结合比特探测技术,给出等价密钥的恢复攻击。最后,进行一般性伪造攻击。复杂度为 2^{99} 次 MAC 询问。

2.1 基于 53(20-72)的 H^2-MAC-SHA-1 区分攻击

H^2-MAC-SHA-1 的区分攻击的关键在于识别特定碰撞路线。利用特定的高概率碰撞路线的特殊结构,结合生日攻击,将特定的碰撞路线与其他类型的碰撞区分开来。一旦检测出碰撞,即可断定是 H^2-MAC-SHA-1;否则,断定为基于随机函数的 H^2-MAC。

我们使用选定基于缩减到 53(20-72)步 SHA-1 的碰撞路线[7]进行区分攻击:

1) 构造 2^{98} 对形如$(M_0||M_1, M'0||M_1)$的消息对,其中(M_0, M'_0)是随机选择的满足特定消息条件的 512 bit 消息分组,M_1 为任意的含有长度填充信息的消息分组,询问相应的 MAC 值。

2) 搜索出第 1)步所有能够产生碰撞的消息对,即:$H^2\text{-MAC}_{\widetilde{K}}(M_0||M_1)=H^2\text{-MAC}_{\widetilde{K}}(M'_0||M_1)$。

3) 区分符合特定差分路线的碰撞。对第 1)步中找到的所有碰撞消息对$(\overline{M}_0||M_1, \overline{M}'_0||M_1)$,选择一个含填充信息的 512 bit 的消息分组 M_1 代替 M_1,对$(\overline{M}_0||M'_1, \overline{M}'_0||M'_1)$做 MAC 询问,如果仍然产生碰撞,则说明此碰撞满足特定的差分路线,即 $ICV_1=ICV'_1$,我们认为该 MAC 算法是基于 53 步的 SHA-1 的 H^2-MAC,否则该 MAC 码算法是基于随机函数的。

复杂度分析:

该攻击的第 2 步需要 2×2^{98} MAC 询问,第 3 步需要 2 次 MAC 询问,故区分攻击的复杂度为 $2\times2^{98}+2=2^{99}$ 次 MAC 查询,数据复杂度为 2^{99} 个选择消息。

2.2 恢复密钥 $\widetilde{K}$

假设$(M_0||M_1, M'_0||M_1)$是利用 2.1 节的区分器识别出的一个符合选定路线的碰撞,利用文献[6]的方法,结合 Contini 和 Yin 提出的比特探测技术[5],利用差分路线和 SHA-1 的性质恢复等价密要 $\widetilde{K}$。攻击步骤如下:

第 1 步:利用 2.1 节的区分攻击找到一对碰撞消息对$(M_0||M_1, M'_0||M_1)$。

第 2 步:攻击者修改(M'_0)的特定比特位获得一个新消息(M_0^*),根据$(M_0||M_1, M_0^*||M_1)$是否仍为碰撞的概率来判断计算 $SHA\text{-}1_k(M)$时的中间寄存器 $S=(A_{31}, B_{31}, C_{31}, D_{31}, E_{31})$的 135 bit。即计算 $H(\widetilde{K}, M)$时,第 31 步的寄存器的值。

第 3 步:攻击者猜测 S 尚未确定的 25 bit,对每一种可能,根据 SHA-1 算法的步操作和消息值,依次计算可能的$(A_{19}, B_{19}, C_{19}, D_{19}, E_{19})$,通过计算对应 MAC 值与已有值进行比较,若相等,即为正确的等价密钥 $\widetilde{K}$。

攻击的复杂度主要由第 1 步决定,由于碰撞路线成立的概率是 2^{98},通过区分攻击识别碰撞,复杂度为 2^{99} 次 MAC 查询。等价密钥恢复攻击的复杂度为 2^{99} 次 MAC 查询。

2.3 一般性伪造攻击

一般性伪造是指攻击者在不知道密钥 K 的情况下,可以计算任意消息 M 的合法 MAC 值。

一旦攻击者恢复基于缩减到 53(20-72)步 SHA-1 的 H^2-MAC 的等价密钥 $\widetilde{K}$,可根据下式进行伪造攻击,计算任意消息 M 的 MAC 值 T:

$T=H^2\text{-MAC}(K, M)=H(IV, H(IV, K\|pad\|M))=H(IV, H(IV, \widetilde{K}\|M))$,式中 $\widetilde{K}$ 为利用 2.2 节的密钥恢复攻击确定的等价密钥。可见,攻击者在不知道密钥 K 的情况下,可计算任意消息的合法 MAC 值。复杂度仅为 1 次 MAC 计算。

3 结语

H^2-MAC 是 2009 年提出的一种新型 MAC 结构。与杂凑函数国际标准 HMAC 相比,只访问一次密钥,更易于算法实现及密钥管理。但是,我们发现,由于将 HMAC 结构的外部密钥用常数代替,一旦中间链接变量泄露,就可以进行一般性伪造。

本文比较 HMAC 结构和 H^2-MAC 结构分别用缩减到 53(20-72)步 SHA-1 实例化后得到的具体算法的安全性。对 HMAC-SHA-1,目前存在利用截断的高概率差分路线的区分攻击[8-11]。而对基于缩减到 53(20-72)步 SHA-1 的 H^2-MAC,本文给出等价密钥恢复攻击,并进行一般性伪造。首先,利用 2.1 区分攻击寻找一个消息分组保证满足特殊差分的中间链接变量,即等价密钥 $\widetilde{K}$ 存在,通过文献[4]的方法恢复 $\widetilde{K}$ 的值,攻击的复杂度为 2^{99} 次 MAC 查询。该等价密钥恢复攻击可直接导致一般性伪造攻击,即攻击者在不知道密钥的情况下可伪造任意消息 M 的合法 MAC 值。

参考文献(References):

[1] Bellare M, Canetti R, Krawczyk H. Keying Hash functions for message authentication [C]//CRYPTO 1996, LNCS 1109. Heidelberg: Springer, 1996: 1-

15.

[2] Yasuda,K. *H*MAC without the "Second" key [C]// ISC 2009, LNCS 5735. Heidelberg: Springer, 2009: 443-458.

[3] Wei Wang. Equivalent Key Recovery Attack on H^2-MAC Instantiated with MD5[J]. Communications in computer and information science,2011,200:11-20.

[4] Liu Fanbao, Xie Tao, Shen Changxiang. Equivalent key recovery attack to H^2-MAC[J]. International journal of security and its application,2012,6(2):56-61.

[5] Contini S, Yin Y L. Forgery and partial key-recovery attacks on *H*MAC and NMAC using hash collisions [C]//ASIACRYPT 2006, LNCS 4284. Heidelberg: Springer,2006: 37-53.

[6] Rechberger C, Rijmen, V. New results on NMAC/ *H*MAC when instantiated with popular hash functions [J]. Journal of universal computer science, 2008, 14(3): 347-376.

[7] Preneel B, Oorschot van P. MDx-MAC and building fast MACs from Hash functions [C]//CRYPTO 1995, LNCS 963. Heidelberg: Springer, 1995: 1-14.

[8] Wang X, Yu H, Wang W, et al. Cryptanalysis on *H*MAC/ NMAC-MD5 and MD5-MAC [C]//EUROCRYPT 2009, LNCS 5479. Heidelberg: Springer, 2009: 121-133.

[9] Wang X, Wang W, Jia K, et al. New distinguishing attack on MAC using secret-prefix method[J]. Computer science,2009,5665: 363-374.

[10] Wang X, Yu H, Yin Y L. Efficient collision search attacks on SHA-0 [C]//CRYPTO 2005, LNCS 3621. Heidelberg: Springer, 2005: 1-16.

[11] Wang X, Yin Y L, Yu H. Finding collisions in the full SHA-1 [C]//CRYPTO 2005, LNCS 3621. Heidelberg: Springer, 2005: 17-36.

本刊相关链接文献:

[1]张串绒,张玉清. 基于身份的前向安全和可公开验证签密方案[J]. 空军工程大学学报:自然科学版,2009,10(3):78-81.

ZHANG Chuanrong, ZHANG Yuqing. Identity based signcryptin scheme with forward security and public verifiability[J]. Journal of air force engineering university: natural science edition,2009,10(3):78-81. (in Chinese)

[2]曹帅,张串绒,宋程远. 基于身份的移动网动态可认证群组密钥协商协议[J]. 空军工程大学学报:自然科学版,2011,12(5):67-71.

CAO Shuai, ZHANG Chuanrong, SONG Chengyuan. Identity-based dnamic athenticated goup key agreement protocol for mobile networks[J]. Journal of air force engineering university: natural science edition, 2011, 12(5):67-71. (in Chinese)

[3]张串绒,肖国镇. 基于签密技术的可认证密钥协商协议[J]. 空军工程大学学报:自然科学版,2006,7,(6):65-67.

ZHANG Chuanrong, XIAO Guozhen. Sign-cryptic technique based on authenticated key agreement protocol[J]. Journal of air force engineering university: natural science edition, 2006,7,(6):65-67. (in Chinese)

[4]魏靓,郑连清,张串绒,崔晓臣. 一种适于 Ad hoc 网络恶意节点处理的多接收者签密算法[J]. 空军工程大学学报:自然科学版,2011,12(1):68-72.

WEI Liang, ZHENG Lianqing, ZHANG Chuanrong, CUI Xiaochen. Multi-recipient signcryption algorithm for dealing with malicious nodes of Ad hoc networks[J]. Journal of air force engineering university: natural science edition, 2011,12(1):68-72. (in Chinese)

[5]柏骏,张串绒,王珏. 关于不使用 Hash 和 Redundancy 函数签密方案的分析与改进[J]. 空军工程大学学报:自然科学版,2010,11(1):91-94.

BAI Jun, ZHANG Chuanrong, WANG Jue. The analysis and improvement of a signcryption scheme without using Hash and Redundancy functions[J]. Journal of air force engineering university: natural science edition, 2010,11(1):91-94. (in Chinese)

(编辑:徐楠楠)