无线局域网WPS安全性分析

刘永磊[1,2],金志刚[3]
LIU Yonglei[1,2], JIN Zhigang[3]

1.天津大学 计算机科学与技术学院,天津 300072
2.天津城市建设学院 电子与信息工程系,天津 300384
3.天津大学 电子信息工程学院,天津 300072
1.School of Computer Science and Technology, Tianjin University, Tianjin 300072, China
2.Department of Electronic and Information, Tianjin Institute of Urban Construction, Tianjin 300384, China
3.School of Electronic and Information Engineering, Tianjin University, Tianjin 300072, China

LIU Yonglei, JIN Zhigang. Security analysis of WPS in WLAN. Computer Engineering and Applications, 2013, 49(21):87-89.

Abstract: In this paper, an overview of Wi-Fi Protected Setup(WPS) is supplied. A brute force attack is pointed out. Using Colored Petri Nets(CPN), the WPS protocol and the improvement are modeled and it is proven that the security flaws exist and the brute force attack is available. Moreover, under setting retry times of connection authentication to be three times, the original protocol can be completely breached and the success breach probability of the improved protocol is only about $3/10^8$.

Key words: Wireless Local Area Network(WLAN); Wi-Fi protected setup; brute force; colored Petri nets; personal identification number; protocol formal analysis

摘 要: 介绍了Wi-Fi联盟的WPS标准并给出了对应的攻击方法——暴力破解攻击,使用CPN对WPS协议及改进协议进行形式化分析并证明AP限制重新发起连接认证的次数为3次时,原协议可完全被攻破而给出的改进协议成功概率仅约为$3/10^8$。

关键词: 无线局域网; Wi-Fi受保护安装; 暴力破解; 着色Petri网; 个人识别码; 协议形式化分析
文献标志码: A **中图分类号:** TP393 doi:10.3778/j.issn.1002-8331.1201-0151

WPS(Wi-Fi Protected Setup)是Wi-Fi联盟提出的一种用于简易快速建立安全WLAN的标准[1],用户采用四种方式接入网络:PIN,PBC,NFC和USB。本文讨论PIN(个人识别码)方式的安全性。

1 WPS协议架构

WPS协议定义了三种类型的网络设备:认证服务器(Registrar),无线终端(Enrollee)和无线接入点(AP)。典型地,AP充当Registrar,用户通过按键接口或带外频道输入设备PIN,接着Enrollee 与AP通过交互基于EAP[2]消息封装的八次握手过程进行认证(如图1所示)。

八次握手包的含义如图2所示。其中$N1$,$N2$为Enrollee和Registrar选取的随机数。R-S1,R-S2,E-S1和E-S2为秘密的128 bit Nonce。HMAC采用HMAC-SHA-256,ENC采用AES-CBC加密。M_n^*为M_n排除消息鉴别码字段。

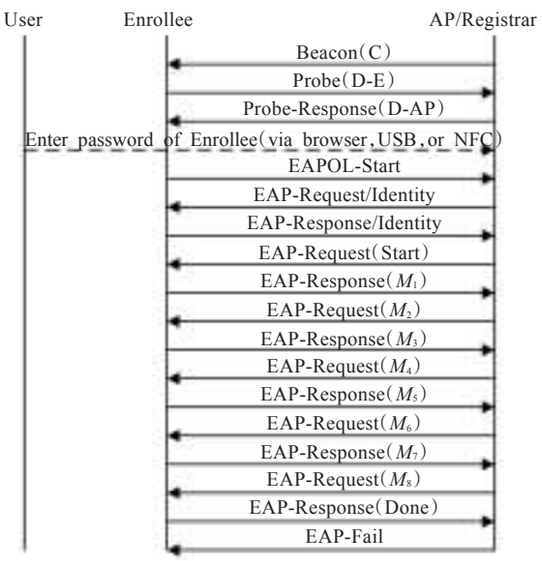

图1 典型的WPS安装过程

基金项目: 天津大学自主创新基金资助。

作者简介: 刘永磊(1983—),男,博士研究生,讲师,主要研究方向:无线网络安全;金志刚(1972—),男,教授,博导,主要研究方向:网络性能评价、计算机网络管理与安全、宽带无线网络。E-mail:zgjin@tju.edu.cn

收稿日期: 2012-01-10 **修回日期:** 2012-02-24 **文章编号:** 1002-8331(2013)21-0087-03
CNKI出版日期:2012-06-18 http://www.cnki.net/kcms/detail/11.2127.TP.20120618.1131.004.html

$M_1=\text{Version}||N1||\text{Description}||PK_E$

$M_2=\text{Version}||N1||N2||\text{Description}||PK_R[||\text{ConfigData}]||HMAC_{\text{AuthKey}}(M_1||M_2^*)$

$M_3=\text{Version}||N2||E\text{-}Hash1||E\text{-}Hash2||HMAC_{\text{AuthKey}}(M_2||M_3^*)$

$M_4=\text{Version}||N1||R\text{-}Hash1||R\text{-}Hash2||ENC_{\text{KeyWrapKey}}(R-S1)||HMAC_{\text{AuthKey}}(M_3||M_4^*)$

$M_5=\text{Version}||N2||ENC_{\text{KeyWrapKey}}(E\text{-}S1)||HMAC_{\text{AuthKey}}(M_4||M_5^*)$

$M_6=\text{Version}||N1||ENC_{\text{KeyWrapKey}}(R\text{-}S2)||HMAC_{\text{AuthKey}}(M_5||M_6^*)$

$M_7=\text{Version}||N2||ENC_{\text{KeyWrapKey}}(E\text{-}S2[||\text{ConfigData}])||HMAC_{\text{AuthKey}}(M_6||M_7^*)$

$M_8=\text{Version}||N1||[ENC_{\text{KeyWrapKey}}(\text{ConfigData})]||HMAC_{\text{AuthKey}}(M_7||M_8^*)$

图2 八次握手包

双方通过Diffie-Hellman密钥交换完成会话密钥的形成。$DHKey=SHA\text{-}256(g^{AB} \bmod p)$。$PK_E$为$g^A \bmod p$，$PK_R$为$g^B \bmod p$。$KDK=HMAC_{\text{DHKey}}(N1||EnrolleeMAC||N2)$。AuthKey和KeyWrapKey由kdf(KDK,“Wi-Fi Easy and Secure Key Derivation”,640)[1]产生。如此经过M_1~M_2完成会话密钥的分发。

PIN为4位或8位十进制数字,如“23458790”。

PSK1=first 128 bit of $HMAC_{\text{AuthKey}}(1^{\text{st}}\text{ half of }PIN(PIN1))$

$PSK2=\text{first 128 bit of }HMAC_{\text{AuthKey}}(2^{\text{nd}}\text{ half of }PIN(PIN2))$

$E\text{-}Hash1=HMAC_{\text{AuthKey}}(E\text{-}S1||PSK1||PK_E||PK_R)$

$E\text{-}Hash2=HMAC_{\text{AuthKey}}(E\text{-}S2||PSK2||PK_E||PK_R)$

$R\text{-}Hash1=HMAC_{\text{AuthKey}}(R\text{-}S1||PSK1||PK_E||PK_R)$

$R\text{-}Hash2=HMAC_{\text{AuthKey}}(R\text{-}S2||PSK2||PK_E||PK_R)$

M_3~M_8进行对PIN的认证,如果验证成功,M_8的ConfigData中会包含此WLAN的Credential,即欲共享密钥PSK。

2 WPS攻击模型——暴力破解

第一轮进攻:攻击者发起到AP的连接认证过程,与AP交互M_1~M_4,获得$R\text{-}S1$,PK_E,PK_R,KeyWrapKey和AuthKey,通过暴力破解[1,3]$R\text{-}Hash1$获得$PIN1$。由于攻击开始阶段$PIN1$未知,M_5发给AP后,AP验证先前M_3中$E\text{-}Hash1$通过的概率仅为$1/10^4$。因此收到EAP-Failure包必须重新发起新的认证过程。

第二轮进攻:攻击者发起到AP新的连接认证过程,由于已经获得$PIN1$,可通过AP对$E\text{-}Hash1$的验证,依次获得M_1~M_6,暴力破解$R\text{-}Hash2$获得$PIN2$,由于攻击开始阶段$PIN2$未知,M_7发给AP后,AP验证先前M_3中$E\text{-}Hash2$通过的概率仅为$1/10^4$。因此EAP-Failure包必须重新发起新的认证过程。

第三轮进攻:攻击者发起到AP新的连接认证过程,由于已经获得$PIN1$,$PIN2$,M_1~M_8交互均可成功,攻击完成。

3 基于CPN的WPS协议分析

着色Petri网(CPN)[4]作为一种形式化协议分析工具,应用逐渐广泛[5-7]。采用CPN对WPS协议进行建模,安全性分析和改进。在引入攻击模型后,协议的CPN模型如图3所示。

该模型中,协议中涉及的$N1$,$N2$,$R\text{-}S1$,$R\text{-}S2$,$E\text{-}S1$,$E\text{-}S2$,PK_E,PK_R均为入侵者(Intruder)和AP随机选择并非变迁产生的结果,KeyWrapKey和AuthKey也为密钥交换后由kdf导出并非变迁产生的结果,因此该模型对协议进行了简化。

定义不安全状态为$a13$,此时攻击者经过几轮进攻获得了PSK,进而可以在未授权的情况下通过AP接入网络。采用矩阵分析法[8]和状态方程(见公式(1)[4])分析WPS协议安全性。

$$\boldsymbol{M}_n=\boldsymbol{M}_0+\boldsymbol{A}\sum_{i=1}^{m}\boldsymbol{\sigma}_i^t \tag{1}$$

$\boldsymbol{M}_n$为不安全状态,$\boldsymbol{M}_0$为初始状态,$\boldsymbol{\sigma}_i^t$为变换向量表示哪个变迁发生为29维列向量,求和符号表示每个变迁可点火多次。$\boldsymbol{A}(\boldsymbol{S}_i,\boldsymbol{T}_j)$为变换矩阵,$\boldsymbol{S}_i$依次为$a1$~$a14$,$c1$~$c8$,$b1$~$b10$,$d1$,$d2$。$\boldsymbol{T}_j$依次为$t1$~$t27$,$t28$,$t29$。$\boldsymbol{A}$为34×29矩阵,篇幅所限不一一列出,特别地,当收到EAP-Failure,$A_{[13][19]}=\text{start}$成立变迁可发生,若为$M_6$,$A_{[9][19]}=PIN2$成立变迁可发生。$E\text{-}Hash1$校验成功$A_{[29][16]}=M_6$,失败时$A_{[29][16]}=\text{fail}$且$A_{[32][16]}=\text{fail}$成立变迁可发生。同理可确定变换矩阵$\boldsymbol{A}$的取值。

首先考察对于原协议的攻击,即去除矩形框内的状态$d1$、$d2$和变迁$t28$、$t29$。为了让变迁顺利进行,假设$b4$和$b5$态有无穷多个标签。

$$\boldsymbol{M}_0^{\mathrm{T}}=[0,0,PIN1,PIN2,0,0,0,0,0,0,0,0,0,0,\text{start},0,0,0,0,0,0,0,0,0,0,0,0,\infty,\infty,0,0,0,0,0]$$

为32维行向量

$$\boldsymbol{M}_n^{\mathrm{T}}=[0,0,0,0,0,0,0,0,0,0,0,0,0,0,\text{success},0,0,0,0,0,0,0,0,0,0,0,0,\infty,\infty,0,0,0,0,0]$$

为32维行向量

将$\boldsymbol{M}_0^{\mathrm{T}}$,$\boldsymbol{M}_n^{\mathrm{T}}$,和$\boldsymbol{A}(\boldsymbol{S}_i,\boldsymbol{T}_j)$中$\boldsymbol{S}_i$为$a1$~$a14$,$c1$~$c8$,$b1$~$b10$,$\boldsymbol{T}_j$为$t1$~$t27$部分组成的32×27维矩阵代入公式(1),此时$\boldsymbol{\sigma}^t$也去除了分量$t28$,$t29$为27维列向量,利用线性代数中方程组解的判别方法可判定$\boldsymbol{\sigma}^t$有解,说明不安全状态$\boldsymbol{M}_n$由初始状态$\boldsymbol{M}_0$可达,因此WPS协议存在安全漏洞据此可发动暴力破解攻击。

假设AP采取了一定的安全防范措施即重新发起连接认证的次数限制为3次。在此条件下暴力破解成功的概率为p,也即$\boldsymbol{M}_n$状态可达的概率。

$$p=\sum_{n=0}^{2}C_2^n\left(\frac{1}{10^4}\right)^n\left(\frac{9\,999}{10^4}\right)^{2-n}=1 \tag{2}$$

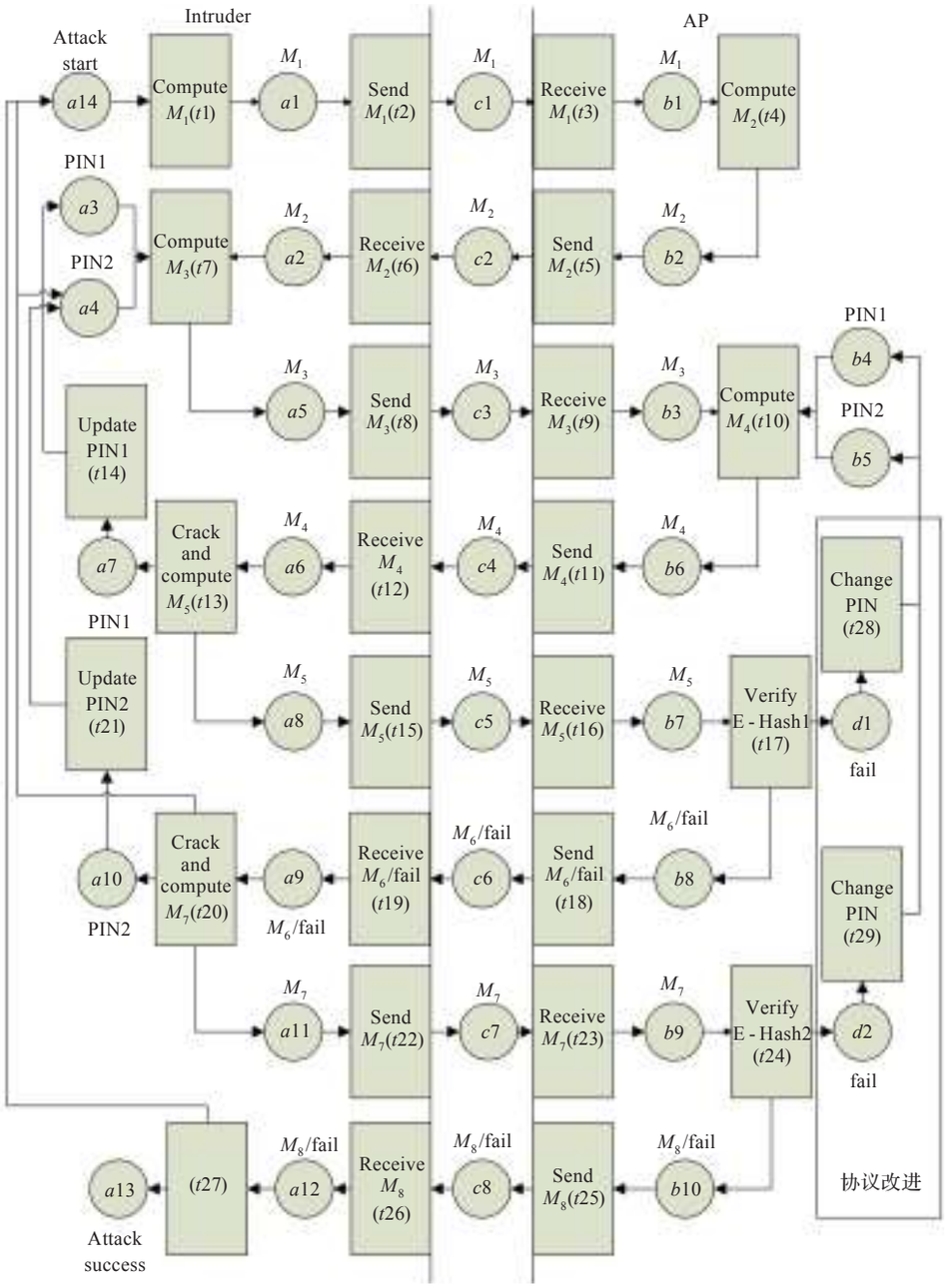

图3　WPS协议攻击模型

4　WPS改进协议安全性分析

由于原协议的安全脆弱,改进方法是认证协议每次重新发起都强制使用不同的PIN(见图3的矩形框),攻击者每轮攻击都必须重新破解新的 $PIN1$,因此攻击者总是陷入第一轮,能进入第二轮的概率为 $1/10^4$,进入第三轮的概率更低为 $1/10^8$。此时:

$$\boldsymbol{M}_0^{\mathrm{T}}=[0,0,PIN1,PIN2,0,0,0,0,0,0,0,0,0,\text{start},0,0,0,0,0,0,0,0,0,0,0,0,PIN1,PIN2,0,0,0,0,0,0,0,0]$$

为34维行向量

$$\boldsymbol{M}_n^{\mathrm{T}}=[0,0,0,0,0,0,0,0,0,0,0,0,0,0,\text{success},0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0]$$

为34维行向量

将 $\boldsymbol{M}_0^{\mathrm{T}}$,$\boldsymbol{M}_n^{\mathrm{T}}$,和 $\boldsymbol{A}$ 代入公式(1),利用线性代数中方程组解的判别方法可判定 $\boldsymbol{\sigma}^t$ 有解,说明不安全状态 $\boldsymbol{M}_n$ 由初始状态 $\boldsymbol{M}_0$ 可达。依然假设重新发起连接认证的次数限制为3次,此时暴力破解成功的概率为 p,也即 $\boldsymbol{M}_n$ 状态可达的概率。

$$p=\sum_{n=1}^{3}\left(\frac{1}{10^8}\right)\left(1-\frac{1}{10^8}\right)^{n-1}<\frac{3}{10^8} \tag{3}$$

相较于原协议,在AP限制重新发起连接认证的次数为3次的情况下,改进使暴力破解成功的概率从1降为 $3/10^8$ 以下,优势明显。但PIN大都基于固定的标签设备,如无线网

(下转105页)