适用于移动云计算的抗中间人攻击的 SSP 方案

陈 凯[1,2,3],许海铭[4,5],徐 震[1,2],林东岱[1,2],刘 勇[6]
(1. 信息安全国家重点实验室,北京 100093;2. 中国科学院信息工程研究所,北京 100093;3. 中国科学院大学,北京 100049;
4. 国家能源局安全司,北京 100824;5. 华北电力大学电气与电子工程学院,北京 102206;
6. 山东省电力公司调度控制中心自动化处,山东济南 250000)

摘 要: 低功率蓝牙(BLE)专为资源受限的设备设计,但现有的研究已经指出其安全简单配对方案(SSP)存在中间人攻击(MITM)漏洞. 文章指出造成 MITM 漏洞的根本原因是:配对信息被篡改以及 JW 模式自身的漏洞. 为此文章中提出了两个适用于移动云计算(MCC)中 BLE 设备的 SSP 改进方案,所提出的方案基于哈希函数并利用 MCC 技术提高 SSP 的安全性. 方案 1 适用于支持 PE 或者 OOB 模式的 BLE 设备,其利用哈希函数确保配对信息的真实性、可靠性. 方案 2 通过哈希序列来解决仅支持 JW 模式的 BLE 设备的 MITM 攻击漏洞. 文章分别从安全角度和性能角度对所提出的方案进行分析,以表明方案在不同级别敌手的攻击下可以提供 MITM 攻击防护能力.

关键词: 蓝牙低功率; 安全简单配对方案; 中间人攻击; 移动云计算
中图分类号: TP309.1 **文献标识码:** A **文章编号:** 0372-2112 (2016)08-1806-08
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2016.08.005

Hash-Based Secure Simple Pairing for Preventing Man-in-the-Middle Attacks in Mobile Cloud Computing

CHEN Kai[1,2,3], XU Hai-ming[4,5], XU Zhen[1,2], LIN Dong-dai[1,2], LIU Yong[6]
(1. *State Key Laboratory of Information Security, Beijing* 100093, *China*;
2. *Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093, *China*;
3. *University of Chinese Academy of Science, Beijing* 100049, *China*; 4. *National Energy Administration, Beijing* 100824, *China*;
5. *School of Electrical and Electronic Engineering, North China Electric Power University, Beijing* 102206, *China*;
6. *State Grid Shandong Electric Power Company, Dispatching Control Center, Jinan, Shandong* 250000, *China*)

Abstract: Bluetooth low energy (BLE) is designed for the devices with computational and power limitations. But it has been confirmed that Secure Simple Pairing (SSP) is vulnerable to the MITM attack. We identify the root causes of the problem: the pairing messages being tampered, and the vulnerability of the JW model. In this paper, we propose two hash-based SSP schemes for the devices in Mobile Cloud Computing (MCC). The proposed schemes enhance the SSP security with the help of MCC. Scheme I is applied into the devices which support the PE or OOB model. It uses the hash function to ensure the authenticity and integrity of the pairing messages. Scheme II is suitable for the devices which only support the JW model. It improves the security of the JW model through using the hash array. At the end of this paper, we examine the performance for the proposed schemes, and perform the security analysis to show that they can provide the MITM protection against the adversaries with different levels of power.

Key words: bluetooth low energy; secure simple pairing; man-in-the-middle attacks; mobile cloud computing

1 引言

低功率蓝牙(BLE)在蓝牙 v4.0 版本中被提出. BLE 的设计初衷是将蓝牙技术应用于仅由“纽扣”电池供电的便携设备中. 借助于 MCC 技术[1],BLE 产品得到了极大的丰富. 对于 MCC 中的 BLE 设备来说,移动终端设备通常作为 master,而周边设备作为 slave.

自蓝牙 v2.1 版本后,安全简单配对(SSP)方案被

收稿日期:2015-01-15;修回日期:2015-03-17;责任编辑:蓝红杰
基金项目:中国科学院先导专项子课题(No. XDA06010701);信息安全国家重点实验室科研仪器设备专项(No. Y4D0031302)

引入蓝牙标准中来实现设备配对过程. 在 BLE 标准中,SSP 提供三种不同的关联模型:Just Work 模型(JW)、Passkey Entry 模型(PE)及 Out of Band 模型(OOB). 其中,JW 模型无法抵抗中间人(MITM)攻击. 近年来,研究人员已经提出了多种方法[2,3],可以强迫对端设备使用 JW 模型,从而利用 JW 模型的漏洞来实施 MITM 攻击. 造成 MITM 攻击漏洞的根本原因为:(1)在 SSP 过程中,用来交换设备输入/输出(I/O)信息的配对消息可能被攻击者篡改;(2)JW 模型在 SSP 过程中无法提供 MITM 攻击防护.

为了提高 BLE 设备的安全性,使其具有抗 MITM 攻击能力,本文首先针对 MCC 环境中 BLE 的典型应用场景进行分析. 作者发现在 MCC 环境中,BLE 设备具有以下特征:(1)所有的 master 设备至少支持两种不同的无线通信信道;(2)大多数 slave 设备仅支持一种通信信道,因此 slave 设备无法直接与云服务连接;(3) master 设备的能力通常强于 slave 设备;(4)计算能力上的限制使得复杂的密码运算无法在 BLE 设备上运行,尤其无法在 slave 设备上运行.

根据以上的分析结果,本文通过如下两种方式来提高 SSP 方案的安全性:(1)由于 master 设备支持多个通信信道,因此,本文引入位于云端的可信第三方(TTP)来协助 BLE 设备交换其 I/O 能力信息;(2)考虑到 BLE 设备的处理能力有限,本文所提出的方案仅在 BLE 设备上运行轻量级的密码算法,以此来最小化 BLE 设备的负载.

2　相关研究工作

Haataja 等人[4,5]建议在应用层增加额外的安全机制来提高 SSP 的安全性. 例如,在应用层增加额外的确认窗口以确保正确的关联模型被使用. Sharmila 等人[6]提出了一种 OOB 信道可变频率的方案来提高 SSP 的安全性. 在他们的方案中,OOB 信道的频率被预置在每个设备中,在特定的周期内,通信双方使用特定的 OOB 频率进行带外通信.

RF 指纹是由 Ureten 和 Serinken[7]提出的一种增强无线网络通信安全性的方法. Pasanen 等人[8]将 RF 指纹技术扩展到蓝牙设备中. 在 Pasanen 等人的方案中,一台专用服务器负责存储所有合法蓝牙设备的 RF 信息,并且以此来判断是否允许正在发射 RF 信号的蓝牙设备相连.

耿君峰等人[9]通过分组净化与蓝牙设备地址绑定来帮助蓝牙设备抵抗自外部设备的窃听攻击、主设备地址假冒攻击、分组伪造攻击和来自内部设备的分组否认攻击.

目前,还有一些研究人员提出了针对蓝牙的入侵检测系统和入侵防御系统[10],这些系统试图从网络的角度防御针对蓝牙设备的攻击.

与本文所提出的方案相比,Haataja 等人的方案要求蓝牙终端必须具有显示输出设备. 而 Sharmila 等人提出的方案对于仅支持 Just Work 模型的 BLE 设备起不到保护作用. FR 指纹能够提供的安全性较高,但是 Pasanen 等人的方案只适用于局部场景中,例如,在一个办公大厦内负责一个公司内的蓝牙设备. 对于入侵检测系统和入侵防御系统来说,需要特定的部署模式才能充分发挥功效.

3　SSP 安全现状

现有的研究[11,12]表明 MITM 攻击对蓝牙设备来说是一个严重的威胁. MITM 攻击者实施攻击的主要手段[4,5,13~16]是强迫配对的 BLE 设备使用 JW 模型,并且利用 JW 模型不提供 MITM 攻击保护的漏洞进行攻击.

如图 1 所示,MITM 攻击者首先中断 BLE 设备的物理层连接,以使得受害用户误以为他们的 BLE 设备出现的问题. 被欺骗的用户很可能会删除设备中已经存储的密钥,并重新进行设备配对. 在设备重新配对过程中,攻击者伪造 BLE 设备的 I/O 能力信息,以使得受害的 BLE 设备误以为对方“既无输入能力,也无输出能力”. 随后,JW 模型被强迫使用. 由于 JW 模型不能提供 MITM 攻击防护能力,所以 MITM 攻击者可以窃听受害 BLE 设备的通信,甚至可以篡改用户的数据.

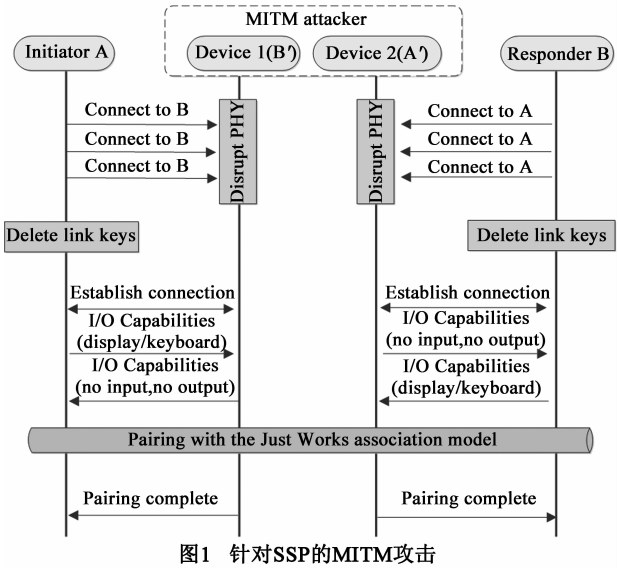

图1　针对SSP的MITM攻击

4　基本假设、威胁模型与目标

本文假设敌手针对 BLE 的 SSP 方案进行 MITM 攻击,作者考虑多级能力的敌手模型并假设 level N 敌手拥有所有级别小于 N 的敌手的能力:

(1)Level 1 敌手:敌手有能力窃听合法设备之间的会话数据,并在随后的攻击中重放窃听得到的数据;

(2)Level 2 敌手:敌手能够主动阻断合法设备之间的信息交换,并可以在合法设备配对过程中插入、篡改信息;

(3)Level 3 敌手:敌手有能力主动询问合法的设备,记录下合法设备回复的信息,并在随后的攻击中进行重放.

本文的目标是,所提出的 SSP 改进方案能够在面对 level 1 到 level 3 级敌手的情况下,向 MCC 中的 BLE 设备提供抗 MITM 攻击能力.

5 基于哈希的 SSP 改进方案

5.1 方案 I:基于哈希函数的 SSP 方案

方案 I 引入位于云端平台的 TTP 来提供配对设备的 I/O 能力信息的哈希值,该哈希值将会和 BLE 设备自身提供的 I/O 能力信息的哈希值进行比较. 为了标识设备,每台 BLE 设备将会被预设一个唯一的内部 ID 值(intid). 如表 1 所示,TTP 维护一个数据库表,来储存所有 BLE 设备的物理地址 Addr、当前内部 ID($intid_c$)、上次使用的内部 ID($intid_l$)和设备的 I/O 能力信息. TTP 为每个 BLE 设备存储两个内部 ID 是为了解决消息丢失问题. 如果由于意外事件或攻击者攻击造成消息丢失,那么 BLE 设备仍然可以通过 $intid_l$ 被正确的识别.

表 1 TTP 中的数据库表格

Address	$intid_c$	$intid_l$	I/O Capabilities
	0x14DA2C21	0x981CF4D2	keyboard
0C:84:DC:	5B121EC8	34263318	input/
DC:FF:2A	2598D64F	4C0F58D1	numeric
	AFA0957B	183F6E2D	output
……	……	……	……

图 2 详细描述了方案 I 的步骤. 设哈希函数为 $h(\,)$,符号 ‖ 表示字符串拼接. 具体的方案流程如下:

(1)Master 设备产生随机数挑战 R_m;

(2)Master 将随机数挑战 R_m 连同配对请求消息发送给 slave 设备;

(3)Slave 设备产生随机数 R_s,并通过公式(1)计算出外部 ID;

$$\text{extid}_s = h(\text{intid}_s \parallel R_m \parallel R_s) \tag{1}$$

(4)extid_s 连同随机数 R_s 一起通过配对响应消息发送给 master 设备;

(5)当收到配对响应消息后,master 设备使用和 slave 设备相同的方法计算出外部 ID 值 extid_m;

$$\text{extid}_m = h(\text{intid}_m \parallel R_m \parallel R_s) \tag{2}$$

(6)Master 设备将含有 R_m、R_s、extid_m 和 extid_s 的验证请求消息发往 TTP;

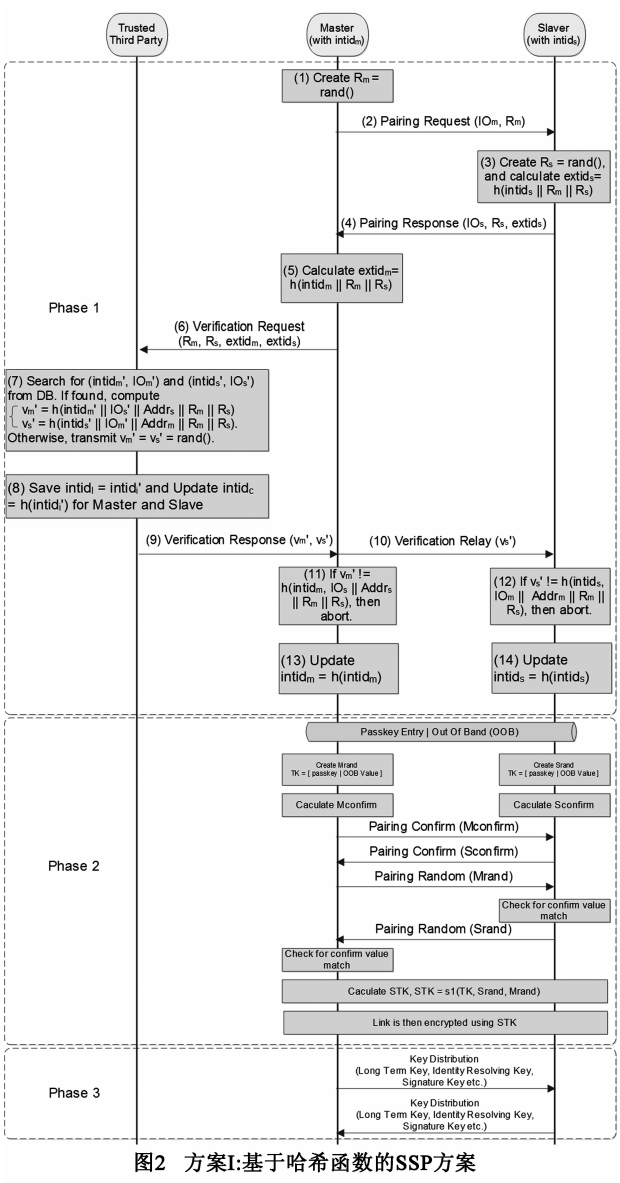

图2 方案I:基于哈希函数的SSP方案

(7)当 TTP 接收到验证请求消息后,根据 Addr_m 和 Addr_s 分别找到 master 设备和 slave 设备的记录. 随后,TTP 为每个设备计算哈希值 $h(\text{intid}_c \parallel R_m \parallel R_s)$ 和 $h(\text{intid}_l \parallel R_m \parallel R_s)$,并将其与接收到的 extid_m 和 extid_s 做对比. 匹配则意味着 TTP 查找到 master 设备的信息(IO_m', $intid_m'$)和 slave 设备的信息(IO_s', $intid_s'$). 其中,$intid_i'$ 表示匹配记录的内部 ID,IO_i' 表示记录中所保存的 I/O 能力信息. 如果 TTP 无法查找到 master 设备或者 slave 设备的信息或者哈希值不匹配,那么验证响应消息(v_m', v_s')将会被设置为随机数. 否则,TTP 按照公式(3)给 master 设备生产验证信息,按照公式(4)为 slave 设备生产验证信息;

$$v_m' = h(\text{intid}_m' \parallel IO_s' \parallel \text{Addr}_s \parallel R_m \parallel R_s) \tag{3}$$

$$v_s' = h(\text{intid}_s' \parallel IO_m' \parallel \text{Addr}_m \parallel R_m \parallel R_s) \tag{4}$$

(8)TTP 首先将 master 设备和 slave 设备的 intid_i'保存为 intid_l,随后根据公式(5)更新 intid_c;

$$\text{intid}_c = h(\text{intid}_i') \tag{5}$$

(9)TTP 将包含 v_m'和 v_s'的验证响应消息发送给 master 设备;

(10)Master 设备接收到验证响应消息后,通过验证转发消息直接将 v_s'转发给 slave 设备;

(11)Master 设备按照公式(6)重新计算出自己的验证消息 v_m,并将 v_m与 v_m'做对比.

$$v_m = h(\text{intid}_m \parallel IO_s \parallel \text{Addr}_s \parallel R_m \parallel R_s) \tag{6}$$

如果 v_m与 v_m'相同,那么 master 将按照原 SSP 方案的步骤继续执行. 否则,master 设备终止设备配对过程;

(12)slave 设备通过公式(7)计算出验证消息 v_s,并将 v_s与 v_s'做对比,一旦发现不一致 slave 设备则终止设备配对过程;

$$v_s = h(\text{intid}_s \parallel IO_m \parallel \text{Addr}_m \parallel R_m \parallel R_s) \tag{7}$$

(13)v_m与 v_m'的一致性检测完毕后,master 设备通过公式(8)更新 intid_m;

$$\text{intid}_m = h(\text{intid}_m) \tag{8}$$

(14)Slave 设备通过公式(9)更新 intid_s;

$$\text{intid}_s = h(\text{intid}_s) \tag{9}$$

(…)方案 I 剩余的步骤与原 SSP 方案相同.

因为 master 设备支持多种通信信道,所以 master 设备可以分别从 TTP 和 slave 设备获得关于 slave 设备的 I/O 能力信息,通过对比来确保 slave 设备所发送的 I/O 能力信息的真实性和完整性. Slave 设备在 master 设备和验证转发消息的帮助下,也可以分别从 TTP 和 master 设备处获得关于 master 设备的 I/O 能力信息. 因此,slave 设备也有能力鉴别 master 设备所发送的 I/O 能力信息的真伪. 一旦鉴定出配对的 BLE 设备的 I/O 能力信息存在问题,那么 master 设备或者 slave 设备将立即终止设备配对过程,并以此来防止错误的关联模型被使用. 避免使用错误的关联模型,这也是防止 MITM 攻击的基本前提.

方案 I 为支持 PE 或者 OOB 模型的 BLE 设备而设计,但对于仅支持 JW 模型的 BLE 设备来说,方案 I 并不适用.

5.2　方案 II:基于哈希序列的 SSP 方案

为了向仅支持 JW 模型的 BLE 设备提供抗 MITM 攻击能力,作者利用哈希序列对方案 I 进行了改进. 造成 MITM 攻击漏洞的根本原因是 JW 模型的 TK 被设置 0. 因此,在方案 II 中 TK 被设置成随机数.

设 $f(\,)$为哈希函数,F 表示由 $f(\,)$生成的哈希序列,F_i表示该哈希序列中的第 i 个元素. 设 R 为长度为 $m \times n$ 的随机数,R_i表示 R 中第 i 个 m 比特长的数据片段($1 \leqslant i \leqslant n$). 假设 R 的取值为 54668(1101 0101 1000 1100),m 的取值为 4,那么 $R_1 = 13(1101)$、$R_2 = 5(0101)$、$R_3 = 8(1000)$、$R_4 = 12(1100)$、$R = R_1R_2R_3R_4$且 $n = 4$.

图 3 显示了方案 II 的详细处理步骤:

(1 ~ 3)方案 II 的前三个步骤与方案 I 相同;

(4)Slave 设备产生随机数 R,随机数的长度为 $m \times n$. 随后按照上文提及的方法将 R 转换成 $R_1R_2 \cdots R_n$的形式. Slave 设备按照算法 1 计算函数 GenHashArray(intid_s

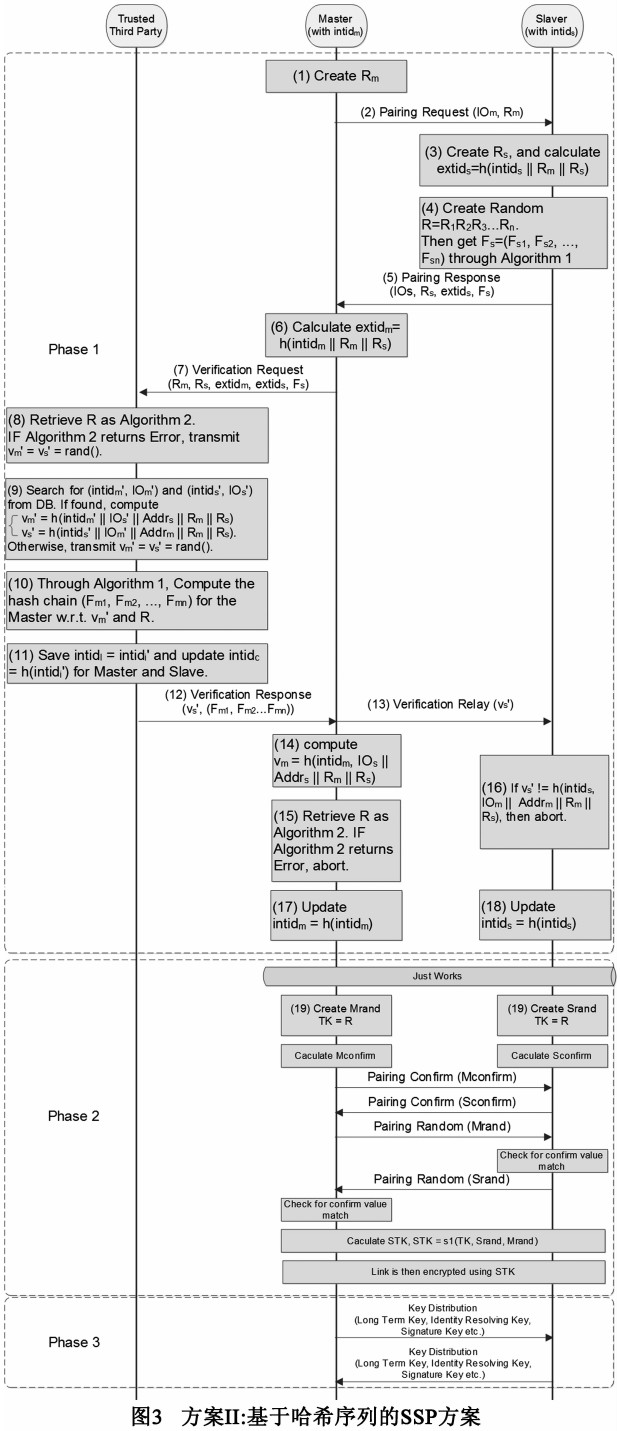

图3　方案II:基于哈希序列的SSP方案

$\| R_m \| R_s, R_1 R_2 \cdots R_n, n)$得到哈希序列 $F_s = (F_{s1}, F_{s2}, \cdots, F_{sn})$;

(5)哈希序列 F_s和 extid_s被封装在配对响应消息中,连同随机数 R_s一起发送给 master 设备;

算法 1 GenHashArray

```
输入:
    [Seed]:          哈希序列生成种子
    [R1R2R3…Rn]:随机数
    [n]:             长度为 m 比特的数据段数量
输出:
    [F]:             哈希序列
1:For i=1 To n Do
2:    //计算哈希序列 F 中的第 i 个元素
3:    Fi=f(Seed⊕Ri⊕i);
4:End For
5:Return(F1,F2,…,Fn);
```

(6)当 master 设备接收到配对响应消息后,master 设备通过公式(2)计算出 extid_m;

(7)Master 设备将包含有 R_m、R_s、extid_m、extid_s和哈希序列 F_s的验证请求消息发送给 TTP;

(8)TTP 按照算法 2 计算函数 RetrieveRandom $(\text{intid}_s \| R_m \| R_s, (F_{s1}, F_{s2}, \cdots, F_{sn}))$,从哈希序列中恢复出随机数 R. 如果算法 2 返回错误,那么 TTP 则将一个随机数直接发送给 master 设备代替验证响应消息;

算法 2 RetrieveRandom

```
输入:
    [Seed]:          哈希序列解析种子
    [F1F2F3…Fn]:     哈希序列
输出:
    [R]:             解析得到的随机数
1:Set R=0;
2:Set R1,R2,R3,…,Rn=0;
3:For i=1 To n Do
4:   For Ri=0 To 2^m-1 Do
5:      If Fi=f(Seed⊕Ri⊕i) Then
6:         // 找到 Ri的值
7:            // 连接 R1,R2,R3,…,Rn到 R
8:R=R<<4|Ri
9:            Break;
10:      Else
11:            continue;
12:         End If
13:   End For
14:   If Ri>2^m-1 Then
15:      //没有找到 Ri
16:      Return Error;
17:   End If
18:End For
19:Return R;
```

(9)TTP 采用和方案 I 相同的流程计算出验证响应消息;

(10)TTP 通过算法 1 函数 GenHashArray$(v_m', R_1 R_2 \cdots R_n, n)$为 master 设备产生哈希序列$(F_{m1}, F_{m2}, \cdots, F_{mn})$,该序列将会随后发送给 master 设备;

(11)TTP 首先将 master 设备和 slave 设备的 intid_i'保存为 intid_l,随后根据公式(5)更新 intid_c;

(12)验证响应消息由 TTP 发送给 master 设备,其中包括发送给 master 设备的哈希序列$(F_{m1}, F_{m2}, \cdots, F_{mn})$以及发送给 slave 设备的验证消息$(v_s')$;

(13)当接收到验证响应消息后,master 设备将验证消息(v_s')转发给 slave 设备;

(14)Master 设备通过公式(6)计算出验证消息 v_m;

(15)Master 设备通过函数 RetrieveRandom$(v_m, (F_{m1}, F_{m2}, \cdots, F_{mn}))$从哈希序列中恢复出随机数 R. 如果该函数返回错误,那么 master 设备必须立刻终止设备配对过程;

(16)Slave 设备通过公式(7)计算出自己的验证消息 v_s,并将其与接收到的验证消息 v_s'进行比较. 通过检测这两者之间的一致性来判断是否继续设备配对流程;

(17)从哈希序列中恢复出随机数 R 之后,master 设备根据公式(8)更新 intid_m;

(18)Slave 设备根据公式(9)更新 intid_s;

(19)当执行到此步骤时,master 设备和 slave 设备均获得了随机数 R. 因此,TK 值可以被设置为 R;

(…)方案 II 剩余的步骤与原 SSP 方案使用 JW 模型时相同.

因为 BLE 设备的内部 ID 从未被揭露,所以可以使用哈希序列$(F_{m1}, F_{m2}, \cdots, F_{mn})$和$(F_{s1}, F_{s2}, \cdots, F_{sn})$来秘密地传输随机数 R. 当使用 JW 模型时,方案 II 中的 TK 被设置为随机数 R. 因此,方案 II 能够向仅支持 JW 模型的 BLE 设备提供抗 MITM 攻击的能力.

6 方案评价

6.1 安全性分析

表 2 呈现了针对方案 I 和方案 II 安全性分析的结果.

表 2 安全分析

	Level 1 敌手	Level 2 敌手	Level 3 敌手
原 SSP 方案(JW/PE/OOB)	○	×	×
方案 I(PE/OOB)	√	√	√
方案 II(JW)	√	√	√

[√] 表示能够抗 MITM 攻击

[×] 表示不能够抗 MITM 攻击

[○] 表示能够在某些场景中抗 MITM 攻击

6.1.1 抵抗 level 1 敌手

Level 1 敌手攻击时存在两种攻击场景.

在第一种攻击场景中,BLE 设备已经相互连接,即 BLE 设备已经完成了设备配对的过程. 因为 level 1 敌手仅能够被动地窃听,或者重放窃听到的消息,所以 level 1 敌手不能够对已经配对的 BLE 设备实施 MITM 攻击. 换句话说,在这种场景中,无论是原 SSP 方案,还是方案 I 或者方案 II 都可以提供针对 level 1 敌手的抗 MITM 攻击的能力.

在第二种攻击场景中,BLE 设备从未遇见过彼此,也就是说,BLE 设备将在 level 1 敌手在场的情况下进行设备配对. 因此,在这种情况下,level 1 敌手可以通过窃听来记录下所有的配对消息,并在需要时进行重放攻击. 当使用原 SSP 方案时,level 1 敌手先窃听下 BLE 设备的配对消息,并在恰当的时候将窃听到的消息进行重放攻击,以强迫受害的 BLE 设备使用 JW 模型进行配对. 因此,在这个场景中,原 SSP 方案无法提供抗 MITM 攻击的能力. 由于有 TTP 的协助,所以方案 I 与方案 II 都可以避免错误的关联模型被使用. 在 level 1 敌手出现的情况下,方案 I 可以为支持 PE 模型或者 OOB 模型的 BLE 设备提供 MITM 攻击防护. 而方案 II 可以提高 JW 模型的安全性. 在方案 II 中,TK 被设置为随机数. 因此,在 level 1 敌手出现的情况下,方案 II 可以为仅支持 JW 模型的 BLE 设备的提供抗 MITM 攻击的能力.

6.1.2 抵抗 level 2 敌手

Level 2 敌手拥有主动阻断受害 BLE 设备之间的信息交换的能力. 即使 BLE 设备已经完成了设备配对,level 2 敌手仍然可以通过阻断现有连接的方式来诱使受害用户删除设备中存储的密钥并重新进行设备的配对. 因此,当使用原 SSP 方案进行设备配对时,level 2 敌手可以对 BLE 设备实施 MITM 攻击. 由于方案 I 和方案 II 中使用了 TTP 来保证设备 I/O 能力信息的正确性,即使 level 2 敌手拥有阻断的能力,他也无法强迫受害设备使用错误的关联模型. 所以,在 level 2 敌手出现的情况下,方案 I 能够为支持 PE 模型或者 OOB 模型的 BLE 设备提供抗 MITM 攻击能力. 因为方案 II 中的 TK 被设置为随机数,所以即使面对 level 2 敌手时,方案 II 也可以为仅支持 JW 模型的 BLE 设备提供 MITM 攻击防护.

6.1.3 抵抗 level 3 敌手

因为 level 3 敌手拥有 level 1 敌手和 level 2 敌手的能力,所以原 SSP 方案在面对 level 3 时已经无法在 BLE 设备配对过程中提供 MITM 攻击防护. Level 3 敌手可以在需要时向合法的 BLE 设备发起询问,并记录下合法 BLE 设备的回复信息. 例如,level 3 敌手可以通过询问 slave 设备获得多个 extid 和哈希序列,或者通过询问 master 设备获得多个验证消息. 但是,在方案 I 和方案 II 中,随机数(R_m 和 R_s)被引入 extid、哈希序列和验证消息的计算过程中. 所以,当使用方案 I 和方案 II 时,重放询问得到的信息无法使 level 3 敌手获得任何好处. 在面对 level 3 敌手时,方案 I 能够为支持 PE 模型或者 OOB 模型的 BLE 设备提供 MITM 攻击防护. 而当 BLE 设备仅支持 JW 模型时,方案 II 可以被用来防止 MITM 攻击.

6.2 性能分析

本章节将在所提出的方案与原 SSP 方案之间进行性能的对比分析,并且本章节还对如何确定方案 II 中的随机数 R 的比特长度、m 的取值及 n 的取值进行说明.

6.2.1 负载对比

表 3 给出了不同方案之间的负载量对比. 因为本文所提出方案的改进步骤集中于 SSP 配对过程的阶段 1 中,所以本章节主要对阶段 1 中的负载进行对比. 具体来说,主要对比不同方案的计算量负载、存储负载以及通信量负载.

表 3　不同方案的负载对比(阶段 1)

		原 SSP 方案	方案 I	方案 II
计算负载	TTP	None	8 Hashes	$((2^m+1)\times n+8)$ Hashes
	Master 设备	0	3 Hashes	$(2^m\times n+3)$ Hashes
	Slave 设备	0	3 Hashes	$(n+3)$ Hashes
存储负载	TTP	None	$(2\times l_d+l_a+l_o)\times N$	$(2\times l_d+l_a+l_o)\times N$
	Master 设备	l_i+l_o	$l_i+l_o+l_d$	$l_i+l_o+l_d$
	Slave 设备	l_i+l_o	$l_i+l_o+l_d$	$l_i+l_o+l_d$
通信负载	TTP 与 master 设备之间	None	$l_r\times 2+l_h\times 4$	$2\times(l_r+l_f\times n)+3\times l_h$
	Master 设备与 slave 设备之间	$2\times(l_i+l_o)$	$2\times(l_i+l_o+l_r+l_h)$	$2\times(l_i+l_o+l_r+l_h)+l_f\times n$

[m]表示随机数 R 中数据片段的比特长度

[n]表示随机数 R 中数据片段的数量

[l_a]表示硬件地址 Addr 的比特长度

[l_d]表示内部 ID 的比特长度

[l_o]表示设备 I/O 能力信息的比特长度

[l_i]表示设备基本信息(包括 OOB 标识等)的比特长度

[N]表示系统内所有 BLE 设备的数量

[l_r]表示由 BLE 设备产生的随机数(即,R_m 和 R_s.)的比特长度

[l_h]表示哈希函数 $h()$ 的输出数据的比特长度

[l_f]表示哈希函数 $f()$ 的输出数据的比特长度

与原 SSP 方案相比,方案 I 所需的额外负载很小.

正如表3所示,与原SSP方案相比,BLE设备仅仅需要多进行3次哈希计算.从数据存储量的角度来对比,方案I中的每个BLE设备仅需要多存储1个内部ID.从数据通信量的角度来对比,master设备和slave设备之间需要多传输4个哈希值.因此,无论是对于master设备来说还是对于slave设备来说,方案I都足够的轻量.

相比之下,由于使用了哈希序列,方案II在计算量负载、数据存储负载和通信量负载上都更大一些.但是,方案II对于slave设备来说依然足够轻量.因为位于云端平台的TTP拥有大量的资源,而MCC环境中的master设备通常比slave设备的能力更强,所以在方案II中TTP和master设备承担了更多的计算任务.如表3所示,与原SSP方案相比,slave设备仅需要多进行$(n+3)$次哈希计算.Slave设备仍然可以保持一个瘦客户端.在下一章节,作者建议m的取值为4、n的取值为5,以使得JW模型能够拥有与PE模型相同的安全等级.

6.2.2 随机数R的长度取值

与原SSP方案相比,方案II中的额外负载主要来自哈希序列的计算.而且,负载量的大小与TK的比特长度,即与随机数R的比特长度,密切相关.随机数R的比特长度为$m \times n$.如表3所示,与原SSP方案相比,slave设备需要进行$(n+3)$次哈希计算,与此同时,需要多传输$(2 \times (l_r + l_h) + l_f \times n)$个哈希值.正如5.2节中所提到的,方案II的一个关键问题就是能够在安全性(即TK的比特长度,随机数R的比特长度)和可用性(即所需的计算量与通信量负载)之间取得平衡.

BLE标准[17,18]中要求,当使用PE模型时,密码应为6位数字.也就是说,PE模型中的密码最大可以提供20比特的信息熵.这意味着,在方案II中,如果随机数R的比特长度设置为20比特,那么JW模型就可以提供与PE模型相同的安全保障.因此,作者建议方案II中的随机数R的比特长度应设置为20比特.根据章节6.2的分析,如果n的取值多大,那么slave设备则需要承担过多的计算任务.相反的,如果n的取值过小则master设备的负载会过重.为了使各方的计算量负载和通信量负载也处于可以承受的水平,作者建议n取值不应大于$\sqrt{\text{len}(R)}$,即当R的比特长度为20时,m的取值应该设置为4,n的取值应当设置为5.在这种情况下,slave设备仅仅需要进行8次哈希计算,并多传输9个哈希值.

7 结束语

本文所提出的方案能够在面对多级能力敌手的情况下,向BLE设备提供抗MITM攻击的能力.但是,额外的负载是不可避免的.本文的下一步工作便是研究如何进一步降低计算量和通信量负载.

参考文献

[1] MCC Forum. The Definition of MCC[EB/OL]. http://www.mobilecloudcomputingforum.com/, 2011-08-16/2014-12-25.

[2] Padgette J, Scarfone K, Chen L. National Institute of Standards and Technology (NIST) Special Publications 800-121: Guide to Bluetooth Security[EB/OL]. http://csrc.nist.gov/publications/nistpubs/800-121-rev1/sp800-121_rev1.pdf, 2012-06-12/2014-03-29.

[3] Kaur S. How to secure our bluetooth insecure world![J]. IETE Technical Review, 2013, 30(2): 95-101.

[4] Hattaja K, Toivanen P. Two practical man-in-the-middle attacks on bluetooth secure simple pairing and countermeasures[J]. IEEE Transactions on Wireless Communications, 2010, 9(1): 384-392.

[5] Haataja K, Hyppønen K. Man-in-the-middle attacks on bluetooth: a comparative analysis, a novel attack, and countermeasures[A]. Proceedings of the 3rd International Symposium on Communications, Control, and Signal Processing[C]. Piscataway, NJ, United States: IEEE Computer Society, 2008. 1096-1102.

[6] Sharmila D, Neelaveni R, Kiruba K. Bluetooth man-in-the-middle attack based on secure simple pairing using out of band association model[A]. Proceedings of the 2009 International Conference on Control Automation, Communication and Energy Conservation[C]. Piscataway, NJ, United States: IEEE Computer Society, 2009. 1-6.

[7] Ueeten O, Serinken N. Wireless security through rf fingerprinting[J]. Canadian Journal of Electrical and Computer Engineering, 2007, 32(1): 27-33.

[8] Pasanen S, Haataja K, Pivinen N, et al. New efficient rf fingerprint-based security solution for bluetooth secure simple pairing[A]. Proceedings of the 43rd Annual Hawaii International Conference on System Sciences[C]. Piscataway, NJ, United States: IEEE Computer Society, 2010. 2819-2826.

[9] 耿君峰,郁滨.基于蓝牙设备地址的分组净荷签密方案设计[J].计算机工程与设计,2015,36(1):103-107.

[10] Haataja K. New efficient intrusion detection and prevention system for bluetooth networks[A]. Proceedings of the 1st International Conference on MOBILe Wireless MiddleWARE, Operating Systems, and Applications[C]. Brussels, Belgium: ICST, 2008. Article No. 16.

[11] Dunning J P. Taming the blue beast: a survey of bluetooth based threats[J]. IEEE Security and Privacy, 2010, 8(2): 20-27.

[12] Sandhya S, Devi K A S. Analysis of bluetooth threats and v4.0 security features[A]. Proceedings of the 2012 Inter-

national Conference on Computing, Communication and Applications[C]. Piscataway, NJ, United States: IEEE Computer Society, 2012. 1 – 4.

[13] Hypponen K, Haataja K M J. "Ni†o" man-in-the-middle attack on bluetooth secure simple pairing[A]. Proceedings of the 3rd IEEE/IFIP International Conference in Central Asia on Internet[C]. Piscataway, NJ, United States: IEEE Computer Society, 2007. 1 – 5.

[14] Haataja K, Toivanen P. Practical man-in-the-middle attacks against bluetooth secure simple pairing[A]. Proceedings of the 2008 International Conference on Wireless Communications, Networking and Mobile Computing[C]. Piscataway, NJ, United States: IEEE Computer Society, 2008. 1 – 5.

[15] Mutchukota T R, Panigrahy S K, Jena S K. Man-in-the-middle attack and its countermeasure in bluetooth secure simple pairing[A]. Proceedings of the 5th International Conference on Information Processing[C]. Heidelberg, Germany: Springer Verlag, 2011. 367 – 376.

[16] 张卫明,李世取. 组合生成器的多线性相关攻击[J]. 电子学报,2005,33(3):427 – 432.
ZHANG Wei-ming, LI Shi-qu, Multi-linear correlation attack on combiners[J]. Acta Electronica Sinica, 2005, 33(3):427 – 432. (in Chinese)

[17] Marquess K, Park W, Jones L, et al. Bluetooth Specification Version 4.0[EB/OL]. https://www.bluetooth.org/docman/handlers/downloaddoc.ashx? doc_id = 229737, 2010-06-30/2014-10-06.

[18] Marquess K, Park W, Jones L, et al. Bluetooth Specification Version 4.1[EB/OL]. https://www.bluetooth.org/DocMan/handlers/DownloadDoc.ashx? doc_id = 282159, 2013-12-03/2014-12-20.

作者简介

陈　凯　男,1985 年生于天津. 中国科学院信息工程研究所博士生. 研究方向为网络与系统安全、身份认证、工业控制系统安全.
E-mail: chenk@iie.ac.cn

许海铭　男,国家能源局安全司处长,华北电力电力大学电气与电子工程学院博士生,主要从事电力系统安全研究.