低功耗蓝牙的安全性研究

刘 伟
(北京工业大学 软件学院, 北京 100124)

摘要: 基于提高低功耗蓝牙安全的目的,通过对其安全机制的深入分析发现所采用的高级加密标准(AES)加密密钥存在安全隐患,结合 RSA 非对称加密算法和 AES 对称加密的特点,提出一种两者相结合的混合加密安全机制,该机制在密钥分发前使用 RSA 加密 AES 的密钥,使用 AES 加密双方的通信信息,使攻击者无法获得 AES 的密钥而无法解密信息,从而提高低功耗蓝牙的安全性。通过模拟实验表明该机制的加密速度和耗时均在可接受范围内。

关键词: 低功耗蓝牙; 安全; RSA; AES
中图分类号: TN918.91 **文献标识码:** A **文章编号:** 1674-6236(2015)22-0078-03

Bluetooth low energy security research

LIU Wei
(*Beijing University of Technology*, *School of Software Engineering*,*Beijing* 100124, *China*)

Abstract: Based on the purpose of improving the security of Bluetooth Low Energy (BLE), through the deep analysis of BLE security mechanisms, a security risk of encryption key of Advanced Encryption Standard (AES) that is used by BLE is found. A cryptographic security mechanism is proposed which combines the advantage of RSA asymmetric encryption algorithm and AES symmetric encryption algorithm. The mechanism uses RSA encrypt AES's key before key distribution, and then uses AES encrypted communication between the two sides, so an attacker cannot get AES encryption key and cannot decrypt the information, thereby improve the security of BLE. Through simulation experiments it proves that the encryption speed and time-consuming of the mechanism is within an acceptable range.

Key words: bluetooth low energy; security; RSA; AES

随着蓝牙 4.0 规范的发布,低功耗蓝牙技术[1]进入大众的视野。近年来物联网技术的火热发展,低功耗蓝牙大量应用到了可穿戴设备、智能手机和平板电脑中[2]。在使用低功耗蓝牙的同时,也面临着大量安全威胁,不法分子和恶意攻击者对低功耗蓝牙网络进行攻击,窃取用户的隐私数据,所以其安全机制的研究就显得尤为重要。

1 低功耗蓝牙的安全机制

低功耗蓝牙的安全机制不同于传统蓝牙的安全机制,传统蓝牙采用安全简单配对协议(Secure Simple Pairing)[1],具有很强的安全保护机制。低功耗蓝牙采用了类似的安全协议但是提供的保护程度却有所不同, 为了实现低功耗的目标,低功耗蓝牙在安全性方面做出了一定的妥协。

低功耗蓝牙的安全机制主要有 5 个方面: 连接模式,密钥生成功能,加密功能,数字签名功能,隐私保护功能[3]。

1.1 连接模式

低功耗蓝牙设定了 3 种连接模式,分别是立即工作(Just Works)、万能钥匙进入(Passkey Entry)和带外连接(Out of Band)[1]。每个连接模式与传统蓝牙的安全简单配对各有相似的地方,但也有以下例外情况:立即工作和万能钥匙进入未提供任何被动窃听保护。这是因为安全简单配对采用了椭圆曲线密钥协商方案,而低功耗蓝牙没有采用。每个连接模式是以设备的 I/O 功能为基础进行使用, 与安全简单配对方式类似。

1.2 密钥生成功能

低功耗蓝牙的密钥是由各设备的主机生成,而该设备与任何其它低功耗蓝牙设备相互独立[1]。低功耗蓝牙会根据数据保密性、设备认证、未加密数据认证、设备识别等情况使用多个密钥。就低功耗蓝牙而言,单个链接密钥是通过来自各设备的资源和配对过程中使用的链接密钥整合而生成的[3]。

1.3 加密功能

低功耗蓝牙采用 AES 密码技术进行加密[3]。低功耗蓝牙有一个密码块,本质为一个单向函数,用于产生密钥、加密和提供完整性检查。该密码块采用 128 位的密钥和 128 位的明文块产生 16 字节的密码块。

1.4 数字签名功能

低功耗蓝牙可支持两台具有受信任关系的设备发送没有保密性的认证数据。这需要签署带有连接签名解析密钥(CSRK)的数据才能实现。发送设备在数据上进行签名。接收

收稿日期:2015-01-28 **稿件编号:**201501253
作者简介:刘 伟(1988—),男,河北保定人,硕士研究生。研究方向:嵌入式软件与系统。

设备会验证签名,如果签名通过验证,则假设数据是来自可信源。该签名由属性协议签名算法生成的消息认证码和计数器构成。计数器是用来防御重放攻击,并且会添加至所发送的已签名的数据上。

1.5 隐私保护功能

隐私保护功能是低功耗蓝牙支持一项新功能,可在一段时间内通过频繁更换地址降低跟踪低功耗蓝牙设备的能力。

为了使设备能够使用隐私保护功来重新连接已知设备,保密功能被激活时所使用的设备地址(私人地址)必须可分解至其他设备的身份。私人地址通过在绑定过程更换设备的识别密钥生成。隐私保护功能定义了允许被绑定设备进行重新连接的重新连接地址,同时也将设备过滤为已知设备。两台设备在每次连接时交换重新连接地址。由于重新连接地址仅在连接之间更改,所以设备过滤可以用来缩短处理过量请求的时间。

2 低功耗蓝牙的安全问题

低功耗蓝牙安全机制的最大问题是密钥的安全性。由于使用 AES 对称加密算法,低功耗蓝牙设备双方使用相同的密钥进行加密和解密。如果密钥交换被破解,攻击者就能持有设备双方的密钥;而如果那些设备是依赖低功耗蓝牙原有的安全性机制,攻击者就可以使用破解的密钥解密设备发送的加密信息,同时可以伪装成其他低功耗蓝牙设备发送加密信息,这样攻击者就能窃取到低功耗蓝牙设备的所有信息。

3 基于 RSA 和 AES 的混合加密机制

针对低功耗蓝牙的安全问题,本文提出了一种新型的安全机制, 采用 RSA 非对称加密方法和 AES 对称加密方法相结合的混合加密机制。混合加密机制的核心思想就是使用 RSA 加密 AES 的密钥。RSA 为非对称加密算法,即在加密和解密时使用不同的密钥:在加密时使用公钥(Public Key);在解密是使用私钥(Private Key)。在密钥分配时使用 RSA 加密 AES 的密钥从而使密钥只能被指定的设备获得。

考虑到 RSA 加密需要较大的计算和运算内存,这种机制将进行通信的双方分成强设备和弱设备,强设备具有将强的计算能力和运算内存,将负责主要的 RSA 加密,弱设备对计算能力和运算内存的要求较低。这种强、弱设备的区分方法也比较符合现实情况, 进行连接的蓝牙设备大多是非对称的,例如电脑和蓝牙键盘、智能手机和蓝牙耳机等,电脑和智能手机属于强设备,蓝牙键盘和蓝牙耳机属于弱设备。

混合加密机制的过程如图 1 所示,主要分为 4 个阶段:

阶段一:RSA 密钥分配

这一阶段主要在强设备端进行。强设备使用 RSA 加密方式生成 Public Key 和 Private Key, 然后向弱设备发起连接请求,同时将 Public Key 传输给弱设备。弱设备收到连接请求和 Public Key 后,将 Public Key 保存,同时向强设备发送连接响应。

阶段二:认证过程

双方根据连接设备信息(如有无显示屏、键盘等)选择配对算法,设置个人识别码(PIN),确定临时密钥(TK);设备双方生成一个随机数 Rand,根据 TK 值、Rand 和配对信息计算出确认值[3],双方依次交换确认值和随机数;双方根据交换的随机数进行计算,检测确认值是否匹配,如果匹配通过则认证成功;根据随机数和 TK 计算出短期密钥(STK)和长期密钥(LTK),并由弱设备存储 LTK。

阶段三:密钥分配

强设备发起加密请求; 弱设备收到请求后使用 Public Key 对 LTK 进行 RSA 加密得到加密信息,然后将其传输给强设备,响应加密请求;强设备收到加密信息后使用 Private Key 进行 RSA 解密得到 LTK; 为了确保低功耗蓝牙通信的安全性,不能直接使用 LTK 作为 AES 的密钥(Secret Key),双方在加密请求和加密相应时, 交换了设备的密钥分散器, 根据 LTK 和双方的密钥分散器计算得出本次通信的 AES 的 Secret Key[3],这样每次加密请求的通信密钥都是重新生成的,不能在两次通信中重复使用。

阶段四:加密通信

双方使用 Secret Key 进行 AES 加密通信。每次通信前,使用 Secret Key 对通信内容进行 AES 加密得到加密信息,然后将信息发送至对方;收到信息后,使用 Secret Key 对加密信息进行 AES 解密,得到原始消息内容。

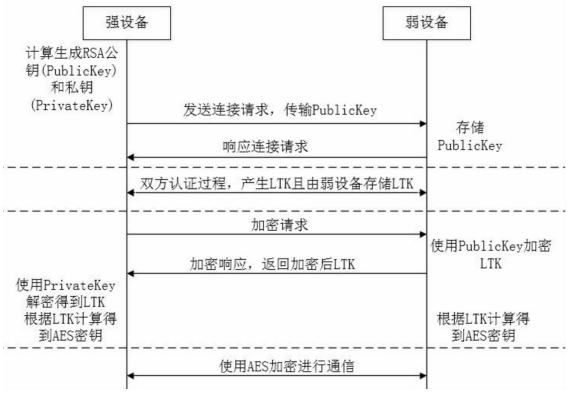

图 1　混合加密过程

Fig. 1　Combined encryption process

4 混合加密机制分析

4.1 对称加密体制的特点

在对称加密体制中,通信双方使用相同的密钥进行加密和解密,这就意味着对称加密体制的安全主要取决于密钥的安全性。对称加密的优点是算法简单,具有较高的效率,加密速度快,可以满足的大量信息的加密需求;缺点是通信前需要进行密钥交换,密钥容易泄露而不能确保安全性。

4.2 非对称加密体制的特点

在非对称加密体制中存在两个密钥:公开密钥和私有密钥,公开密钥用于加密,私有密钥用于解密。在通信前需要将

己方的公开密钥传递给对方,对方使用公开密钥加密,加密内容只有用私有密钥解密,这意味着只有己方能够解密。非对称加密具有密钥分配简单、安全性高的特点;缺点是计算量大,加密速度慢。

4.3 混合加密的特点

混合加密机制结合了对称加密体制和非对称加密体制的特点,如表 1 所示,具有如下优点:结合了 AES 加密具有运算要求低,加密速度快的优势[4];利用 RSA 加密具有加密安全性高[5]的优势,提高了 AES 密钥的安全性;每次加密连接只进行一次 RSA 加密解密,避免了 RSA 运算开销。

表 1 混合加密与其他加密方式对比

Tab. 1 Comparison between combined encryption and other encryption

	密钥安全性	运算量	运复杂度
AES 加密	低	小	低
RSA 加密	高	高	高
混合加密	高	中等	中等

与低功耗蓝牙的安全机制相比,混合加密机制有 3 点不同:设备发起连接请求前需要计算出 RSA 加密的 Public Key 和 Private Key,并将 Public Key 传输给设备另一方来存储;设备收到加密请求时,将 LTK 进行加密后再进行传输;设备并非直接接收到 LTK,接收到的是经 RSA 加密后的信息,需要经过相应解密后才能得到 LTK。

5 实验与结果分析

分别使用台式电脑、笔记本电脑和 Android 智能手机为实验平台,使用 Java 语言模拟实现混合加密机制,每组进行 10 次实验得到数据如表 2 所示。

表 2 混合加密耗时时间

Tab. 2 Time consuming of combined encryption

	台式电脑	笔记本电脑	手机
CPU/GHz	3.19	2.6	1.2
内存/GB	3	2	1
阶段 1 平均耗时/ms	193.0	178.6	937.0
阶段 3 平均耗时/ms	6.0	7.6	43.0

通过表格中的数据可以发现:

1) 混合加密机制的主要耗时在阶段 1, 即 RSA 生成 Public Key 和 Private Key 阶段。耗时最长为 Android 智能手机端,平均耗时 937.0 ms;耗时最短为台式电脑端,平均耗时 193.0 ms。

2)阶段 3 的耗时比较短。耗时最长为 Android 智能手机端,平均耗时 43.0 ms;耗时最短为台式电脑端,平均耗时 6.0 ms。

3)混合加密的整体耗时比较短,在 1 秒钟以内。

4) 混合加密的耗时与设备的计算能力和运算内存成反比,Android 智能手机 CPU 主频最低,运算内存最小,耗时最长;台式电脑的 CPU 主频最高,运算内存最大,耗时最端。

分析以上表格可以得结论:使用混合加密机制总体耗时较小,用户使用时不会产生延时感觉。随着用户使用的设备硬件配置的计算能力和运行内存的提高,相信这一数据将会越来越小。

6 结 论

本文在分析低功耗蓝牙安全机制的基础上,发现了其中的密钥的安全隐患, 提出一种新的 RSA 和 AES 混合加密安全机制,以此来提高低功耗蓝牙的安全性。

RSA 算法具有算法简单,易于实现的特点,因此成为应用最为广泛的非对称加密算法。但是它也存在着计算量过大缺点[6],考虑到低功耗的目标,未来可考虑分析提高 RSA 算法的效率或使用其他计算量较小的非对称加密算法,例如椭圆曲线加密算法等。

参考文献:

[1] Bluetooth SIG. Bluetooth specification version4.0 [EB/OL]. (2010-06)[2015-01]. https://www.bluetooth.org/DocMan/handlers/DownloadDoc.ashx?doc_id=229737.

[2] 张瑞吟. 低功耗蓝牙技术市场应用前景广阔[J]. 集成电路应用,2012(10):32-33.

[3] Robin Heydon. Bluetooth Low Energy: The Developer's Handbook[M].伦敦:普伦蒂斯霍尔出版社,2012.

[4] 郑行. AES算法的硬件优化实现及应用研究[D]. 厦门:厦门大学,2014.

[5] 胡云. RSA算法研究与实现[D]. 北京:北京邮电大学,2010.

[6] 卓先德,赵菲,曾德明. 非对称加密技术研究[J]. 四川理工学院学报:自然科学版,2010(5):562-564,569.

欢迎投稿! 欢迎订阅! 欢迎刊登广告!

国内刊号:CN61-1477/TN 国际刊号:ISSN 1674-6236

在线投稿系统:http://mag.ieechina.com dzsjgc@vip.163.com(广告)

地 址:西安市劳动南路 210 号 5-1-3 信箱 邮政编码:710082