基于蓝牙协议漏洞的 BLUEBORNE 攻击综合分析报告

安天联合分析小组

首次发布时间：2017 年 9 月 17 日 18 时 00 分

本版更新时间：2017 年 9 月 18 日 16 时 30 分

扫二维码获取最新版报告

目 录

1 概述

使用蓝牙通信协议的设备数量随着物联网时代的开启日益增多。近期，物联安全公司 Armis Labs 纰漏了一个攻击向量 BlueBorne[3]，称攻击者可利用一系列与蓝牙相关的安全漏洞，在一定场景下可实现对具有蓝牙功能的远端设备的控制，进而窃取受害者数据、进行中间人攻击以及在感染一个设备后蠕虫式感染其它设备，且此攻击方式无需向用户申请认证授权，具有较大的危害性。为此，安天微电子与嵌入式安全实验室和安天移动安全公司两部门组成联合分析小组，认真剖析了整个攻击流程并做出威胁总结。

2 攻击背景

蓝牙协议是中短距离无线通信采用的常用协议，但由于其规则庞大、架构复杂、功能模块繁多，且一些功能允许厂商自定义，直接导致很多蓝牙设备并未选择相对安全的加密通信方式；另外，一些设备由于自身性质原因，无法执行特定身份认证过程(例如蓝牙耳机无法执行“密钥输入”安全模式，因为耳机设备上就没有可供键盘输入的接口)。这是造成此次蓝牙安全威胁的两大直接原因。

此次攻击首先需要知道目标设备的蓝牙地址。由于很多用户日常习惯默认开启蓝牙设备，便于攻击者扫描进而获得地址；另外在手机、电脑等设备中蓝牙地址与无线 WiFi 地址很接近或完全相同，使得攻击者很容易通过嗅探无线网络数据包进而推出目标蓝牙设备的地址。

不像其它驱动一样，每个操作系统都只有一个蓝牙协议栈，这导致一个漏洞的发现将会影响一系列基于此系统的设备。

3 安全漏洞

蓝牙协议栈的主要模块及此次安全威胁的漏洞分布情况：

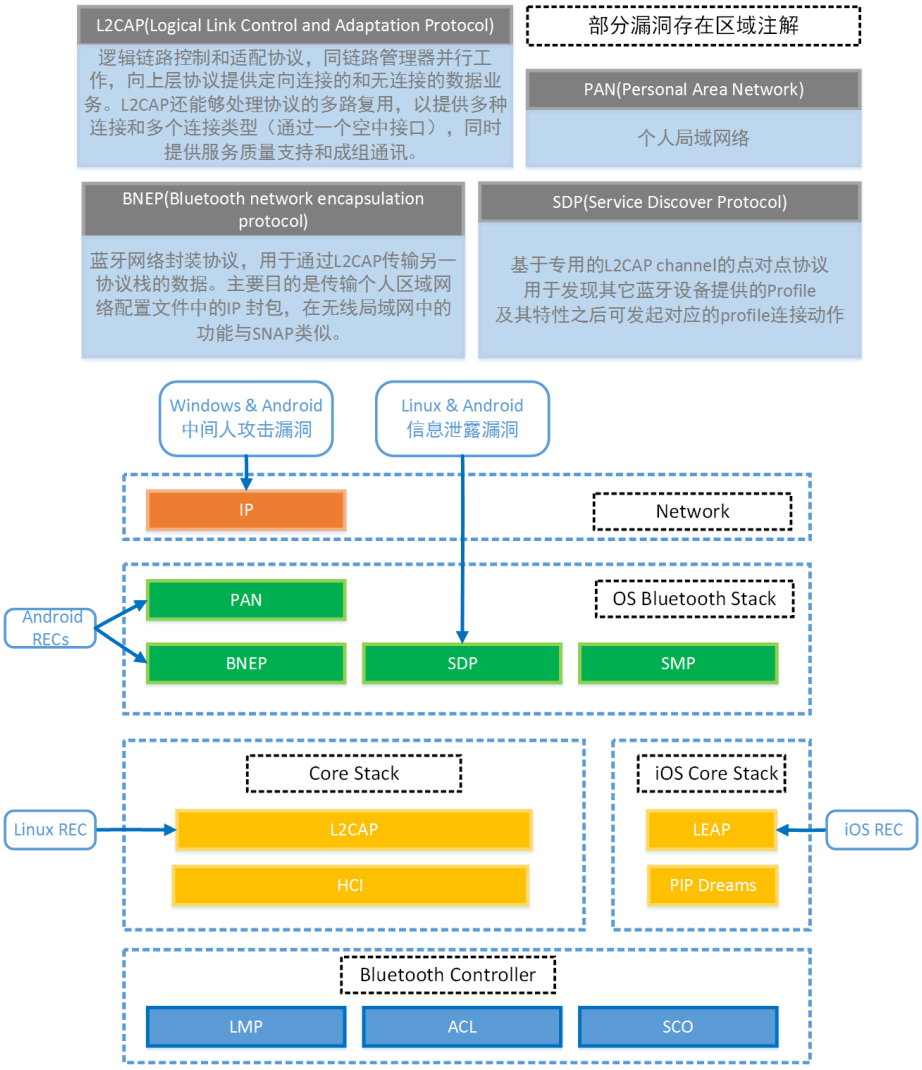

图 1 漏洞分布情况

针对(CVE-2017-1000251)Linux 内核的 RCE(远程控制执行)漏洞，攻击者可利用此溢出漏洞向蓝牙协议的 L2CAP 层发送畸形数据包，对目标设备进行恶意配置，为下一步攻击做准备。

针对(CVE-2017-1000250)Linux BlueZ(蓝牙协议栈)信息泄露漏洞，由于蓝牙协议在设计规范方面存在不足，导致基于 SDP 模块的“续传模式”(SDP Continuation) 在上述内核溢出漏洞存在的前提下，在部分 Linux 与 Android 系统中会被攻击者完全控制，进而执行进一步的堆溢出攻击。

针对(CVE-2017-0785)Android 信息泄露漏洞，类似于在 Linux BlueZ 上的漏洞，利用 SDP 服务器的一个记录数目整数值的下溢出漏洞，攻击者可进而利用“续传模式”在 Android 设备上反复传输指令，达到绕过计数验证和 ASLR(Address space layout randomization，内存空间地址随机化）保护机制的效果。

蓝牙协议引入了的 SSP(Secure simple pairing，简化安全配对)安全模式，提供了如下四种认证方式：

安全认证方式	应用场景
“数据比较”认证 (Numeric Comparison)	两个蓝牙设备都有显示6位数字的能力并允许用户输入“是”或“否”响应
“只比较不确认认证” (Just Works)	至少有一个配对设备既没有显示也没有键盘来输入数字（例如:耳机）
“密码输入认证” (Passkry Entry)	一个蓝牙设备具有输入能力（例如:键盘）而另一个设备有显示但没有输入能力
“外带认证”OOB认证 (Out of Band)	支持共同的额外无线或有线技术（例如:近场通信或NFC）来作为设备发现和加密值交换

图 2 SSP 认证方式

因为很多蓝牙设备自身或待连接的远端设备不具有外置输入接口以及显示能力，故会采用“只比较不确认认证”的方式，而此方式无法进行可靠的身份认证过程。攻击者在攻击采用 Android 系统的设备(一些 Android 系统版本有效)时，其利用场景就是基于对方设备具备显示和输入能力，但攻击者设备不具备输入和显示能力(攻击者可自行构造此状态)的情况，故可以远程发起一个无需与目标设备的用户进行交互的连接请求，接着建立连接并通信；对于采用 Windows 操作系统的设备(一些 Windows 系统版本有效)，攻击者采用同样的原理，发起构造的“无输入和显示能力-无需 MITM(Man in the Middle，中间人攻击)防护”的连接请求，接着完成认证并进行后续通信。因为攻击者已经完成身份认证，而蓝牙在几乎所有操作系统中都具有最高权限，因而攻击者具有访问很多高权限服务的能力，进而实现对目标设备的进一步控制。

BNEP(Bluetooth network encapsulation protocol，蓝牙网络封装协议)能够利用蓝牙协议的功能实现网络共享(例如，一台连接有线网络的电脑，可自建热点并打开蓝牙，让一台手机通过蓝牙连接到此电脑进而实现共享网络)，且能够添加数据包头标记实现包含额外控制指令的功能。另外，在此协议层上可支持构建 PAN(Personal Area Network，个人局域网络)，并提供对应的流量控制功能。

针对(CVE-2017-0781)Android RCE 漏洞，由于 Android 上的 BNEP 服务在消息处理的代码逻辑部分存在一处逻辑错误，使得继 8 bytes 的堆溢出被触发后，后续的缓存区大小填写不受限制。

针对(CVE-2017-0782) Android RCE 漏洞，由于 Android 上的 BNEP 服务在控制帧数据包处理的代码逻辑部分存在一处记录长度的数值的整型下溢出漏洞，且后续代码并未对此数值及限制条件进行严格检查，此漏洞可被用以绕过传输数据包过程中的 MTU(Maximum Transmisson Unit，最大传输单元)大小限制。

以上两个漏洞可让攻击者在基于此前的漏洞建立 BNEP 的连接后，通过制定控制指令进而利用由此带来的堆溢出漏洞使得远程控制代码被执行。通过漏洞利用的恶意代码，基于 com.Android.bluetooth 服务的权限，攻击者可访问手机的文件系统(电话本、文档、照片等)，也可以通过自行模拟键盘、鼠标等设备，与目标设备相连接，实现更深入的控制。攻击者甚至可以自建代理，通过蓝牙接口实现“蠕虫”式入侵其他设备的目的。

针对(CVE-2017-0783)Android 信息泄露安全漏洞和(CVE-2017-8628)Windows 信息泄露安全漏洞，攻击者可构建 PAN 自组网络，并设置自己为 NAP(Network Access Point，网络访问点)，进而设置 DHCP(Dynamic Host Configuration Protocol，动态主机配置协议)服务器构造恶意中继，进行 MITM 攻击。另外，PAN 协议文档自 2003 年后就没更新过，至今依旧是 V1.0 版本，这造成了安全缺失。

因为蓝牙协议的部分功能允许厂商自定义，其中包括一些核心功能，因而苹果公司自定义了多种规则，与蓝牙协议一起共同构造了 L2CAP 协议层，即制定了苹果公司的蓝牙专有协议。此协议禁止了非用户交互认证下的“Just Works”模式以及一些服务的连接构建，除非用户给予授权，这大大降低了攻击面。但各种自定义协议的嵌入也造成了一定的安全隐患。在基于苹果专有的“Pipe Dream”协议设计的模式下，代码的复用造成了新的攻击面。

针对(CVE-2017-14315)Apple RCE 漏洞，LEAP(Low energy audio protocol，低功耗语音协议)，由于基于蓝牙 BLE(Bluetooth low energy，低功耗蓝牙)的语音控制命令传输在消息来源验证方面存在逻辑漏洞，默认传入的控制指令长度为 104(0x68)，对传入指令大小验证不严格可导致堆溢出漏洞，进而使得远程控制代码在 iOS 的蓝牙协议栈上被执行。

4 影响范围

- 根据分析，以下版本的操作系统会受到影响：
  - **Linux**：Linux kernel 3.3-rc1 版本至 Linux kernel 4.13.1 版本；
  - **Windows**：Microsoft Windows Server 2016，Windows Server 2008 SP2，Windows RT 8.1，Windows 8.1，Windows 7 SP1，Microsoft Windows 10，Windows 10 版本 1511，Windows 10 版本 1607，Windows 10 版本 1703；
  - **Android**：4.4.4 版本，5.0.2 版本，5.1.1 版本，6.0 版本，6.0.1 版本，7.0 版本，7.1.1 版本，7.1.2 版本，8.0 版本；
  - **iOS**：iPhone, iPad, iPod 在 iOS 9.3.5 及以下版本，AppleTV 7.2.2 及以下版本(iOS10 版本得到缓解)。
- 以下安全模式下的蓝牙认证机制会受到影响：
  - **Just Works**：只比较不确认认证模式。

注：

关于基于其他系统的蓝牙耳机、蓝牙等设备原则来说不受影响，可以正常使用。但攻击者会伪造自己的设备是一个只支持“Just Works”模式的蓝牙外设去连接受害者的电脑/手机(目标用户使用上述系统)，而此过程不需要与用户进行交互，会在用户不知情的情况下连接至其设备。

5 安全建议

1. 请用户自行将系统升级至最新版本，并及时安装更新补丁。对安全要求高的用户，若对应系统/补丁暂未发布，建议请等待系统更新或补丁升级后再使用蓝牙设备(Android8.1 系统将于 10 月 4 日发布)；
2. 在日常生活中，不使用蓝牙设备时将其关掉(此次组合攻击模式在蓝牙未开启时无法进行攻击)；
3. 因蓝牙属于中短距离无线通信协议，不建议在安装更新和补丁前在公共场合等非信任场景下使用蓝牙设备；
4. 强烈建议不要使用蓝牙共享网络(包括 BNEP 和 PAN)；
5. 其他建议：日常生活中，面对无外接输入和显示功能的设备(即默认认证方式为“Just Works”方式的设备，如部分蓝牙耳机、蓝牙鼠标等)，在无法信任此设备或无法确定此设备是否安全时(如路边某咖啡厅的蓝牙音响)，请不要主动进行连接此设备。

6 安天的研究

安天长期关注硬件外设、信号等领域的新威胁、中短距离无线通信的安全防护等方向，安天在 2004 年，组建了微电子与嵌入式安全实验室，并针对 2.4G 无线信号、蓝牙、工业短距协议、受时信号等进行了多项研究探索，部分研发成果在历年的 XCON、ISF 和 XDEF 等重要行业安全会议上发表演讲，展示研究成果，也引发了相关企业和单位对物联网安全威胁的关注。安天移动安全公司针对车联网等物联网安全环节做了大量研究工作，并向主管部门提供了内部研究报告。

在最近的 Xcon 安全峰会上，安天微嵌的工程师简述了蓝牙 4.0 通信的安全机制及机器学习预测模型的构建流程。并以蓝牙 4.0 通信过程为例，通过无线电设备跟踪跳频、捕获并破解蓝牙键盘键入的数据，将加密通信数据、破解后的明文信息与同时记录的流量特征进行对比分析，揭示了三者间的联系及由此可能带来的信息泄露威胁，同时用简单的实例展现了安全风险。

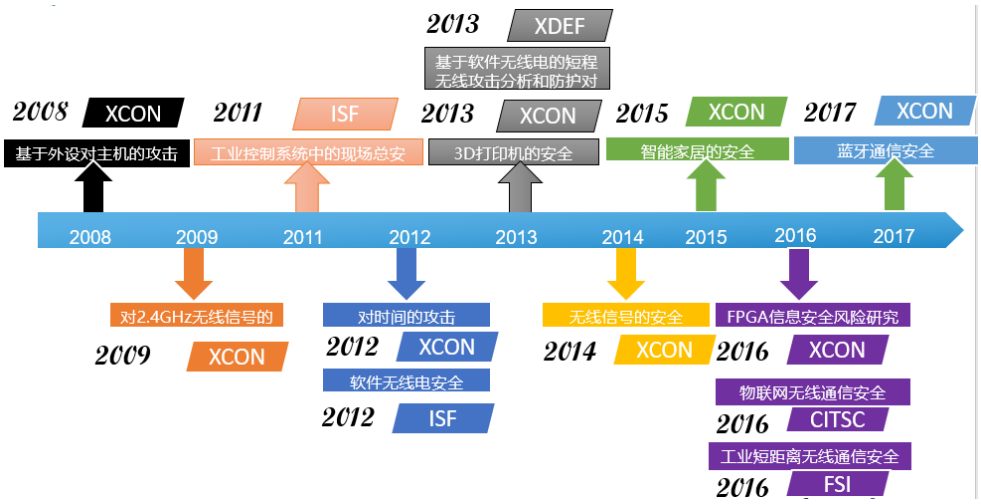

图 3 安天针对外设、短距通信等相关领域的研究

附录一：参考资料

[1] 《BlueBorne: Critical Bluetooth Attack Puts Billions of Devices at Risk of Hacking》

http://thehackernews.com/2017/09/blueborne-bluetooth-hacking.html

[2] 《蓝牙协议手册 Core 5.0》

https://www.bluetooth.com/specifications/bluetooth-core-specification

[3] 《BlueBorne Technical White Paper》

http://go.armis.com/hubfs/BlueBorne%20Technical%20White%20Paper-1.pdf?t=1505319664351

[4] 《The Attack Vector “BlueBorne” Exposes Almost Every Connected Device》

https://www.armis.com/blueborne/

附录二：关于安天

安天是专注于威胁检测防御技术的领导厂商。安天以提升用户应对网络空间威胁的核心能力、改善用户对威胁的认知为企业使命，依托自主先进的威胁检测引擎等系列核心技术和专家团队，为用户提供端点防护、流量监测、深度分析、威胁情报和态势感知等相关产品、解决方案与服务。

安天的监控预警能力覆盖全国、产品与服务辐射多个国家。安天将大数据分析、安全可视化等方面的技术与产品体系有效结合，以海量样本自动化分析平台延展分析师团队作业能力、缩短产品响应周期。安天结合多年积累的海量安全威胁知识库，综合应用大数据分析、安全可视化等方面经验，推出了可抵御各类已知和未知威胁的多样化解决方案。

全球超过一百家以上的著名安全厂商、IT 厂商选择安天作为检测能力合作伙伴，安天的威胁检测引擎目前已为全球近十万台网络设备和网络安全设备、超过八亿部移动终端设备提供安全防护，其中安天移动检测引擎是全球首个获得 AV-TEST 年度奖项的中国产品，并在国际权威认证机构 AV-C 的 2015 年度移动安全产品测评中，成为全球唯一两次检出率均为 100%的产品。

安天技术实力得到行业管理机构、客户和伙伴的认可，安天已连续五届蝉联国家级网络安全应急服务支撑单位资质，亦是中国国家信息安全漏洞库六家首批一级支撑单位之一。

安天是中国应急响应体系中重要的企业节点，在红色代码 II、口令蠕虫、震网、破壳、沙虫、方程式、白象、魔窟等重大安全事件中，安天提供了先发预警、深度分析或系统的解决方案。

安天实验室更多信息请访问： *http://www.antiy.com（中文）*

http://www.antiy.net（英文）

安天企业安全公司更多信息请访问： *http://www.antiy.cn*

安天移动安全公司（AVL TEAM）更多信息请访问： *http://www.avlsec.com*