HZ BOOKS
华章IT

物联网核心技术丛书

密码技术与物联网安全

mbedtls开发实战

徐凯 崔红鹏 ◎编著

理论结合工程样例，详解密码技术和TLS/DTLS/CoAPs协议，书中配有丰富的图表和示例代码，简便易读。

紧扣物联网安全发展趋势，全面分析认证加密算法和椭圆曲线密码算法，确保设备更安全地连接网络。

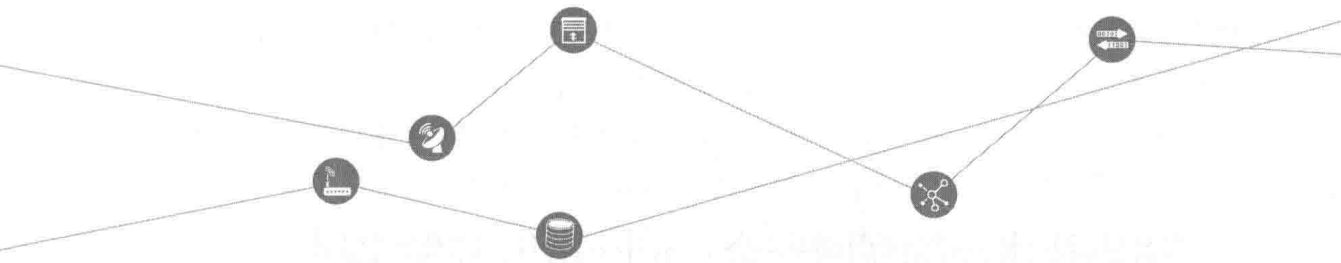
机械工业出版社
China Machine Press

物联网核心技术丛书

密码技术与物联网安全

mbedtls开发实战

徐凯 崔红鹏 ◎编著



机械工业出版社
China Machine Press

图书在版编目（CIP）数据

密码技术与物联网安全：mbedtls 开发实战 / 徐凯，崔红鹏编著 . —北京：机械工业出版社，2019.2
（物联网核心技术丛书）

ISBN 978-7-111-62001-3

I. 密… II. ①徐… ②崔… III. ①互联网络 - 应用 - 安全技术 - 密码术 ②智能技术 - 应用 - 安全技术 - 密码术 IV. ① TP393.4 ② TP18 ③ TN918.4

中国版本图书馆 CIP 数据核字（2019）第 032917 号

密码技术与物联网安全：mbedtls 开发实战

出版发行：机械工业出版社（北京市西城区百万庄大街 22 号 邮政编码：100037）
责任编辑：陈佳媛　　责任校对：李秋荣
印　　刷：三河市宏图印务有限公司　　版　　次：2019 年 3 月第 1 版第 1 次印刷
开　　本：186mm × 240mm　1/16　　印　　张：23
书　　号：ISBN 978-7-111-62001-3　　定　　价：79.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88379426　88361066　　投稿热线：（010）88379604
购书热线：（010）68326294　88379649　68995259　　读者信箱：hzit@hzbook.com

版权所有 · 侵权必究
封底无防伪标均为盗版
本书法律顾问：北京大成律师事务所　韩光 / 邹晓东

Foreword · 推荐序一

物联网已经成为在云计算、大数据、AI 之后的又一个重要的基础技术，吸引了众多的产业链上下游参与者，在全球范围内呈现迅猛发展的态势。物联网在智能生活、智慧城市、智能制造、物流管理、健康医疗等众多的领域已经有多样化的应用场景和业务落地。物联网应用的普及和物联网技术的成熟将推动世界进入万物互联的新时代，数以百亿计的设备会接入网络，拥有百万亿连接的数字化物联世界即将到来。

物联网 IoT 的核心理念是把物理世界中的物体联接上网络和云端，通过对物的模型化抽象来提升对物的认知，通过对物的数据化分析来提升物的智能，从而实现物理世界的最终数字化。作为坚信这一理念的践行者，阿里云 IoT 以解决产业数字化转型升级中的痛点为出发点，通过全面搭建 IoT 基础设施，打造使能平台，完善生态系统，推动物联网向智能网发展。阿里云 IoT 已经构建了云管边端一体化的安全的物联网体系，在云侧推出了物联网平台和开发者平台，在管侧发布了国内首个 LoRa 城域物联网并试运营，在边缘侧发布了边缘计算产品，在端侧提供了适用于不同设备的物联网开源操作系统，建设了物联网标准化联盟，为众多的物联网芯片商、开发者、应用方案商等各种参与方搭建了开放的物联网市场，通过整合场景化的生态应用，为智能生活、智能工业、智慧城市等各行业提供数字化物联的基础设施，助力于物理世界的数字化。

数字化的物联网世界，离不开物联网安全技术的应用。随着物联网终端设备的规模不断增大，随之而来的威胁也越来越大，各种物联网安全事件层出不穷。针对物联网设备的攻击，如漏洞利用、数据泄露、恶意软件、大规模 DDoS 攻击等造成了大量的资产损失或品牌影响。因此，保障物联网的安全显得至关重要并且刻不容缓。从物联网安全的角度，需要结合多种多样、多种维度的安全技术，如设备的身份安全，设备跟云端的安全接入，各种数据链路的安全通信协议，云端安全防护，设备运营监控等。通过对这些安全技术的广泛应用，

构建从设备、边缘、网络到云服务间的安全全链路防护体系，为数字化的物联世界提供可靠的安全基础保障。

本书的两位作者，正是构建安全的数字化物联网世界的践行先锋和布道者。本书的诞生，最初是从解决实际的设备安全连接问题出发，通过对基础密码技术的深入研究，在总结安全开发实践经验的基础上，形成了物联网安全的重要知识积累。在数字化物联世界的理念下，对物联网安全有着积极思考的两位作者进行了勇敢的尝试，最终把这些内容和知识归结成书，实属不易，令人赞叹！本书的内容既涵盖了密码学的基础数论知识，涉及大量安全密码算法和技术原理，又包含了安全连接协议，mbedtls 软件框架和安全开发实用工具，还提供了大量的工程实践案例和指导建议。对物联网安全有兴趣的读者，可以从本书了解到物联网安全的基础知识和应用技术；物联网安全的开发者，也可以通过本书提供的工程移植样例以及示例代码，提升对物联网安全协议和基础安全算法的理解；物联网设计架构师，可以通过本书提供的参考解析和性能分析，获得先验性的实践经验和安全指导。正如作者在书中所言，传播知识比学习知识更有价值。真诚地希望本书的推出，能够为物联网安全开发者赋能，让广大的物联网从业者受益，为构建安全的数字化物联世界贡献知识与力量。

阿里云智能 IoT 事业部 总经理 库伟

2019 年 2 月

此为试读，需要完整PDF请访问：www.ertongbook.com

Foreword · 推荐序二

伴随着传感器、遥感、移动互联、大数据、云计算等技术的不断发展，物联网在各行业得到了广泛应用。2016 年，国家“十三五”规划中指出：要积极推进云计算和物联网发展，推进物联网感知设施规划布局，发展物联网开环应用。这显示了国家非常重视物联网基础设施的建设和推广。

在物联网应用高速发展的同时，物联网安全将面临严峻的挑战。大量物联网设备将直接暴露在网络上，如果有部分设备存在安全隐患，那么攻击者可以通过丰富的攻击手段获取用户隐私，影响用户的财产安全甚至人身安全。在一些大规模的物联网系统中，存在安全漏洞的主机可能会被恶意代码感染成为僵尸主机，变成僵尸网络的一部分，对互联网上的业务造成严重影响。

物联网安全问题主要包括设备安全、网络安全和应用安全，解决物联网安全问题需要分步走，其中设备安全更多的是解决物理攻击造成的影响。设备面临的物理攻击手段主要包括：版图攻击、计时攻击、能量分析攻击、电磁攻击和故障攻击。清华大学硬件安全和密码设备实验室在可重构计算和芯片安全领域深耕多年，形成了完善的芯片安全解决方案，在物理攻击防护方面有丰富的知识积累，在此基础上实现了多种主流国密和商密密码学算法，并提供了完善的密钥管理机制和可信计算服务，可以适用于各类安全应用系统进行高速、安全的密码运算。

本书两位作者的写作初衷是解决设备安全连接问题，让设备更安全的连接网络，为推动物联网系统的网络安全和应用安全贡献力量。本书是一本理论结合实践的物联网安全书籍，按照数论基础知识、密码学算法、TLS/DTLS 协议、物联网安全协议 CoAPs 的结构展开。密码学算法部分除了理论知识，还提供了相关工具和 mbedtls 示例代码，可以帮助读者更好地学习理解。本书中对密码学中较为重要的算法进行详细描述，如认证加密算法 GCM/CCM 和

椭圆曲线算法。在 TLS/DTLS 协议相关章节中，对协议实现进行详细描述，并使用网络抓包数据作为示例样本，按照密钥交换、密钥计算、对称加密的结构进行展开，详细描述每个过程的具体流程。在物联网安全协议 CoAPs 章节中，详细描述了物联网安全协议 CoAPs 的实现方法，可以在占用较少资源的情况下为物联网设备提供安全连接服务。为了对开发者有一定的指导意义，本书提供了丰富的示例，所有示例均基于嵌入式硬件平台实现，示例中更加关注硬件资源的消耗情况。

本书的两位作者作为物联网安全的探索者和实践者，为构建安全稳定的物联网系统提供了重要的知识积累，对于物联网开发者或爱好者而言，本书可以提供实践经验和安全指导，值得一读。

清华大学硬件安全和密码设备实验室主任　刘雷波教授

为何写作本书

2015 年，我和本书的另一位作者崔红鹏同在无锡物联网产业研究院从事无线传感网方面的开发工作。那年，物联网概念虽然已被炒作多年，但无论是技术路线还是开发手段都还处于摸索阶段。2015 年，共享单车才刚刚出现，NBIoT 还在协议制定阶段，云计算也没有迎来爆发式增长。当时工作室采购了一套带网络接口的 STM32F4 开发板，我们想利用这块开发板进行一次 HTTPS 实验：把 STM32F4 开发板作为 HTTPS 服务器，用浏览器作为 HTTPS 客户端，通过浏览器访问开发板提供的 HTTPS 服务。我们想将这个嵌入式 HTTPS 实验作为学习物联网安全的第一步。但万事开头难，我们始终没有完成这个嵌入式 HTTPS 实验，冗长的调试信息和复杂的握手过程使我们不知所措。在排错过程中，我们查阅了大量的资料，发现了一个又一个新名词或概念，例如 SSL、TLS、RSA 加密、数字签名和椭圆曲线等，这些密码学基础知识让我们一头雾水。除了一个又一个新名词或概念之外，我们还了解到“ RSA 已经被破解了”或“哈希算法 SHA1 已经被破解”这些网络传言，这些真真假假的网络传言让我们在排错过程中束手束脚，生怕使用了不安全的算法。经过几天的努力，我们把问题总结为“ TLS 握手过程的证书校验出现了问题”。由于大量基础知识的缺失，我们并没有完成这次 HTTPS 实验。虽然嵌入式 HTTPS 实验并没有成功，但是我们还是总结了以下经验教训：

1）相对于资源受限制的物联网终端而言，HTTPS 协议非常复杂，运行时也需要消耗大量资源。我们也开始思考是不是存在更合适的物联网终端的安全连接方案。

2）HTTPS 涉及 TLS 协议和密码学基础知识，这些内容都需要花时间和精力系统学习。

3）该实验通过 PolarSSL 开源组件实现 SSL/TLS，而 SSL/TLS 正是 HTTPS 的安全传

输层。如果要熟练掌握嵌入式 HTTPS，首先需要掌握 PolarSSL。2015 年，Polar 更名为 mbedtls，开启了物联网安全应用的新篇章。

当时我们还有另外一个共识：要想让物联网设备安全地联网，应该分为两步——第一，让物联网设备方便地连接网络；第二，让物联网设备安全地连接网络。

为了完成“两步走”的第一步，我在 2016 年到 2017 年间编写了国内第一本关于物联网专用协议 CoAP 的图书——《IoT 开发实战：CoAP 卷》，这本书解决了物联网设备方便连接网络的问题。CoAP 好比互联网应用中的 HTTP，而互联网应用不仅有 HTTP，还有 HTTPS，我想物联网应用中也应该有 CoAPs。2017 年到 2018 年间，三大运营商——中国电信、中国移动和中国联通在国内大力推进 NBIoT 网络建设，市面上出现了各种各样的 NBIoT 模组。2018 年 3 月底，阿里巴巴宣布物联网成为继电商、金融、物流和云计算之后的第 5 条“主赛道”，从此，物联网进入了“云连物”时代。NBIoT 和云计算的脱颖而出极大地推动了物联网的发展，当百万亿连接不再是遥不可及的梦想时，物联网应用不再满足于“方便”，同时对“安全”也提出了更高的要求。

在这种大背景下，2017 年 6 月，我找到了本书的另一位作者崔红鹏，此时他已经在清华大学无锡应用技术研究院从事安全芯片的开发工作。我表示希望结合 mbedtls 写一本详细描述物联网连接安全的图书，我们很快达成了共识并付诸实践。我已经有编写技术图书的经验，我本以为上一次的成功经验可以使这次图书编写变成一次“愉快的写作之旅”，但是没过多久我就发现自己错了。物联网连接安全涉及大量密码学知识，而密码学又涉及很多数学基础知识，例如初等数论和抽象数学等。数学基础知识的缺失使得图书的编写过程举步维艰，我们花费大量的时间学习各种数论公式，甚至还研究公式或定理的证明过程。大学毕业之后很少有系统地学习数学理论知识的机会，这次特殊的自主学习经历让我们深刻体会到了数学的力量，那些经典的公式居然在几百年之后依然发挥着巨大的作用。

目标读者

本书适合物联网工程师、嵌入式工程师和 Web 开发工程师阅读。

- 对于物联网工程师而言，通过本书可以系统地学习物联网安全连接的基础知识。本书借助深入浅出的示例讲解密码学算法，这些算法是构成物联网连接安全的利器。
- 对于嵌入式工程师而言，本书详细讲解了 mbedtls 不同模块的使用方法，这些使用方法可以帮助你构建物联网安全应用。本书还分析各种安全算法的性能，这些分析结果将帮助你在实际项目中做出正确的选择。
- 对于 Web 开发工程师而言，通过本书可以从设备角度了解物联网连接安全的限制条

件，在这些限制条件下，物联网设备不能直接使用互联网应用中常见的安全套件。

总而言之，本书试图消除物联网工程师、嵌入式工程师与 Web 开发工程师之间的知识鸿沟，在物联网连接安全方面达成共识。

如何阅读本书

本书主要内容分为三部分。

第一部分：第 1 ～ 3 章。第一部分是全书的基础。第 1 章主要讲解密码学安全常识、mbedtls 和 OpenSSL 相关基础知识。本书虽然以 mbedtls 为核心，但在多个章节中使用了 OpenSSL 工具，所以在第 1 章的后面部分将详细讲解 OpenSSL 的安装和使用方法。第 2 章介绍 mbedtls 的安装和使用方法，由于本书的大多数硬件示例均基于 Zephyr 构建，所以第 2 章还介绍了 Zephyr 的构建过程和使用方法。第 3 章讲解数论基础知识，包括素数、模运算、群、域和有限域等概念，这些数论知识是密码学算法的基础。

第二部分：第 4 ～ 12 章。第二部分主要讲解密码学 6 种主要密码技术——单向散列函数、对称加密算法、消息认证码、随机数、公钥密码和数字签名。第二部分还介绍了多种密码技术，分别是 SHA256、AES、HMAC、GCM、CCM、CTR_DRBG、RSA、DH、ECDH、DSA、ECDSA 和 X.509，每章均包括原理说明和 mbedtls 示例代码，试图通过理论结合实践的方式向读者展现 mbedtls 的全貌，其中椭圆曲线相关的 ECDH 和 ECDSA 涉及较多数学知识，是本书较难理解的内容。

第三部分：第 13 ～ 16 章。第三部分主要包括 mbedtls 移植与性能分析、TLS/DTLS/CoAPs 等内容。mbedtls 性能分析部分将比较各种安全算法，这些分析结果可以帮助读者在实际项目中做出正确选择。第三部分还介绍了 TLS 和 DTLS 协议，虽然 TLS 协议异常复杂且仍在不断发展，但它是物联网连接安全的核心协议。第 14 章详细介绍 TLS 协议，包括 TLS 握手协议、密钥交换、密钥计算和对称加密等，这些是本书最复杂的内容。为了讲解 CoAPs，第 15 章还介绍了 DTLS 协议，重点介绍了 DTLS 协议与 TLS 协议之间的联系与区别。最后一章介绍了 CoAPs，CoAPs 可被理解为 CoAP 协议与 DTLS 协议的结合，它将成为物联网连接安全的主流协议。

相关资料

本书提供多个基础示例，这些示例代码可以帮助读者更好地了解 mbedtls。

示例代码仓库网址为：https://github.com/iotwuxi/iot_security。

勘误与支持

由于作者水平有限，书中难免有错误之处，恳请读者批评指正。如果读者在阅读过程中发现任何问题，可通过邮件与本书的两位作者取得联系。

徐凯的邮箱：xukai19871105@126.com

崔红鹏的邮箱：xianrenqiu90@126.com

徐凯的致谢

感谢机械工业出版社华章公司的编辑，没有他们的策划与鼓励就不会有这本书。

感谢阿里巴巴阿里云 IoT 无锡团队的汪亮（画安）和罗日健（悠仔），感谢他们营造了一个具有创新精神的工作环境，这种氛围激励我不断前进；感谢一起并肩战斗的小伙伴们，他们是黄浩（先道）、赵峰（新安）、林达（靖明）、龙超（瞻龙）、吴叶俊（安悟）、庞海亮（胖亮）、谢娟（无鱼）、刘愿（毕险）、李迪晞（平休）、彭微（师尘）、三帖（张云）；感谢阿里云 IoT 的两位师兄李锟（怀明）和杨骁（羽升）；感谢崔杨（懿侬），是他让我明白“传播知识比学习知识更有价值”。

感谢我的导师江南大学君远学院院长张秋菊教授，感谢您帮助我开启物联网世界的大门。

感谢我的妻子左文娟一如既往地支持我写作，感谢家人的默默付出与包容。

崔红鹏的致谢

感谢微纳电子实验室的朱敏、吴有余、张继璠和龚雪，是他们为实验室创造了良好的工作环境和学习氛围。感谢实验室与我一起工作的同事，他们是：杨锦江、王宇峰、孙进军、徐翔、张扣、姚俊、张沛、李植、章俊、李康、胡永鑫、赵新成、赵启义、徐健、郭唯、贾德存、蒋广隶。

感谢妈妈和老婆的默默付出，是她们让我有充足的时间和精力完成写作。在此祝家人健康快乐。

此为试读，需要完整PDF请访问：www.ertongbook.com

Contents · 目录

此为试读，需要完整PDF请访问：www.ertongbook.com