轻量级密码学算法库

向嘉豪[1]

[1] 衡阳师范学院

2024 年 7 月 15 日

目录

密码学算法库

- 特性
  - 数据的机密性，对于攻击者来说不可见原始信息。
  - 数据的完整性，防止攻击者修改原始信息。
  - 数据的可用性，实际应用中的易用性和有效性，如加密性能。
  - ...
- 上层通信协议
  - SSL/TLS：安全套接字层（SSL）和传输层安全（TLS），常用如 HTTPS 协议。
  - IPsec：互联网协议安全（IPsec）是一组协议，通常用于建立虚拟专用网络（VPN）。
  - SSH：安全外壳协议（SSH）是一种用于在不安全的网络上安全地访问远程计算机的协议。
  - PGP：非常好的隐私（PGP）是一种用于加密和解密数据的程序，通常用于保护电子邮件通信的安全。
- 我们每天都在使用这些协议，每天都在使用密码学算法库。

轻量级密码学算法库

- 资源受限的环境下，实现的密码学算法库。
  - 低功耗，如受限设备功耗为 100mW，而 PC 机为 250W。
  - 低存储，如受限设备存储为 64KB，而 PC 机为 1TB。
  - 低计算频率，如受限设备为 64MHz，而 PC 机为 5GHz。
- 上层通信协议
  - MQTT: 轻量级的发布/订阅消息传输协议。例如，智能家居设备使用 MQTT 协议来传输传感器数据和控制命令。
  - CoAP: 受限制应用协议，近似与 HTTP，常用于物联网（IoT）环境。例如，智能照明系统使用 CoAP 协议来控制灯光的开关和亮度。
- 如何在资源相差约 1000 倍的设备上实现密码学算法库？

目录

安全

- 安全是密码学算法库最基本的要求。
  - 攻击者可以在获取设备的物理访问权限后，通过侧信道攻击（如功耗分析、时序分析、电磁分析等）来窃取设备中的敏感信息。
  - 利用协议漏洞，如重放攻击、中间人攻击、拒绝服务攻击等，干扰设备正常工作。
- 如何在资源受限的设备上实现更安全的密码学算法库？

性能

- 性能限制加密库的使用场景。
  - 加密性能：加密速度、解密速度、加密延迟、解密延迟。
  - 存储性能：存储空间、存储延迟。
- 如何在资源受限的设备上实现更高性能的密码学算法库？

可移植性

- 可移植性影响到加密库的可用性。
  - 跨平台：支持多种硬件平台，如 ARM、MIPS、X86 等。
  - 跨编程语言：支持多种编程语言，如 C、C++、Python 等。
- 如何在资源受限的设备上实现更可移植的密码学算法库？

目录

性能

- 使用预计算、查找表、位运算等通用优化技术，提高加密性能。
- 采用扩展指令集、硬件加速器等特定优化技术，提高加密性能。

可移植性

- 使用标准化接口，如 OpenSSL、mbedTLS 等，提高可移植性。
- 使用模块化设计，提高可移植性。
- 多平台支持，如 ARM、MIPS、X86 等。

更安全

- 使用轻量级的密码原语，去设计加密算法。
- 设计抵抗侧信道攻击的实现方案。
- 修改通讯协议，增加安全性。

Thank You

Thank you for your attention!

项目参考：`https://github.com/Tongsuo-Project/tongsuo-mini`.