白皮书

用于物联网的安全互联通信

Brad Rex，物联网基础设施业务部门高级产品营销经理，瑞萨电子株式会社

2020 年 1 月

摘要

如今，全面保护互联设备变得比以往更加重要，然而保障互联网安全并没有放之四海而皆准的方法。每种嵌入式解决方案的需求各不相同，任何一种安全保护方案都无法抵御所有存在的漏洞。嵌入式开发人员需要在具有竞争力的设计和其他优先选项（如开发成本和时间投入等）之间平衡取舍，。本白皮书将研究保障物联网通信安全的各种方法以及正确实施这些安全保障方法所面临的挑战。

威胁日益增长的形势

如今，我们生活中最简单的物件，比如咖啡杯、药瓶之类，也可能会连接到互联网和云环境。这意味着，我们的很多日常环境都已成为潜在攻击面。随着互联设备面临的网络威胁变得攻击性更强，更为恶意，日常生活的每个方面几乎都可能被黑客和恶意软件入侵。

目前，开发人员的首要考虑是保护嵌入式应用程序，以此保护数据和预期功能，所以任何通过互联网的通信都必须是安全的。

重要的是，嵌入式安全不能在事后弥补，必须从开始就做好规划和设计。事后可能可以添加一些安全功能，，但这种做法会大幅增加嵌入式安全的成本。或者更有可能的是，对于某些安全漏洞，在设备发布后根本无法充分解决安全缺陷。

我们需要的是一种安全策略，利用软硬件安全领域最新的技术发展，提供多层防护，为互联网通信实施深入而全面的保护。

保护通信的方法

主动实现互联设备之间安全通信，需要有多层防护。为了帮助设备抵御多种安全威胁，我们需要通过基于硬件生成的密钥来保护设备标识。该标识应安全存储在片内闪存中，用来建立互信，或将标识添加到产品设计中，用于配置目标应用，以保护隐私。

建立强大而安全的设备标识，可使每台设备都能被单独识别并进行身份验证，成为唯一的设备。创建标识后，强设备标识可以通过多种方式满足嵌入式安全的核心需求，因为设备标识可以确保互连时的身份验证和识别。

简单的建立唯一设备标识的方法是将产品序列化，比如使用产品序列号或者设置设备 ID，但使用非对称加密，能提供更加强大安全性，适用的实例范围更广。

基于密钥的加密。创建加密设备标识的第一步是生成密钥。这些密钥可在设备内部生成，也可在外部安全工具中生成后再注入设备。一旦生成或注入了设备密钥，证书颁发机构(CA)就会颁发数字证书。CA 可能是公用的（位于云服务器中），也可能是私有的（位于本地，通常托管在安全服务器上）。在设备上创建标识，并将标识烧录到设备中后，，必须将其安全存储到只有通过“安全代码”才能访问的安全存储器中，以防该设备标识（密钥和认证）被清除或重写。

非对称加密算法需要创建公钥和私钥，并且是通过数字证书提供身份验证的公钥基础架构(PKI)加密方法的一部分。公钥可对任何人公开，而对应的私钥只有需要解密公钥加密数据的一方知道。

当具有单一安全标识的设备连接到网络时，它必须进行身份验证，并和具有唯一标识的其他设备、服务以及用户之间建立**互信**，受信任的系统成员间能够进行安全通信，交换加密数据与信息。唯一设备标识的另一项优点是**隐私保护**，安全网络中交换的数据可能包括一些私有和保密的信息，如个人信息、敏感信息和财务信息，这些信息通常受到都法规监管。设备**完整性**涵盖受信任生态系统中的设备和数据。设备的完整性首先从证明设备身份开始，强设备标识可以确保设备的合法性，从而减少仿冒产品，保护公司品牌。

保护动态数据安全。设备标识是安全产品、安全制造和安全通信的基础，但网络数据的安全传输需要不同类型的保护。

传输层安全(TLS)是对计算机网络提供通信安全的加密协议。它不断演变推出采用更强安全措施的新标准，以便跟上新出现的威胁形势。它会同时运用非对称加密和对称加密，以提供高度的安全性，同时又不影响加密和解密的速度。TLS 通过以下方式保障两个通信应用的保密性和可靠性：

- **加密：**使用对称加密方法对相互通信的应用之间交换的数据进行加密，以确保连接是私密的。
- **身份验证：**采用基于证书的机制验证标识。
- **完整性：**为确保连接可靠和消息完整性，使用消息验证代码(MAC)机制检测消息是否遭受篡改和伪造。

数据报传输层安全(DTLS)通信协议旨在保护基于数据报的通信，并防范数据遭受窃取和篡改。它基于 TLS 协议，提供类似级别的安全性。该协议可用于网页浏览、邮件、即时消息和 VoIP。DTLS 采用用户数据报协议(UDP)，而 TLS 使用传输控制协议(TCP)。相比 TLS，DTLS 的开销更低，延迟更短，是时间敏感型传输的理想之选。DTLS 是通过简单 JavaScript API 用于网页浏览器网页实时通信(WebRTC)技术的安全协议之一。

保护物联网和云通信

最近，物联网(IoT)和云计算的发展对安全数字通信提出了新的要求。

物联网将了一系列技术和互联智能设备（例如传感器和致动器）通过智能手段融合在一起，在用户和设备之间实现了全新的沟通方式。在这个过程中，物联网设备会产生大量数据，但运算能力有限；而云计算则能够让数据传输到预期的目的地，或执行那些超出物联网设备处理能力的运算。

物联网实例包括智能家居、智慧城市、可穿戴设备、电子健康、农业和能源管理。这些智能网络能够收集和分析信息，甚至做出决策，无需任何人员参与。在这些情况下，鉴于物联网系统中未经验证的恶意设备可能造成的影响，数字通信安全变得至关重要。尽管物联网的安全需求（保密性、完整性或身份验证等需求）主要由其服务的应用类型决定，但受到物联网设备和网络的资源限制，传统的身份验证或加密方法可能无法胜任。

物联网设备需要执行身份验证和配置云服务。目前，大多数云提供商使用超文本传输协议(HTTP)、消息队列遥测传输(MQTT)和受限应用协议(CoAP)的组合方式，使用配置证书和生成的密钥验证设备凭据或通过副通道机制来保障通过 TLS/DTLS 传输的数据安全。

HTTP 是互联网使用的基本协议。它设计用于网页浏览器与网页服务器之间的通信，但也能用于其他目的。不过，HTTP 最初设计为明文协议，容易遭受窃取和中间人攻击。安全超文本传输协议(HTTPS)是 HTTP 的扩展，适用于计算机网络和互联网内的安全通信。HTTPS 为 HTTP 增添了 TLS 加密功能，以确保联网设备之间交换的所有数据受到双向加密。

实现这一目标的方法是：通过 PKI 并使用 X.509 证书为受信任设备、个人、公司和网站附加加密密钥对。如果某个 HTTPS 网站提供的证书已由公开的受信任证书颁发机构签署，则可向用户保证该网站的标识已通过受信任的第三方验证。每个密钥对都包括一个私钥（需要保密）和一个公钥（可广泛分发）。私钥相当于解码器，允许应用程序对使用公钥加密的消息进行解密。此外，发送者也可以使用私钥对消息执行数字签名。即使互联网本身不是安全网络，加密系统也可在网络上建立安全的连接。

对于大多数物联网设备而言，基于 HTTP 的协议过于繁重，请求响应速度往往不够快。**MQTT** 是一种更加轻量化的在客户端-服务器之间发布-订阅消息的传输协议，具有开放和易用的特点。MQTT 适用于性能受限设备（例如传感器节点及其他物联网设备）以及低带宽、高延迟或不可靠的网络。这些特征使得 MQTT 非常适合在各种环境下使用，例如机器到机器(M2M)和物联网环境中的通信，因为这些通信需要短代码，并且/或者网络带宽资源非常宝贵。MQTT 支持 TLS，实施后可对客户端与中间人之间的通信完全加密，防止黑客拦截传输数据。

CoAP 是一种特殊的网络传输协议，适用于物联网中资源受限的节点和网络。该协议适用于智能能源和建筑自动化等 M2M 应用。CoAP 依靠 UDP 传输来传送数据以及 DTLS 安全方面来保护信息。

保护互连设备面临的挑战

尽管 MQTT 和 CoAP 都用来满足物联网的特殊需求，而且两者都支持常见的安全协议，但若未正确加以保护，它们都很容易受到攻击。基于这些协议的网络特别容易面临以下安全威胁。

分布式拒绝服务(DDoS)攻击。DDoS 是最常见、破坏性最大的网络攻击形式之一，通过向目标涌入大量互联网流量来阻止目标服务器、服务或网络的正常操作。这些攻击会导致系统或网络关闭，阻止授权用户访问数据或服务。这些攻击的出现，通常是因为黑客攻破了成千上万台联网设备，然后协同其消息发送功能对中央服务器进行轰炸，直至中央服务器由于计算资源耗尽而出现故障。不安全的物联网设备常常被 DDoS 攻击牵连。2016 年 10 月，通过使用被入侵的安保摄像头和数码摄像设备，针对 Dyn 发动了大规模攻击就是，导致网络大面积瘫痪。

TCP SYN 泛洪。另一种 DDoS 攻击形式是 TCP SYN 泛洪，这种攻击会操控客户端与服务器之间的三次 TCP 握手过程，使用不完整的 TCP 请求阻止目标服务器打开连接端口。通过重复发送初始连接请求(SYN)数据包而不完成连接，攻击者可以耗尽目标服务器上的所有可用端口，使其无法响应。[1]

Slowloris。另一种 DDoS 攻击类型是 Slowloris，它允许攻击者使用单一机器，打开并维持与目标服务器的众多并发 HTTP 请求，从而阻塞服务器。由于可用来处理并发连接的线程数量有限，目标服务器将不得不等待请求完成（攻击者不会完成请求）。在超出服务器的最大可连接数时，则会发生拒绝服务。

不安全 MQTT。尽管 MQTT 本身并不安全，但我们可以通过几种机制来保护 MQTT 连接，包括简单的用户名和密码组合以及 TLS，后者为 MQTT 上的消息提供加密管道。

使用 MQTT，务必要注意的是 MQTT 中间人或服务器实施的安全限制，并且客户端节点必须单独配置。这样不仅会增加复杂性，设计人员在规划物联网实施安全性时还必须考虑 MQTT 客户端的功能，因为支持能力不足，可能无法在简单客户端（例如非常基本的传感器）上使用安全功能。

不安全 CoAP：CoAP 的安全问题与 MQTT 类似，但部署不良的波及面更广。由于增加 DTLS 安全性会掩盖 CoAP 的一些规模和速度优势，一些公共基础架构设计忽略了这方面的需求，由此导致互联网中出现成千上万台不安全设备。鉴于 TCP 与 UDP 之间的差异，不安全 CoAP 设备可能被人用来发动 DDoS 攻击，倍增系数甚至高达 51,000 倍。[2]

不过，MQTT 的问题不在于协议，而在于许多 MQTT 网络的安全配置不当，甚至在毫无安全配置的情况下运行。特别是在小型组织的智能家居部署或物联网网络中，通常需要由客户或物联网供应商来负责实施和配置安全机制，以保护 MQTT 通信。

对于配置不当且没有密码的 MQTT 服务器，在互联网上可被公开发现，这让黑客能够潜入与该服务器关联的任何智能家居或业务。另外，由于 MQTT 采用一对多订阅架构的方式访问 MQTT 服务器，这意味着可以访问网络内传输的所有数据。
网络罪犯可以轻松利用这类配置缺陷和漏洞来执行侦察，秘密盗取数据和发动 DDoS 攻击。

在敌对环境下保护互联设备

即便对于有经验的开发人员，保障互联设计安全也充满挑战且十分耗时，更有多种风险和恶意企图会乘人不备。要为基于嵌入式器件的产品提供全面而深入的安全保护，需要综合运用多种协议和安全保护措施，多方面保障安全。

十余年来，瑞萨电子一直处于嵌入式系统安全领先地位，能够充分了解并解决当今互联产品日益强化的安全需求。瑞萨电子提供多种嵌入式安全解决方案，具有多层次的开发基础架构，可为各种嵌入式产品带来全面的安全保护。

Renesas Synergy™平台是一个全覆盖的优质开发平台，其中包括以 Synergy 软件包(SSP)的形式提供的量产级软件，还有一系列可扩展的引脚兼容的 MCU，并且预先经过集成和测试，能够提供多层级安全保障。Synergy 平台可确保在安全可靠的技术基础上构建物联网应用。

此外，瑞萨电子的新型 RA 系列 MCU 提供具有更高平台灵活性的选项，将 Arm Cortex-M 内核与瑞萨先进的外设 IP 相结合。RA 的灵活配置软件包(FSP)提供经过优化的 HAL 驱动程序，还提供基于 FreeRTOS 和相关中间件构建的基线软件平台。使得开发人员能够轻松灵活地整合所选的中间件和库。

Synergy 平台和 RA MCU 都包含名为安全加密引擎(SCE)的集成加密子系统。SCE 为常用加密算法提供硬件加速，还提供密钥生成和真随机数生成器(TRNG)。Synergy 平台和 RA FSP 均支持公钥基础架构(PKI)。

此外，开发人员还需要确保通过开发平台能够使最终产品安全轻松地连接到云。Synergy SSP 通过内置 MQTT 和 TLS 模块为云连接提供支持，Synergy 云连接应用还提供了内置的安全云连接，可连接到 Amazon Web Services (AWS)、Google Cloud 和 Microsoft Azure 等领先的云环境。RA FSP 利用 Arm 生态系统软件提供类似的功能。

结论

为互联应用提供全面深入的安全保护需要综合各种技术共同发挥作用，在多个层面提供防御。瑞萨电子可提供多种方式来深度保护设备、服务和网络，帮助嵌入式开发人员应对保护互联设备面临的挑战。

瑞萨电子提供了多种 MCU[3] 来解决本白皮书中探讨的问题。请访问我们的网站，了解更多信息。

参考资料：

[1] Hacked Cameras Were Behind Friday's Massive Web Outage

[2] In-the-Wild DDoSes Use New Way to Achieve Unthinkable Sizes

[3] RA 系列 32 位 Arm Cortex-M MCU
RX 系列 32 位 MCU
Synergy 平台 32 位 Arm Cortex-M MCU + 合格软件