doi :10.3969/j.issn.1671-1122.2017.09.004

物联网设备信任体系架构与轻量级身份认证方案设计

武传坤，张磊，李江力
（北京匡恩网络科技有限责任公司，北京 100191）

摘 要：物联网设备的身份标识和身份认证技术是物联网设备安全通信必不可少的前提。文章针对物联网设备的特点，建立了一种针对物联网设备的信任体系架构，分别提出了如何基于公钥证书建立信任体系和基于对称密钥建立信任体系。在此基础上，基于公钥证书配置和预置共享密钥配置两种情况，分别设计了物联网设备的身份认证方案。

关键词：物联网；信任体系架构；身份认证；公钥证书
中图分类号：TP399 **文献标识码：**A **文章编号：**1671-1122（2017）09-0016-05

中文引用格式：武传坤，张磊，李江力．物联网设备信任体系架构与轻量级身份认证方案设计[J]. 信息网络安全，2017（9）：16-20.

英文引用格式：WU Chuankun, ZHANG Lei, LI Jiangli. Design of Trust Architecture and Lightweight Authentication Scheme for IoT Devices[J]. Netinfo Security, 2017(9):16-20.

Design of Trust Architecture and Lightweight Authentication Scheme for IoT Devices

WU Chuankun, ZHANG Lei, LI Jiangli
(*Beijing Acorn Network Technology Co, Ltd, Beijing* 100191, *China*)

Abstract: The identification and authentication of IoT devices are two fundamental problems in secure communications of those devices.Noticing the characteristics of IoT devices, this paper designs an architecture of trust, proposes how to establish a trust based on public key certificates and on symmetric key settings respectively.Based on the above, this paper designs two authentication schemes for IoT devices based on the public certificate setup and the shared secret key setup respectively.

Key words: IoT; trust architecture; authentication;public key certificate

《中华人民共和国网络安全法》（以下简称《网络安全法》）已于2017年6月1日开始实施，这意味着国家已经从技术和管理保护网络安全阶段，走向依法治理网络安全的新时代。依法治理网络安全，并不意味着技术和管理所起的作用小了，相反，需要更多的技术和管理，为法律的实施提供辅助。同时，对已有技术的淡漠造成的网络安全问题，也可能导致违法行为，因此，《网络安全法》的实施，将进一步加强专业技术和规范管理在网络安全领域的作用。物联网作为网络安全的重要应用领域，目前在技术方面还很不成熟，国家《网络安全法》第二十四条指出："国家实施网络可信身份战略，支持研究开发安全、方便的电子身份认证技术，推动不同电子身份认证之间的互认"。在这一条款背景下，本文研究物联网设备的可信机制和身份认证技术[1]。

1 可信的定义

"可信"或"信任"在网络环境中是指能够确认对方身份并有能力建立安全通道的一种状态，与生活中人们之间的信

收稿日期：2017-8-1
作者简介：武传坤（1964—），男，山东，博士，主要研究方向为网络安全、物联网安全与工业控制系统安全；张磊（1981—），男，山东，博士，主要研究方向为网络安全、物联网安全与工业控制系统安全；李江力（1971—），男，湖北，硕士，主要研究方向为网络安全、物联网安全与工业控制系统安全。
通信作者：武传坤 chuankun.wu@acorn-net.com

任的含义是不同的。例如，设备A信任设备B（或等价地说，B对A是可信的），意味着A可以与B建立安全通信通道，并确信与其通信的对方必定为B。信任具有可传递性，即A信任B，且B信任C，则可通过一定安全协议建立起A对C的信任。但信任不是自然双向的，也就是说，A信任B，并不意味着B同时也信任A。

信任是可以通过一定步骤来建立的，但是建立信任的基础是“初始信任”。信任只能传递，不能无中生有。初始信任的建立不能通过网络协议，一般需要人工操作，通过离线方式完成。常用的初始信任建立方式是将关键信息写入通信设备中。在物联网系统中，物联网设备的初始信任就由设备生产商在出厂前写入。

建立初始信任的常用方法是在设备中写入公钥证书，或预置共享密钥。写入公钥证书，可建立设备对公钥证书签发机构（CA）的初始信任[2]。以此为基础，可扩展到对由该CA签发证书的其他设备的信任。预置共享密钥，可建立设备与任何拥有该密钥的设备之间的信任。因此，预置共享密钥所建立的信任是双向的。

信任或可信不同于身份认证。信任是身份认证的基础。没有信任就无法实现身份认证，而信任本身并不意味着已经得到身份认证了。网络环境中的信任与可信计算技术也有明显区别。可信计算概念中的“可信”是指执行环境的可控性，与网络通信环境中表示掌握确切的、不可伪造的信息意义下的“信任”是不一样的。

2 物联网系统已知的可信架构

2016年，Tempered Networks发布了“身份定义网络（Identity-Defined Network，IDN）架构”白皮书[3]。在IDN架构中，每个设备有一个唯一的密码学身份标识（Cryptographic Identity，CID），设备之前的安全通信通过主机身份标识协议标准来实现。要建立IDN网络，必须同时建立两个或多个HIP服务端，每个HIP服务端需要知道其他服务端的IP层状态，而且保存基于身份的路由表。

IDN网络使用了AES-256加密模块，但仅仅这一个密码模块是不够的。在Tempered Networks的另一份报告[4]中，介绍了HIP交换机使用的密码模块还包括：基于RSA-2048的X.509公钥证书、用于数字签名的散列函数SHA-2、用于消息完整性的散列函数SHA-1、用于3方密钥协商的Diffie-Hellman协议。

不难看出，如果3个HIP服务端进行群组通信的机会不大，或每次通信的数据量不大的话，使用Diffie-Hellman协议的功能是多余的。另外由于公钥证书由Tempered Networks签发，因此后期的网络设备都要基于对Tempered Networks的信任和安全性依赖，才能进行正常的安全数据交换。

赛门铁克提出了物联网的一个“强信任模型”[5]。在数十亿物联网设备中嵌入同一个CA列表，每个设备有唯一一个身份和由某个CA签署的公钥证书。物联网设备之间通过公钥证书可以随时建立信任和安全通道，实现端到端的安全通信。

3 一种面向实用的物联网可信架构设计

不难看出，Tempered Networks的IDN平台所使用的HIP服务端，与赛门铁克的唯一设备身份的物联网架构雷同。不同的是，Tempered Networks的IDN平台需要使用自己签署的公钥证书，而赛门铁克的架构允许使用多家不同CA（证书签发中心）签发的公钥证书。无论哪种情况，都没有国内机构作为CA，因此“信任”的基础是国外的CA，不是非常适合国内对“安全可控”的安全策略要求。因此需要根据国内具体情况，建立新的安全架构[6]。

3.1 身份标识

要建立网络通信安全环境，身份标识和对通信端的信任是前提。身份标识是在通信系统中能够被识别的一种长期有效的信息，不用于通信路由和物理定位，而是用于对通信端设备的识别和身份认证。为此，相互进行通信的设备应该有能力识别对方的身份标识，也就是说需要在系统中建立这样一种机制，使得身份标识在网络内具有唯一性、可知性、可识别性。对身份标识的可知性，是指身份标识符合身份标识机制所规定的格式；对身份标识的可识别性，是指身份标识属于这个特定的网络，是“合法”的。

在合理的身份标识和信任机制下，要建立安全通信通道是很容易的，包括对数据机密性和数据完整性的保护，都可以通过加密来实现。建立安全通道常用的方法是认证与密钥协商（Authentication and Key Agreement，AKA）协议。在物联网环境中，传统的AKA协议一般不适用，因为数据的交互所占用网络资源和计算资源、时延、功耗等都是资

源受限的物联网设备所不能容忍的，因此需要更合理的认证方案，即需要轻量级认证方案。

3.2 对物联网设备的身份标识方法

为了使得电脑设备和现代通信设备能够在全球范围内进行通信，每个网络设备都有一个全球唯一的MAC地址。能否用设备的MAC地址作为标识呢？从唯一性和可知性上是满足条件的，但不满足可识别性。一般地，要建立网络内部的设备身份，需要在网络内重新定义，本文提出如下两种方法。

1）基于生产批次的身份标识。每生产一批，使用一个批次的身份标识。格式为XX-YY，其中前2字节“XX”表示批次，后2字节“YY”表示序号。在批次标识XX中，可以用第1个字节标识部门，第2个字节表示批次，允许有256个不同的批次。如果这个数字不满足要求的话，可以牺牲第一个字节的含义，用第一个字节前4比特表示生产部门，后4比特连同第二个字节用于标识批次，这样就可以允许4096个批次了。如果一个批次生产的物联网设备数量超过65535个，则可以在一个批次中使用多个批次序号，这只是管理问题，不增加技术上的实现复杂度。

基于批次的身份标识的优点是，无需在使用中设置身份标识，因为出厂时就已经设置好了，而且相关安全参数可以在出厂时同时设置，直接在应用环境中连接、调试就行了。对设备标识的识别可使用模糊识别方法，即仅识别批次信息即可。该方案的缺点是不适合将不同批次、不同厂家的产品组到同一网络中，这方面的灵活性差。

2）基于网络的身份标识。针对不同的网络，重新设置网络内设备的身份标识。格式为XX-YY，其中前2字节“XX”表示网络标识，后2字节“YY”表示网络内设备序号。在这种情况下，一个网络中可以允许的设备最多有65535个。实际中一个网络中的设备数可能远小于65535，这种情况下可以利用这些多余信息表示设备类型、设备特征等。这些具体的设置可由用户定义。

基于网络的身份标识需要注意对网络标识的定义。目前没有标准可参考，但基本宗旨是要避免不同网络之间使用同一网络标识。如果网络标识是随机选的，发生碰撞的概率不大。但是在大的范围内一定存在网络标识的复用，但只要网络之间没有交互，包括信号交互、管理交互、应用交互，则不影响不同网络的独立正常工作。

基于网络的身份标识方法的优点是，组网所用设备的厂商、批次无限制，灵活性好，可扩展性强。对设备标识的识别可使用模糊识别方法，即仅识别网络标识信息即可。网内设备的身份标识可使用6LowPan标识协议生成。但这种方案需要在组网前对设备参数重新设置。对大规模网络，会增加一些工作量。

3.3 物联网设备信任的建立方法

建立信任的目的是防止假冒攻击、伪造攻击等主动攻击。如果没有信任，即使两个设备之间建立了“安全”通道，也不能防止通信主体为攻击者的“内部攻击”的情况。针对国内对安全可控的方针政策，以及物联网设备资源受限等实际情况，考虑到物联网系统的多样性，本文提出两种建立“信任”的方法。

1）基于预置对称密钥的信任。如果物联网设备在一个可控的环境中使用，则网络信任的建立可以使用人工配置的方式。任何拥有共享密钥的设备之间被认为具有“信任”关系。当一个群组中建立相互之间的信任关系时，可以使用群组密钥，也可以建立两两之间的共享密钥。但考虑到可操作性，可使用小群组密钥，以及不同群组之间通过组代表（如网关）之间建立的共享密钥来完成。

事实上，在物联网环境中，多数情况下物联网设备之间不需要通信，只需要与网关进行通信，此时可以让网关与每个物联网终端设备共享一个不同的密钥。网关与后台数据处理平台之间的密钥管理，也可以采用一对一的方式。

为了能建立安全通道，还需要内置密码算法。为了适应国家对密码算法的管理要求，可使用SM4。这是一种与AES类似的分组密码，这种密码算法已公开，因此可以通过嵌入式软件实现。

基于预置对称密钥来建立信任的优点是，无需第三方参与随时可以完成配置，资源占用少包括较小的密钥数据量。但这种方法也有缺点，就是使用不方便，必需首先需要信任的建立阶段，只能在可控范围内使用。如果使用者涉及多个利益冲突的机构，则不适合。

2）基于公钥证书的信任。在设备出厂时内置一个公钥证书，但存在的问题是公钥证书选择的问题。目前国内市

场上的公钥证书主要是以RSA密码算法为基础的公钥证书不适合物联网设备。建议使用国内密码算法标准SM2，该算法有标准规范《基于SM2密码算法的数字证书格式规范》（GM/T 0015-2012）可供参考。

4 对物联网设备的身份认证

对物联网设备的身份认证是物联网感知层信息安全的核心。根据信任基础的不同，需要建立不同的身份认证方案。

4.1 基于对称密钥的设备身份认证方案

如果信任的建立是基于预置对称密钥的，则可以直接使用密钥加密数据，这样在完成身份认证的同时，也完成了对数据的保密传输。方案架构如下：

$A \rightarrow B: ID_A \| ID_B \| E_k(ID_A, ID_B, k_s \| k_i) \| E_{k_s}(data) \| MAC(k_i, data)$

其中 $\|$ 为数据的连接符，ID_A 为设备 A 的身份标识，k_s 和 k_i 分别为用于数据加密和数据完整性保护的会话密钥，$E_{k_s}(data)$ 为密钥 k_s 下的数据加密算法，$MAC(k_i, data)$ 为密钥 k_i 下的数据完整性保护算法（Message Authentication Code，MAC）。

当设备 B 收到上述数据后，根据前面的身份标识信息可选择解密密钥，解密后检查密文中的身份信息，若正确无误，则设备 B 完成了对设备 A 的身份认证，而且同时得到两个会话密钥，进一步可对数据 $data$ 进行解密和完整性验证。

上述无交互协议实现了设备 B 对设备 A 的身份认证的同时，也使得设备 A 得以将业务数据以安全方式传递给 B。简单地说，这不是一个单纯的身份认证方案，而是将身份认证、数据机密性保护和数据完整性保护整合于一体的安全方案，而且只需一轮的通信，因此可以认为是一种轻量级安全协议。同样地，当需要设备 B 向设备 A 发送秘密数据时，按照同样的协议流程，可以实现 A 对 B 的认证，同时实现数据的机密性和完整性保护。

4.2 基于公钥证书的设备身份认证方案

如果信任的建立是基于公钥证书的，则可以使用如下方案完成身份认证和数据传输：

$A \rightarrow B: ID_A \| ID_B \| Cert_A \| ID_{CA}$

$B \rightarrow A: ID_B \| ID_A \| Cert_B \| ID_{CA} \| E_A(ID_A, ID_B, k_s \| k_i) \| SB(ID_A, ID_B, k_s \| k_i) \| E_{k_s}(data) \| MAC(k_i, data)$

当 A 将自己的公钥证书发给 B 后，B 首先检查是否有CA的根证书。如果 B 没有记录CA的根证书，则不能完成身份认证。如果有，则可以验证公钥证书的合法性，从而提取 A 的公钥。然后 B 使用 A 的公钥对 $ID_A, ID_B, k_s \| k_i$ 进行加密，同时使用自己的私钥对 $ID_A, ID_B, k_s \| k_i$ 进行签名。同时，使用加密会话密钥 k_s 对数据 $data$ 进行加密，使用完整性会话密钥 k_i 对数据进行完整性保护，并将这些信息连同自己的公钥证书发给 A。

当 A 收到 B 返回的数据后，验证 B 的公钥证书的合法性，提取 B 的公钥，使用自己的私钥对数据 $ID_A, ID_B, k_s \| k_i$ 进行解密，同时使用 A 的公钥验证数字签名的合法性，这样就完成了对数据来源的身份认证，同时实现了数据的机密性保护和完整性保护。

上述对机密性和数据完整性的处理过程仅用于说明原理，实际处理时，还要考虑完整性处理的对象是原始消息还是加密后的密文消息。根据有关研究结果，对加密后的密文进行完整性保护，比对原始消息进行完整性保护具有更高的安全性。

上述步骤是典型的握手协议，实际中可能需要使用3次握手协议，最后一次握手是对前面协议执行成功与否的确认。需要说明的是，具体实现身份认证方案时还包括许多其他参数。当不需要完整性或不需要机密性保护时，可对协议中的数据格式和验证流程进行适当裁剪，如删除对 k_i 的处理和对MAC的计算。

上述方案实现了设备 A 对设备 B 的身份认证，同时完成了 B 向 A 安全传输数据的过程，这一过程可提供数据机密性和数据完整性保护。上述方案虽然通过公钥证书的验证，建立了双向信任，但设备 B 对设备 A 的身份认证并未完成，也就是说，通信结束后，设备 B 并不确定与之通信的是设备 A。但是这种假冒攻击对攻击者来说没有任何收获。如果需要设备 B 对设备 A 进行身份认证的话，可能需要更多轮的通信。

5 安全性分析

下面简单分析关于身份标识定义格式的合理性和身份认证协议的安全性。这里分析的前提是假设攻击者不能获得除公开密钥之外的任何秘密信息，因为一旦秘密信息被泄露，则对数据的安全保护无从谈起。

5.1 关于物联网设备身份标识的可扩展性

前面定义的格式为XX-YY的物联网设备身份标识显然不具有全球唯一性，因为该架构的目标是企业产品的唯一性。事实上，在有些特殊情况下，也不能做到企业唯一性。

如果在同一个物联网系统中，遇到不同厂商的设备标识格式不一致的情况如何处理。首先在一个物联网系统中，有安全配置的物联网设备和没有安全配置的物联网设备应该由不同的服务器进行处理。即使使用同一个云计算平台，也要有不同的虚拟服务器进行处理。如果有另外厂家的设备也有安全配置，则不同厂家的设备安全服务需要使用不同的安全管理服务器。对一个物联网系统中的设备可以统一管理，但虚拟服务器作为安全服务的第一层处理，将使得不同厂商的设备，包括有安全机制的和没有安全机制的，可以最终集成到同一个处理平台。

如果这个格式被不同厂商分别采用，可能导致设备身份标识冲突问题。当发生在同一个物联网系统时，可以采取如下方法解决：每个厂商的设备使用单独的安全服务器（因为安全设置等因素，分开管理是有必要的），这些安全服务器的数据在汇总时，前面再灵活地增加一个服务器的身份标识符就可以解决身份标识冲突的问题。

如果身份标识是在物联网系统的具体使用环境中配置的，则不存在设备身份标识冲突问题，也不存在身份标识短缺问题。虽然在全球范围内身份标识的重复性会很严重，但这些复用的身份标识分布在不相关的物联网系统中，相互之间没有影响。

5.2 基于对称密钥的设备身份认证方案的安全性

下面分析当设备 A 向设备 B 发送数据 $ID_A\|ID_B\|Ek(ID_A, ID_B,k_s\|k_i)\|E_{k_s}(data)\|MAC(k_i,data)$ 时，是否有任何安全问题。因为通过公开信道传输，因此这一传输的数据容易被攻击者截获。

因为攻击者没有加密密钥 k，因此无法解密 $Ek(ID_A,ID_B,k_s\|k_i)$，因此得不到 k_s 和 k_i。假设攻击者猜测这些密钥是没意义的，因为密钥长度一般为128比特，只要有一个比特的不同，解密得到的结果将面目全非。没有 k_s，就不能解密 $E_{k_s}(data)$，因此数据机密性得到保障。没有 k_i，就不能产生 $MAC(k_i,data)$，包括伪造的 $data$，即使所使用的MAC算法容易找到随机碰撞。

攻击者假冒攻击也将不成功，任何假冒的数据，除了明文部分 $ID_A\|ID_B$ 可以伪造外，密文部分一旦解密不成功，伪造马上被识破。非法篡改攻击的效果是一样的。

5.3 基于公钥证书的设备身份认证方案的安全性

上述基于公钥证书的设备身份认证方案，攻击者都有能力得到所有通过公开信道传输的数据。但是，攻击者除了能验证 A 和 B 的公钥证书并得到他们的公钥外，对使用公钥加密的数据不能解密，因此攻击者不能得到 $k_s\|k_i$，从而不能得到数据 $data$，也不能破坏数据的完整性。

攻击者的假冒攻击仅限于第一步：可以将 A 的证书连同CA的身份标识发给 B，然后收到 B 返回的数据。这些数据对攻击者没有意义。如果实际中 B 需要确认 A 成功得到了数据，可以使用3次握手协议，让 A 返回确认。这时需要在数据中引入一个随机数，例如，在 $data$ 中添加一个随机数 R，然后 A 可以向 B 返回如下数据：

$A\rightarrow B: ID_A\|ID_B\|E_B(ID_A,ID_B,R)$

当 B 验证这一数据的正确性后，就知道3次握手协议已成功完成，完成了对 A 的身份认证。

6 结束语

本文针对物联网设备的特点，设计了一种可信安全架构，从初始信任为起点，通过信任的传递，可以建立不同设备之间的信任关系，从而可建立一条可信的数据安全传输通道。本文提出的是一个通用架构，通过适当配置和裁剪，可以适用于不同的物联网行业。进一步，本文给出了一种设备身份标识方法和设备身份认证方法，以验证可信架构的实际应用。●（责编 程斌）

参考文献：

[1] 赵阔，邢永恒．区块链技术驱动下的物联网安全研究综述[J]．信息网络安全，2017（5）：1-6.

[2]SCHNEIER B, Applied Cryptography -- Protocols, Algorithms, and Source Code in C[J]. Government Information Quarterly , 1995 , 13 (3) :336.

[3]Tempered-Networks.Identity-Defined Network (IDN) Architecture[EB/OL].http://www.temperednetworks.com/products,2017-4-15..

[4]Tempered-Networks.A New Approach to Safeguarding Your Industrial Control Systems and Assets[EB/OL]. http://www.temperednetworks.com/,2017-4-15.

[5]Symantec.Roots of Trust for the Internet of Things[EB/OL].http://www.symantec.com/rot/,2017-4-15.

[6] 廖竞学，陈福臻，程久军，等．面向社区物联网创新服务平台的隐私保护系统[J]．信息网络安全，2016（12）：60-67.