智能连接物联网边缘节点的安全性

白皮书

Eustace Asanghanwa和Ronald Ih
安全芯片和加密验证市场部

物联网（Internet of Things，IoT）反映了数十年来最大的技术浪潮之一。预计到2020年，联网设备的数量将达到500亿，物联网极有可能触及我们身边的一切。物联网将遍布工业、商业、医疗、汽车和其他应用领域，消费类产品的实现将有可能影响数十亿人。考虑到受影响的个人、机构和系统的范围，安全性作为任何物联网系统的关键组成部分已占有举足轻重的地位。现在人们普遍认为，任何认真的商业物联网企业都必须重视安全性，才能做大做强。

简介

在评估物联网网络的安全隐患时，开发人员已经瞄准最基本的元素——*边缘节点*。这些最基本的元素在物联网中也称为“物”，包括大量的传感器和执行器，它们为物联网提供数据并从云端或通过计算机、手机，车载系统、智能家电或其他平台等进行交互的用户处获取指令。

边缘节点通常是小型、低成本，但资源非常有限的智能设备。它们通常被误认为有一定的安全隐患。但是实际上，与它们通信的服务器及其所接入的网络都采用了完善的安全技术，因此边缘节点通常不会受到攻击；至少目前如此。

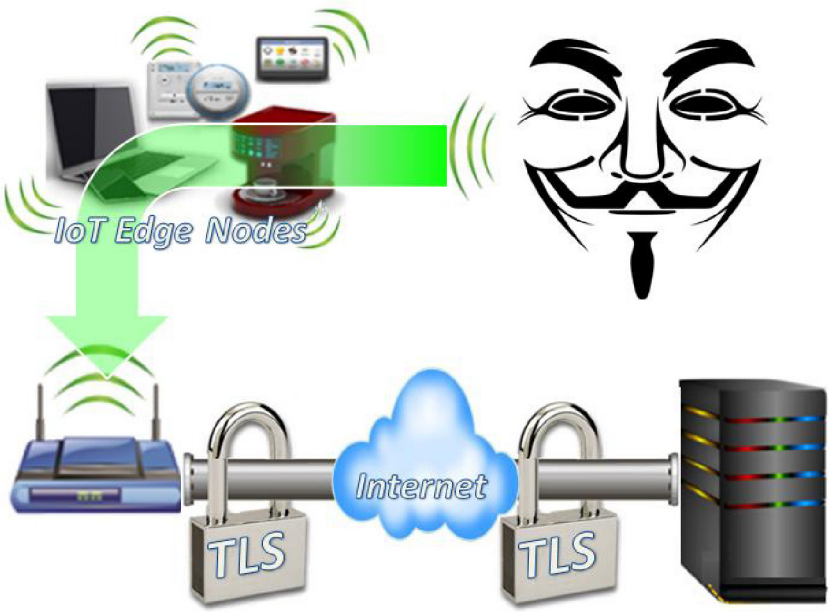
谈到保护此类系统，人们常常把“加密”和“安全”等同起来，事实上前者只是安全难题的一部分。要创造一个安全环境，首先要做的事情之一是要以可靠的方式发现并证明网络中所连入元素的*身份*。必须先确定*谁*要连接到网络，因为如果没有事先建立安全的身份验证机制，加密和传输层安全（如SSL/TLS）惟一能做的就是避免最初不应出现在网络上的人使用网络。

为了获得更优异的节点安全性能，我们以登录您的在线银行账户为例加以说明。首先要在您的计算机和银行的网站（这是一个https链接）之间建立一个安全（即经过加密和验证）的连接。但是，此安全链接不会对您进行身份验证——它仅在您的计算机与银行之间建立加密通信通道时验证您的计算机。此时，银行不清楚您是否为冒名顶替者。这就需要用到您的密码。您的密码就是您的密钥，因此理论上只有您和银行知道该密码。当您将其发送到银行后，立即会将其与您存储的密码进行比较。如果二者匹配，那么就银行而言，可以证明您是账户所有人。从这个例子中可以看出，网上银行安全分两层实现：

- 建立安全连接的传输层。
- 通过密码证明（验证）您身份的应用层。

同样，如果要认真对待物联网，物联网节点安全也必须分多层实现。

图1.　即使建立了安全通道，攻击者也可以通过节点访问



对于物联网节点，TLS也用于创建安全连接，例如与云建立安全连接。但是，为了真正实现安全性，物联网节点还必须实现应用层安全性。这意味着节点本身，而不仅仅是通信通道（即管道）应当进行身份验证。除了通道验证之外，还应在应用层建立加密和数据完整性，以保护流经管道的数据。

基于这一思想，物联网设备正为网络连接提供新的范例，因为这些设备通常非常小巧、简单，操作中极少或不涉及人员交互。通常会出现的问题将覆盖整个领域。一方面，出于对基础设施安全性担忧，人们会问：“您如何知道物联网设备值得信赖？您如何知道连接到网络的确实是物联网设备，而不是伪装成物联网节点的恶意设备？”这个问题也可通过几个实际问题来回答，例如“如果有人知道我的恒温器设置的温度，有什么大不了的？”“谁在乎是否有人知道我的灯开着？”“谁在乎是否有人知道我的计步器记录了多少步？”

如果您不仅要考虑设备上有哪些数据，还要考虑设备在网络上访问了哪些超出自身权限范围的数据，这个问题就变得更加实质化了。一些著名的数据泄露事件是通过骗取不安全网络节点的身份来达到目的的，恶意实体能够通过伪装成物联网节点进入公司网络。一旦它们进入网络内部，安全性就变得非常差，最终能够访问受害者的客户数据库并破坏工业流程。如果您认为除了访问云服务，还可能访问和控制节点本身的操作是一个隐患，则确认节点身份（身份验证）便成为一个至关重要的考虑因素。

尽管SSL/TLS等现有互联网安全技术可以很好地保护无损边缘节点和服务器之间的通信通道，但并非坚不可摧。对于不涉及传入网络的攻击，这些技术将毫无办法。应该很容易看出，如果攻击者控制边缘节点，SSL/TLS将不起作用。

严密安全性涉及三个基本要素，我们简称它为“CIA”：

- **保密性**——无论存储中的还是传输中的报文数据都仅对授权人员可见；
- **完整性**——发送的报文在向目标传输的过程中不应改变；
- **可靠性**——需确信报文的来源可靠。

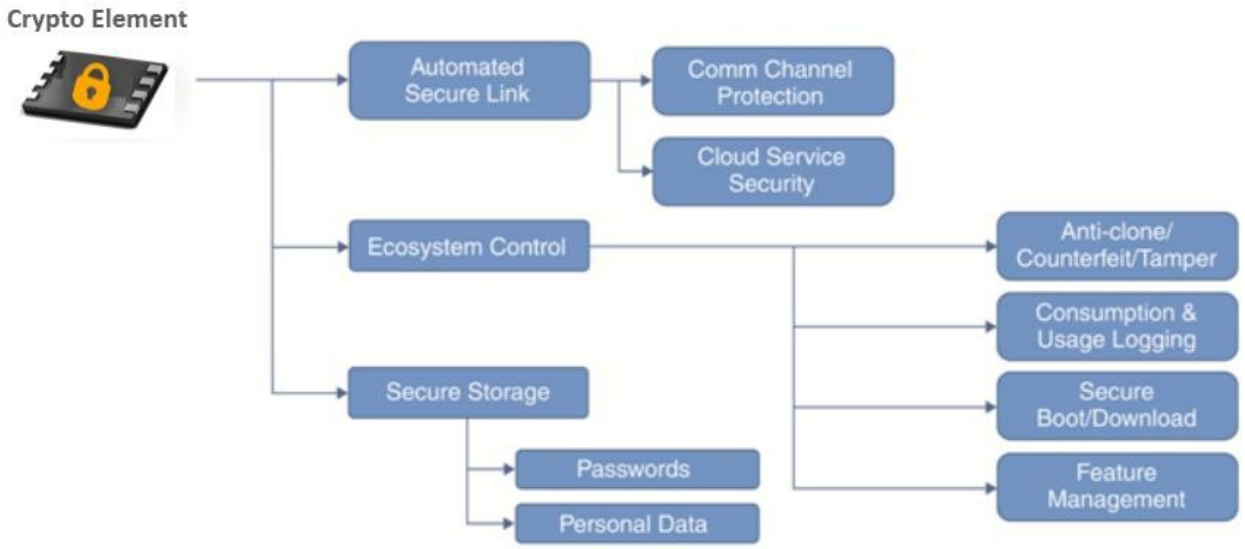
不同的技术催生了这些要素，但其中最常见的是使用机密密钥或私钥作为特有可验证识别标签的一部分。如何管理这些密钥（其存储和通信方式）决定了系统的安全性。

面临的挑战是实现边缘节点的安全性，同时保持在有限的可用计算、存储器和电源资源范围内并且不得超出预算。本文的目的是确定边缘节点的关键安全策略，说明中心角色在任何安全解决方案中的作用，并概述成功的密钥管理技术。

安全身份的众多优势

节点或设备被确认为“可信”后，即可充分实现各种其他优势。其中包括安全通信、生态系统控制和安全存储。

图2.　身份经验证的节点可实现各种优势



如果您能够验证某个物联网设备与其事先的声明相一致，则您可实现仅存在于可信安全环境中的优势。

边缘节点漏洞：哪些地方可能出错？

在讨论解决方案之前，我们需要更好地了解这些漏洞，以便提供有效的保护。可从两个方面入手：确定攻击者攻击节点的方式，并推断这种行为的后果。

攻击模式

有四种方法可以进入边缘节点：

- 通过网络
- 通过外部端口
- 通过接近攻击（也称为“边信道攻击”）
- 侵入设备

网络攻击

虽然网络是最受保护的端口，但这只能做到安全措施到位这一程度。完全不受保护的节点不能再企图通过“低调行事”而免于攻击。Shodan[1]等网络工具可在网络上抓取信息，识别出每个不受保护的节点。虽然TLS保护可以发挥很大的作用，但是由于边缘节点的TLS实施中存在缺陷、加密算法中的随机数使用率较低、未检测到某些恶意软件、确定的专家主动发起协议攻击，甚至由于协议本身存在不足（如最近确定的FREAK[2]攻击所述），仍然会存在难以捉摸的漏洞。

即使对于完全受保护的网络，攻击者也可能通过伪造固件更新，并使用攻击者编写的代码替换合法代码来攻击防御不佳的边缘节点。

端口攻击

网络端口（有线或无线）可能是小型骨干边缘节点上惟一可用的连接端口。但是，复杂的边缘节点可能具有用于插入不同传感器的模块端口，也可能具有用于配件、消耗品（如墨盒）或测试和调试设备的USB或其他端口（甚至无线端口）。上述每个端口都可用于访问边缘节点。攻击可以通过一个未使用的端口实现，也可以通过移除附件，然后更换为旨在实现攻击的某个其他硬件来实现。与网络端口不同，没有明确的标准来保护这些端口。

接近攻击

复杂的攻击也可以在未与边缘节点建立连接的情况下发生。通过窃听电源线或测量未受保护设备上的辐射或振动，可以提取有关密钥的信息。通过利用未记录的行为或错误（例如发出电涌），可将设备置于未记录的非安全状态。

物理攻击

最后，确定的攻击者可通过物理方式拆开边缘节点以试图探测内部电路（有电或无电），甚至去除和解密IC以学习嵌入式存储器的内容。

全面的安全功能必须能够防止上述所有攻击模式。

结果

当然，我们只锁定那些我们认为有价值的部分。对于攻击者而言，一个简单传感器节点的价值看似有限，但是一旦攻击成功，其后果可能是将整个网络以及连接到该网络的一切都置于危险之中。

侵入边缘节点时（即使是通过网络安全漏洞实现），攻击者可以访问安全功能应保护的所有机密信息——特别是需要实现安全功能的密钥。一旦获得密钥，便可破坏所有其他的安全保护——包括加密和消息验证。

一旦攻击者控制了边缘节点，他或她就可以改变网络上节点的行为，而不会警告网络发生了哪些问题。就其他服务器而言，边缘节点仍然是一个“可信”实体，因此机密信息会“自愿”泄露，而丝毫不会察觉“自己”落入了不法之手。

丢失这些机密信息可能会打击客户对其财务、医疗、身份和其他私密数据安全性的信心，还可能违反法规，其中涉及（在美国）FTC针对贸易问题、HIPAA/FDA针对医疗应用或SEC/FDIC针对金融交易的法规。对空中管制和道路交通系统、电网、飞机和汽车等一些网络的攻击也可能影响公共安全，而且即使不是完全不安全，工业运行也可能变得不可靠。

保护边缘节点的正确方法

我们已经了解了破坏边缘节点的一些方法。以下措施均涉及以某种方式进行密钥存储，将确保阻止此类攻击。虽然这从来不能保证100%安全，但这些措施提供了最好的保护，可确保攻击者无法确定关键的系统密钥。这些方法各自支持CIA的重要组成部分：

- **可靠性**——证明通过网络进入的访问者的身份。
- **可靠性**——对尝试连接到节点的任何配件进行身份验证。
- **保密性**——加密报文。
- **完整性**——向所有报文附加报文验证代码（Message Authentication Code，MAC），以证明没有人在过程中更改了报文。

另外，可以采取相应措施来防止“邻近”或“边信道”攻击。这些在本质上非常实用，可以在整个系统上实现，也可以在关键子系统上实现。

- 将密钥存储在受保护的硬件中，防止对密钥进行电气访问。
- 屏蔽系统，防止电磁辐射泄露密钥信息。
- 专门添加电路，扰乱尝试监视电源或其他信号的行为。其中可能包括虚拟计数器或具有某些随机性元素的电路，以加扰有用的信息。
- 加密存储中的密钥。即使密钥可能无法以电气方式访问，有目的性的攻击者也可能会尝试通过剥离设备各层来窥探嵌入闪存，并以此检索密钥。加密将使这种攻击无效。
- 除去无关的端口。例如，包含一个调试端口似乎很有用，但是如果可能永远不会用到该端口，那么没有它的话，您的系统将更加安全。

在整个制造过程中保护密钥也非常重要。我们需要一个深思熟虑的方案，该方案能够在密钥从生成到插入密钥存储器件的过程中始终保持机密状态。使用硬件安全模块（Hardware Security Module，HSM）以加密格式在受保护的硬件中存储密钥是一种卓越、可靠的方法。

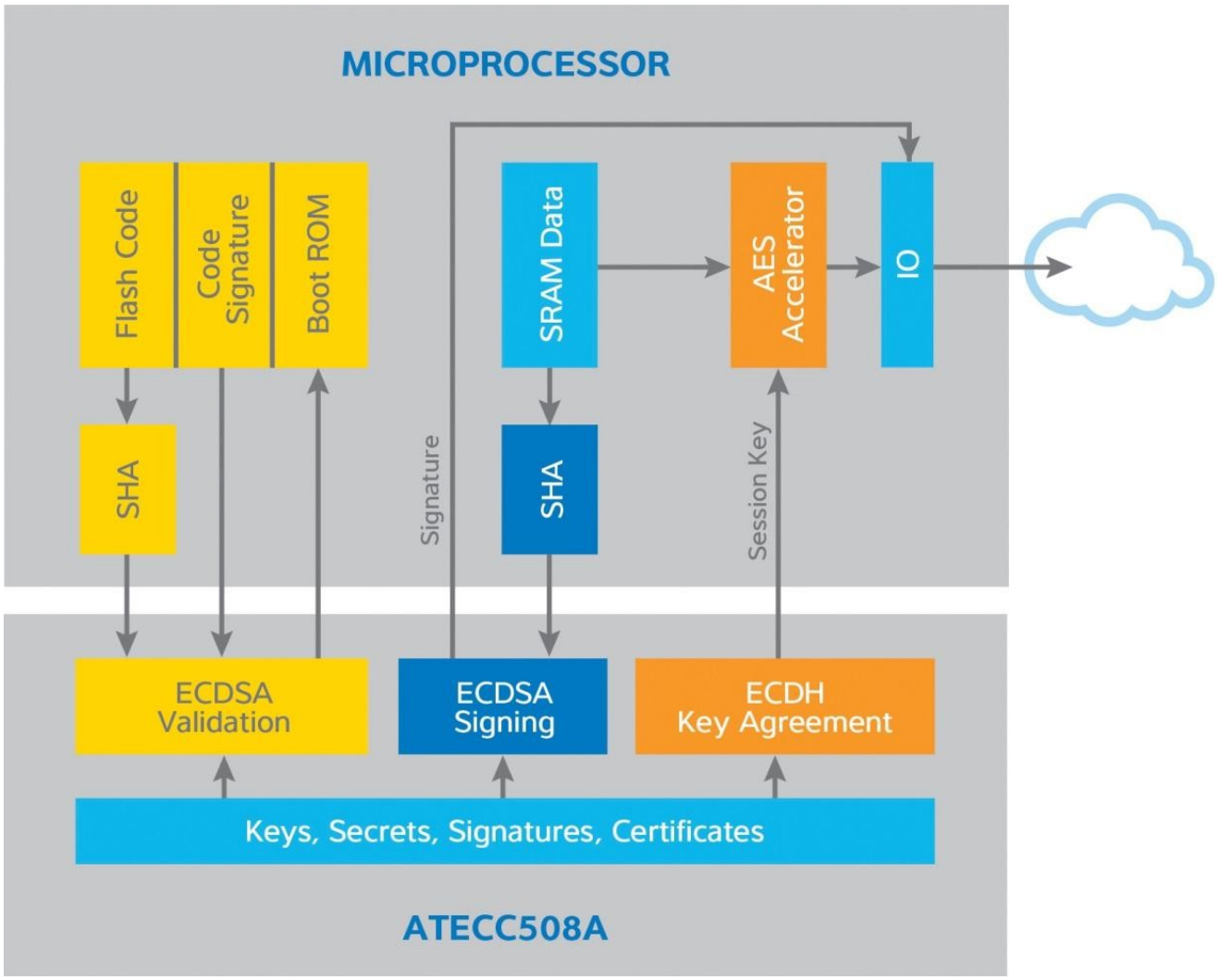
真正的密钥保护解决方案

Microchip以加密元器件[3]的形式提供一系列加密解决方案。由于这些器件充当硬件加密加速器，因此重点往往放在从主机处理器上卸载复杂数学任务的作用上。但还有一个更重要的方面：加密操作涉及到密钥，因此它们必须存储在非常隐蔽的受保护硬件中，以确保当您尝试在软件中或在不受保护的硬件中执行相同的计算时，密钥将永远不可见。

最新的ATECC508A CryptoAuthentication™加密元件是一种基于ECC的器件，其包含ECDH[4]密钥协议，内置有基于ECDSA[5]的非对称身份验证功能，并且具有基于受保护硬件的最强大安全密钥存储功能。

ATECC508A同时具有ECDSA和ECDH，非常适合用于保护物联网边缘节点。将微型ATECC508A添加到任何带有单片机的系统（包括物联网节点）中，都可轻松高效地将机密性、完整性和身份验证集成到该系统。

图3. ATECC508A可与任何微处理器配合使用，确保机密性、数据完整性和可靠性



ATECC508A可以极低成本与任何单片机一起添加。单线或I^2C连接可最大程度减少引脚数，封装选项可以小至2 mm × 3 mm。休眠电流小于150 nA时，功耗极低。

加密元件在内部执行算法，获取处理器提供的输入并返回计算结果（即签名、身份验证和会话密钥等），而不揭示计算的手段。高质量的真随机数生成器（True Random Number Generator，TRNG）有助于成功防止事务重新执行。内部序列号有助于确保密钥的惟一性，高容量计数器可用于跟踪身份验证。

物理和加密对策使得攻击者无法通过嗅探操作来学习密钥，或者通过探测设备来获得密钥。

- 整个设备采用蛇形金属模型进行屏蔽，防止内部信号发射被外界检测到，并可为打开封装观察和探测操作的人员带来视觉屏障。屏蔽层电气连接到电路的其余部分。如果屏蔽层遭到破坏，器件将无法再运行，从而防止有目的性的攻击者通过探测电路节点来了解机密信息。
- 调节器和计数器用于混淆电源和信号签名。
- 没有额外的内部焊盘可供测试和调试使用，因此打开封装后没有额外的接入点。

Microchip加密元器件的一个重要优势是通过使用简单的模块大幅简化生产配置，从而将机密信息和签名证书安全地插入到加密元器件中。也可由Microchip或Microchip授权分销商进行配置。

图4. ATECC508A生产配置

总结

安全性是物联网[6]成功上市的基本要求。边缘节点当前是确保物联网安全性的最薄弱环节，保护加密密钥会锁定边缘节点。通过受保护的硬件是实现锁定的最佳方式。这是确保这些密钥和其他机密信息远离窥探的惟一方法。CryptoAuthentication™系列加密元件提供绝对可靠的方法将密钥存储到受保护硬件中并对其进行管理，以实现多层安全。凭借Microchip丰富的单片机、无线设备和加密元件产品组合，可实现最先进的智能化和物联网安全连接等功能。

参考资料

1. “The Search Engine for the Internet of Things,” Shodan. 2015. www.shodan.io
2. “FREAK,” Wikipedia. September 5, 2015. http://en.wikipedia.org/wiki/FREAK.
3. “Smarter Security For Your Everything, Atmel Has You Covered,” Atmel. 2015 www.atmel.com/Microsite/security/overview.aspx.
4. www.semiwiki.com/forum/content/3966-ecdh-key-exchange-practical-magic.html. “ECDH Key Exchange is Practical Magic,” SemiWiki.com, Bill Boldt. October 28, 2014.
5. “The ABCs of ECDSA,” Atmel, William Boldt. August 6, 2014. http://blog.atmel.com/2014/08/06/the-abcs-of-ecdsa-part-1/.
6. “Is the Internet of Things Just a Toy?” Atmel, William Boldt. January 2, 2015. http://blog.atmel.com/2015/01/02/is-the-internet-of-things-just-a-toy/.

Microchip简介

Microchip Technology Inc.（纳斯达克股市代号：MCHP）是全球领先的整合单片机、混合信号、模拟器件和闪存专利解决方案的供应商，为全球数以千计的消费类产品提供低风险的产品开发、更低的系统总成本和更快的上市时间。Microchip总部位于美国亚利桑那州Chandler市，提供出色的技术支持、可靠的产品和卓越的质量。详情请访问公司网站www.microchip.com。

请注意以下有关Microchip 器件代码保护功能的要点：

- Microchip 的产品均达到 Microchip 数据手册中所述的技术指标。
- Microchip 确信：在正常使用的情况下， Microchip 系列产品是当今市场上同类产品中最安全的产品之一。
- 目前，仍存在着恶意、甚至是非法破坏代码保护功能的行为。就我们所知，所有这些行为都不是以 Microchip 数据手册中规定的操作规范来使用 Microchip 产品的。这样做的人极可能侵犯了知识产权。
- Microchip 愿与那些注重代码完整性的客户合作。
- Microchip 或任何其他半导体厂商均无法保证其代码的安全性。代码保护并不意味着我们保证产品是 “牢不可破”的。

代码保护功能处于持续发展中。Microchip 承诺将不断改进产品的代码保护功能。任何试图破坏 Microchip 代码保护功能的行为均可视为违反了《数字器件千年版权法案（Digital Millennium Copyright Act）》。如果这种行为导致他人在未经授权的情况下，能访问您的软件或其他受版权保护的成果，您有权依据该法案提起诉讼，从而制止这种行为。

Microchip 位于美国亚利桑那州 Chandler 和 Tempe 与位于俄勒冈州 Gresham的全球总部、设计和晶圆生产厂及位于美国加利福尼亚州和印度的设计中心均通过了 ISO/TS-16949:2009 认证。 Microchip 的 PIC® MCU 与 dsPIC® DSC、KEELOQ® 跳码器件、串行 EEPROM、单片机外设、非易失性存储器和模拟产品严格遵守公司的质量体系流程。此外，Microchip 在开发系统的设计和生产方面的质量体系也已通过了 ISO 9001:2000 认证。

QUALITY MANAGEMENT SYSTEM
CERTIFIED BY DNV
═ ISO/TS 16949 ═

10/25/17

全球销售及服务网点

美洲

公司总部 Corporate Office
2355 West Chandler Blvd.
Chandler, AZ 85224-6199
Tel: 1-480-792-7200
Fax: 1-480-792-7277
技 术 支 持 ：
http://www.microchip.com/support
网址：www.microchip.com

亚特兰大 Atlanta
Duluth, GA
Tel: 1-678-957-9614
Fax: 1-678-957-1455

奥斯汀 Austin, TX
Tel: 1-512-257-3370

波士顿 Boston
Westborough, MA
Tel: 1-774-760-0087
Fax: 1-774-760-0088

芝加哥 Chicago
Itasca, IL
Tel: 1-630-285-0071
Fax: 1-630-285-0075

达拉斯 Dallas
Addison, TX
Tel: 1-972-818-7423
Fax: 1-972-818-2924

底特律 Detroit
Novi, MI
Tel: 1-248-848-4000

休斯敦 Houston, TX
Tel: 1-281-894-5983

印第安纳波利斯 Indianapolis
Noblesville, IN
Tel: 1-317-773-8323
Fax: 1-317-773-5453
Tel: 1-317-536-2380

洛杉矶 Los Angeles
Mission Viejo, CA
Tel: 1-949-462-9523
Fax: 1-949-462-9608
Tel: 1-951-273-7800

罗利 Raleigh, NC
Tel: 1-919-844-7510

纽约 New York, NY
Tel: 1-631-435-6000

圣何塞 San Jose, CA
Tel: 1-408-735-9110
Tel: 1-408-436-4270

加拿大多伦多 Toronto
Tel: 1-905-695-1980
Fax: 1-905-695-2078

亚太地区

中国 - 北京
Tel: 86-10-8569-7000

中国 - 成都
Tel: 86-28-8665-5511

中国 - 重庆
Tel: 86-23-8980-9588

中国 - 东莞
Tel: 86-769-8702-9880

中国 - 广州
Tel: 86-20-8755-8029

中国 - 杭州
Tel: 86-571-8792-8115

中国 - 南京
Tel: 86-25-8473-2460

中国 - 青岛
Tel: 86-532-8502-7355

中国 - 上海
Tel: 86-21-3326-8000

中国 - 沈阳
Tel: 86-24-2334-2829

中国 - 深圳
Tel: 86-755-8864-2200

中国 - 苏州
Tel: 86-186-6233-1526

中国 - 武汉
Tel: 86-27-5980-5300

中国 - 西安
Tel: 86-29-8833-7252

中国 - 厦门
Tel: 86-592-238-8138

中国 - 香港特别行政区
Tel: 852-2943-5100

中国 - 珠海
Tel: 86-756-321-0040

台湾地区 - 高雄
Tel: 886-7-213-7830

台湾地区 - 台北
Tel: 886-2-2508-8600

台湾地区 - 新竹
Tel: 886-3-577-8366

亚太地区

澳大利亚 Australia - Sydney
Tel: 61-2-9868-6733

印度 India - Bangalore
Tel: 91-80-3090-4444

印度 India - New Delhi
Tel: 91-11-4160-8631

印度 India - Pune
Tel: 91-20-4121-0141

日本 Japan - Osaka
Tel: 81-6-6152-7160

日本 Japan - Tokyo
Tel: 81-3-6880-3770

韩国 Korea - Daegu
Tel: 82-53-744-4301

韩国 Korea - Seoul
Tel: 82-2-554-7200

马来西亚 Malaysia - Kuala Lumpur
Tel: 60-3-7651-7906

马来西亚 Malaysia - Penang
Tel: 60-4-227-8870

菲律宾Philippines - Manila
Tel: 63-2-634-9065

新加坡Singapore
Tel: 65-6334-8870

泰国 Thailand - Bangkok
Tel: 66-2-694-1351

越南 Vietnam - Ho Chi Minh
Tel: 84-28-5448-2100

欧洲

奥地利Austria - Wels
Tel: 43-7242-2244-39
Fax: 43-7242-2244-393

丹麦 Denmark - Copenhagen
Tel: 45-4450-2828
Fax: 45-4485-2829

芬兰 Finland - Espoo
Tel: 358-9-4520-820

法国 France - Paris
Tel: 33-1-69-53-63-20
Fax: 33-1-69-30-90-79

德国 Germany - Garching
Tel: 49-8931-9700

德国 Germany - Haan
Tel: 49-2129-3766400

德国 Germany - Heilbronn
Tel: 49-7131-67-3636

德国 Germany - Karlsruhe
Tel: 49-721-625370

德国 Germany - Munich
Tel: 49-89-627-144-0
Fax: 49-89-627-144-44

德国 Germany - Rosenheim
Tel: 49-8031-354-560

以色列 Israel - Ra'anana
Tel: 972-9-744-7705

意大利Italy - Milan
Tel: 39-0331-742611
Fax: 39-0331-466781

意大利Italy - Padova
Tel: 39-049-7625286

荷兰 Netherlands - Drunen
Tel: 31-416-690399
Fax: 31-416-690340

挪威 Norway - Trondheim
Tel: 47-7289-7561

波兰 Poland - Warsaw
Tel: 48-22-3325737

罗马尼亚 Romania - Bucharest
Tel: 40-21-407-87-50

西班牙Spain - Madrid
Tel: 34-91-708-08-90
Fax: 34-91-708-08-91

瑞典 Sweden - Gothenberg
Tel: 46-31-704-60-40

瑞典 Sweden - Stockholm
Tel: 46-8-5090-4654

英国 UK - Wokingham
Tel: 44-118-921-5800
Fax: 44-118-921-5820