边缘智能第4部分：边缘节点安全性

Ian Beavers和Erik MacLean
ADI公司

物联网系统攻击登上新闻头条，网络、边缘节点和网关不断暴露出安全漏洞。最近，Mirai僵尸网络通过登录到运行telnet服务器且未更改默认密码的设备，感染了愈250万物联网节点[1]。Mirai后来发展到能够引发服务器拒绝服务，导致全球很大一部分的互联网接入中断。Reaper僵尸网络通过利用软件漏洞并感染系统，攻击了愈一百万台物联网设备。一个接入互联网的鱼缸提供了侵入赌场网络的入口点，导致10 GB数据被盗。智能电视已被用于间谍和监视活动。

嵌入式传感器系统已开始联网并暴露于互联网之中。作为工业物联网(IIoT)的一部分，这些传感器没有像Web服务器那样在恶劣的环境中经历二十年的演进。因此，该行业正在目睹这些系统遭受20世纪90年代及更早期常见的很多攻击。工业物联网系统的生命周期通常要比传统计算系统的生命周期长得多。一些设备在部署后可能会持续运行数十年，而维护计划则不明。

服务器和PC非常复杂，足以支持设置安全措施，但工业物联网节点的功耗和处理能力通常很低，为设置安全措施而留下的功耗预算很小。由于涉及开发成本，安全在很大程度上是权衡的结果。虽然工业物联网的成本可能高于消费物联网，但其在可扩展性成本方面仍然面临挑战。如果忽视安全性，产品部署后将会产生隐藏的影响，这些成本最终也需要解决。

传感器和执行器使得工业物联网设备能与物理世界进行交互。网络攻击主要限于数据丢失，但通过工业物联网攻击，黑客比以往更容易侵入物理世界。现在的攻击有可能造成人身伤害。这在工业物联网中更为显著，因为故障可能导致价值数百万美元的工业流程被关闭或摧毁，或者引发危及生命的情况。

联网世界

工业物联网设备一般会连接到某种网络，常常是互联网。正是这种连接导致其最容易受到攻击。与流行病学相似，感染是通过与其他机器的接触而传播。攻击途径存在于系统与外界交互的地方。攻击者之所以能够与系统进行交互，完全是因为其能连接访问系统。需要问的第一个系统设计安全问题是：“设备是否真的需要连接到网络？”将其连接到网络会显著增加安全风险。

保护系统的最佳方式是阻止其连接到网络，或将其限制在封闭网络中。许多工业物联网设备联网的原因仅仅是因为它们能联网，而没有其他什么理由。让设备联网的利益是否超过与此相关的安全风险？另外，任何其他与联网系统进行交互的遗留系统也可能面临风险。

很多情况下，本来安全的网络和节点还必须与已有旧网络进行互操作，而这种老式网络本身的安全性可能要差很多。这就带来一个新问题：最弱的安全风险可能超出了工业物联网系统的影响范围。在这种情况下，工业物联网系统也需要防范来自系统内部的风险。

节点的安全考虑：[2]

- 保密性——防止数据泄露给未获授权的人，例如防范仿冒攻击
- 身份验证——在两台机器之间使用数字证书验证身份
- 安全引导——ROM引导加载程序存储器验证二级引导加载程序的真实性
- 安全固件更新——仅认可制造商提供的授权代码
- 授权——只有正品节点才能获得网络访问权限
- 完整性——保护数据不被更改
- 记录——正确记录数据、节点数和时间戳有助于防止对工业物联网网络的不受欢迎访问
- 安全通信——使用能驻留在低功耗节点上的加密协议
- 可用性——确保用户在需要的时候可以访问
- 认可——确保无法拒绝真实的通信请求
- 可靠性——即使在恶劣的电气环境中，接入也必须可靠

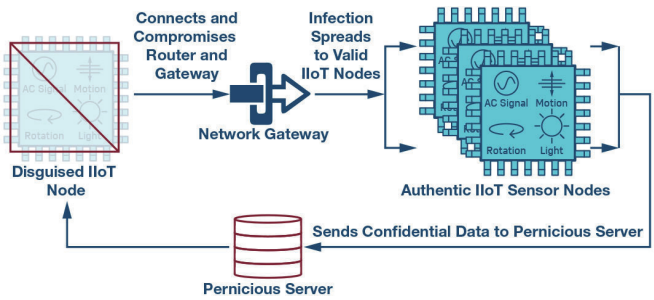

图1. 冒充已知节点欺骗网关的仿冒攻击。

隔离

系统彼此隔离可以减少攻击面并限制恶意软件的传播。将不需要网络连接的系统与暴露于网络的系统隔离开来。考虑建立一个单独的隔空或严格监控的网络，将它与其他高风险系统的网络分开。理想情况下，关键系统应当与外界完全隔离[3]。

联网汽车的信息娱乐系统可能会让车辆遭受许多前所未见的新攻击。主发动机控制单元(ECU)与信息娱乐系统毫无关系，不应通过信息娱乐系统与之交互。虽然车辆中通常有两条独立的CAN总线，以将最重要的系统与其他系统隔开，但它们仍以某种方式连接在一起，仍然有可能通过破坏一条总线而获取对另一条总线的控制权。如果这些网络之间完全隔离，那么类似风险将会从威胁生命的程度降低到远没有那么严重的程度。

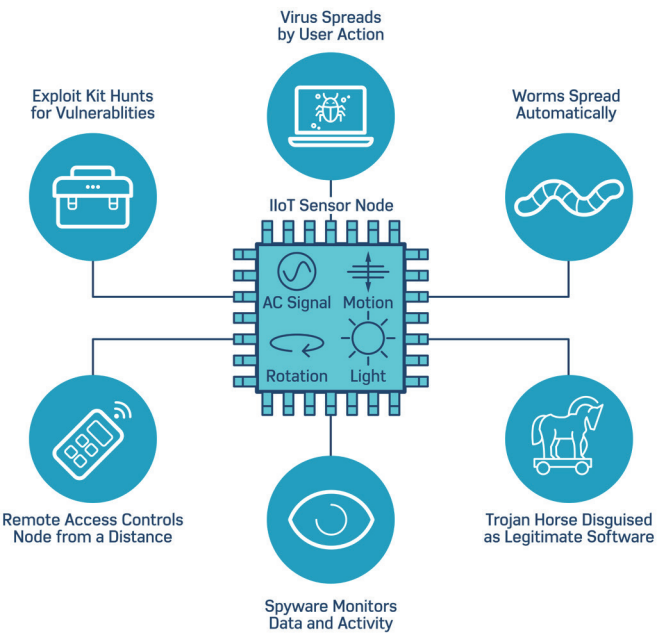

图2. 可能感染工业物联网系统的各类恶意软件。

转移至边缘

许多工业物联网系统连接到云服务器，云服务器收集并处理设备发送来的信息，同时也管理设备。随着设备数量大幅增加，云可能难以跟上步伐。很多系统正在将处理向外转移到工业物联网设备的边缘，以减少流向云的流量。

我们常常把数据视为资产。数据被挖掘和出售，以在大型数据集中发现隐藏模式。然而，收集到的大部分数据通常不是很有用，但它对攻击者可能有用。敏感数据为攻击者提供了目标，因而也是问题。对收集到的数据应进行过滤，只留下需要的部分，其余部分应尽快删除。这不仅能提高安全性，也能改善所收集数据的效用。识别潜在的敏感信息并禁止或限制其收集非常重要。

在边缘处理数据可以减少发送和暴露给云的数据量。发送数据的地点越多，保密就越困难。每个新节点都是可能泄露数据的风险源。攻击面呈指数式增长。

把敏感数据留在边缘以内可以限制专门针对机密数据的攻击面。如果将其限定在一个边缘节点中，则数据不太可能被盗。停车位占用传感器如果执行检测和图像处理，然后仅通过二进制信号报告有无车辆存在，那么就无需传输视频流，从而消除图像中包含的大量不必要数据。这会减轻接收服务器的负担，使其不能被恶意监视所利用。

与消费物联网系统类似，工业物联网系统也有必须维护的专有和机密信息：

- 专有算法
- 嵌入式固件
- 客户信息
- 财务信息
- 资产位置
- 设备使用模式
- 竞争情报
- 竞争情报

雾模型

一些工业物联网设备仍然缺乏边缘处理所需的功能和性能。另一种拓扑结构——雾模型——正在兴起，它是基于云和边缘系统的混合体。在雾模型中，边缘节点首先连接到网关，网关接收数据并进行一些处理，然后将数据发送到云端。许多工业物联网设备可能共用一个网关。网关不需要采用电池供电，处理功耗的预算可以高很多，而且成本高于受限制的工业物联网设备。

雾起源于扩展性问题，但在安全性方面也能发挥作用。网关设备可以帮助保护易受攻击的边缘节点，边缘节点受到的限制较多，可能无法自行保障安全性，但提供某种程度的保护比无任何保护会更好。网关可用来帮助管理其下的所有节点，而不是直接管理每个节点。在工业物联网中，雾模型还能作出应急响应，避免服务中断。例如，安全响应可以是与网关进行交互，而不是关闭关键任务生产线。

预配和部署

工业物联网最大的挑战之一是部署和管理大量设备。影响广泛的工业物联网系统非常难以建立和配置。工业物联网的生命周期很长，系统可能由一个团队部署，然后运行许多年，但由另一个团队提供支持。

工业物联网系统的默认身份验证机制很弱，往往不够安全。正如Mirai僵尸网络事件所展示的，大多数用户从不登录工业物联网设备以进行配置。他们甚至不知道应该配置设备。大多数工业物联网用户认为设备开箱即可使用。系统必须具有默认安全性。应当设定这样的系统期望：除了默认配置以外，用户可能永远不会配置设备。默认密码较弱是一个常见错误。

网络安全性

在工业物联网中，边缘受到的关注最多，但也不能忽视系统的云端或服务器端。测试常见服务器端漏洞（例如跨站点脚本、SQL注入和跨站点请求伪造），并检查API有无漏洞，以确保服务器上运行的软件及时得到修补。

跨网络传输的数据需要受到保护，否则可能会被恶意拦截和修改。使用TLS或SSH之类的安全加密协议来保护传输中的数据。最好为数据提供端到端保护。

工业物联网网络的边界可能很模糊。工业物联网传感器节点在空间上常常驻留在网络的外围。但是，通过它们以及一个固定网关，还可以轻松访问更大的工业网络[4]。对访问网络的这些设备进行释放身份验证，有助于防止流量遭到恶意第三方篡改。

保护网络数据流量要求使用安全通信协议。最佳实践应当是使用已知安全的标准协议。利用IEEE 802.1AE MACsec可以保障以太网LAN的安全。无线局域网更易于访问且无处不在，因而风险更高。WPA2为IEEE 802.11无线网络提供安全性。常常用在无线工业物联网解决方案中的低功率IEEE 802.15.4标准，提供了自己的一套安全协议。但是，这些是第2层协议，仅保护局域网上的流量。

为保护需要路由到局域网外部（例如通过互联网）的流量，需要提供端到端安全性的更高层协议。TLS常用于保护互联网流量并提供端到端安全性。尽管TLS使用TCP，而很多物联网设备利用UDP进行通信，但DTLS（数据报传输层安全性）可在UDP上工作。虽然物联网设备的功耗和存储器受限，但只需很少的工作就能为大多数受限应用实施TLS。对于限制更严格的设备，目前IETF正在开发一种新协议——受限应用协议(CoAP)。

端点安全性

虽然保护传输中的数据很重要且有必要，但攻击更多是针对端点。面向网络的接口需要强化以消除漏洞。保障工业物联网安全的一种方法是直接在传感器节点设备中设置防护。这就提供了第一个关键的安全层，设备不再依赖企业防火墙作为其唯一的保护。这对移动式企业设备和部署在远程位置的工业物联网传感器尤其重要。

工业物联网设备的安全解决方案必须防范各种各样的网络攻击。它必须确保设备固件没有被篡改，能够保护设备中存储的数据，能够保护入站和出站通信，并且必须能够检测和报告任何网络攻击企图[5]。这只有通过在设计的早期阶段纳入安全性才能实现。

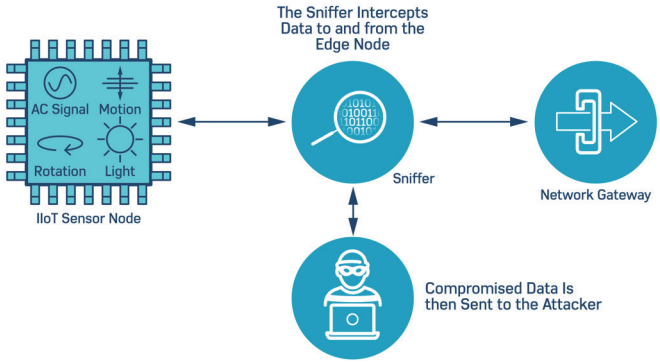

图3. 中间人攻击在节点和网关之间插入恶意接入点。

对于嵌入式设备，从不存在一个万能的安全解决方案。有些解决方案为原始设备制造商提供了一个通用框架。但是，完整安全框架必须考虑保护特定设备、网络和整个系统所需的核心能力，还必须根据具体要求灵活定制解决方案，同时确保包含关键安全功能。

高压灭菌器与自动机

在医学中，灭菌对于手术工具的重复使用和防止疾病传播至关重要。高压灭菌器是灭菌设备的典范。它用过热高压蒸汽快速杀菌。它能杀灭所有细菌，使仪器恢复到已知的良好状态。这样，外科医生就能利用手术刀进行手术，并在消毒后安全地重复使用手术刀。

系统受损之后将其恢复到已知良好状态的能力，比让它对所有攻击免疫更重要。弹性系统可以快速恢复并很有把握地恢复运作。

一旦系统受到感染，如何对其消毒？当一个系统受到感染时，病毒即以某种未知方式改变系统状态。远程攻击会控制处理器，向系统注入新的恶意代码。通常，固件会以某种方式被修改或替换为恶意软件，所以系统现在表现异常。一旦发生这种情况，就不能再信任处理器。

嵌入式系统的设计常常较为特别，难以可靠地从受损状态中恢复。通常，净化系统和验证系统是否干净的唯一办法是将所有非易失性存储器直接转储至外部读取器，然后对照原始固件进行验证，如果原始固件有改变，则用原始固件替换。大多数系统的设计不支持这种做法。

一种保护系统完整性的方法是用机械开关实现对非易失性存储器的物理写保护。当该开关设置为写保护时，存储器受到硬件的物理保护。存储器控制权转移到处理器域之外，要在物理上不接入设备的情况下将永久恶意软件远程安装到存储器中是不可能的。这样就把潜在攻击者名单从世界上任何拥有互联网连接的人缩减为只有那些可以长时间对设备进行物理访问的人。固件更新通常是很罕见的事情。当固件需要更新时，用户可以将开关设置为写使能以授权更新存储器，在更新完成后再次对设备设置写保护。

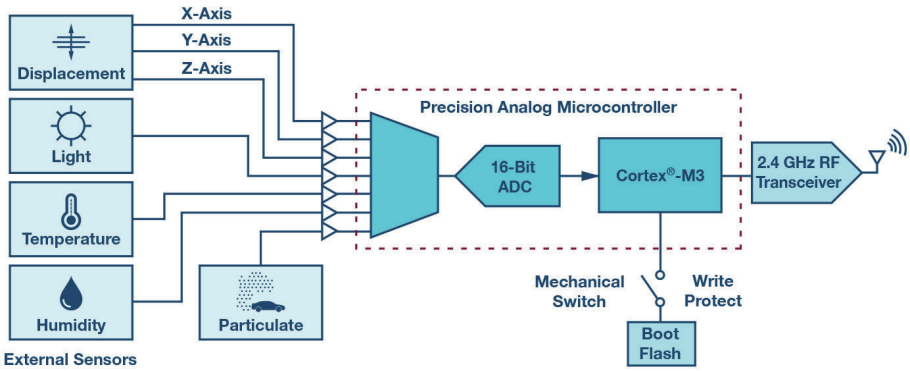

图4. 固件受物理写保护（执行更新时除外）是保护设备完整性的有效方法。

许多设备还使用非易失性存储器来存储写访问所需的数据。在高安全性系统中，可以使用单独的非易失性存储器芯片来存储数据（但不存储软件）。攻击者仍可以通过向该存储器写入恶意数据并利用软件漏洞来危害某些系统，因此应彻底分析和测试系统，无论该存储器存储什么数据，系统都不会受到影响。增加额外存储器芯片会增加成本，但有些闪存允许某些扇区设置写保护，而其他扇区仍能写入。

安全引导

安全引导可防止引导过程中将未经授权的软件加载到设备上。它是信任链的起点。安全引导从节点上只读非易失性存储器位置编程的第一阶段引导加载程序开始。此引导加载程序仅验证第二阶段引导加载程序的真实性。第二阶段引导加载程序往往比较复杂，可存储在可重新编程的闪存中。它重复此过程[6]，验证操作系统和加载的应用程序是否确实来自可信来源。

拥有安全引导和安全固件更新功能的工业物联网节点，可确保设备运行的是授权代码，而非篡改的或恶意代码，从而防止永久安装恶意软件或代码。设备要么仅运行未修改的代码，要么无法完成引导。

安全引导过程通常依靠数字签名来保护代码的真实性。代码映像由原始设备制造商在制造组装时利用原始设备制造商的私钥进行签名。然后，节点利用原始设备制造商的相应公钥验证固件映像的签名。

代码还可以利用对称加密的消息认证码(MAC)加以保护，但这需要将私钥存储在设备上，因而有风险。不过，使用MAC在计算上更容易。

安全引导虽然可以增强安全性，但对于最终用户来说，有时会太受限制，因为它能阻止用户更改设备上运行的软件或运行自己的软件。根据应用程序的不同，用户可能需要更多的灵活性和配置安全引导的能力，从而允许其信任自己的代码。

安全固件更新与安全引导相似，用于在升级过程中验证新代码映像已由原始设备制造商签名。如果下载的映像无效，则会丢弃文件并停止升级。只有有效的映像才被接受，并且随后保存到设备存储器中。

假设某个漏洞会在某个时候被发现。应该制定一个计划，以便在发现漏洞或漏洞被利用时知道如何处理。通常需要通过某种方法来将软件更新和修补程序安装到设备上以修复漏洞。更新过程同样需要正确实施，使它不至于被用作攻击途径——任何人都可以通过它将恶意软件安装到设备上。仅仅为了提供修补功能而让设备可通过网络加以访问，可能会引入比所要解决的问题更大的风险。

安全通信

大多数工程师将安全性视为通信协议，如SSL/TLS、SSH和IPsec等，原因是许多嵌入式设备增加了安全通信。然而，尽管这是安全威胁的一部分，但其他攻击途径提出了新的挑战。许多工业物联网传感器节点以低功耗配置运行，使用一些不能支持某些最佳选项（如TLS或IPsec）的较低功耗处理器。安全协议为构建安全设备提供了一个很好的出发点[7]。安全协议的设计目的是防范数据包嗅探、中间人攻击、重放攻击和未经授权与节点通信的企图。

小型工业物联网边缘传感器设备通常采用无线协议，如Zigbee、Bluetooth®低功耗(BLE)以及其他无线网状网络协议。这些协议具有一定的内置安全性，但是安全性相对较弱。许多可以利用漏洞的方法已经公开，老练的黑客已经熟知。小型工业物联网设备通常使用成本非常低、功耗较低且不支持TLS或IPSec的处理器。对于小型边缘设备，可以使用DTLS（基于UDP的TLS）来实现安全通信。

物理安全性

物理攻击针对的是工业物联网系统的实际边缘硬件节点或网关，可以包括针对前端传感器的破坏。这些攻击常常需要从物理上接触系统，但也可能只是仅仅限制工业物联网硬件效能的操作。攻击者可以篡改节点，以控制工业物联网环境中的传感器或其他设备。然后，他们可以从源头提取机密数据和嵌入固件代码。利用恶意节点注入策略，攻击者可以将恶意节点部署在工业物联网网络的合法节点之间[8]。

为了应对此类攻击，在设计阶段可以提前做一些硬件考虑。在使用带引脚的器件对信号进行物理探测的时候在设计中应尽量、减少裸露的铜过孔或未使用的连接器。应当移除可为潜在黑客提供额外信息的详细元器件丝印，除非认为它是设计绝对需要的。虽然可能会增加系统复杂性，但工业保形涂层不仅可以减轻自然力对硬件的影响，还能增加额外的步骤来防止对PCB上的电子元件进行直接探测。

器件内部的任何嵌入式非易失性存储器内容都应该加密并设置写保护。微控制器和DSP器件之间的接口应该位于PCB的内层走线。即便嵌入式存储器的内容被获取，数据的加密和验证机制也会使其变得毫无意义。

制造商常常使用调试或测试端口。这些端口通常是串行或JTAG，可用来访问并控制大部分系统。在生产中，应确保这些端口在功能上被禁用或受到保护，因为仅仅不配备调试接头是不够的，顽固分子可以自行配备或焊接到引脚上。如果需要在生产设备中启用这些接口，使用之前应进行身份验证。可以用密码加以保护，但务必要让用户能够设置强密码。

随机数生成

加密功能通常需要某种随机数发生器(RNG)。随机数可能需要无法预测的密钥生成，或者要求不得重复。由于缺乏资源和熵，在受约束的嵌入式系统中生成随机数通常是一个巨大挑战。

很多嵌入式系统存在熵过少的问题。这可能导致灾难性的中断，中国台湾的居民身份智能卡就发生过严重问题。研究人员发现：由于熵不足，许多身份证件是从相同数字产生相关的密钥。因此，尽管使用了强大的RNG，密钥仍然能被破解[9]。类似地，研究人员在2012年发现公钥服务器上0.38%的RSA密钥共享弱随机数生成，能够被破解[10]。

验证RNG的强度非常困难，几乎不可能。过去的RNG设计相当特别，人们对其了解不多。但近年来，鲁棒密码随机数发生器的设计和形式分析取得了重大进展。

现代鲁棒的RNG设计往往有三级[8]。一个熵源提供原始熵，一个熵提取器让熵均匀分布，还有一个扩展级，用来扩展可用的少量熵。

第一级是熵源。它可以是某种物理噪声源，例如时钟抖动或热噪声。某些处理器（例如ADI Blackfin® DSP）为硬件提供可用于生成熵的随机数生成器。

密码的随机数字需要有均匀的统计分布。所有熵源都有一定的偏差，将其用于加密应用之前需要消除这种偏差。这是通过熵提取器来完成的，它利用高熵的非均匀分布的输入，生成高熵的均匀分布的输出。代价是会有一定的熵损失，因为熵提取器需要的熵输入大于其能提供的输出。结果，需要从熵源中收集更多的比特，并将其提炼成一个小的高熵数字，该数字可用来为密码安全的伪随机数发生器提供种子[11,12]。

利用错误

几乎所有工业物联网节点都要使用某种形式的嵌入式固件或算法。从功能上看，这种固件在履行要求方面完全正常，没有明显问题。但是，所有软件都有一定程度的缺陷或错误，这可能导致一些异常操作，从而引发安全问题。例如，99.99%无错误固件很少会发生运行问题。但是，剩下的小小的0.01%错误可能会被入侵者利用，迫使节点在该特定工作模式下运行时100%失败。软件缺陷来源于复杂性，而任何有用的系统都需要一定的复杂性。基本上所有系统都存在软件缺陷和漏洞。

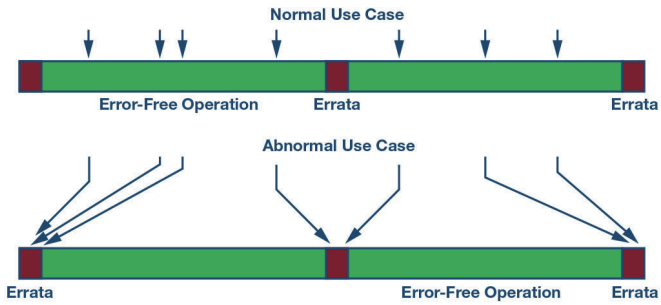

图5. 利用小错误迫使系统在100%的时间内都无法正常运行。

安全性设计

系统设计的安全性必须从一开始就考虑。它应该是设计过程的一部分，而不是在项目结束时附加的东西。安全性的关键不是添加安全功能，而是管理风险。对于任何工业物联网系统开发，安全设计方法都很重要。

现有的安全设计实践仍然适用。使用威胁建模来识别风险，并选择合适的风险缓解策略。识别系统的入口点，从而找到系统中风险最高的区域。大多数攻击途径都是通过外部接口，因此应检查设计方案有无安全漏洞。仔细处理未知数据并验证所有输入，验证和安全性不应局限于入口点。纵深防御很重要，这样在外层遭到破坏时，仍有安全层可供御敌。

许多处理器提供不同级别的权限。ARM®有Trustzone，ADI Blackfin DSP提供用户级执行模式和特权执行模式。尽可能以最低级别的权限执行尽可能多的代码，以将最重要的代码保留在特权模式下执行。工业物联网设备的安全要求必须考虑安全失效的代价、攻击的可能性、主要攻击途径以及实施安全解决方案的成本。

结语

上述许多建议彼此冲突，且与系统的其他设计目标相抵触。保障安全性通常涉及某种权衡，例如成本、功能或可用性。一些权衡非常有效且代价不高，而另一些则是高成本且影响小。安全性需要与设计的其他需求相平衡，并且应通过安全设计流程在特定应用的基础上确定。

为了帮助保护工业物联网，ADI公司有多种处理器可提供基于硬件的安全增强功能，有助于突破边缘节点的可能边界。ADF7023 RF低功耗收发器利用ISM频段和许多不同的调制方案提供内部AES加密。

ADuCM3029内部的嵌入式收发器提供AES和SHA-256硬件加速以及一个真正的随机数发生器，还有多奇偶校验保护的SRAM。ADSP-BF70X Blackfin系列数字信号处理器提供嵌入式一次性可编程存储器，用于安全密钥存储和快速安全引导，为系统在遭到破坏后返回已知良好状态提供有力保证。

借助基于硬件的只递增计数器，Blackfin DSP中的回滚保护允许在出现问题更新固件以修复漏洞。这与密钥存储的不变性相结合，能够实现强大而有弹性的边缘节点。此外，Blackfin DSP提供加密硬件加速器、基于硬件的真随机数生成器、特权和非特权代码执行的分离、MMU以及限制多个DMA通道访问的能力，从而以低成本实现并行、高功效、安全的DSP。

参考文献

[1] Mirai僵尸网络泄露源代码。

[2] Ross Yu。“全性和可靠性是工业物联网无线网络的关键”。ADI公司，2017年。

[3] Patrick Nelson。“组织机构必须将物联网与常规IT隔离开来——Telco”。*Network World*，2016年3月。

[4] Brian Girardi “端点安全性和物联网”。*CSO*，2017年。

[5] Tristan O'Gorman。“物联网安全风险入门”。*Security Intelligence*，2017年2月。

[6] Abhijeet Rane。“物联网安全性始于安全引导”。*Embedded Computing Design*，2017年1月。

[7] Amitrajan Gantait、Ayan Mukherjee和Joy Parta。“保护物联网设备和网关”。IBM，2016年5月。

[8] Boaz Barak和Shai Halevi。“伪随机数生成的模型和架构及其/dev/random应用”。第12届ACM计算机和通信安全会议论文集，2005年11月。

[9] Chen-Mou Chang、Daniel J. Bernstein、Chang、Li-Ping Chou、Nadia Heninger、Nicko van Sormersen、Tanja Lange和Yun-An Chang。“分解认证智能卡中的RSA密钥：野生铜匠”。*Springer*，2013年。

[10] Arjen K. Lenstra、Christopher Wachter、James P. Hughes、Joppe W. Bos、Maxine Augier和Thorsten Kliengun。“Ron是错的。Whit是对的”。*Cryptology ePrint Archive*，报告2012/064，2012年。

[11] Boaz Barak、Eran Tromer和Ronen Shaltiel。“在不断变化的环境中保护真随机数发生器”。*Springer*，2003年。

[12] Boaz Barak、François-Xavier Standaert、Hugo Krawczyk、Krzysztof Pietrzak、Olivier Pereira、Yevgeniy Dodis和Yu Yu。“剩余哈希引理再探讨”。第31届密码学进展年会，2011年8月。

作者简介

Ian Beavers是ADI公司自动化、能源和传感器部（美国北卡罗来纳州格林斯博罗）的产品工程经理。他于1999年加入公司。Ian拥有超过19年的半导体行业工作经验。Ian于美国北卡罗来纳州立大学获得电气工程学士学位并于格林斯博罗分校获得工商管理硕士学位。联系方式：*ian.beavers@analog.com*。

Erik MacLean是ADI公司可信安全解决方案部门（位于美国坦帕市）的硬件工程师。他在嵌入式硬件设计和安全方面拥有6年的经验。他于2009年获得佛罗里达大学电气工程学士学位，2011年获得南佛罗里达大学电气工程硕士学位。联系方式：*erik.maclean@analog.com*。

在线支持社区

访问ADI在线支持社区，与ADI技术专家互动。提出您的棘手设计问题、浏览常见问题解答，或参与讨论。

EngineerZone™ ANALOG DEVICES 中文技术论坛

请访问*ezchina.analog.com*

全球总部
One Technology Way
P.O. Box 9106, Norwood, MA
02062-9106 U.S.A.
Tel: (1 781) 329 4700
Fax: (1 781) 461 3113

大中华区总部
上海市浦东新区张江高科技园区
祖冲之路 2290 号展想广场 5 楼
邮编 : 201203
电话 : (86 21) 2320 8000
传真 : (86 21) 2320 8222

深圳分公司
深圳市福田中心区
益田路与福华三路交汇处
深圳国际商会中心
4205-4210 室
邮编 : 518048
电话 : (86 755) 8202 3200
传真 : (86 755) 8202 3222

北京分公司
北京市海淀区西小口路 66 号
中关村东升科技园
B-6 号楼 A 座一层
邮编 : 100191
电话 : (86 10) 5987 1000
传真 : (86 10) 6298 3574

武汉分公司
湖北省武汉市东湖高新区
珞瑜路 889 号光谷国际广场
写字楼 B 座 2403-2405 室
邮编 : 430073
电话 : (86 27) 8715 9968
传真 : (86 27) 8715 9931

TA16680sc-0-3/18

analog.com/cn

ANALOG DEVICES
超越一切可能™