技术文章

无线接入控制安全性的发展

作者：Vivien Delport（应用总监）与 Cristian Toma（应用工程师）
Microchip Technology Inc. 安防、单片机与技术开发部

摘要

随着人们对无线部署安全性需求的增加，要求进行安全认证的无线系统还需要更高级别的安全性。无论应用是安防系统（例如，键盘、无线感测器或访问控制）、汽车的遥控无钥门禁（RKE）系统还是身份验证系统，如今的无线系统都变得越来越复杂。由于是消费品，必须保持尽可能低的成本，同时还应提供足够的安全级别。这需要在成本和性能之间权衡。尽管如此，好的设计仍可利用相对有限的资源达到良好的效果。

无线领域的安全级别与正在传输的资讯的重要性密切相关。例如，无线门铃或电脑滑鼠可能无任何安全问题，而汽车的无钥门禁应用却需要高级别的安全性。与处理能力相对有限的消费品安防系统不同，台式电脑具有更强的处理能力且价格在日益下降。因此，安全级别有限的无线安防系统更易受外部攻击，通常包括代码窃取和暴力破解攻击等。

本文将介绍无线安防系统的最新发展以及对抗外部攻击的措施。同时，本文还将介绍如何确保总成本最低。

增强的系统安全性

为什么无线应用需要安全性？无线应用使用射频（RF）波将命令从发送方发送到接收方设备。然而，该RF消息是在公共媒介中发送的，这意味着在发送方侦听范围内具有类似接收方设备的任何人都将可接收到完全相同的消息。例如，如果将锁定和解锁消息简单地发送给车辆报警系统，那么在侦听范围内的任何人均可轻松确定这些命令。然后，他们只需重发这些消息即可非法进入车辆。此类攻击通常称为“代码窃取”攻击方法。

为了帮助保护RF消息中包含的资讯，首先使用加密演算法扰乱消息。加密是使用演算法（密码）转换资讯（明文）的过程，使此资讯对除了具有特殊资讯（如加密密钥和/或加密演算法）之外的其他人不可读（密文）。只有掌握完全相同的加密演算法和加密密钥的人才能成功破解或解读密文消息。遗憾的是，仅扰乱消息还远远不够。因为即使消息无法被破解，不法份子仍可利用它来进入车辆。为了防止这种情况发生，还必须在每次发送时使加密消息发生改变。此消息变化模式有时还称为“跳码”或“滚动码”模式，这可防止复用先前发送的消息。Microchip Technology（美国微芯科技公司）拥有专利的KEELOQ®跳码安全解决方案即为众所周知的跳码模式的一个例子。KEELOQ跳码技术采用强大的加密演算法来实现始终变化的消息。

推动因素：为什么需要更强的安全演算法？

那么，为什么不断需要更强的安全演算法？学术界、加密技术领域的专家和意图破解演算法而非法使用的个人都在不断审视安全演算法以找到其弱点。其中一种方法是尝试所有可能的位元组合以确定密码或加密密钥。该方法称为“暴力破解攻击”。可能的组合越多，猜到正确数值的时间越长。随着电脑的计算处理能力和速度的提高，可在较短时间段内同时进行多个暴力破解攻击计算。十年前需要几个月才能完成的攻击使用现在的技术只需几天。获取密码和密钥使骇客能够看到加密消息中存储的实际命令资讯。在破解或解读加密消息后，骇客能很容易迅速确定各种控制消息之间的哪些资讯变化可使其作为有效命令被接收方接受和理解。

安全演算法：专有和公共安防系统

目前有多种安全演算法供选择，分为专有和公共。这就意味着演算法所采用的实际计算方式可以是公众知悉的也可以不是。在安防领域中，有两种学派分别代表专有和公共演算法。只要安全演算法通过非常熟悉当前各种攻击方法的主题专家彻底审查，选择哪个演算法并不重要。然而，仍有许多人认为公共安全演算法通常更好，因为它已经过更多攻击者审查，而这些攻击者可能有时会使用全新和创新的密码分析方法来破解演算法。

通常，破解演算法意味着减小猜到称为“密钥”的密码所需的组合数。例如，资料加密标准（DES）使用56位的加密密钥并转化为2^56或72,056,594,037,927,936种可能的组合，通过破解演算法曾经将可能的组合数减少至2^39或549,755,813,888种。通过目前的现场可编程闸阵列（FPGA）或个人电脑处理能力，可在几天内轻易计算出密钥。

由此得出一般规则，即安全演算法的加密密钥中的位元数越多，演算法越强。例如，高级加密标准（AES）演算法可使用128或256位密钥，后者被视为两者中较强的解决方案。然而，在仅依懒于加密密钥的位数或被加密的资料块的大小时必须小心，因为有许多密码分析攻击方法可检测出密钥实际与原始演算法计算混合的方式中的任何弱点。行业专家和骇客等通过使用今天在许多安全应用中确认为标准的各种攻击方法，已仔细审查了AES演算法。

选择安全解决方案

那么，为什么不干脆选择目前最强的演算法（例如，使用256位加密密钥的AES），用于您的下一款无线系统设计呢？遗憾的是，安全不是免费的，演算法越强，计算越复杂，支援该演算法所需的软体记忆体需求越大，通常就需要更昂贵的单片机。所有这些增加了安全解决方案的总成本及其复杂性。我们还需要记住在保持解决方案对于实际购买该系统的最终消费者简单易用的同时，仍要提供足够好的保护级别，以防止非法使用。较强的演算法通常需要传输较长的加密消息。在空中发送无线包时，会延长延迟时间及增加功耗，因为无线包要花费更多的时间来发送。发送较长的资料并不总是件好事，这可能会对产品的现场验收造成负面影响。

高级单片机更实惠

当今的嵌入式单片机不仅集成度更高，性能更佳，而且成本更低。这些高性价比的单片机能够支持在十年前只能通过专用积体电路（ASIC）实现的解决方案。这些单片机支援更高级的安全加密演算法，并且需要的开发时间也很短。如今的单片机还包含片上振荡器和其他集成功能部件，这有助于减少元件数并因此降低了无线解决方案的总成本。单片机使无线产品的开发更加容易，同时通过使用采用高阶语言（如C语言）编写的支援大部分加密演算法的软体模组提供高级别安全性。这显着简化了安防无线应用的开发工作，稍作修改即可适应瞬息万变的消费者市场需求。

低功耗设计

嵌入式单片机行业的另一个有助于无线设计的重要设计改进重点关注于降低功耗。例如，降低单片机在执行应用程式码或处于不活动低功耗休眠状态所需的功耗量。以采用超低功耗（XLP）技术的Microchip PIC®单片机（MCU）为例，其休眠电流可低至20 nA。这些新的低功耗器件可帮助系统级设计人员创建更小、更紧凑的可携式手持设备，从而可使用较小的电池运行较长的时间。

集成RF解决方案

对集成RF发送器、接收器或收发器的普遍青睐是如今推动产品短时间上市的显着行业进步。这些集成的器件将所需的大部分RF电路集成到单个硅器件中，降低了RF设计的复杂性。这些新一代RF积体电路（IC）器件只需要一些基本的外部元件，就能完全实现高性能RF无线应用。此外，这些器件通常具有一个SPI介面，可方便连接单片机，由单片机采用合适的设定值对无线RF进行配置并发送/接收实际解调的资料包。

影响无线解决方案的设计因素

影响无线解决方案的最终设计的因素有许多。下面列出了一些在设计低成本移动无线产品时必须评估和了解的因素。

设计复杂性

结合所有这些技术——高级嵌入式单片机、集成RF器件和高级安全加密演算法，设计人员可以轻松地开发一个完整的安全无线解决方案，并提供合适的安全级别。采用高集成度单片机和集成RF IC器件也有助于显着降低当今无线解决方案的成本和复杂性，这是因为集成简化了工艺并减少了印刷电路板上所需的元件数。

解决方案的成本

有时，选择合适的安全级别可能是一项艰巨的任务。然而更复杂的是，所选的安全级别并不总是可用的最强解决方案。如上文所述，设计人员必须充分了解他们试图保护的内容，然后决定使用哪个安全解决方案，这必将在多方面影响到成本。基于单片机的解决方案比基于ASIC的解决方案更具灵活性。如果需要进行一些更改，设计人员只需提供在单片机上运行的软体即可实现。其灵活性还体现在，采用相同的硬体设计仅需对代码做一些微小的更改，即可支援多个国家或地区的法规。通过简单地更改软体，设计人员可针对其他区域分别配置无线RF晶片。通过使用其他加密库，设计人员可轻松地为最终用户提供其他安全选项。

易于使用

设计安全解决方案最容易犯的错误是使设计过于复杂。设计一个安全解决方案的最好方式是保持其简单和用户友好特性。如果过于复杂或麻烦，对于消费者来说，这可能会有负面影响。设计无线系统的基本宗旨是要让用户感觉到比直接靠近受控应用进行操作更方便。如果掏出口袋中的钥匙来开车门比直接按钥匙扣上的按钮更方便，那么就完全偏离了设计目标。

保持安全系统简单的另一个充足的理由是：越复杂，越难测试视为薄弱点的所有可能组合。做的测试越少，您未完全确定系统内所有薄弱环节的机率就越高。遗憾的是，即使您使用的是目前最强的安全演算法，安全强度也仅与系统中最薄弱的环节一样。例如，在车辆报警系统中，如果仅使用很强的安全演算法加密锁定和解锁消息，但不在每次传输时更改消息，或者没有更改足够多的资讯，那么小偷可轻松捕捉到这些消息并重放。在这种情况下，他们仍能进入车辆，而无需知道您所使用的演算法或密钥。

物理尺寸

通常，RKE单元由一个小的CR2032纽扣电池供电。这些纽扣电池仅具有大约200 – 240 mAh的电量。通常，希望该器件在适度的日常使用情况下，可持续使用三至五年。因此，用于此类设计的器件（如XLP PIC®单片机）非常关键。此外，在设计时，对移动部件（且许多时候甚至在是主控部件）的物理尺寸有所限制。例如，发射器电路必须能放入一个已预定形状和外形的小钥匙扣中。鉴于这些电路频率相对较低，将天线放入如此小的空间可能是项设计挑战。

选择RF频段、资料调制方案和性能

使用的频率主要取决于应用和法规。例如，在美国，工业、科学和医学（ISM）频段为315 MHz和915 MHz。在欧洲，ISM频段为433 MHz和868 MHz。还存在与无线链路所能覆盖距离相关的要求。典型的RKE应用要求至少20米，且有时有最大距离要求。例如，在日本，由于较严格的RF法规，最大覆盖范围仅为5米（这千真万确）。最常见的理解错误之一是会提出“发送器可提供的最大范围是多少？”这一问题。当评估覆盖范围时，设计人员应牢记发送器和接收器同样重要。良好的天线设计可显着提高从弱发送器接收的能力。

RF调制方案和资料速率对无线链路的可靠性也有很大的影响。调频无线链路通常较少产生杂讯。但是，这种技术会增加成本。更高级的无线链路还会增加移动部件及固定部件（即接收器）的成本。然而，随着如今集成RF发送器和接收器的发展，这些器件往往与低成本混合RF模组位于同一价格区间。一些最新的RF器件可同时充当发送器和接收器，使双向通信成为可能。

选择单片机

设计人员在选择单片机时，应从片上程式存储和资料存储容量考虑，选择最适合应用的单片机。板上带有加密模组，固然会有帮助，但这一般不免费，因此采用软体实现方案在有些时候可能是更好的选择。如果加密演算法可用软体轻松实现，那么这是一个更可取的解决方案，因为它为设计人员提供更广泛的单片机挑选范围。此外，接收器通常会被融入较大的应用中，例如汽车防盗器或车库门遥控开关。有时，甚至发送器本身就是一个较大应用电路的组成部分，如图形键盘介面。单片机必须提供足够的记忆体来容纳主应用程式和安全无线链路软体。

安全是个系统问题

读者应牢记，RF解决方案始终具有两个要素——移动/发送器部分和基点/接收器部分。在设计安全系统时，需要从安全角度来充分审查这两个部分。包括为作业选择合适的单片机和了解硬体设计的弱点。再次强调，安全系统的强度仅与其最薄弱的环节一样。

什么决定系统的安全？

许多因素会影响确定一个安全无线设计的最佳解决方案。系统设计人员应将所有这些因素一起评估以确定最佳解决方案，了解各种设计权衡以及每个设计涉及的成本。

安全演算法

选择安全演算法可能是个困难的决定，特别是在设计人员不知道存在的所有攻击方法时。攻击方法有明文、边通道、差分加密分析、中间相会攻击和滑动攻击等多种。最好是谘询行业专家或评估一些业界普遍接受的演算法，如AES加密（已被广泛接受，包括美国政府）。

密钥管理

决定实施一个安全解决方案时，要牢记的最重要因素之一是，如何生成、交换、存储、保护、使用和更换整个系统中的安全加密密钥以破解或解读加密消息。当谈到安全问题时，最重要的一点是要记住Kerckhoff原理，该原理陈述了“安全系统不应依赖于安全演算法的保密，而依赖于密钥的保密”。回顾一下破解任何加密消息所需要的三个因素——完整的加密消息、破解该消息所需的演算法和密钥（仅授权用户知道的密码）。我们应始终假设加密消息和演算法将在某个时间点为公众所知，即使是拥有专利的演算法也是如此。因此，系统安全从来都不应依赖于安全演算法的保密，因为该资讯迟早会泄露于世。

灵活性和扩展性

对于任何密钥管理方案来说，所有设备不能使用相同的密钥非常关键。这有助于提高整个系统的安全性，因此，如果一个移动部件被破解，也不会危及整个安全系统。实现此功能的最简单方法是，为每个移动部件分配其自己的唯一密码或加密密钥。一个经常用来实现此功能的方法是给每个移动部分分配一个唯一的编号作为序列号，然后基于该序列号和主制造商代码进行唯一的加密密钥的计算。一个需要同时支援多个移动部件的接收器部件，可轻松使用序列号导出破解发送自特定移动设备的资讯所需的加密密钥。移动设备的序列化通常通过以下方法在生产时完成：在将嵌入式单片机置于印刷电路板前预烧写该资讯，或者在电路板组装后使用在线串行编程（ICSP）烧写单片机。

可生产性

如前文所述，在任何安防系统中，一直保护加密密钥非常关键。这包括生产过程，尤其在实际的产品组装是由第三方契约制造（CM）公司完成时。在该情况下，仅向CM提供预编程的代码保护单片机比尝试确保生产流程安全更易于确保加密密钥不会被非法复制。大部分单片机供应商，如Microchip，在他们的所有单片机上提供“带序列号的快速批量编程”选项。通过向制造商提供器件序列化资讯，他们可在生产测试期间将应用程式软体和序列化资讯预烧写到单片机中。

物理安全性

对安防系统的攻击远远超出了仅分析资料和试图对安防系统执行数学攻击。更确切地说，攻击包括分析应用电路和试图查看是否可篡改任何硬体以访问安防系统。如果接收器的输出仅拉高资料线来启动继电器，那么这就是一个易被攻击的薄弱点。这些类型的攻击显然只在您能够物理访问正在工作的接收器部件的硬体时才能凑效。

另一种攻击方案涉及从物理元件端分析移动发送器部件。这包括分析实际电路和施加规范电压以对单片机发送信号或对应用限流，以查看攻击者是否有机会读取存储在器件非易失性记忆体中的安全资讯。还有其他各种侵入性和非侵入性攻击方法，试图破坏这些单片机内置的代码保护锁定机制。

没有器件是攻不可破的。只要有时间和金钱，最终一定能找到方法破解器件并读取受保护的资讯。正因为如此，单片机晶片设计人员需不断添加更多物理隐匿层以保护器件中存储的资讯，尤其是加密演算法代码或密钥。因此，最好始终与单片机供应商密切合作，以了解哪些器件采用了最新的防篡改电路来保护器件内存储的资讯。

变化对安全来说是好事

另一个保护安防系统的好方法是定期更改相关事物。不要在较长时间段内使用具有完全相同的安全密钥资讯的同一安全解决方案。可混合使用以下方法：更改密钥管理方案，用于导出各个移动部件的唯一加密密钥的主加密代码，或在新一代安全演算法可用时移植至新一代演算法。不尽如人意的是，变化会使产品丧失向后相容性。系统设计人员在进行设计时，需要权衡利弊。在这些类型的设计中使用嵌入式单片机的最大好处是可随时进行这类变化，而无需完全重新设计。相同的硬体设计可用于不同的产品。

结论

在低成本无线领域提供更好的安全级别的需求日益增加。需要了解和评估各种因素，才能找到以合理的成本提供足够保护的最佳解决方案。不存在一个适合所有应用的解决方案。单片机、RF IC和紧凑安全演算法的最新进步显着简化了设计这些低成本的安全无线解决方案的复杂性。选择合适的无线RF、单片机和安全演算法需要深入了解当今用于攻破安防系统的各种攻击方法。只有系统设计工程师考察了开发安全无线解决方案的所有方面，才有可能找到一种价格合理的应对措施。

最好的建议是与您的单片机供应商公开讨论各种设计选项和替代方式，而非只关注器件资料手册列出的特定安全特性。安全是系统级问题，也应按以下流程开发：首先选择安全演算法，然后支援生产/制造需求，最后设计密钥分发机制。请记住，安全系统的强度仅与其最薄弱的环节一样。