单片机解密的“攻”与“防”

1 引言

单片机（Microcontroller）一般都有内部 ROM / EEPROM / FLASH 供用户存放程序。为了防止未经授权访问或拷贝单片机的机内程序，大部分单片机都带有加密锁定位或者加密字节，以保护片内程序。如果在编程时加密锁定位被使能（锁定），就无法用普通编程器直接读取单片机内的程序，这就是所谓拷贝保护或者说锁定功能。事实上，这样的保护措施很脆弱，很容易被破解。单片机攻击者借助专用设备或者自制设备，利用单片机芯片设计上的漏洞或软件缺陷，通过多种技术手段，就可以从芯片中提取关键信息，获取单片机内程序。因此，作为电子产品的设计工程师非常有必要了解当前单片机攻击的最新技术，做到知己知彼，心中有数，才能有效防止自己花费大量金钱和时间辛辛苦苦设计出来的产品被人家一夜之间仿冒的事情发生。

2 单片机攻击技术

目前，攻击单片机主要有四种技术，分别是：

（1）软件攻击

该技术通常使用处理器通信接口并利用协议、加密算法或这些算法中的安全漏洞来进行攻击。软件攻击取得成功的一个典型事例是对早期 ATMELAT89C 系列单片机的攻击。攻击者利用了该系列单片机擦除操作时序设计上的漏洞，使用自编程序在擦除加密锁定位后，停止下一步擦除片内程序存储器数据的操作，从而使加过密的单片机变成没加密的单片机，然后利用编程器读出片内程序。

（2）电子探测攻击

该技术通常以高时间分辨率来监控处理器在正常操作时所有电源和接口连接的模拟特性，并通过监控它的电磁辐射特性来实施攻击。因为单片机是一个活动的电子器件，当它执行不同的指令时，对应的电源功率消耗也相应变化。这样通过使用特殊的电子测量仪器和数学统计方法分析和检测这些变化，即可获取单片机中的特定关键信息。

（3）过错产生技术

该技术使用异常工作条件来使处理器出错，然后提供额外的访问来进行攻击。使用最广泛的过错产生攻击手段包括电压冲击和时钟冲击。低电压和高电压攻击可用来禁止保护电路工作或强制处理器执行错误操作。时钟瞬态跳变也许会复位保护电路而不会破坏受保护信息。电源和时钟瞬态跳变可以在某些处理器中影响单条指令的解码和执行。

（4）探针技术

该技术是直接暴露芯片内部连线，然后观察、操控、干扰单片机以达到攻击目的。为了方便起见，人们将以上四种攻击技术分成两类，一类是侵入型攻击（物理攻击），这类攻击需要破坏封装，然后借助半导体测试设备、显微镜和微定位器，在专门的实验室花上几小时甚至几周时间才能完成。所有的微探针技术都属于侵入型攻击。另外三种方法属于非侵入型攻击，被攻击的单片机不会被物理损坏。在某些场合非侵入型攻击是特别危险的，这是因为非侵入型攻击所需设备通常可以自制和升级，因此非常廉价。大部分非侵入型攻击需要攻击者具备良好的处理器知识和软件知识。与之相反，侵入型的探针攻击则不需要太多的初始知识，而且通常可用一整套相似的技术对付宽范围的产品。因此，对单片机的攻击往往从侵入型的反向工程开始，积累的经验有助于开发更加廉价和快速的非侵入型攻击技术。

3 侵入型攻击的一般过程

侵入型攻击的第一步是揭去芯片封装。有两种方法可以达到这一目的：第一种是完全溶解掉芯片封装，暴露金属连线。第二种是只移掉硅核上面的塑料封装。第一种方法需要将芯片绑定到测试夹具上，借助绑定台来操作。第二种方法除了需要具备攻击者一定的知识和必要的技能外，还需要个人的智慧和耐心，但操作起来相对比较方便。芯片上面的塑料可以用小刀揭开，芯片周围的环氧树脂可以用浓硝酸腐蚀掉。热的浓硝酸会溶解掉芯片封装而不会影响芯片及连线。该过程一般在非常干燥的条件下进行，因为水的存在可能会侵蚀已暴露的铝线连接。接着在超声池里先用丙酮清洗该芯片以除去残余硝酸，然后用清水清洗以除去盐分并干燥。没有超声池，一般就跳过这一步。这种情况下，芯片表面会有点脏，但是不太影响紫外光对芯片的操作效果。最后一步是寻找保护熔丝的位置并将保护熔丝暴露在紫外光下。一般用一台放大倍数至少 100 倍的显微镜，从编程电压输入脚的连线跟踪进去，来寻找保护熔丝。若没有显微镜，则采用将芯片的不同部分暴露到紫外光下并观察结果的方式进行简单的搜索。操作时应用不透明的纸片覆盖芯片以保护程序存储器不被紫外光擦除。将保护熔丝暴露在紫外光下 5～10 分钟就能破坏掉保护位的保护作用，之后，使用简单的编程器就可直接读出程序存储器的内容。

对于使用了防护层来保护 EEPROM 单元的单片机来说，使用紫外光复位保护电路是不可行的。对于这种类型的单片机，一般使用微探针技术来读取存储器内容。在芯片封装打开后，将芯片置于显微镜下就能够很容易的找到从存储器连到电路其它部分的数据总线。

由于某种原因，芯片锁定位在编程模式下并不锁定对存储器的访问。利用这一缺陷将探针放在数据线的上面就能读到所有想要的数据。在编程模式下，重启读过程并连接探针到另外的数据线上就可以读出程序和数据存储器中的所有信息。

还有一种可能的攻击手段是借助显微镜和激光切割机等设备来寻找保护熔丝，从而寻查和这部分电路相联系的所有信号线。由于设计有缺陷，因此，只要切断从保护熔丝到其它电路的某一根信号线，就能禁止整个保护功能。由于某种

原因，这根线离其它的线非常远，所以使用激光切割机完全可以切断这根线而不影响临近线。这样，使用简单的编程器就能直接读出程序存储器的内容。

虽然大多数普通单片机都具有熔丝烧断保护单片机内代码的功能，但由于通用低档的单片机并非定位于制作安全类产品，因此，它们往往没有提供有针对性的防范措施且安全级别较低。加上单片机应用场合广泛，销售量大，厂商间委托加工与技术转让频繁，大量技术资料外泻，使得利用该类芯片的设计漏洞和厂商的测试接口，并通过修改熔丝保护位等侵入型攻击或非侵入型攻击手段来读取单片机的内部程序变得比较容易。

4 应对单片机破解的几点建议

任何一款单片机，从理论上讲，攻击者均可利用足够的投资和时间使用以上方法来攻破。所以，在用单片机做加密认证或设计系统时，应尽量加大攻击者的攻击成本和所耗费的时间。这是系统设计者应该始终牢记的基本原则。除此之外，还应注意以下几点：

（1）在选定加密芯片前，要充分调研，了解单片机破解技术的新进展，包括哪些单片机是已经确认可以破解的。尽量不选用已可破解或同系列、同型号的芯片。

（2）尽量不要选用 MCS51 系列单片机，因为该单片机在国内的普及程度最高，被研究得也最透。

（3）产品的原创者，一般具有产量大的特点，所以可选用比较生僻、偏冷门的单片机来加大仿冒者采购的难度。

（4）选择采用新工艺、新结构、上市时间较短的单片机，如 ATMELAVR 系列单片机等。

（5）在设计成本许可的条件下，应选用具有硬件自毁功能的智能卡芯片，以有效对付物理攻击。

（6）如果条件许可，可采用两片不同型号单片机互为备份，相互验证，从而增加破解成本。

（7）打磨掉芯片型号等信息或者重新印上其它的型号，以假乱真。当然，要想从根本上防止单片机被解密，程序被盗版等侵权行为发生，只能依靠法律手段来保障。