超越传统的加密锁－ET199

北京坚石诚信科技股份有限公司

2008-7-25

根据《计算机世界》统计调查表明，绝大多数软件开发商都有过辛苦开发出的软件被盗版的痛苦经历，每年盗版软件给整个软件行业带来数以亿计的损失，软件行业正面临着投入回报比例极度失调，陷入无秩序，无持续性，无规模的不良发展状态，盗版风潮愈演愈烈。大量的软件开发商面对盗版几乎到了束手无策的地步。

造成这种局面的主要原因是加密锁技术停滞不前，硬件落后，破解手段更加先进等。传统的加密锁产生于上世纪 90 年代，功能单纯，如：存储，模块号，算法变换，种子码等，已经远远不能满足新世纪软件加密的要求。现在的破解技术主要有硬破解和软破解两种：硬破解指的是通过硬件克隆达到破解目的；软破解则通常是通过 OllyDbg 等反编译工具跟踪程序，或者分析软件与锁之间的通讯数据进行解密。

传统加密锁根本不能有效的抵御上述的破解攻势，造成软件开发商在与破解者的对抗中处于劣势。其根源在于：

薄弱点 1：设计原理简单，有很大缺陷

传统加密锁中的读写功能和算法变换功能的致命缺点就是数据相对固定，或者变化范围有限。

- 伪自定义算法

虽然这种传统加密锁号称提供自定义算法，但算法只有加、减、异或等简单的处理，我们称为伪自定义算法。这种假算法由于过于简单，并没有什么实际的应用意义，算法的计算结果也只能起到核对的作用。

- 种子码算法

同样，那些在硬件中由加密锁厂商设计而不公开的算法，如种子码算法，开

发商只能设置输入，由算法计算产生一个输出。由于算法不公开，开发商不能根据自身软件的实际需要修改算法，那么这种计算的结果也只能起到核对的作用。

- 存储区

多数开发商存储区中存放的是固定数据，固定数据非常容易就可以被跟踪替换，造成软件被破解。

综上，针对这种核对或者存储固定数据方式，如果破解者截获这些数据，通过统计、分析，做出算法变换对照表，就可达到解密目的。

薄弱点 2：功能上不能满足软件发展趋势

密码学在软件中的应用是当今软件发展的一个明显的趋势，越来越多的开发商已经不满足于将数据进行简单的处理，而是使用强度高，历经多年实践的，成熟标准的，国际公认的对称和非对称加解密算法。其典型代表就是 RSA，DES/3DES 等。传统加密锁由于硬件的限制，通常采用通用 8 位单片机或同档次的 ASIC 芯片作为核心微处理器，根本就不具备这样的功能，势必被软件行业所淘汰。

薄弱点 3：硬件核心芯片防攻击性差

随着集成电路设计、生产技术的不断提高，硬件核心芯片受到攻击的可能性越来越大。典型的硬件攻击手段有电子探测攻击（如 SPA 和 DPA）和物理攻击（探测，如采用 SiShell 技术）。

电子探测（SPA 和 DPA）攻击技术的原理是：通过特殊的电子设备来测定电子元件的功率消耗。当核心芯片执行不同的指令时，对应的功率消耗也相应的变化。攻击者通过检测和分析这些变化，从中得到核心芯片中的特定关键信息。

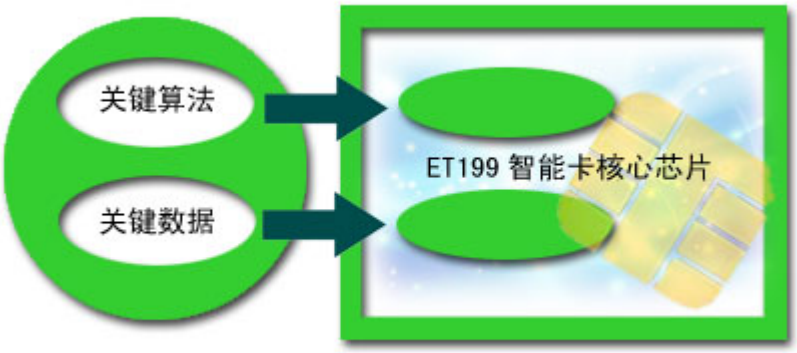
物理攻击的原理是：通过电子扫描显微镜对芯片内部存储器或其它逻辑直接进行分析读取，或者通过测试探头读取存储器内容。

传统加密锁中的核心芯片没有任何手段来防止上述的攻击方法。很容易通过电子探测和物理攻击，或者利用加密锁厂商不公开的测试接口获取硬件中的数据

信息，做出一模一样的克隆加密锁。

ET199 做为新世纪软件保护行业内超越传统的领导产品，具有以下突出的优势：

超越 1：代码镂空技术



由上图可以看出，运行在计算机中的应用软件的关键代码和数据被镂空了，即计算机中是一个“消失”了关键代码的，不能运行的，不完整的软件。这部分关键代码被安全地移植到 ET199 硬件中保护起来。在需要使用时，应用软件可以通过调用执行命令来指令 ET199 运行硬件中的关键代码和数据并返回结果，将镂空的部分填充上，使软件完整正常的运行。

关键代码的存储和运行都是在 ET199 中，由于计算机硬盘和内存中没有副本存在，各种反编译或者跟踪工具都是无效的，破解者无从猜测算法或者窃取数据，从而根本上保证了整个软件系统的安全性。完全实现了不可破解的效果。

同时，ET199 可提供高达 64K 字节的程序和数据空间，可容纳万行以上的 C 语言代码。

超越 2：智能卡核心芯片

智能卡芯片具有很高的集成度，与传统低档的单片机不同，只有已通过国际安全机构检测和认证的专业安全芯片制造商才能提供智能卡芯片。

智能卡硬件设计阶段就提供了完善的安全保护措施。它通过产生额外的噪声和干扰信号，再加上若干保护层，采用特殊的材料（对电子束敏感的材料）等，使监测芯片内执行的指令序列不可能实现。有效的抵御了电子探测和物理攻击等破坏措施。

智能卡还具备以下防攻击特性:

- 较强的机械强度和电气保护措施
- 防止地址和数据总线的截取，总线和存储器的物理保护层
- 存储区分类访问保护，不同的区域有不同的访问权限。
- 硬件随机数发生器，随机数可以在做为对称密钥，混淆明文数据等应用中起到重要作用。硬件本身带有高强度随机数发生器对安全而言意义重大。
- 持卡人身份 PIN（Personal Identification Number）验证，PIN 码有锁死次数限制，当破解者试图暴力破解 PIN 时，会造成卡片自我锁定，对卡片的各种操作均会无效。

超越 3: 智能卡的“心”－COS（Chip Operation System）系统

ET199 集成了 COS 和虚拟机技术，COS 提供了文件管理、安全管理、内层管理、输入输出管理等各种功能，通过 COS 提供的功能，可以保证数据的安全存储、数据的安全访问等各种应用。同时 ET199 的 COS 完全符合国际标准化组织 ISO 对智能卡的物理和电器指标以及应用标准做出的 ISO7816 规定。

虚拟机技术提供了一种 CPU 的指令集支持和基于此指令集的开发接口及开发环境。通过虚拟机的支持，用户的核心算法和数据可以转移到智能卡内部，并在智能卡内部运行，在智能卡操作系统的管理下，形成一个与计算机平行的小型计算机系统，并通过 USB 接口同计算机交换数据。

超越 4: 强大的运算处理能力

ET199 能够支持单双精度浮点运算功能、数学函数运算功能、安全文件管理功能、标准输入和输出功能等；这些对提高加密强度起着至关重要的作用。

超越 5：RSA 非对称算法和 DES/3DES 对称算法

ET199 智能卡硬件中自带 RSA 协处理芯片，能够在硬件中快速的完成各种 RSA 运算。RSA 私钥始终在智能卡芯片中，外界没有私钥的备份，加上智能卡硬件不能被复制的特性，破解者没有任何办法去破解。同时 ET199 完全支持 DES/3DES 对称算法，为软件开发商提供更多的加密手段。

ET199 引领以智能卡为核心的标志性的技术升级，超越了传统意义上的加密方式。为软件行业健康蓬勃发展，业绩腾飞保驾护航。