基于SRAM的微控制器提供更高的安全性

无论是自动应答机、护照/身份验证设备，或者是便利店内的销售点终端，都有一些重要信息，例如口令、个人身份识别号(PIN)、密钥和专有加密算法等，需要特别保护以防失窃。金融服务领域采用了各种精细的策略和程序来保护硬件和软件。因此，对于金融交易系统的设计者来讲，在他设计一个每年要处理数十亿美元业务的设备时，必将面临严峻挑战。

安全微控制器最有效的防护措施就是，在发现入侵时迅速擦除存储器内容。

为确保可信度，一个支付系统必须具有端到端的安全性。中央银行的服务器通常放置在一个严格限制进入的建筑物内，周围具有严密的保护，但是远端的支付终端位于公共场所，很容易遭受窃贼侵袭。尽管也可以将微控制器用保护外壳封闭起来，并附以防盗系统，一个有预谋的攻击者仍然可以切断电源后突破防盗系统。外壳可以被打开，如果将外壳与微控制器的入侵响应加密边界相联结，对于安全信息来讲就增加了一道保护屏障。为了实现真正的安全性，支付系统应该将入侵响应技术建立在芯片内部，并使用可以信赖的运算内核。这样，执行运算的芯片在发生入侵事件时就可以迅速删除密钥、程序和数据存储器，实现对加密边界的保护[1]。安全微控制器最有效的防护措施就是，在发现入侵时迅速擦除存储器内容。DS5250安全型高速微控制器就是一个很好的典范，它不仅可以擦除存储器内容，而且还是一个带有SRAM程序和数据存储器的廉价的嵌入式系统。

物理存储器的信心保证

多数嵌入式系统采用的是通用计算机，而这些计算机在设计时考虑更多的是灵活性和调试的便利性。这些优点常常又会因引入安全缺口而成为其缺陷[2]。窃贼的首个攻击点通常是微控制器的物理存储器，因此，对于支付终端来讲，采用最好的存储技术尤其显得重要。利用唾手可得的逻辑分析仪，例如Hewlett-Packard的HP16500B，很容易监视到地址和数据总线上的电信号，它可能会暴露存储器的内容和私有数据，例如密钥。防止这种窃听手段最重要的两个对策是，在存储器总线上采用强有力的加密措施，以及选择在没有电源时也能迅速擦除的存储技术。有些嵌入式系统试图采用带内部浮置栅存储器(例如EPROM或闪存)的微控制器来获得安全性。最佳的存储技术应该能够擦除其内容，防止泄密。但紫外可擦除的EPROM不能用电子手段去擦除，需要在紫外灯光下照射数分钟才可擦除其内容，这就增加了它的脆弱性。闪存或EEPROM要求处理器保持工作，并且电源电压在规定的工作范围之内，方可成功完成擦除。浮置栅存储技术对于安全性应用来讲是很坏的选择，当电源移走后，它们的状态会无限期地保持，给窃贼以无限长的时间来找寻敏感数据。更好的办法是采用象SRAM这样的存储技术，当电源被移走或入侵监测电路被触发时以下述动作之一响应：

窃贼的首个攻击点通常是微控制器的物理存储器，因此，对于支付终端来讲，采用最好的存储技术尤其显得重要。

- 当电源被移走后存储器复零。
- 入侵监测电路在数纳秒内擦除内部存储器和密钥。
- 外部存储器在应用软件的控制下以不足100ns的写时间进行擦除。

有些设计者倾向于采用微控制器和存储器集成在同一块芯片的方案来克服浮置栅存储器的弱点。这种方案可以拒绝未经授权地访问其存储器内容。很多情况下这是通过一个或更多的内部锁定位来实现的，通常是在编程的最后一步设定这些位。设定好之后，如果微控制器被从PC板上拆卸下来放入编程器中(例如广泛使用的BP Microsystems的BP-1700通用工程编程器)，

这些锁定位能够阻止微控制器泄漏其中的内容。实际上，擦除锁定位的唯一方法是擦除所有存储器，以便对器件进行重新编程，同时也销毁了程序存储器中的内容。进一步提高安全性的尝试是在内部增加一个存储器加密阵列，当编程器试图验证或转储其内容时，加密阵列会对存储器的输出进行加密。这种方案的一个实例可以从Intel MCS® 51系列的处理器中找到，它采用一个64字节、用户可编程的加密阵列，在验证期间用加密阵列对存储器内容进行异或。除非用户知道加密阵列的内容，否则在验证操作期间所获得的信息将无法解读。然而，即便是加锁定位的方法也不能确保安全。利用技术手段突破浮置栅器件(例如EPROM、EEPROM和闪存)的保护，并选择性地擦除安全锁定位的方法很容易在技术期刊和因特网新闻组中找到[3]。一些器件制造商建议采用一次性可编程器件，认为结实的塑料封装能够对锁定位的安全提供某种程度的保护。然而，“某种程度的保护”只是相对而言。采用热酸溶液可以轻而易举地溶解掉晶片外面的塑料封装而不会损伤晶片。然后，利用一些简单而且廉价的工具例如Karl Suss PM 8 Manual Probe Station，对晶片的布局进行仔细研究之后就可找到安全锁定位的位置。这种技术经常被用于紫外可擦除的EPROM。去掉封装后，在晶片上敷一层不透明的涂料或绝缘胶带，在锁定位上方仔细地留一个针孔。然后将晶片暴露于强紫外线下就可擦掉锁定位，同时保持存储器主体不受影响。去掉锁定位的器件就可在标准编程器上读出，就象锁定位从来没有被设置一样(图1和2)。这个简单工序事实上已经成为半导体公司进行失效分析的例行程序。

浮置栅存储技术对于安全性应用来讲是很坏的选择，当电源移走后，它们的状态会无限期地保持，给窃贼以无限长的时间来找寻敏感数据。更好的办法是采用象SRAM这样的存储技术。

浮置栅存储技术的另一个缺点是存储单元固有的非易失性，即使微控制器失去电源其内容依然保持。浮置栅器件在没有电源的情况下数据能够保持上百年的时间。在基于私有密钥基础结构(PKI)的系统中[4]，如此长的保持时间会给私有密钥的长期保护带来问题，因为它给窃贼提供了无限长的时间来突破芯片的物理防护，并在器件执行入侵响应之前进入存储器。

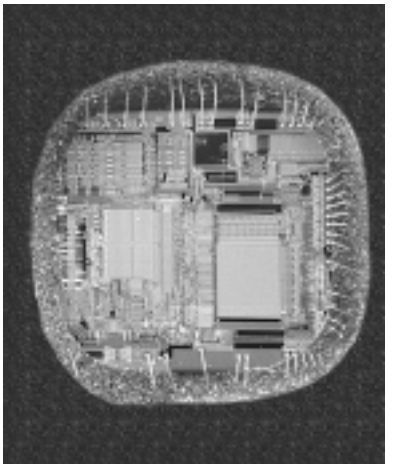

图1. 利用酸液去除封装后，微控制器上的EPROM显露出来。

SRAM和速度

所有安全性应用都要求尽可能快的读/写时间，以便实现更高级的保护。SRAM是所有存储技术中速度最快的。作为入侵响应的一部分，它可以在瞬间擦除或“复零”。此外，SRAM已广泛使用，价格适中，独特的性能很适合于安全数据的存储。尽管本身是易失性的，但利用一个备用锂电池，很容易使其成为非易失存储器，在没有V_{CC}的情况下保证10年以上的数据保持时间，同时备用电池还可用于驱动一个实时时钟，以便为交易业务提供时间和日期标记。这些特性是浮置栅存储技术所没有的。

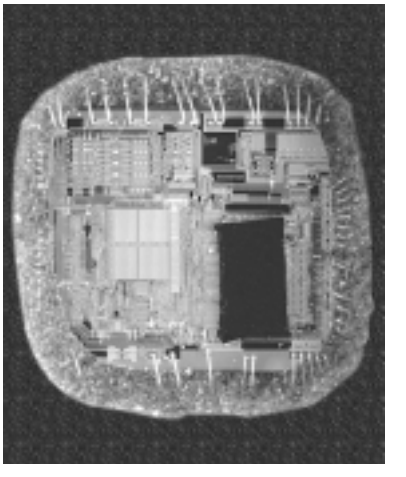

图2. 将微控制器的EPROM阵列覆盖起来，暴露出锁定位，然后就可轻易地将其擦除。

认证交易

支付终端的PINpad模块为金融支付系统提供核心可靠性。受银行监管机构和信用卡发行方管制的这个模块要求采用一个安全微控制器，微控制器的驻留软件应包括键盘、磁卡阅读器、智能卡阅读器和LCD显示器等设备的驱动器。同时还应该具备一些和通用主机(PC、486、ARM等)进行高速串行通信的手段，以及用于实现安全端到端通信的PKI加密程序。PINpad模块微控制器的存储器需求高达数百k字节，超出了单芯片实现的经济容量，因此需要采用外部存储器。前面已经提到，外部存储器很容易被窃听，除非微控制器和外部存储器之间的通信采用了强有力的加密手段。这种加密方案具有一些彼此相互依存的特殊要求：

MCS是Intel Corporation的一个注册商标。

关于支付系统用 EMV 集成电路卡技术规范的更多信息，参见 www.emvco.com。

- 加密/解密操作必须和指令的执行具有相当的速度。加密操作必须对每次取指或一组字节执行(如果采用的是诸如数据加密标准(DES)这样的块加密的话)。加密算法应该是健壮、快速并基于硬件的。比较优秀的方案之一是采用专用的片上3DES硬件实现的三重DES (3DES)算法，执行速度要比多次执行单DES加密的方案快的多。

- 外部存储器必须是SRAM，以便支持加密引擎所要求的高数据传送速率。另一方面，为了在检测到入侵事件时能够迅速擦除存储器，也需要采用有备用电池的SRAM。

- 对于加密操作至关重要的数据，例如加密密钥，永远不能在处理器外部看到。处理器必须至少生成并安全地保存部分加密密钥。作为入侵响应的一部分，这些密钥被迅速擦除，致使外部存储器无法解读。

SRAM 是所有存储技术中速度最快的，作为入侵响应的一部分，它可以在瞬间擦除或“复零”。

- 程序和数据的初始装载和加密应该由微处理器内部的自举装载器实施。这样可以防止应用代码被未经授权者看到，并将加密方法隐匿起来，使自举装载器成为一个防火墙。自举装载器不仅要防止对已装载信息的访问，还必须防止恶意地装载一些没有授权的欺诈软件。一个例子就是控制正在工作的PINpad或ATM，擦除其软件，然后装载一些刻意设计的软件来收集不知情使用者的PIN码。所以，自举装载器和主系统之间的所有通信都应该是加密的，以防被敌方截获并破译。

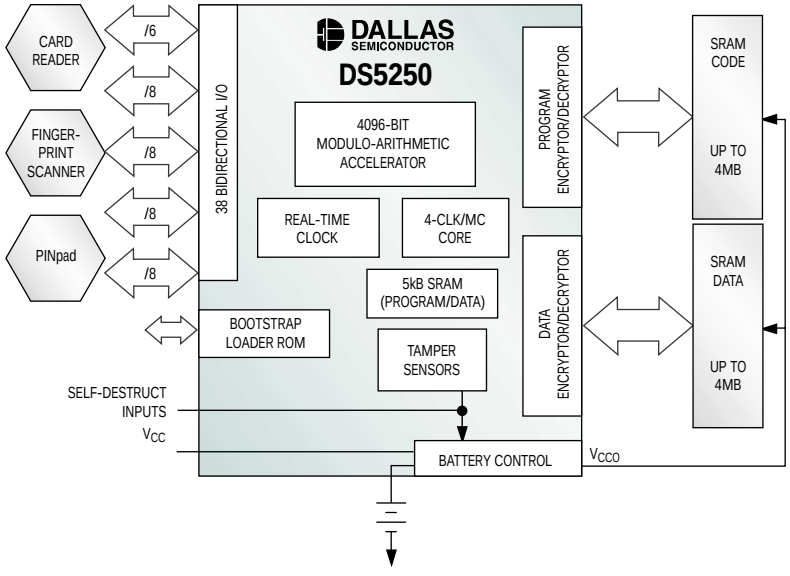

图3. DS5250运行速度高达6.25 MIPS，程序和数据保存在高达8MB的外部SRAM中。

DS5250——全部整合

加密手段的采用，使我们有可能用SRAM作为程序和数据存储介质构建嵌入式系统。DS5250安全微控制器便是这样一种系统(图3)。它每秒可执行多达6.25百万条8051指令，程序和数据存储在容量高达8MB的外部SRAM中。最敏感的信息可以保存在5kB的内部数据存储器中。SRAM数据的保持由微处理器内部的专用电池切换硬件控制，由它负责向外部存储器提供V_{CC}或电池电源。该系统可被装配到用于身份验证的外设上，例如ISO-7816标准的智能卡阅读器，指纹扫描仪和键盘等。

程序和数据总线上专用的加密/解密引擎保证了外部总线的安全。DS5250的程序存储器总线采用单或3DES，以8字节块进行加密。数据存储器总线可选由专用硬件实时加密。密钥是在一个真随机数产生器的协助下产生的，这个随机数产生器通过了联邦信息处理标准出版物140-1 (FIPS PUB 140-1)第4.11.1节，*Security Requirements for Cryptographic Modules*所描述的统计随机数产生器测试。程序存储器完整性校验功能对比各个独立块的校验和与事先计算的数值，进一步提高了存储器的安全性。若块校验和与保存数值匹配失败，就会唤醒由用户编程的入侵响应，阻止置换方式的攻击。

除了支持NV SRAM以外，DS5250还结合了许多系统安全特性。一个由高性能4096位模运算加速器(MAA)单元驱动的RSA运算能够在6ms内执行对1024位的幂取模。另外还有5kB的内部SRAM可用于存放安全密钥、数据存储器和/或程序存储器，同时还作为MAA的临时存储

器。应用软件由自举装载器通过串行口安全装载，自举装载器采用基于一种链式密码、双密钥3DES加密算法的质询/响应协议。作为另一种选择，DS5250还允许系统设计者充分利用微控制器的全部安全特性，生成应用特有的自举装载器软件。

内部的入侵感测器能够监测对微处理器晶片的物理攻击，并启动入侵响应，擦除用于译码外部存储器的加密密钥。由用户设立的传感器或开关可以连接到自毁输入引脚，一旦触发可以启动相同的入侵响应，此外还销毁保存在内部代码/数据RAM存储器内的所有数据。另外，自毁输入还切断供给SRAM的所有电源，确保程序和数据存储器丢失。连接到外部引脚的自毁中断源允许系统软件根据特定的应用要求，灵活生成用户化的入侵响应。不过，DS5250安全微控制器晶片具有自带的、具有入侵反应的加密边界，这样可以省掉外加的入侵响应装置，降低系统成本。图4A和4B对比了普通的安全措施和DS5250的措施。

保证安全和保密

任何一种金融终端，无论是PINpad、POS终端或者是ATM，都需要处理一些保存在其RAM和ROM中的机密信息。这就使存储器成为影响金融交易安全性的关键元件。随着窃贼的日益诡诈，用于保护机密信息的安全手段也必须更加完善。尽管有了很多层的保护，加密SRAM还是嵌入式存储信息的最佳保护手段。

也许最重要的是，DS5250安全型高速微控制器保护了敏感信息并维护了支付系统的可靠性，使其符合金融行业相关法规的要求。在有必要时，随着入侵响应它将无条件地擦除私有密钥、程序和数据，保证数据的安全和保密。

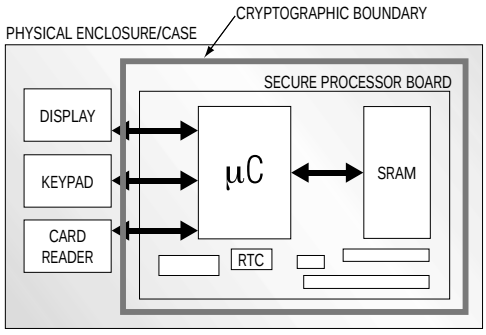

图4A. 嵌入式系统设计者在建立安全计算机时，常常试图采用带有相关外设/存储器的通用微控制器，然后用多个昂贵的入侵传感器将PC板包围起来。

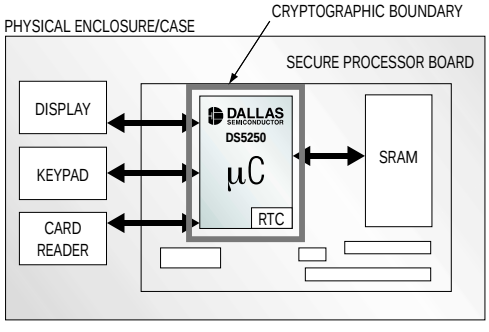

图4B. DS5250安全微控制器具有自带的、具有入侵反应的加密边界，这样可以省掉外加的入侵响应装置，降低系统成本。

参考文献：

1. Smith, Sean; Palmer, Elaine; Weingart, Steve. *Using a High-Performance, Programmable Secure Coprocessor*. Proceedings of the Second International Conference on Financial Cryptography, Springer-Verlag Lecture Notes in Computer Science, 1998.

2. J. D. Tygar and B. S. Yee. *Dyad: A System for Using Physically Secure Coprocessors*. Proceedings of the joint Harvard-MIT Workshop on Technological Strategies for the Protection of Intellectual Property in the Network Multimedia Environment, April 1993.

3. 很多地方有关于这个主题的讨论，通过web搜索引擎，利用关键字“EPROM”、“plastic”和“acid”就可找到。

4. RSA Laboratories. *PKCS #1 v2.1: RSA Cryptography Standard*, Bedford, Massachusetts, 2002.