MIDP 2.0 安全性分析

笪五三[1]，杨维康[2]

（1.清华大学深圳研究生院软件工程中心 深圳 518055; 2. 清华大学信研院 北京 100084）

[摘要] J2ME 平台是一种应用于资源受限的消费类电子设备的 Java 运行时环境，应用广泛；然而，深受众多移动终端支持的 MIDP1.0 缺乏足够的安全机制，使得这些设备上的信息安全受到威胁和攻击，这种状况有望在 MIDP2.0 中得到改善。本论文首先简要介绍了 J2ME 和 MIDP 的概念，讨论了移动环境下支持 MIDP1.0 的设备受到的安全威胁和攻击，阐述了 MIDP2.0 规范中新增的安全机制和特征--主要表现在增加了安全的网络协议（如 SSL）和采用了对 MIDlet 应用程序签名的策略等，分析了这些增强的安全机制如何防止和抵御对敏感信息的威胁和攻击，从而得出结论，MIDP2.0 虽然仍然存在威胁和攻击，但在安全性方面比 MIDP1.0 有了很大的提高。

[关键词] J2ME 平台； MIDP 2.0 规范； 信息安全；

中图法分类号: TP309

Analysis of MIDP 2.0 Security

DA Wu-san[1],YANG Wei-kang[2]

(1.Software Engineering Center, ShenZhen Graduate Institute, Tsinghua University, Shenzhen, 510855; 2.Operating System and Middleware R&D center, Computer Science Department, Tsinghua University, Beijing,100084)

[Abstract] J2ME is a micro Java runtime environment for resource-constrained devices. There are already many mobile devices that support MIDP 1.0 in J2ME. Many security threats exist in MIDP1.0 since the specification has only little security issues. It's supposed that the next version of MIDP will improve the security for the business information and personal privacy. This paper gives brief introduction of the J2ME and MIDP at first, explains the security threats and attacks in the J2ME environment as following, then covers the new security mechanisms and features in MIDP2.0 and analyzes against presented threats, finally concludes that MIDP2.0 improves the mobile information security.

[key words] J2ME Platform; MIDP 2.0 Specification; Security

1．引言

J2ME 是“一种以广泛的消费性产品，诸如寻呼机、移动电话、可视电话、数字机顶盒和汽车导航系统等，为目标的的高度优化的 Java 运行时环境。”完整的 J2ME 平台包括 Java 虚拟机(JVM)、配置层(Configurations)、框架层(Profiles)。配置层由核心运行库、类库、以及编程 API 等组成；而框架层则针对特定类型的设备进一步定义了 J2ME 的运行平台，从而适配设备的需求。（图 1）不同类型的设备有着不同的计算能力和存贮容量，而完善的安全机制通常需要消耗相当的 CPU 和内存资源，所以不同的配置和框架提供了不同程度和层次的安全措施。本论文只讨论 MIDP 的安全机制。

1.1 配置层和框架层

J2ME 的配置层是一个 Java 的基本运行时环境，包括一组核心类和一个运行在特定类型设备上的特定 Java 虚拟机。虽然将来可能定义其他配置，但当前 J2ME 存在两种配置：（1）连接受限设备配置（Connected Limited Device Configuration：CLDC）与 KVM 或者 CLDC HotSpot VM 一起用于内存有限(160KB-512KB)的 16 位或 32 位的设备。这是用于开发小型 J2ME 应用程序的配置。CLDC 通常还包含了到带宽有限的无线移动通信网络的连接。支持 J2ME 的智能手机（比如 Motorola E398）便是一个运行小应用程序的小型无线设备的示例。（2）连接设备配置(Connected Device Configuration：CDC)与 C 虚拟机(CVM)一起使用，用于内存超过 2 兆的 32 位体系结构。CDC 通常也可以连接到某种网络，但这种网络不一定是无线通信网络。

基金项目：国家高技术研究发展计划（863 计划）项目（编号 2001AA113400）。

作者介绍：笪五三(1981-)，男，安徽省桐城县人，硕士研究生，主要研究方向：构件技术，嵌入式操作系统。杨维康（1959-），男，北京人，清华大学信息技术研究院操作系统与中间件技术研究中心主任，博士，主要研究方向：操作系统，构件技术。

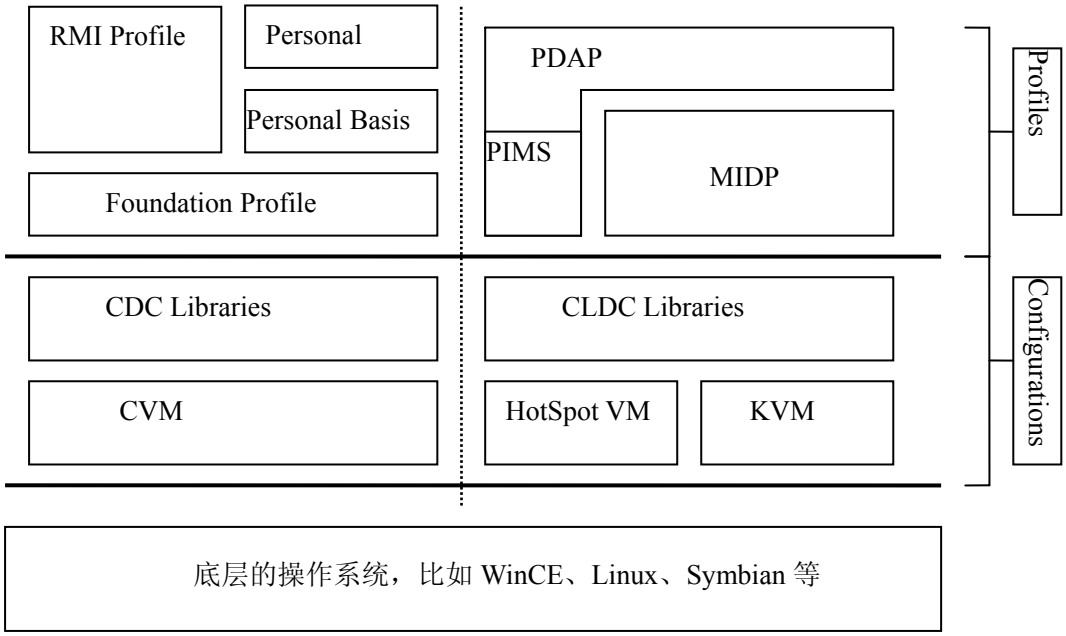

图 1　J2ME 的体系结构图

例如电视机、冰箱等电力充裕的体型较大的设备[1]。

框架层定义了特定的 J2ME 适用的硬件和软件框架，并提供了这个框架要实现的基本功能及其标准接口。和以上两种配置层相对应的框架有：（1）移动信息设备框架（Mobile Information Device Profile:MIDP），是 CLDC 配置相对应的核心框架，后来添加的 PDA(Personal Digital Assistants)框架则包含了 MIDP 和 PIM(Personal Information Management) APIs。（2）个人基本框架和个人框架（Personal Basis Profile & Personal Profile），个人框架包含了个人基本框架，这两者都基于一个更基本的框架：基础框架（Foundation Profile）。这些框架和 CDC 配置相对应，都是针对消费类电子产品的，比如数字视频广播平台（DVB）、HAVi(Home Audio-Video interoperability)等。和 CDC 配置相对应的框架还有 RMI Profile(lightweight Java Remote Method Invocations)等。

1.2 MIDP(Mobile Information Device Profile)

MIDP 用于手机、智能手机、双向寻呼机等移动信息设备。MIDP1.0 规范于 2000 年 9 月份定稿，MIDP 规范一经推出得到了众多厂商的支持；到了 2002 年底，据估计能支持 MIDP1.0 的无线设备已经过亿了。2002 年 11 月份，Sun 发布了 MIDP2.0 规范；现在，主流型号的彩屏手机、智能手机都支持 J2ME 应用程序的下载和运行，并将支持 MIDP2.0/CLDC1.0 作为软件环境的标准配置了。正是因为 J2ME 应用广泛，信息涉及各个方面，其安全问题更需要关注。

MIDP 规范，相比较其它版本的 Java 运行时环境，定义了 MIDlet 应用程序模型，增加了 javax.*软件包；定义了一系列的软件接口，包括基本输入输出（java.io 包）、图形化用户接口（GUI,javax.microedition.lcdui 包等）、网络（javax.microedtion.io 等）、文件系统（javax.microedtion.rms 等）、应用程序管理系统（AMS）等。而 MIDP 2.0 要求更高的 CPU 频率和更大的内存，增加了游戏接口、声音输出接口、安全网络机制等[2]。可以相信的是，因为 Java 语言的平台独立性，应用程序的丰富多样性，J2ME 会得到更加广泛的应用。

2．无线移动网络中的威胁和攻击

智能手机、掌上电脑等无线信息设备的底层系统都是专用的嵌入式操作系统，比如 Symbian、WinCE、PalmOS、Linux 等。最终用户的应用程序包括这些操作系统直接支持的二进制程序、J2ME 的 MIDP 应用程序、基于浏览器的 HTTP/WAP 程序等。这些设备通常都是利用无线通信网络如 GSM、GPRS 等连接上网的，而最终用户的应用程序则依靠 Internet 协议（如 HTTP 等）和无线协议（如 WAP）等接入网络环境。在这样的移动网络环境中，MIDP 应用程序会受到几乎所有类型的信息安全的威胁和攻击，比如对 Internet 或者无线协议的威胁、移动通信网络（GSM、GPRS）的信号截取和攻击、针对 Java 应用程序的特有的威胁和攻击等。以下将从三个方面讨论。

通常，安全的无线移动通信环境应该提供数据机密性、数据完整性、不可抵赖性、服务器端和客户端的认证和授权等保障，同时还能对设备本身诸如设备可用性等提供保障。不过，这些对敏感信息的保障，不仅仅是安全的无线通信环境的要求，也是所有其他类型的信息安全的要求。数据机密性要求只有被授权

的对象才能访问数据；完整性要求数据在传输/存储时没有被恶意篡改、添加、删除；不可抵赖性则提供“消息确实是消息的发送者发送的”等类型的证据；可用性指对象请求使用设备时设备能满足这样的请求[3]。考察 MIDP 的安全性，就需要检验 MIDP 能否提供这些对敏感数据的基本的安全保障。[4]

2.1 Internet 中一直存在的安全威胁

Internet 上的应用程序饱受各种类型的安全威胁和攻击，这是由于早期的硬件设备比较落后，设计 Internet 的各种协议时并没有考虑安全主题。这些攻击按照不同的标准可以分为不同的类型，比如主动/被动攻击、对网络/主机的攻击等。下面从安全的基本保障方面分析各种类型的攻击：（1）对数据机密性的攻击，包括窃听/监视网络传输数据、偷取主机资料（比如安置木马）、收集网络传送的流量和流量变化等动态信息并加以分析利用等。Internet 上的应用通常以加解密系统来预防和抵御这类攻击。（2）对数据完整性的攻击，包括添加、修改、删除用户数据和网络传输包中的关键数据等，以达到破坏用用户数据或者欺骗通信双方的目的。（3）拒绝服务（DoS）攻击是针对设备可用性的攻击，通常是恶意过度占用设备从而使得正常的设备使用请求不能满足。比如，恶意大量连接服务器、强制关闭正常的用户进程、无用的数据填充内存和磁盘等。众多原因包括不能严格界定恶意使用和正常使用等，使得 DoS 攻击直到现在还很难阻止。（4）对认证和授权的攻击，包括冒充、欺骗攻击，通常是假冒其他对象的标识。这类攻击中，比较流行的是 DNS 欺骗攻击、IP 冒充攻击、网络数据包重放攻击、中间人攻击等。这类攻击一般不单独出现，都伴随以上的一种或者几种攻击同时出现。Internet 所受的安全威胁和攻击还有其他类型，比如偷看、窃取管理员密码等，和 Internet 及终端设备的本身特性相关性不大，不予讨论。

2.2 对无线移动通信网络和移动设备的物理攻击

移动信息设备通常是通过一种无线移动通信网络，比如 GSM 或者 GPRS、3G(CDMA)等连入网络中，有些手持终端则利用无线局域网（WLAN）接入网络中。所有这些无线接入技术和无线通信协议同样存在信息安全的威胁和攻击[6,7,8]。相比有线网络，无线信号更容易被窃听和截取。而且，GSM 网络并没有提供诸如相互认证、点到点的安全、不可抵赖性等重要安全保障[7]；GSM 通信协议和加密算法也有问题和漏洞。对 GSM 网络，可以列举的攻击有：针对 A5 密码算法的攻击[9]，复制 GSM 的 SIM 卡等。这些威胁和攻击同样存在于 GPRS 网络和 WLAN 网络上[8]。

无线通信网络相比有线互联网更容易被攻击，用户受到的损失也可能更大。无线通信网络里有一种独特的攻击方式：“电话被盗打”类型的攻击，这种攻击是未经过移动设备的用户授权而使用无线移动通信网络连接。无线移动通信网络的计费通常是基于通话时间或者利用网络连接传输的数据流量。恶意攻击的软件在用户毫不知情的情况下任意使用移动设备的网络连接，从而产生网络数据流量，使用户蒙受损失。

另外，移动信息设备，比如智能手机、掌上电脑，因为方便使用和携带，常被用作同步分散的系统的商业信息的工具；许多用户也非常乐意将一些个人信息保存在移动信息设备里面。然而，由于这些设备的便携性，他们常常被随身携带，相比锁在屋子里的 PC 和服务器，这些设备被盗和遗失的风险要大得多；这也是对敏感信息和用户隐私的潜在的威胁。

2.3 Java 代码的安全缺陷

尽管安全是 Java 语言的重要组成部分，但仍然存在一些信息安全的威胁。Java 程序是真正的可移动的代码，可从网络上任意下载执行。但由于 DNS 欺骗攻击的存在，或者用户的 TCP/HTTP 连接被篡改，使得实际下载的程序并非用户期望的。而且像 Java 程序这样的可移动代码很容易导致 DoS 攻击。恶意的程序抢占 CPU 时间，繁殖消耗系统资源的线程，极力占用内存空间，有时候还滥用视音频设备。由此可见，虽然 MIDlet 程序受沙箱（sandbox）模型和代码签名的保护，也不是完全可信任的。

2.4 MIDP1.0 的安全和问题

MIDP1.0 也采用了 Java 语言通用的安全机制--沙箱（sandbox），所有的 MIDP1.0 的程序都必须在沙箱内执行，只能访问有限的系统资源。受到移动信息设备的硬件条件的限制，同时也考虑到 J2ME 系统的安全和性能，MIDP1.0 规范舍弃了一些 J2SE 中的 Java 语言的特色，包括 Java Native Interface（JNI）、反射机制（reflection）、自定义类的加载器、与安全相关的包（security package）和安全管理器（Security Manager）。字节码校验器也作了修改，分成了开发阶段的预校验和执行阶段的有限检验。所有这些和 J2SE 不一致的方面都对 MIDP 应用程序的安全有所影响。不支持 JNI，使得 MIDP 程序行为被限制，增加了系统的安全性；但，缺少了与安全相关的包、执行期的有限检验等都减弱了系统的安全性。而且，MIDP1.0 规范里不含有任何的加解密函数，只提供了唯一的网络连接协议 HTTP。

在一个 MIDlet suite(一个 J2ME 的 MIDP 应用程序的包装、发布和执行单元)的生存周期里，安全威胁无时不在。当 MIDlet suite 经过 HTTP 连接从 Internet 上下载时，由于没有任何针对网络连接的保护措施，同时 MIDP1.0 也不支持代码签名，应用程序的完整性和真实性完全无从验证。当 MIDlet suite 在沙箱（sandbox）

里面执行时，虚拟机就得承受恶意程序对其自身的安全漏洞的攻击和 DoS 攻击。

当应用程序连接上 Internet 时，更多的在前面提及的安全攻击便成为可能。敏感信息如明文密码、商业机密、个人信息等可轻易的监听网络获得。HTTP 协议不提供对连接的保护，使得传输数据被删除、修改、重放都轻而易举的实现。针对 Internet 的其他类型的攻击也容易出现。无线通信网络 GSM、GPRS 等无线传输信号相比有线网络更容易截取和窃听。

由此可见，MIDP1.0 对信息安全的支持是远远不能满足商业机密信息的安全需要的。同时，支持 MIDP 的设备正在广泛的应用开来，针对敏感的商业机密信息、个人私密信息的安全保护益发显得重要了。

3. MIDP2.0 的安全性分析

如前所述，MIDP2.0 已经在 2002 年底由 Java Community Process 定稿发布了。MIDP2.0 规范不仅添加了新的编程接口如 game、audio 等，也引入了新的安全保障机制。下面先介绍 MIDP2.0 中引入的新的安全机制和可以采用的安全保障措施，然后详细分析这些机制和措施是如何提供安全的最基本保障。

3.1 应用程序级别的保护措施

由应用程序自身维护信息传输和存储的安全，虽然繁琐和困难，但是当应用程序为机密的商业行为服务时，采用这项安全保障措施还是必要且可行的。这种技术--由应用程序自身维护安全性，验证信息的完整性、确保信息的机密性等--在 MIDP1.0 的应用程序中也可以完成。虽然 MIDP1.0 没有提供加密包，但是现在的移动信息设备硬件水平已经提高到了足以支持一些效率很高的加解密算法实现，J2ME 系统可以采用第三方的安全包。这里，最常用的加解密库是 Bouncy Castle Crypto API 包和 MIDP 可选的包 Security and Trusted Service for J2ME(SATSA)。利用这些加解密库，可以构造基于 HTTP 连接的比较安全的应用程序。比如，利用 HTTP 协议传输 XML 格式的数据，对这些敏感数据加密并进行 XML 数字签名然后再传送到网络中。参考文献[10]详细描述了这种实现技术。

3.2 可信任的 MIDlets

MIDP2.0 引入了一个新的概念：可信任的 MIDlets。在 MIDP1.0 中，所有的 MIDlet 无差别的对待，都“一视同仁”的在沙箱（sandbox）中执行，且只能访问和使用少数几个系统资源，只能使用不危险的 APIs。MIDP2.0 可以对 MIDlet suite 进行数字签名，并且这些签名可以被验证。对于签名的 MIDlet suite，可以验证签名者的真伪，可以校验 MIDlet suite 的完整性。J2ME 系统对可信任的 MIDlets 开放了更多的 APIs，例如网络访问、消息(message)和 PIM APIs 等。

对 MIDlet suite 的签名和验证签名都是基于已经存在的 Internet 标准--X.509 公钥体系（X.509 PKI）。每个移动信息设备都保存了一套根证书。MIDP 中采用的 X.509 证书是基于 WAP Certificate Profile 的。MIDP 按照 PKCS#1 标准为 MIDlet suite 签名，采用的签名的算法是 RSA，计算消息摘要的算法是 SHA-1，签名的结果以 base64 格式编码并保存在 MIDlet 的应用程序描述文件（jad）中。

下载 MIDlet suite 后，移动信息设备就根据描述文件中的证书链一直验证到根证书。验证主要包括以下几点：1）证书路径是否有效；2）签名是否吻合，同时验证 MIDlet suite 是否被篡改过；3）证书是否在有效期内。MIDP2.0 规范并没有强制要求更新过期的证书，而是将这一点留作虚拟机的可选实现；如果设备实现了相关的函数，那么将采用 OCSP(Online Certificate Status Protocol)在线验证证书状态。

3.3 API 权限管理策略

MIDP1.0 的 MIDlet suite 被限制使用敏感的、对设备的软硬件系统构成威胁的 API--在这里，我们不妨称这些 API 是受保护的 API；也就是说，MIDP1.0 对待受保护的 API 的策略是通通不让用，这虽然加强了系统的安全性，但是对程序所能完成的功能限制过多了。MIDP2.0 对此进行了改进，MIDP2.0 为受保护的 API 赋予一定的权限，MIDlet suite 要使用这些受保护的 API，必须先申请相应的权限并能获得准许使用的权限。

MIDP2.0 有两种类型的权限，每种都有和用户不同的交互模式：其一是“被准许”（allowed），当受保护的 API 的权限被标识为“被准许”（allowed），MIDlet suite 请求使用这些 API 时不再需要经过用户明确的授权就可以使用；另外一种是“用户模式”（user），MIDlet suite 请求使用这些权限标识的 API 都需要经过用户明确的直接授权，授权的模式有以下三种：（1）“终身制”（blanket authorization），这个 MIDlet suite 每次调用第一次被授权的受保护的 API 都不需要再次明确被授权，除非这个 MIDlet suite 被卸载或者受保护的 API 的权限被修改了；（2）“临时制”（session authorization），在这个 MIDlet suite 当前执行期内，系统对这个 MIDlet 申请使用的受保护的 API 的授权一直有效，当这个 MIDlet suite 重新执行后，调用这里的受保护的 API 需要重新请求权限；（3）“一次性”（oneshot authorization），此次授权仅仅在当前调用有效，当受保护的 API 再次被调用时需要重新申请权限。

MIDP 中受保护的 API 数目众多，如果对每一个函数都赋予权限，那么用户执行一个 MIDlet suite 的时候，绝大部分时间都用来给每一个函数调用进行授权认可，即使授权设置为“终身制”只需要第一次调用时设置，那也是不可忍受的。因此，MIDP2.0 将这些受保护的 API 分组(group)管理，然后针对每一个组进

行权限管理，MIDlet suite 请求授权的权限都是以组为单位的。例如，MIDP2.0 为 GSM 和 UMTS 的设备定义了以下几个组：打电话（phone call）、访问网络（network access）、使用短消息和多媒体消息（messaging）、程序自动执行（application auto invocation）、使用本地连接（local connectivity）、记录多媒体信息（multimedia recording）、读写用户数据（user data access）。

MIDP2.0 应用程序非常丰富，每个移动信息设备上存贮的 MIDP2.0 的应用程序数目众多，对每一个 MIDlet 进行权限的管理也是繁琐和困难的，因此 MIDP2.0 针对不同的 MIDlet suite 进行分组管理。这就是下面要介绍的“保护域”（protection domain）。

3.4 保护域

保护域是 MIDP2.0 中的一个很重要的新概念。一个保护域有一套使用受保护的 API 的权限，这些权限被自动赋给属于这个域中的 MIDlet suite。每一个根证书--前面提到的用于验证 MIDlet suite 的数字签名--都属于一个唯一的确定的保护域。一个移动信息设备拥有一个或者几个保护域，每一个保护域都拥有一套相关的根证书。

当一个 MIDlet suite 被验证为可信任的 MIDlet 时，根据这个 MIDlet suite 的签名追溯到的根证书，这个 MIDlet suite 被划分到与这个根证书对应的唯一的确定的保护域中。一个 MIDlet 不可能既属于这个保护域，有拥有另一个保护域的访问受保护的 API 的权限。MIDP2.0 为 GSM/UMTS 的设备定义了以下的保护域[5]：（1）厂商域（Manufacturer Domain），这是功能最强大的一个保护域，包含预安装的厂商的应用程序。这个域中的所有权限都被设置为“被准许”（allowed），属于这个域的 MIDlet 可以毫无限制的使用 MIDP2.0 以及 JVM 的所有功能。（2）使用者域（Operator Domain），包含了由移动设备的使用者签名的应用程序。这个域中的所有权限都被设置为“被准许”（allowed）。（3）第三方域（Third-Party Domain），包含除厂商和使用者之外的签名的程序。这个域中的所有权限都被设置为“用户模式”（user），调用受保护的 API 需要使用者明确的批准。（4）非信任域（Untrusted Domain），包含所有没有数字签名的程序或者数字签名验证没有通过的程序。所有 MIDP1.0 的程序都属于这个域。

每一个支持 MIDP2.0 的移动信息设备都支持几个保护域，并且都精确的规定了每个保护域的权限集合，保存了和具体的 MIDlet suite 相关的授权和授权交互的模式。权限和保护域的使用，在不损失系统的安全性的前提下大大增强了系统的功能性，并且对 MIDlet 的签名本身就降低了系统受恶意程序攻击的风险，增强了系统的安全性。

3.5 引入安全网络协议 SSL 和 HTTPS

MIDP2.0 规范规定设备必须支持安全的 HTTP（HTTPS）协议。安全的 HTTP（HTTPS）是运行在安全套接层（Secure Socket Layer:SSL）上的 HTTP 协议，提供了 Internet 上的两个端点间的安全连接。MIDP2.0 同样要求设备实现 SSL 协议，以用作提供安全连接来完成安全的通信。Sun 提供的一种支持 MIDP2.0 的 J2ME 虚拟机--作为 J2ME 虚拟机的参考实现--提供了 kSSL（Kilobyte SSL）协议的实现，这个虚拟机实现了 SSLv3.0 的客户端，支持最常用而且最快的密码套件 RSA __ RC4_128_MD 5 和 RSA_RC4_40_MD5；通过 RSA 签名提供服务器认证，支持缓存重用的服务器证书和 SSL 会话；还提供 KSecurity 包，使用 Java Card API 增加了基本的加密函数— 随机数生成、加密和散列函数等，其中一些计算量密集的函数采用 C 语言写的本地方法来实现，以确保快速运行[11]。

需要注意的是，kSSL 不支持客户端的证书认证，而且也没有做为一个独立的 API 公布使用，所以不能利用 kSSL 来创建其他协议的安全连接，目前仅仅用作支持 HTTPS 协议的实现。

3.6 对安全性的分析

如前所述，MIDP1.0 的应用程序遭受各种类型的信息安全的威胁，而仅支持 MIDP1.0 的设备是不足以提供足够的安全机制来保障敏感信息的安全。虽然在后来的 3.1 节描述了 MIDP1.0 可以采用应用程序级别的安全维护，但这终究不能解决所有的问题，仅是权宜之策。那么，在前面几小节中提及的 MIDP2.0 中新引入的许多种安全机制，对信息的安全保护做的如何呢？

通过对 MIDlet suite 进行数字签名来构造可信任的 MIDlet,从而保证了应用程序的完整性和真实性。基于 X.509 PKI 的对 MIDlet 的签名的验证如果能起作用，那么就能保证 MIDlet 确实是最初签名者提供的 MIDlet，不会在网络传输或者发布的其他过程中被篡改或者替换掉。

MIDP2.0 强制规定必须支持 HTTPS 连接，从而在传输敏感信息的时候采用 HTTPS 协议取代不安全的 HTTP 连接。HTTPS 协议保证了 Internet 上的两个端点间的连接的安全性，提供了对传输的数据的机密性和完整性的保障，并且 SSL 协议在建立 SSL 连接的时候，采用服务器端的证书认证，支持了端点的认证和鉴别的功能。

对付恶意的移动代码（可从网络上轻易下载就可以执行的 MIDlet 应用程序）和 DoS 攻击，可采用只安装和执行值得信赖的保护域内的 MIDlet suite，比如厂商域或者使用者域中的应用程序，即使不是这两个域中的 MIDlet，至少也是签名了的可信任的 MIDlet。如

果仍然使用未签名的或者对签名验证不通过的 MIDlet suite，那么就会面临和 MIDP1.0 一样的对安全构成威胁的困境。

综上所述，MIDP2.0 新引入的安全机制，包括：对受保护的 API 进行权限管理、提供几个不同的保护域给不同的 MIDlet suite、增加的安全网络协议 HTTPS 和 SSL 等，保障了敏感数据比如商业信息和个人隐私数据的数据机密性、完整性，同时也提供了对服务器的认证，提供了对 MIDlet suite 的认证和发布者的鉴别能力，降低了系统遭受各种类型的攻击--包括 DoS 攻击等--的风险，从而大大提高了 MIDP 系统整体的信息安全性。

3.7 仍然存在的问题

MIDP2.0 引入了新的安全机制，相比 MIDP1.0 已经大大提高了系统的信息安全，但并没有解决全部的安全问题，在 MIDP2.0 中安全依然存在问题，下面简要分析之：

可信任的 MIDlet 基于 X.509 PKI，但是 PKI 系统也时时承受着安全的威胁和攻击，如果 PKI 系统被攻破，比如攻击者将格式正确的根证书安装到移动信息设备的系统中，或者某个根证书由于安全问题已经在 Internet 上被取消了但是设备并没有同步取消这个根证书，那么可信任的 MIDlet 就不再值得信赖了，并且由于可信任的 MIDlet 的权限非常大，对系统的安全的危害性更大。关于 PKI 系统的安全性和攻击的可能性，这里不详细讨论了，具体可参考文献[12]。

MIDP2.0 中支持的 HTTPS 协议和 SSL 连接，增加了 MIDlet 访问网络的连接的安全性。然而，当设备试图访问一个支持和使用 https 的 Web 服务器的时候，Web 服务器给出的许多关于证书或者安全的提示、判断需要用户确认，但实际上为数众多的用户并不是很清楚什么时候选“yes”，什么时候选“No”，大多数用户也没有足够的耐心和精力弄清楚这些选择的后果。这是 https 和 SSL 协议的不安全的方面，另一方面 https 协议/SSL 协议针对网络连接进行保护，是端对端的保护，不适用于现在日益发展的 Web 服务的 Internet 模式和多播广播的传输模式，而 MIDP2.0 并没有为此提供统一的解决方案。

以上简单分析了 MIDP2.0 中仍然存在的安全问题，其中一些问题虽然在 MIDP2.0 中存在，但并不是 MIDP2.0 中独有的，同时也是其他领域如 Internet 上的信息安全问题。总的来说，MIDP2.0 新引入的安全机制，解决了 MIDP1.0 中存在的安全问题，但并没有完全解决所有的移动信息相关的安全问题。

4. 结论

MIDP1.0 没有提供任何保障信息安全的机制，也没有提供公开使用的安全相关的 API 和函数实现，这使得仅支持 MIDP1.0 的移动信息设备不能处理需要强安全保障的商业机密信息和个人私密信息，同时也增加了丢失或者损坏移动信息设备的信息安全的风险，留下了一些信息安全问题。虽然应用程序自身可以维护一些安全信息，利用第三方产品提供另外的安全机制，但让程序自身处理安全问题，对应用程序不仅繁琐而且很难实施。

MIDP2.0 引入新的安全机制，尝试解决 MIDP1.0 遗留的安全问题和移动信息的其他安全问题。采用基于 X.509 PKI 体系来对发布到 Internet 上的 MIDlet suite 数字签名，防止了 MIDlet 在网络传输或存贮的过程中被修改或者被替换了，从而保证了 MIDlet 的真实性和完整性；将不同来源的 MIDlet 划分到拥有不同权限集合的保护域，避免了设备受到恶意程序的攻击；对受保护的 API 分组管理并对每组设定权限控制策略，从而不损失安全性的前提下大大提高了设备的功能；使用基于 SSL 的 https 连接来保证 MIDlet 连接 Internet 的数据的安全性。总的来说，MIDP2.0 引入的新的安全机制和措施，解决了 MIDP1.0 中的部分的安全问题，也降低了系统被攻击的风险；但这些新的安全策略也不是万能的，MIDP2.0 仍然存在一些安全相关的问题。这些问题，相信随着移动信息设备的硬件水平的提升和 Internet 上的信息安全的研究水平的提高，都将在不远的将来得到很好的解决。

参考文献

[1] 孙开翠,王汝传,杨立扬.J2ME 中 CLDC 的安全性机制的研究[J].通信技术,2003/08.P106

[2] 曹军,罗蕾.MIDP2.0 及其移植技术分析[J].单片机与嵌入式系统应用,2004.P36

[3] -.Message Authentication, Integrity, and Non-repudiation from Paper to PKI[OL],http://www.imforumgi.gc.ca/

[4] 刘赛,熊律,吴晶,王剑昆. Java 卡平台安全性研究与应用[J]. 计算机工程与设计. 第 25 卷第 10 期.P1753-1759.

[5] JCR.MIDP 2.0/1.0 specification[S]. http://jcp.org/en/jsr/detail?id=118/37，2002.11

[6] Monly M, Pautet M-B.The GSM system for mobile communications[M]. 北京.电子工业出版社, 1996 . 1499

[7] S. Jun-Zhao, D. Howie, A. Koivisto, and J. Sauvola,.A hierarchical framework model of mobile security.[R] in Personal, Indoor and Mobile Radio Communications, 2001. IEEE, 2001.

[8] 熊江,顾君忠.无线局域网络安全性的研究[J].计算机科学,2003 .Vol.30 No.7 P.42-45

[9] L.Tarkkala.Attacks against A5[OL]. http://www.hut.fi/u/ltarkkal/netsec.ps

[10] 聂成蛟,王乘.数字签名技术在 J2ME/MIDP 程序中的应用[J].微机发展.第 14 卷第 9 期.P50-52

[11] 周赞,谢炜,高传善.基于 J2ME 的无线应用的安全性[J].计算机应用与软件.2004.第 21 卷第 8 期.P100-102.

[12] C. Ellison and B. Schneier, “Ten Risks of PKI: What You’re not Being Told about Public Key Infrastructure,” Computer Security Journal, 1, 2000.

基金项目：国家高技术研究发展计划（863 计划）项目（编号 2001AA113400）
收稿日期：2005-03-04

作者简介：笪五三(1981-)，男，安徽省桐城县人，硕士研究生，主要研究方向：构件技术，嵌入式操作系统。杨维康（1959-），男，北京人，清华大学信息技术研究院操作系统与中间件技术研究中心主任，博士，主要研究方向：操作系统，构件技术。