

Java 卡安全性研究

张雪莲, 吴震, 杜之波, 王敏, 向春玲

(成都信息工程大学信息安全工程学院, 四川 成都 610225)

摘要: 为了保护个人隐私以及财产的安全性, 提出了 Java 卡安全性研究。在系统论述 Java 卡基本组成结构的基础上, 对逻辑攻击、故障注入、联合攻击等攻击方式的研究工作进行了总结, 探讨了其中存在的一些问题, 进一步对各种攻击方式提出了相应的防御措施并分析其存在的不足。最后对未来的研究方向进行了展望。

关键词: Java 卡; 逻辑攻击; 故障注入; 联合攻击; 防御措施

中图分类号: TP39

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2017.00173

Research on Java card security

ZHANG Xue-lian, WU Zhen, DU Zhi-bo, WANG Min, XIANG Chun-ling

(School of Information Security Engineering, Chengdu University of Information Technology, Chengdu 610225, China)

Abstract: To protect privacy and the safety of property, the security research of Java card was proposed. On the basis of systematically discussing the basic composition of Java card, the key of attacking methods were summarized, including logical attack, fault injection and combined attack. At the same time, some problems with the attack process were presented. Moreover, some corresponding countermeasures were put forward and their shortages were analyzed. Finally, the future research direction was prospected.

Key words: Java card, logical attack, fault injection, combined attack, countermeasure

1 引言

Java 卡是基于 Java 编程技术开发的多应用智能卡, 以多应用的支持、良好的安全特性、面向对象的编程环境、应用程序动态下载等众多优点成为智能卡技术在网络时代的主流应用, 同时也使这一技术成为智能卡领域研究和发展的热

门^[1]。随着磁条卡被发现存在着许多安全隐患, Java 卡开始广泛应用于通信、医疗、银行、国家电网等众多领域。由于卡片内存储着一些很有价值的敏感信息(个人的身份信息、密钥等), 因此一直以来都是黑客攻击的目标。Java 卡规范在制定时充分考虑了安全特性, 并提供了几种安全机制^[2]: 通过防火墙机制将各应用进行隔离以确保

收稿日期: 2017-02-28; 修改日期: 2017-04-23。通信作者: 吴震, wzhen@cuit.edu.cn

基金项目: 国家重大科技专项基金资助项目 (No.2014ZX01032401-001); 国家高技术研究发展计划 (“863” 计划) 基金资助项目 (No.2012AA01A403); “十二五” 国家密码发展基金资助项目 (No.MMJJ201101022); 四川省科技计划项目基金资助项目 (No.2017GZ0313); 四川省教育厅科研基金资助项目 (No.17ZB0082)

Foundation Items: The National Science and Technology Major Project (No.2014ZX01032401-001), The National High Technology Research and Development Program (863 Program) (No.2012AA01A403), “The 12th Five-Years” National Cryptogram Development Fund (No.MMJJ201101022), Sichuan Provincial Science and Technology Support Programmer (No.2017GZ0313), The Project of Provincial Education Department Key Scientific Research of Sichuan Province (No.17ZB0082)

运行环境的安全性; Java 卡虚拟机(JCVM, Java card virtual machine)检查堆栈和缓存溢出以保证非法的内存访问; Java Card 3.0^[3](标准版(classic edition)和连接版(connected edition))连接版本强制在卡上进行字节码校验(BCV, bytecode verifier)确保了执行程序的类型安全。另外, Java 卡产品一般也都实现了 Global Platform 规范,能够对卡片中应用的下载、安装、个人化和删除达到安全管理的目的。虽然有如此多的保护措施,但是攻击者还找到了不同的方法来攻陷智能卡的安全体系。

密码算法的实现都是以硬件为载体的,针对硬件层面普遍使用物理攻击方式中的故障注入。它的研究主要在密码分析领域^[4],但也可以对任何代码层产生威胁。虽然故障注入能够在智能卡攻击方面改变智能卡内存单元或寄存器的内容^[5],但是这对硬件设备和技术要求比较高,相比之下,软件层面的攻击则不需要专门的设备作为支撑。在 Java 卡 3.0 版本发布之前,要实现卡上字节码校验功能的代价较大,此时字节码校验都是在卡外执行的。在此背景下,攻击者能够实施软件层面的逻辑攻击,经典的攻击方式是修改已经通过卡外校验的应用程序的 CAP 文件,使其变成恶意的应用后装载到卡片上。然而,Java 卡 3.0 连接版引入强制卡上字节码校验的新特性,使直接加载恶意程序不再可能,于是出现了一种将硬件层面的故障注入与软件层面的逻辑攻击相结合的新型攻击方式——联合攻击^[6]。联合攻击利用故障

注入绕过某种安全机制,使攻击能够在新版本的 Java 卡平台实施。联合攻击不仅弥补了逻辑攻击只能依赖于未经验证的恶意程序进行攻击的不足,而且能够永久地改变或访问卡上敏感信息,成为目前智能卡攻击的主流攻击方式之一。

2 Java 卡系统架构

Java 卡是在智能卡硬件系统基础上,在片内通过软件构造的一个支持 Java 程序下载、安装并运行的软、硬件系统。其基本系统架构由以下部分组成:底层硬件及操作系统、Java 卡虚拟机(JCVM, Java card virtual machine)、Java 卡的运行时环境(JCRE, Java card runtime environment)、应用程序编程接口(API, application programming interface)和装载的应用(applet)^[7],如图1所示。其中 JCVM 负责执行字节码(byte code)以及实现内存的自动管理机制^[7]。由于智能卡本身有限的硬件资源,故不能在卡上实现全部 JCVM 的功能,因此 Java 卡虚拟机分为卡内、卡外虚拟机这两部分。卡外虚拟机主要负责将编译后的 class 文件转换为更加紧凑、高效的下载安装文件,即 CAP 文件;卡内虚拟机是 Java 卡的核心,一般由智能卡商开发并提供给用户;JCRE 层承载了卡上所有 applet 和对象之间的通信,担任了对象通信过程中的超级管理员职责;Java 卡 API 是一套供应用开发人员调用的开放 API,它使程序员在开发应用过程中只需关心其功能的实现,不用关心底层硬件相关的各属性,

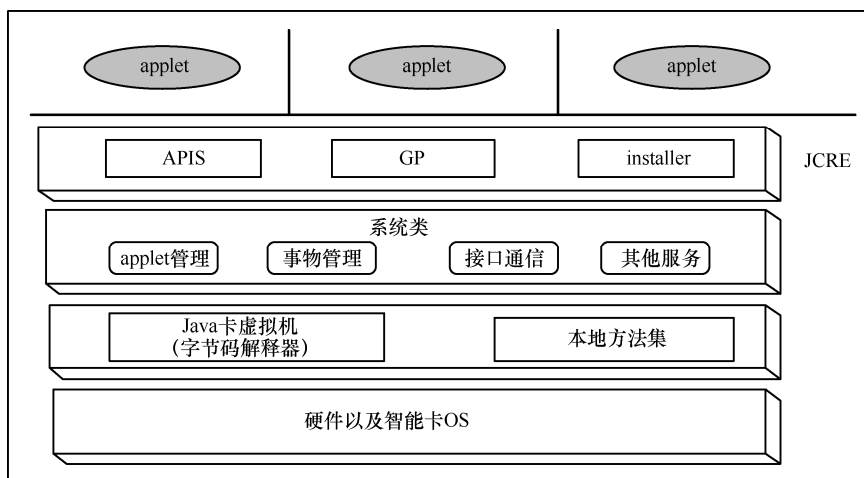


图1 Java 卡系统组成结构

并且可跨平台使用,开发者只需熟练掌握相关编程接口即可。

3 Java 卡攻击分类

关于智能卡的攻击,从大的方面来说可以分为两类:一是硬件层面的攻击;二是软件层面的攻击。硬件层面的攻击是指借助一些专门的设备,对卡片运行时的一些物理环境进行分析或破坏,从而达到攻击的目的^[8];软件层面的攻击,即利用执行程序在 JCVm 或 JCRE 实现上的一些漏洞,通过加载不规范代码对卡片进行攻击。由于硬件层面的攻击需要借助专门的设备,其中有些设备价格非常昂贵,并且对攻击者的综合素养要求较高,需要有丰富的逆向工程经验,因此一般只有专业的安全实验室才有能力实施。相比之下,软件层面的攻击则不一定需要专业设备的支撑,花费的时间也很短,但对智能卡的安全威胁相对更大。针对 Java 卡的威胁具体可分为以下几种^[2]。

1) 逻辑攻击(logical attack):又称为软件攻击,即利用软件运行环境(如 JCVm、JCRE)针对程序上的漏洞进行攻击。

2) 物理攻击(physical attack):对 Java 卡运行时的物理环境进行分析或修改。

3) 联合攻击(combined attack):物理攻击与逻辑攻击相结合。

4) 其他攻击(other attack):在不改变硬件设备的情况下,对软件实现过程中的时间、路径、功耗等信息进行分析。

3.1 逻辑攻击

总体来说,逻辑攻击主要是由 Java 卡实现上的漏洞和有限的运行时执行安全检查导致的。2003 年, Witteman^[9]首次提出了基于 Java 卡平台进行逻辑攻击的概念。之后出现了大量的逻辑攻击,大致可归为类型转换、共享接口机制、对象共享机制、事物本身在实现上的一些漏洞攻击通信协议等大量的逻辑攻击,一些典型的逻辑攻击总结如下。

1) 恶意程序攻击

基于 CAP 文件的篡改引入类型混淆的字节码,并将修改后的应用装载到 Java 卡中,这是使恶意代码能在卡上运行最简单有效的方式。但此

方法仅适用于在卡外进行字节码校验和未签名的 CAP 文件。例如,通过卡外修改 CAP 文件将数组引用指向的目标由 byte 类型改为 short 类型,并将修改后的 CAP 文件装载到卡里。由于数组的引用值本身不存在类型这一说法,则进行类型转换时不会抛出异常。如果成功运行篡改后的应用,那么修改后可以读出原来两倍长度的数组数据,偏移溢出到原 byte 数组对象外面,导致访问其他内存空间并返回有效的结果。

2) 滥用对象共享机制

攻击者可以不直接对 CAP 文件进行篡改而是基于滥用实例共享接口的引用跨防火墙访问,此方法主要依赖于 Java 卡共享机制在实现上的缺陷,即使强制卡上字节码校验仍有效。Montgomery 等在文献[10]中详细描述了利用对象共享接口机制允许未经授权访问 Java 卡内存的攻击方法,过程如下。

① 在服务器 A 定义一个可以共享的接口,并且在接口中定义将要被客户端 B 访问的方法。

② 在服务器 A 定义一个类 C 并实现该共享接口,在类 C 里面具体实现接口中定义的方法,实例化对象 O。

③ 若客户端 B 想要访问服务器 A 中的实例对象 O 时,则可以通过调用 JCSysTem.get Applet Shareable Interface Object 方法,将访问请求和 B 的 AID 交给 JCRE 处理。

④ JCRE 把该请求发送至 A,若 A 确认请求并且 AID 合法,则可以进行访问。

此时,攻击者设计一个含有恶意代码且和客户端 B 具有相同 AID 的应用 D。应用 D 被装载到卡中之后对共享接口请求访问,由于服务器 A 只对 D 的 AID 进行检查而对其内容未进行校验,所以无法识别出应用 D 的非法行为。

针对这种攻击,可以通过在共享接口生成对象前定义多种身份校验方法识别伪造 AID 以实施防御。

3) 滥用事务机制

事物漏洞的根源在于事务机制在实现上具有一定的差异性。事物处理操作过程只对永久数据的更新有效,而对于临时对象及全局数组不能保证数据的原子性。利用事物机制在实现上的漏洞

制造类型混淆。例如,局部变量存储于栈内存中,创建的对象和非静态成员变量在堆内存中分配空间。由于存储的位置差异,导致终止事务时前者不会进行回退操作,后者会回退到最初状态(一般为0,引用值为空)。如果让不同的局部变量和成员变量指向同一引用值,终止事务会删除事务中创建的对象并释放空间,导致下一次新分配对象的引用与未正常重置的引用值相同,从而使指向同一对象地址能够访问之前的数据。当然,对事物机制的攻击确实也存在一定问题:假设非原子方法在没有事物的过程中被中断,一些卡片返回了无法预测的结果;另外,如果对象引用既指向局部变量又分配给多个实例字段,那么当事物被终止时,很难确定哪个引用应该被置空。

3.2 物理攻击

物理攻击中最有效的攻击方式是故障注入。故障注入是在某些合适的时间改变芯片的工作条件,使芯片的中间状态(如程序计数器、堆栈指针以及内存)发生改变,进而引起错误的输出或异常的旁路泄露,从而获取卡上的一些敏感信息。当然,故障注入这种错误行为会造成不可避免的随机性和不准确性,而且所需设备的成本也有很大的差异性:一般光攻击需要昂贵的设备费用,尖峰、毛刺和电磁攻击的成本比较低。因此,在成本预算较低的情况下,毛刺和尖峰攻击比较常用。根据硬件层面故障注入实施方式的不同,可以将故障攻击模型分为以下几种。

1) 尖峰脉冲攻击 (spike attack)

通过改变发送给芯片的电源信号,可能干扰计算。该攻击方式成本较低且不会对芯片造成永久性伤害,但空间精度也比较低,时间精度取决于电压降在持续时间与目标芯片同步的准确度。

2) 毛刺攻击 (glitch attack)

通过修改芯片工作电压或时序电压扰乱芯片运算。这种攻击可以不留下任何篡改的痕迹,其产生的错误也是暂时的,不会对芯片造成任何损失。但在实际攻击过程中对时钟的修改技术具有一定的难度,随着目标设备攻击频率的增大,攻

击难度会相应增大。

3) 电磁扰乱攻击 (electromagnetic perturbation attack)

电磁扰乱攻击主要通过通过在内存单元附近产生强大的磁场,导致内存中表示状态的离子在内存空间杂乱无章地到处移动,以达到干扰的效果。电磁干扰会影响整个攻击设备,有可能会对芯片造成永久性改动。电磁扰乱攻击比毛刺攻击的时间精度稍微低一些。

4) 光学攻击 (optical attack)

光学攻击需要光能够穿过保护层直接到达芯片,一方面可以通过特定波长的光聚焦到一起,实现内存单元的逆转;另一方面可以通过光电效应,改变和修改内存单元的内容。由于该攻击技术允许攻击者攻击芯片底部部分电路,所以可能会永久地烧坏芯片。该技术的优点是可以更高效注入单个或多个故障,并且能达到较高的时间和空间精度。但实施该技术不仅需要花费巨大的成本,而且还需要攻击者具有一定逆向工程的能力。

3.3 联合攻击

2009年之前对Java卡逻辑攻击的方式,基本上都是通过篡改CAP文件和Java卡自身实现上的一些缺陷。但随着Java卡3.0版本的逐步推广,Java卡3.0连接版强制在卡上进行字节码校验这一新特性使仅修改CAP文件的逻辑攻击不再具有可行性。2010年,Barbu等^[6]提出了联合攻击的概念。联合攻击实施起来操作比较复杂,涉及故障注入以及代码攻击这2个攻击过程。下面以文献[11]中如何攻击操作数栈为例说明。

操作数栈是整个Java虚拟机里一个至关重要的数据结构。所有的Java指令都涉及将数据加载到栈中、对栈上的数据进行运算以及将操作结果压回栈等一系列操作。Java卡里的操作数栈保存在调用Java方法所产生的栈帧里面,这也是Java卡RAM的一段存储空间。

实例混淆是将一个类(或是某个接口实现的)的实例i当作同一个类(或是同一接口实现的)的另一个实例i*来使用。如果来自2个不同应用进行实例混淆,则必须绕过防火墙应用。在Java卡3.0规范中,引入了认证服务(authentication

service) 的概念, 这个认证服务由一系列接口的方式实现, 如图 2 所示。图 2 中认证服务的接口提供了 3 种重要方法, 其中, `check` 方法用来验证用户, `isvalidated` 方法用来检查用户是否验证成功, `reset` 方法用于重置用户认证状态, 由于这些方法都是共享对象, 因此可以通过 Java 卡防火墙应用。

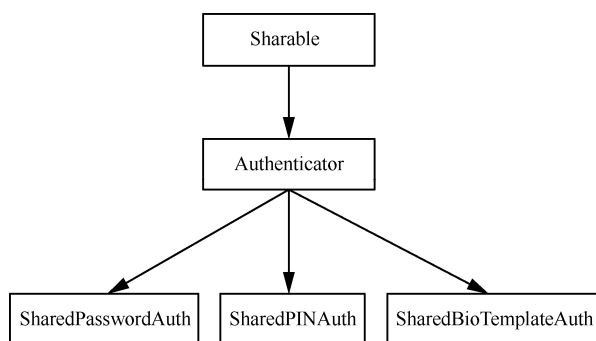


图 2 Sharable 接口的组织结构

假设被攻击的应用提供了 `SharedPassordAuth` 这个接口给其他应用, 然后攻击者创建一个应用, 包含实现了 `SharedPasswordAuth` 接口的若干个实例, 只需产生一个故障使实例里的 `check` 和 `isValidated` 方法的返回值总是真, 则攻击者自己伪造的认证服务实例将会与真正的认证服务实例成功混淆, 认证就会通过, 从而获得非法访问。由于实验在 Java card 2.2.2 版本没有认证接口, 因此下面使用一个共享接口证明该方法具有可行性。

① 在应用中定义一个共享接口 `I`, 并在共享接口中定义共享接口方法。

② 创建实现了共享接口 `A` 类的一个实例 `a` 和实现了共享接口 `B` 类的 256 个实例 ($b_0 \sim b_{255}$)。

③ 通过虚拟方法 `getA` 方法获取 `A` 类的一个引用, 并将其存储到 `I` 类型的局部变量 `a` 中, $Ia = getA()$ 。

④ 在将 `a` 压到栈顶时产生一个故障, 迫使 `a` 变成 `B` 类实例的引用。

实验结果: 在进行了 10 000 次攻击之后, 8.74% 的概率成功将 `a` 混淆为 `B` 的实例, 25.42% 的概率 `a` 仍然是 `A` 的实例, 其余情况卡片抛出异常或阻塞, 最后没有返回。实验表明, 针对操作数栈进行故障攻击达到实例混淆的方法具有可行性。

3.4 其他攻击

侧信道攻击: 利用密码设备在运行过程中的执行时间、功率消耗、电磁辐射等信息泄露和密码算法的设计和实现特点进行攻击的方法^[12]。由于侧信道攻击具有低成本、攻击效果显著的特点, 所以严重威胁了 Java 卡等密码设备的安全性。

Vermoen 等^[13]提出了基于 Java 卡逆向工程进行功耗分析的攻击实验, 为了能够逆向 applet 每一个字节码指令的轨迹, 还专门对 JVM 不支持的指令序列进行了测定。目前, 此种攻击方式已经成功被应用于商业用途。

4 防御措施

4.1 逻辑攻击防御措施

1) 引用对象类型检查

由于数组具有多种不同的类型, 在使用某个指令加载数组中特定类型的数据时, 数组引用只能指向该类型的数组。这意味着数组的引用只能指向一个 `short` 类型的数组。

2) 强制卡上字节码校验

强制卡上字节码校验这一功能能有效地防止基于 CAP 文件篡改的逻辑攻击。

3) 制定更规范的 Java 卡规范

利用 Java 卡规范使客户端和服务端不通过共享接口就能意识到彼此的服务器端和客户端, 从而避免滥用共享接口。

4) 正确执行终止操作

规范代码的书写, 切勿滥用。以便当事物操作被终止时能进行正确的回退操作。

4.2 物理攻击防御措施

1) 在芯片中增设传感器来监测芯片工作环境的变化, 一旦监测到恶意攻击, 立即启动自毁机制, 从而避免敏感信息的泄露。

2) 采用健壮的硬件设计, 通过设计多层电路, 限制微型探针探测; 增加检测电路, 防御毛刺注入、激光注入等对芯片的干扰, 使芯片工作处于稳定正常状态。

3) 在密码算法层面, 采用安全的算法设计, 能够对算法的运行状态进行检测, 最大程度防止错误注入的引入, 进一步提高芯片的安全性。

4.3 联合攻击法防御措施

1) 冗余检查

对于操作数栈,防止故障注入最简单有效的方法是冗余法。即在入栈和出栈时都做一次检查,进而比较栈顶元素和所期望的值是否一致。但该方法也存在一些不足:只能发现在入栈和出栈瞬间写入或读取数值的异常,而对入栈后出栈前这段时间内栈内元素的突变不能及时检查出来。另外,如果对入栈和出栈的瞬间都进行冗余检查操作,势必会对 Java 卡的性能造成一定的影响。

2) 诱导错误到当前上下文

利用 JCRE 规范中的应用防火墙机制将潜在的错误传播到当前上下文。如果当前上下文被改变,那么它在调用本身所创建对象的方法或访问对象的属性时会被防火墙禁止而抛出异常。尽管将故障的检测传递到防火墙来完成,实现起来会相对简单并且也降低了冗余检查带来的开销,但此方法也存在不足之处:有可能在应用防火墙中打开一个缺口,从而对 Java 卡中的其他应用造成安全隐患。

3) 强制隔离内存区域

针对不同上下文的内存区域实施强制隔离,可以有效地防止攻击者访问敏感上下文。对于嵌入式系统智能卡来说,从硬件的角度进行防御可以通过 ARM 中配备的有效保护系统资硬件控制,如内存保护单元(MPU, memory protection unit),实现强制隔离。

4.4 侧信道攻击防御措施

1) 降低侧信道信息泄露。例如,采用平衡电路降低信号能量,设置金属防护抑制电磁辐射等措施。

2) 执行并行随机处理以加大幅值对噪声的影响。例如,将内部编程电压产生电路用作并行噪声发生器。

3) 用随机值隐蔽中间媒介值。能量的泄露取决于一个数据中的位数。如果在实际数据上加上随机数据,处理完之后再减去,那么传递的路径将不会泄露有用的信息。不过,这种隐蔽会导致传递函数的非线性并产生错误的结果。因此,这些函数需要仔细地重新设计,以补偿由随机数据引起的背离。

5 结束语

近年来,随着磁条卡暴露出的诸多安全隐患,具有集多应用于一身的芯片卡迅速占领了国内市场,一卡通天下的愿景也逐步成为了现实。与此同时,金融诈骗等案件日益上升,随着 Java 卡的广泛应用凸显出了其存在的安全性。未来对 Java 卡的攻击主要还是从软件层面对嵌入式系统漏洞的挖掘入手(例如,卡删除应用时是否所有相应的内存清空,虚拟机非法指令实现上的差异性,AES、RSA 等密码算法的密钥是否安全)。对 Java 卡的保护是一个软硬件相互协同的过程,仅从软件层面不能根本解决问题,只有在强有力的硬件保护机制下才能将 Java 卡安全性发挥到极致,进而为国家安全、社会稳定和经济的发展做出巨大贡献。

参考文献:

- [1] 党彦峰. Java 智能卡软件平台的设计与实现[D]. 上海: 上海交通大学, 2008.
DANG Y F. The design and implementation of Java smart card software platform[D]. Shanghai: Shanghai Jiao Tong University, 2008.
- [2] SÉRÉ A A K, JULIEN I C, JLANET J L. Evaluation of counter-measures against fault attacks on smart cards[J]. International Journal of Security and Its Applications, 2011, 5(2): 49-60.
- [3] 于晖. 基于混合攻击的 Java 卡 3.0 安全性研究[J]. 信息安全与通信保密, 2014(9): 125-128.
YU H. Security study on Java card 3.0 based on hybrid attack[J]. Information Security and Communications Privacy, 2014(9): 125-128.
- [4] AUMÜLLER C, BIER P, FISCHER W. Fault attacks on RSA with CRT: concrete results and practical countermeasures[C]//The International Workshop on Cryptographic Hardware and Embedded Systems. 2002:260-275.
- [5] GIRAUD C, THIEBEAULD H. A survey on fault attacks[M]//Smart Card Research and Advanced Applications. Berlin: Springer, 2004: 159-176.
- [6] BARBU G, THIEBEAULD H, GUERIN V. Attacks on Java card 3.0 combining fault and logical attacks[C]// The International Conference on Smart Card Research and Advanced Application, IFIP Wg 8.8/11.2. 2010:148-163.
- [7] WU Y C, SUN Y Q. Analysis and research of securing from attack for java card[C]//The International Conference on E-Business and E-Government. 2010:1296-1298.

- [8] CHAUMETTE S, SAUVERON D. An efficient and SIMPLE way to test the security of Java cards TM[C]//The International Workshop on Security in Information Systems.2006:331-341.
- [9] WITTEMAN M. Java card security[J]. Information Security Bulletin, 2003, 8(10): 291-298.
- [10] MOSTOWSKI W, POLL E. Malicious code on Java card smart-cards: attacks and countermeasures[C]//The International Conference on Smart Card Research and Advanced Applications, IFIP Wg 8.8/11.2. 2008:1-16.
- [11] BARBU G, DUC G, HOOGVORST P. Java card operand stack: fault attacks, combined attacks and countermeasures[M]//Smart Card Research and Advanced Applications. Berlin Heidelberg: Springer, 2011:297-313.
- [12] PAUL C. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems[M]//Advances in Cryptology — CRYPTO '96. Berlin: Springer, 1996:104-113.
- [13] VERMOEN D, WITTEMAN M, GAYDADJIEV G N. Reverse engineering Java card applets using power analysis[C]//The International Workshop on Information Security Theory and Practices. Smart Cards, Mobile and Ubiquitous Computing Systems, First IFIP TC6 / WG 8.8 / WG 11.2.2007:138-149.



吴震（1975-），男，江苏苏州人，成都信息工程大学副教授，主要研究方向为信息安全、密码学、侧信道攻击与防御、信息安全设备设计与检测。



杜之波（1982-），男，山东聊城人，成都信息工程大学讲师，主要研究方向为信息安全、侧信道攻击与防御、天线应用和物联网安全。



王敏（1977-），女，四川资阳人，博士，成都信息工程大学讲师，主要研究方向为网络攻防、侧信道攻击与防御。

作者简介:



张雪莲（1992-），女，四川达州人，成都信息工程大学硕士生，主要研究方向为信息安全、智能卡安全。



向春玲（1990-），女，湖北宜昌人，成都信息工程大学助教，主要研究方向为信息安全、密码学、侧信道攻击与防御、智能卡安全。