基于 FPGA 的可信平台模块攻击方法

李健俊[1]，方 娟[2]，季 琦[1]，刘 鹏[1]，毛军捷[2,5]，林 莉[2]，姜 伟[2,3,4]
(1. 浙江中烟工业有限责任公司，杭州 310009；2. 北京工业大学 计算机学院，北京 100124；
3. 中国科学院软件研究所 信息安全国家重点实验室，北京 100190；
4. 公安部第三研究所 信息网络安全公安部重点实验室，上海 201204；
5. 中国信息安全测评中心，北京 100085)

摘 要： 为测试可信计算平台的安全性，提出了一种使用现场可编程门阵列(field program gate array，FPGA)搭建监控平台，针对可信平台模块被动工作模式的特点，采用监听、篡改和伪造输入数据等手段对可信平台模块进行攻击，达到攻击可信计算平台的目的. 实验结果证明，现有可信计算平台存在中间人攻击的安全隐患.

关键词： 可信计算；现场可编程门阵列(FPGA)；可信平台模块(TPM)；被动模式
中图分类号： TP 309 **文献标志码：** A **文章编号：** 0254 - 0037(2013)01 - 0070 - 06

FPGA-based Trusted Platform Module Attack

LI Jian-jun[1], FANG Juan[2], JI Qi[1], LIU Peng[1], MAO Jun-jie[2,5], LIN Li[2], JIANG Wei[2,3,4]
(1. China Tobacco Zhejiang Industrial Co. Ltd., Hangzhou 310009, China;
2. College of Computer Science, Beijing University of Technology, Beijing 100124, China;
3. State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing 100190, China;
4. Key Laboratory of Information and Network Security, 3rd Research Institute, Ministry of Public Security, Shanghai 201204, China; 5. China Information Technology Security Evaluation Center, Beijing 100085, China)

Abstract: To test the security of trusted computing platform, a method using the field program gate array to build a monitor platform was proposed. By monitoring, tampering with and forging input data etc, this method deceived the trusted platform module (TPM) of the passive working mode, doing attacking experiments to the existing trusted platform and TPM. Result of this experiment proves that the existence of man in the middle attack in trusted platform.

Key words: trusted computing; field program gate array; field program gate array (FPGA); trusted platform module (TPM); passive mode

目前，可信计算已经成为国内外信息安全领域的研究热点，基本思想是在计算平台上嵌入可信平台模块(trusted platform module，TPM)芯片[1]，将其作为可信计算平台的可信存储根和可信报告根，保证平台的完整性. TPM 作为密码协处理器为可信计算应用提供密码服务，其内部的平台配置寄存器(platform configuration register，PCR)用于表征平台的可信状态. 但目前 TPM 还存在一些不足尚未解决，如被动工作模式下度量根的安全性问题、待度量数据的真实性和时效性问题等，攻击者可以利用这

收稿日期：2011-01-06.
基金项目：国家“863”计划资助项目(2009AA012437)；信息网络安全公安部重点实验室开放课题资助项目(C11610)；信息安全国家重点实验室(中国科学院软件研究所)开放课题资助项目(04-04-1).
作者简介：李健俊(1970—)，高级工程师，主要从事可信计算、工业信息化方面的研究，E-mail：lijj@zjtobacco.com.
通信作者：姜 伟(1979—)，讲师，主要从事可信计算、网络与信息安全方面的研究，E-mail：j8w8@sohu.com.

些不足，对可信计算平台进行攻击. 目前针对 TPM 的攻击方法大致可归结为 2 类：软件攻击和物理攻击. 软件攻击包括拒绝服务攻击、内存数据攻击[2]、缓冲区溢出攻击、页表攻击[3]等；物理攻击包括 Reset 攻击[4-5]、旁路攻击和物理破坏攻击[6-7]等. 其中，拒绝服务攻击是指由于 TPM 单进程工作且可信设备驱动库(trusted device driver library，TDDL)是单线程同步接口[8]，当多用户访问可信软件栈(trusted software stack，TSS)或可信设备驱动(trusted device driver，TDD)时，会出现拒绝访问现象；内存数据攻击是指攻击者窃取或者篡改内存中应用程序和 TSS 代码空间；缓冲区溢出攻击是指在信任链建立过程中通过缓冲区溢出的方法攻击完整性度量操作；页表攻击是指攻击者通过修改页表指针替换度量代码和数据[3]；Reset 攻击是指使用复位命令或者物理方式复位 TPM 的 PCR 值，然后再将 PCR 恢复成理论值以欺骗远程验证方；内存的低温攻击是指在低温环境下内存单元掉电后数据仍然可以长时间保存，攻击者可以窃取内存单元中的密钥或者加密前的数据；旁路攻击是指包括温度攻击、功率攻击和能量脉冲攻击，大都通过入侵式攻击和反向工程的方法获取 TPM 的设计信息，以获得密钥等重要数据.

在 TCG 规范中，规定 TPM 作为独立模块通过低针脚(low pin count，LPC)[9]总线与计算机主板相连接，但忽视了中间人攻击方法. 本文针对 TPM 的从设备工作方式，提出了一种基于 FPGA 的攻击平台对 TPM 进行中间人攻击的方案，形式化证明了 TPM 的从设备工作模式存在安全性问题，并对 TPM 芯片进行攻击测试，证明了该攻击方案的有效性.

1　基于 FPGA 的攻击方案

1.1　可信平台完整性相关原理

可信平台的完整性是衡量平台可信度的重要依据. 可信平台的完整性度量是指通过判断代码或数据与参考值的一致性来表征平台完整性的方法，其包括静态度量和动态度量. 静态度量是针对程序和数据加载前进行检查，以保证程序运行时平台的安全性，其主要度量对象包括计算机启动过程参与控制权转移的各个部件以及运行的程序代码. 动态度量主要是针对操作系统环境中活动的进程或模块进行实时的完整性度量和监视，度量对象包括进程代码和参数堆栈等[10].

定义 1　完整性度量：

$$P_n = \text{SHA-1}(P_o \parallel M)$$

式中：P_n表示平台配置寄存器的新值；P_o表示平台配置寄存器的旧值；SHA-1 表示杂凑运算函数；M 表示待运算的数据.

通过定义 1 可知，无论静态度量还是动态独立，其度量值是以拼接后度量的方式进行杂凑运算，最终形成 160 位的摘要值存储在 TPM 中指定的平台配置寄存器，用于表征任何长度的计算平台的配置信息.

定义 2　远程证明：

$$\text{Message} = \text{Sign}\{P, K_i\}$$

式中：Message 表示本地发送给远程验证方的认证信息；P 表示本地平台的所有平台配置寄存器值 PCR；Sign 表示使用密钥 K_i 对 PCRS 值进行数字签名，当第三方需要验证目的计算平台的完整性时，目的计算平台的操作系统会把 TPM 的完整性度量值加密和签名后发送给第三方进行认证.

定义 3　数据封装：

封装　$S = \text{Encrypt}((D \parallel P \parallel T), K)$

解封　$D \parallel P \parallel T = \text{Decrypt}(S, k)$

式中：S 表示被封装后的数据；Encrypt 表示封装操作；Decrypt 表示解密操作；$\parallel$ 表示数据拼接操作；D 表示原始数据；P 表示 PCR 值；T 表示平台证明信息；K 表示密钥.

将数据与特定的平台配置特征信息(PCR 值)及 TPM 绑定在一起，这种操作称为数据封装. 数据解封装后 TPM 需要判断 P 和 T 是否正确.

通过上述定义可知，TPM 中存储的 PCR 值关系到平台的私密性和平台的可认证性. 在 TCG 规范中规定，计算机每次执行 Reset 操作时，都要对 TPM 的 PCR 进行复位操作，然后再按照计算机启动流程，依次重新计算平台的 PCR 值. 当平台的 PCR 值与某状态下的 PCR 值一致时，使用此时的 PCR 值才可以成功解出加密数据和验证数字签名. 因此，只要攻击者企图获取保密信息的目标就可以变成 PCR 的攻击.

1.2　安全问题分析

只要提供同样的待度量数据，度量结果 PCR 值就相同，因此，攻击者通过伪造待度量数据，就可以轻易实现对可信计算平台的远程证明和数据封装的攻击. 此外 Biba 模型规定，禁止一个主体向更高等级的可信客体写入数据[11]. 如果一个主体需要改变一个具有更高可信度的客体时，它可能会导入不正确的或者伪造的信息，同时客体的可信度将会降低[12]. TPM 作为可信根是整个计算平台中安全级

别最高的部件,却工作在被动模式,被系统调用. 在计算平台上,软件代码的执行单元(处理器)通过可信度较低的部件(南北桥控制器和总线)向 TPM 写入数据,攻击者可以通过此方式篡改输入数据欺骗 TPM,达到提高计算平台可信度的目的. 因此,现有的计算平台对 TPM 的使用与 Biba 模型的策略不一致.

1.3 攻击原理分析

现有 TPM 与主板的 LPC 总线相连接且工作在被动方式. 针对 TPM 的此种特点,本文的攻击方法主要以待度量的数据和 TPM 内部的 PCR[1] 为攻击对象,利用 FPGA 设计通讯监控模块,嵌入到计算平台与 TPM 之间实施中间人攻击,监听在信任链建立过程中 CPU 与 TPM 之间的交互数据,再由 FPGA 伪造信任链部件代码和启动序列,以过滤、重发、篡改等方式欺骗 TPM.

下面使用通讯顺序进程(communicating sequential processes, CSP)[13-16] 描述 CPU 与 TPM 之间数据通讯过程,通过伪造待度量的输入数据,分析可能存在的安全问题,实现对基于 TPM 度量流程的攻击,证明本攻击方案的可行性. C_i 表示部件的代码; Process(C_i) 表示 C_i 对应的进程; Process(C) = {Process (C_i)}, $i=1,2,3$; ^表示若干个判断条件之间的与逻辑操作; B 表示进程; CMP. B. TPM. V. V^F 表示 B 判定 TPM 提交的度量结果 V 与完整性度量参考值 V^F 是否一致; Trust. B. Process(C_i) 表示进程 B 信任进程 Process(C_i). 且有

$$\text{CMP. } B\text{. TPM. } V_i\text{. } V_i^F = \begin{cases} \text{TRUE}, & \wedge(V_i = V_i^F) \\ & i=1,2,3 \\ \text{FALSE}, & \text{其他} \end{cases}$$

可信平台上电启动过程是 CPU 先执行若干部件后再执行 C_1,由 C_1 将部件代码 C_2 和 C_3 发送 TPM 生成度量值,然后 TPM 将度量结果发送给远程认证进程 B. 其中,完整性度量操作参与者包括可信平台 TP、TPM 和远程认证进程 B. 在攻击过程中,攻击者先于 CPU 执行 C_1 之前,篡改 C_1、C_2 和 C_3,并将篡改前的部件代码发送给 TPM 生成度量值,达到攻击的目的. 在 CSP 描述的攻击过程中,INTRUDER、TP、TPM、B 和 SYSTEM 分别代表攻击者进程、可信平台的控制进程、TPM 的主控进程、验证进程和攻击系统对应的进程.

攻击者的行为建模如下:

INTRUDER = Env? TP: Agent
→Copy. TP. INTRUDER. ($\wedge_{i=1,2,3} C_i$)
→Change. INTRUDER. TP. ($\wedge_{i=1,2,3} C_i$). ($\wedge_{i=1,2,3} C_i^K$)
→Stop)

ENV? PC: Agent 表示攻击者 INTRUDER,先于可信平台发起活动,在 CPU 执行度量操作执行之前,先备份正确的代码,然后将事件代码 C_1、C_2 和 C_3 分别篡改成了 C_1^K、C_2^K 和 C_3^K,最后攻击操作结束. Stop 表示操作结束.

可信平台的行为建模如下:

PC = Change. INTRUDER. TP. ($\wedge_{i=1,2,3} C_i$). ($\wedge_{i=1,2,3} C_i^K$)
→Send. TP. TPM. ($\wedge_{i=1,2,3} C_i$)
→Stop)

其中 Send. TPM. B. d 表示 TPM 将数据 d 发送给进程 B. 其含义是 CPU 执行完第 1 个部件后,开始执行篡改后的部件代码 C_1^K,并将备份的部件代码 C_2 和 C_3 依次发送给 TPM 芯片,然后进行操作.

TPM 的行为建模如下:

TPM = REC. TPM. TP. ($\wedge_{i=1,2,3} C_i$)
→Hash. TPM. ($\wedge_{i=1,2,3} C_i$). ($\wedge_{i=1,2,3} V_i$)
→Send. TPM. B. ($\wedge_{i=1,2,3} V_i$) →Stop)

Hash. TPM. C_i 表示 TPM 对代码 C_i 进行完整性度量; Rec. B. TPM. d 表示 TPM 收到进程 B 发送的数据 d.

验证进程的行为建模如下:

B = REC. TPM. B. ($\wedge_{i=1,2,3} V_i$)
→if(Trust. B. Process(C). ($\wedge_{i=1,2,3} V_k$). ($\wedge_{i=1,2,3} V_k^F$) = True)
→Stop
else →Reset

上述攻击过程对应的进程 System 是子进程 INTRUDER、TP、TPM 和 B 的组合,并通过 3 个返回信号(A、A_{ok} 和 A_{error})进行同步.

攻击系统 System 的行为建模如下:

$$\text{System} = \text{INTRUDER} \underset{A}{\|} \text{TPM} \underset{A_{ok}}{\|} \text{TP} \underset{A_{error}}{\|} B$$

TPM 作为被动设备使用时,攻击者的篡改操作对 TPM 透明,无法检查度量操作的请求行为是否可信,攻击者可以通过缓冲区溢出、伪造待度量数据或复位 PCR 的攻击方法,轻易地欺骗 TPM 和远程认证进程. 显然上述认证过程中,认证进程 B 未查出进程 Process(C) 受到攻击.

1.4 攻击方法

为完整地记录计算平台向 TPM 发送的原始数据包,需要修改驱动程序或者搭建 LPC 总线的硬件

监控平台，监听通讯数据的原始数据流. 而对于支持处理器动态度量指令的 TPM，由于其若干指令对软件系统透明，则必须使用硬件监控平台. 除去使用 FPGA 搭建硬件平台对 TPM 进行监听外，还可以使用逻辑分析仪通过飞线方式监听 LPC 总线. 作者使用泰克的 TLP7200 系列逻辑分析仪时，针对不同的 TPM 将 START 位和 FRAME 位设置触发条件(trigger)[9]进行数据过滤，并记录监听数据.

1.4.1　TPM 工作流程

TCG 采用装载前度量的手段，在计算平台启动过程中采用一级传递一级的链式方法，在各部件之间传递机器的控制权. 如图 1 所示，a 表示初始化 CPU 部分的 BIOS 代码；b 表示 HASH 操作部分的 BIOS 代码；c 表示控制硬件系统部分的 BIOS 代码；d 表示完整性度量结果；e 表示 OS 引导程序；f 表示操作系统内核；g 表示 TPM 存在性确认请求信号；h 表示 TPM 操作性应答信号. 系统从一个尽量小的信任根开始启动，信任根是整个系统第一个获得控制权的模块. CPU 通过控制器读取 BIOS 代码 a 进行初始化后，将 BIOS 代码 b 读入 Cache 中执行，并将 BIOS 代码 c 的完整性度量结果 d 存储在 TPM 中，接着执行 BIOS 对 TPM 的存在性判断，然后依次对 OS 引导程序和 OS 内核进行完整性度量，最后将结果存储在 TPM 内部.

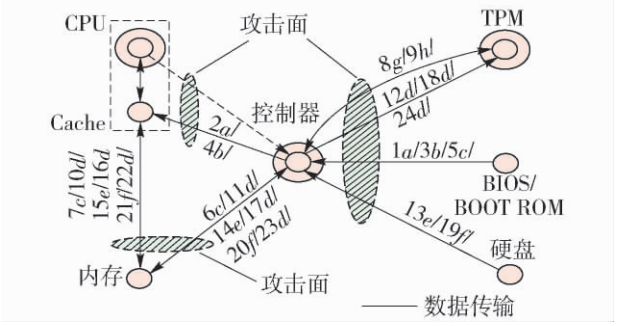

图 1　TPM 的工作流程分析

Fig. 1　Workflow analysis of TPM

1.4.2　对 TPM 的攻击流程

如图 1 所示，在对 TPM 进行攻击前，将硬件监控平台插入到 TPM 与控制器之间，并在 FPGA 中实现监听、中转、屏蔽和伪造数据等功能，具体流程如下.

1) 使用 FPGA 模拟 LPC 总线以及通讯协议、处理器特殊波形.

由于度量数据中不携带随机数，所以可以使用监听数据对 TPM 进行重放攻击. 为实现重放攻击还需要使用 Verilog 硬件描述语言和状态机，在 FPGA 上实现 LPC 总线的 HOST 端的功能. 在 LPC 总线协议中规定，HOST 和 SLAVE 不可以混合使用，两者主要区别于通讯的发起权由谁控制. 此外，针对 TCG1.2 规范中的动态度量根功能，AMD 处理器和 INTEL 处理器分别提供了 SENTER 指令和 SKINIT 指令[8]，并在此类指令中用到了特殊的 LPC 周期，因此，在监听和重放攻击中需要对此类周期进行特别处理.

2) 复位 TPM，将备份的信任链部件代码依次发送给 TPM.

可信平台及 TPM 中 PCR 的相关操作包括计算机启动阶段的完整性度量和程序运行期间的动态度量. 作为被动设备的 TPM，其完整性度量过程的输入数据来自 CPU. 在平台启动过程中，当 FPGA 在 LPC 总线上检测到 TPM 的通讯周期，并访问地址是 FED40XXXH ~ FED44XXXH 时[9]，FPGA 需要对上述周期内传输的数据进行屏蔽，并发送相应的伪造数据或参考数据. 当进行动态度量时，处理器执行 SENTER 或者 SKINIT 指令，会将 PCR17 ~ PCR23 的值(RESET)设置为 -1[8]，此后，FPGA 需要屏蔽处理器发送给 TPM 的度量数据，并将伪造的数据或参考数据发送给 TPM，并将 SLB(secure loader block)的杂凑运算结果扩展到 PCR17 中.

2　实验与分析

2.1　实验平台搭建

如图 2 所示，可信平台与 TPM 采用 LPC 总线方式连接，因此，使用 FPGA 开发板搭建包含微处理器、SDRAM、FLASH、LPC 总线 Host 控制器和 LPC 总线 Slave 控制器的硬件监控平台，并将 TPM 与监控平台的 LPC 总线 Host 控制器连接，将监控平台的 LPC 总线 Slave 控制器与可信平台连接.

攻击平台需要针对 TPM 不同的 LPC 通讯类型，

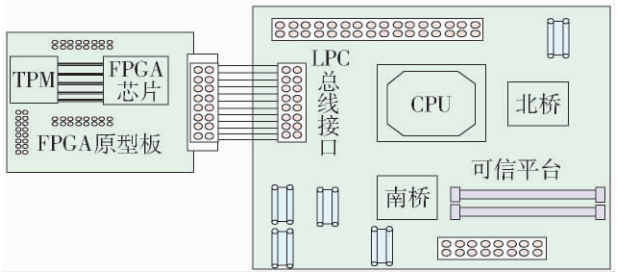

图 2　TPM 攻击实验环境

Fig. 2　Attacking experiment environment of TPM

选择不同类型的通讯时序. Intel 公司的 LPC 总线协议包括 TPM、IO、Memory、Memory Firmware 等周期类型[9],它们的不同之处在于通讯起始位以及每个通讯周期中有效数据所占周期的个数. 其中: IO 类型用于符合 TCG1.1 规范的 TPM; TPM 类型用于符合 TCG1.2 周期类型的可信芯片. 此外,考虑到 TPM 和 IO 类型的通讯速度过低,一些厂商开始使用 Memory 和 Memory Firmware 通讯类型,Memory Firmware 类型的读周期有效数据量最大可以达到 128 kB. 例如: 英飞凌 SLB9635TT1.2[17] 使用的是 TPM 类型; 瑞达 TCM[18] 使用的是 Memory Firmware 类型; 中兴 TCM[19] 使用的是 IO 类型.

2.2 实验结果与分析

本实验使用 FPGA 搭建硬件监控平台对可信平台进行中间人攻击,分别针对带有 TPM 的计算机进行攻击测试. 攻击测试的芯片包括英飞凌 TPM (SLB9635TT1.2) 和中兴 TCM. 在测试过程中,FPGA 监控平台作为中间人,依次截取 BIOS Boot Block、Post BIOS、MBR、设备的 Option ROM、操作系统内核和文件系统的待度量数据,并读取对应的 PCR 值(即表 1 所示的初始度量结果),然后篡改可信平台的上述部件,并向可信芯片发送 Reset 命令或复位 TPM 的 Reset 管脚. 在 TPM 重新启动过程中,监控平台向 TPM 发送备份的各部件的待度量数据. 实验结果发现,攻击结束后从 TPM 中读出的 PCR 值与之前的 PCR 初始度量结果一致,即达到了攻击目的.

本实验利用 TPM 的 Reset 命令或者 Reset 管脚可对可信平台的 PCR 值进行强制复位. 根据定义 1、定义 2 和定义 3 可知,当中间人攻击方式使得可信平台达到某个 PCR 值对应的状态时,又可以进一步地实现对可信平台的完整性度量、远程证明和数据封装的攻击. 通过表 1 的实验结果可以发现,本实验利用 TPM 的 RESET 操作的漏洞,采用中间人的攻击方法可以在计算机启动后,记录 Boot Block、Post BIOS、MBR、设备的 Option ROM 和操作系统的内核与文件系统对应的待度量数据,并在对可信平台的软硬件系统进行攻击后,再通过强制复位 TPM 和伪造待度量数据的方法,使得本机的验证程序和远程验证方无法获取被篡改部件的真实度量值,因此,TPM 中的 PCR 并没有真实地反映出可信计算平台当前的可信状态. 同时,在此种状态下攻击者可以很容易地获取远程验证方的信任以及对平台上存储的保密数据进行解密,甚至本机会成为对可信网络进行攻击的跳板.

表 1 对信任链组件的攻击结果

Table 1 Results after the attack to trust chain

名称	篡改目的	初始度量结果	被篡改部件的真实度量值
Boot Block	将 Post BIOS 的度量参考值发送给 TPM	7FB0F7CC333DFB91FF818 7E1D9DC166131CA4B5E	A81F18A9758F331264F48 9CF971D7F2E3904BF02
Post BIOS	将 MBR 和 Option ROM 等数据的度量参考值发送给 TPM,并禁用身份识别设备和访问控制策略	D09B7056E0D96BC8AAB7 1C202566CF0D6112FAB4	C3176B465DAAC6EF0BC8 B9D884140BAFCE62FB83
MBR	引导至其他分区	6910DDE730B800A339691 53B5A612D942C2719E0	7B41B794AA81F23F21A0 F03676E4FA23064A9ABE
设备的 Option ROM	CPU 执行被篡改的代码,与攻击者交互数据	3EF892F2470661018BC313 4E880C572D7917BD6D	085AA0E1FDF608F1DDDC D5AA7FAE4522ACF30FF3
内核和文件系统	引入黑客程序	52BE2C7780FEA913D8750 6D32258B0FD0D76FE2D	716E00E57188264129F83E 8DC547B10DFBA7A195

3 结论

本文提供了一种使用 FPGA 搭建监控平台对 TPM 等安全芯片进行攻击的方法. 针对安全芯片作为从设备的被动工作方式进行攻击实验,达到欺骗远程认证方或者窃取被 PCR 封装的保密数据的目的,并通过实验验证了本方案的有效性.

参考文献:

[1] Trusted Computing Group. TCG specification architecture overview [EB/OL]. [2011-01-15]. http://www.trustedcomputinggroup.org/groups/TCG_1_2_Architecture_

Overview. pdf.

[2] HALDERMAN Alexh J，SCHOEN Seth D，HENINGER Nadia，et al. Lest we remember: cold boot attacks on encryption keys [EB/OL]. [2011-01-15]. http://citp.princeton.edu/memory/.

[3] SPARKS，EVAN R. A security assessment of trusted platform modules [EB/OL]. Dartmouth: Computer Science Technical Report [2011-01-15]. http://www.cs.dartmouth.edu/~pkilab/sparks/thesis.ps.

[4] Trusted Computing Group. TCG platform reset attack mitigation specification version 1 [EB/OL]. [2011-01-15]. http://www.trusted-computinggroup.org/files/temp/6452209B-1D09-3519-AD815636FC36C5CF/Platform%20Reset%20Attack%20Mitigation%20Specification.pdf.

[5] KLAUS K，DRIES S，BART P. Analyzing trusted platform communication [EB/OL]. [2011-01-15]. http://www.cosic.esat.kuleuven.be/publications/article-591.pdf.

[6] 张涛. 面向密码芯片的旁路攻击关键技术研究 [D]. 成都：电子科技大学计算机科学与工程学院，2009.
ZHANG Tao. The research on the key technologies of side-channel attack oriented to cryptographic chips [D]. Chengdu: School of Computer Science and Engineering，University of Electronic Science and Technology of China，2009. (in Chinese)

[7] 李海军. 加密芯片的旁道攻击防御对策研究 [D]. 哈尔滨：哈尔滨工程大学计算机科学与技术学院，2010.
LI Hai-jun. Research on side channel attack countermeasures of encryption chip [D]. Harbin: College of Computer Science and Technology，Harbin Engineering University，2010. (in Chinese)

[8] DAVID C，KENT Y，RYAN C，et al. A practical guide to trusted computing [M]. Lebanon: IBM Press，2007: 1-35.

[9] Intel. Low pin count interface specification [EB/OL]. [2011-01-15]. http://www.intel.com/design/chipsets/industry/lpc.htm.

[10] 刘孜文，冯登国. 基于可信计算的动态完整性度量架构 [J]. 电子与信息学报，2010，32(4)：875-879.
LIU Zi-wen，FENG Deng-guo. TPM-based dynamic integrity measurement architecture [J]. Journal of Electronics & Information Technology，2010，32(4)：875-879. (in Chinese)

[11] MA Xin-qiang，HUANG Yi. Trusted computing model based on lattice [J]. Journal on Communications，2010，31(8A)：105-110.

[12] 王立斌，黄征. 计算机安全学导论 [M]. 北京：电子工业出版社，2005：20-100.

[13] 周巢尘. 通信的顺序进程及其研究 [J]. 计算机学报，1983(1)：1-9.
ZHOU Chao-chen. An applicative notation for communicating processes [J]. Chinese Journal of Computers，1983(1)：1-9. (in Chinese)

[14] 周巢尘. 通信进程的确定性语义学 [J]. 计算机学报，1983(2)：81-89.
ZHOU Chao-chen. A deterministic semantics of communicating processes [J]. Chinese Journal of Computers，1983(2)：81-89. (in Chinese)

[15] 周巢尘. 通信协议的设计 [J]. 计算机学报，1983(5)：321-329.
ZHOU Chao-chen. A rigorous approach to the design of protocols [J]. Chinese Journal of Computers，1983(5)：321-329. (in Chinese)

[16] HOARE C A R，ZHOU Chao-chen. Communicating sequential processes [M]. Beijing: Beijing Peking University Press，1990: 10-50.

[17] Infineon. Trusted platform module (SLB9635TT1.2) [EB/OL]. [2011-01-15]. http://www.infineon.com/cms/en/product/channel.html?channel=ff80808112ab681d0112ab6921ae011f&pt=db3a304329a0f6ee0129ac094b1e5603.

[18] Jetway. Jetway information security industry Co. Ltd. J281 security chip [EB/OL]. [2011-01-15]. http://www.jetsec.com.cn.

[19] Nationz. Nationz-TC trusted platform module [EB/OL]. [2011-01-15]. http://www.nationz.com.cn/en/Solutions2.aspx?id=40.

(责任编辑　梁　洁)