我国可信计算研究与发展*

张焕国 何炎祥 赵 波 彭国军 等
武汉大学

关键词：可信计算 安全计算机 信息安全

信息安全事关国家安全

信息安全事关国家安全和社会稳定，因此必须采取措施确保我国的信息安全。

信息安全主要包括设备安全、数据安全、内容安全和行为安全。信息系统硬件结构安全和操作系统安全是信息系统安全的基础，密码和网络安全等是信息系统安全的关键技术。只有从硬件和软件底层做起，从整体上采取措施，才能有效地确保信息系统的安全。

对于微机，只有从芯片、主板、BIOS（Basic Input Output System，基本输入输出系统）和操作系统做起，采取综合措施，才能提高微机的安全性。正是这一思想推动了可信计算的产生和发展。

可信计算的发展历程

国外可信计算的发展

可信计算概念最早可以追溯到1983美国国防部的TCSEC准则及之后出现的彩虹系列信息系统安全文件，1999年，IBM、HP等企业成了TCPA（2003年改名为TCG组织，主要致力于形成可信计算的工业标准，联想、兆日等国内单位已成为该组织的单位成员，武汉大学的一些教师和研究生也加入了该组织，成为其个人会员）。目前TCG已经制定了包括TPM、TSS、TNC等一系列技术规范，一些厂商也生产了可信PC、可信PDA等产品。

除此之外，还有Dependable Computing，Trustworthy Computing，欧洲的Open TC等一批不同的可信计算流派，我们认为在可信计算发展过程中，不同的专家学者从不同的角度来研究问题，出现不同的流派是很正常的，是学术研究繁荣的体现。随着可信计算技术的发展和应用，不同的流派将会逐渐融合趋同。

我国可信计算研究的一些重要事件

我国在可信计算领域起步不晚，水平不低，成果可喜。

2000年6月，武汉瑞达公司和武汉大学合作，开始研制安全计算机，2004年10月，其通过国家密码管理局主持的技术鉴定。这是我国第一款自主研制的可信计算平台。

2005年，联想公司的可信平台模块芯片和可信计算机相继研制成功。同年，兆日公司的可信平台模块芯片也研制成功。两公司的产品都通过了国家密码管理局的认证。

2006年国家密码管理局主持制定了《可信计算平台密码技术方案》和《可信计算密码支撑平台功能与接口规范》两个规范。

2007年在全国信息安全标委会的主持下，我国开始制定了一系列的可信计算标准，包括芯片、主板、软件、网络连接、测评等标准。

*国家自然科学基金项目（60673071）、国家863计划项目（2006AA01Z442，2007AA01Z411）资助。

国家自然科学基金委启动了“可信软件重大研究计划”。深圳中兴集成电路公司的“可信计算机密码模块安全芯片”和联想公司的“可信计算密码支撑平台”通过国家密码管理局的认证。

2008年中国可信计算联盟（Community Trust Credit Union，CTCU）成立。北京兆日公司的“可信计算机密码模块安全芯片”和“可信计算密码支撑平台”、深圳中兴集成电路公司的“可信计算密码支撑平台”通过国家密码管理局的认证。在国家863计划项目的支持下，武汉大学研制出我国第一款“可信PDA”和第一个“可信计算平台测评软件系统”。

2009年瑞达公司的“可信计算机密码模块安全芯片”通过国家密码管理局的认证。

至此，我国的可信计算技术与产品得到了国际同行的高度评价，已经站在国际可信计算领域的前列。我国的可信计算事业进入了蓬勃发展的阶段。

可信计算的基本思想与主要技术

可信计算组织认为，可信计算的总体目标是提高计算机的安全性。现阶段的主要目标为：确保系统数据的完整性，提供数据的安全存储、平台身份和可信性的远程证明。可信计算技术与产品主要用于安全风险管理（使发生安全事件时的损失降至最小）、安全检测与应急响应（及时发现攻击并采取相应措施）、电子商务（减少电子交易的风险）和数字版权管理（阻止数字媒体的非法复制）等。

可信计算的基本思想

可信计算组织用行为定义可信：如果一个实体的行为总是以预期的方式达到预期的目标，那么它是可信的。可见，可信计算组织对可信的定义强调了行为的预期性。

可信计算的基本思想是：首先在计算机系统中建立一个信任根，再建立一条信任链，从信任根开始，经过硬件平台和操作系统，再到应用，一级测量认证一级，一级信任一级，从而把这种信任扩展到整个计算机系统。

可信计算组织的这种可信计算的思想源于社会，是把人类社会成功的管理经验用于计算机系统。

可信计算的主要技术

可信计算是一种新的信息系统安全技术，但是它所使用的具体技术都是信息安全的成熟技术。其主要技术包括：信任根技术、信任链技术、可信支撑软件技术、可信计算平台技术、平台证明技术、可信网络连接技术等。

我国可信计算的研究与发展

可信的理论研究

可信的定义与属性

可信的定义 可信计算首先要回答什么是可信。目前，关于可信尚未形成统一的定义，不同的组织机构有不同的解释。主要有以下几种说法。

（1）可信计算组织用实体行为的预期性来定义可信：如果一个实体的行为总是以预期的方式，达到预期的目标，那么称这个实体是可信的。这一定义抓住了实体的行为特征，符合哲学上实践是检验真理的惟一标准的基本原则。

（2）ISO/IEC 15408 标准定义可信为：参与计算的组件，其操作或过程在任意的条件下是可预测的，并能够抵御病毒和物理干扰。IEEE CS可信计算技术委员会（IEEE Computer Society Technical Committee on Dependable Computing）认为，所谓可信是指计算机系统所提供的服务是可以论证其是可信赖的，即不仅计算机系统所提供的服务是可信赖的，而且

这种可信赖是可论证的。

（3）我们给出自己的观点：可信计算系统是能够提供系统的可靠性、可用性、信息和行为安全性的计算机系统。系统的可靠性和安全性是现阶段可信计算最主要的两个属性。因此，可简称为：可信≈可靠+安全。

信任的属性

（1）信任是一种二元关系。它可以是一对一、一对多（个体对群体）、多对一（群体对个体）或多对多（群体对群体）的；

（2）信任具有二重性。既具有主观性又具有客观性；

（3）信任不一定具有对称性。即A信任B，不一定就有B信任A；

（4）信任可度量。也就是说信任有程度之分，可以划分等级；

（5）信任可传递，但不绝对，而且在传播过程中可能有损失，传递的路径越长，损失的可能性就越大；

（6）信任具有动态性。即信任与环境（上下文）和时间因素相关。

信任的获得方法 信任的获得方法主要有直接和间接两种。设A和B以前曾有交往，则A对B的可信度可以通过考察B以往的表现来确定。我们称这种通过直接交往得到的信任值为直接信任值。设A和B以前没有任何交往，这种情况下，A可以去询问一个与B比较熟悉的实体C来获得B的信任值，并且要求实体C与B曾有直接的交往经验。我们称这种通过间接交往得到的信任值为间接信任值，或者说是C向A的推荐信任值。有时还可能出现多级推荐的情况，这时便产生了信任链。

信任链模型

可信计算组织的信任链采用了一种链式的信任测量模型，RTM（可信测量根）→BIOS→OSLoader→OS构成了一个串行链。又由于采用了一种迭代计算哈希值的方式，即将现值与新值相连，再计算哈希值并作为新的完整性度量值存储起来。

$$New\ PCR_i = HASH(Old\ PCR_i \,\|\, New\ Value)$$

这种链式信任链具有如下缺点：信任链越长，信任损失的可能性就越大。在链中加入或删除一个部件，PCR的值需要重新计算，很麻烦。信任链中的软件部件可能会更新（如BIOS升级，OS打补丁等），而PCR的值也得重新计算，这样一来使得部件更新工作很麻烦。

我们提出了一种带数据恢复的星型信任模型，其结构如图1所示。它将可信测量根置入可信平台模块内部NVRAM（Non-Volatile Random Access Memory，非易失性随机访问存储器）中，在信任链中增加了数据恢复功能，并将信任链延伸到应用。与可信计算组织的链式信任链相比，该模型具有如下特点：可信测量根被保护，安全性更高；具有数据恢复功能，安全性更高；都是一级测量，没有多级信任传递，信任损失少。但是，所有测量都由可

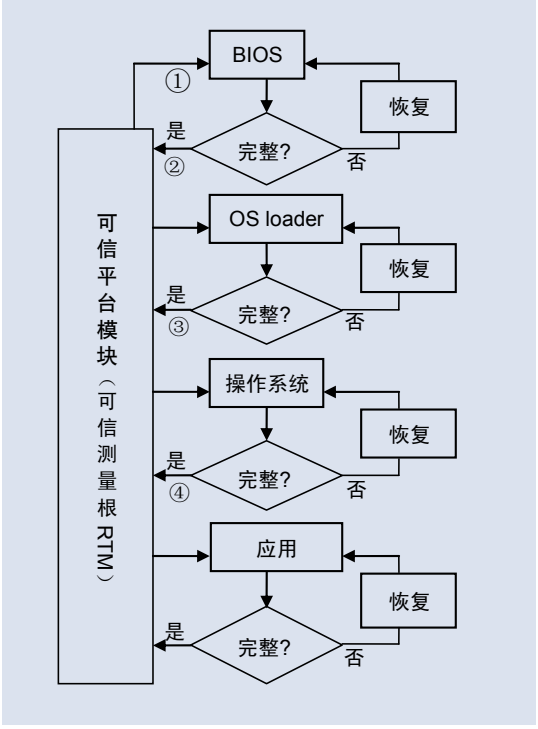


图1 带恢复的星型信任模型

信测量根执行，可信测量根通过可信平台模块完成任务，这使得可信平台模块负担加重。

可信度量理论

在可信计算中的信任链中应当度量的是可信性。但是，由于可信性目前尚不易直接度量，所以可信计算组织在信任链中采用的是度量数据完整性，而且是通过校验数据哈希值的方法来度量数据的完整性。但是，可信≈可靠+安全，完整性≠可信性，完整性⊂可信性，即完整性只是可信性中的一个侧面。因此，可信计算组织的信任链测量是有局限性的。另外，可信计算组织还把信任值二值化，只考虑可信和不可信两种极端状况，而且认为在传递过程中没有信任损失。这显然是一种理想化的处理方法。

由于可信计算组织在信任链中采用的是度量数据完整性，因此它能确保数据的完整性，确保BIOS、OSLoader和OS的数据完整性。但是完整性只能说明这些软件没有被修改，并不能说明这些软件中没有安全缺陷，更不能确保这些软件在运行时的安全性。基于数据完整性的度量是一种静态度量，我们需要基于软件行为的动态度量。

由我国学者出版的《软件行为学》一书对软件的行为进行了形式化的刻画和分析。我们也提出了一种基于软件行为的动态完整性度量方法，通过分析可执行文件或源代码的API函数调用关系得到软件的预期行为，建立软件预期行为描述集并发布；然后对软件进程的实际API函数调用行为进行监控；如果在软件执行过程中，软件行为一直符合软件预期行为描述集中的相关规则（软件行为认证码），则认为软件是可信的；否则说明软件不可信，此时应该对该软件进行控制。图2给出了这种动态完整性度量的结构。

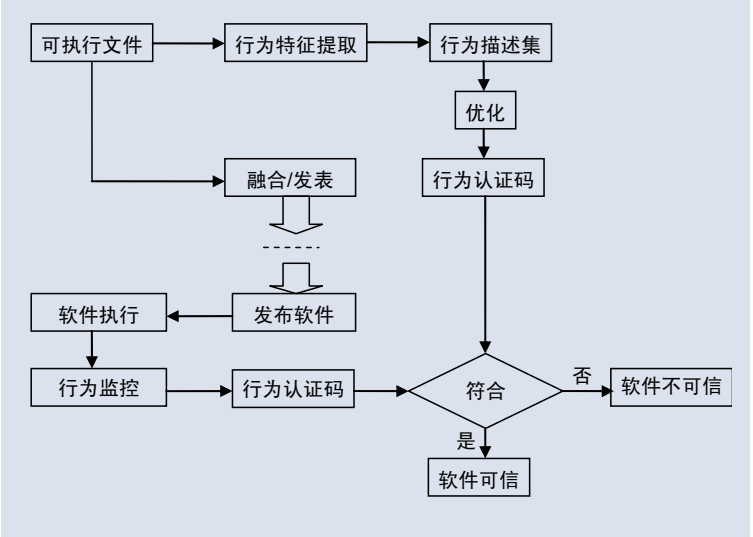


图2 基于软件行为的动态完整性度量

在实验系统中，我们把静态度量与动态度量相结合，收到很好的效果。当然动态度量也增加了一定的成本。

最后需要强调的是，虽然可信计算组织在信任链中采用的是度量数据完整性，存在上述的不足之处，但是它足以确保系统资源的数据完整性和抵御大量计算机病毒等恶意软件的攻击，在很大程度上提高了计算机的安全性。

可信平台模块

由国家密码管理局主持制定的《可信计算平台密码技术方案》和《可信计算密码支撑平台功能与接口规范》两个规范是指导我国可信平台模块芯片和接口软件的指南。

瑞达公司和武汉大学合作研制出一种新型可信平台模块芯片J3210。其最大特点是既支持我国技术规范，又支持可信计算组织的技术规范，而且计算资源和密码资源非常丰富，可以满足可信计算的大部分应用。图3给出了J3210芯片的结构。

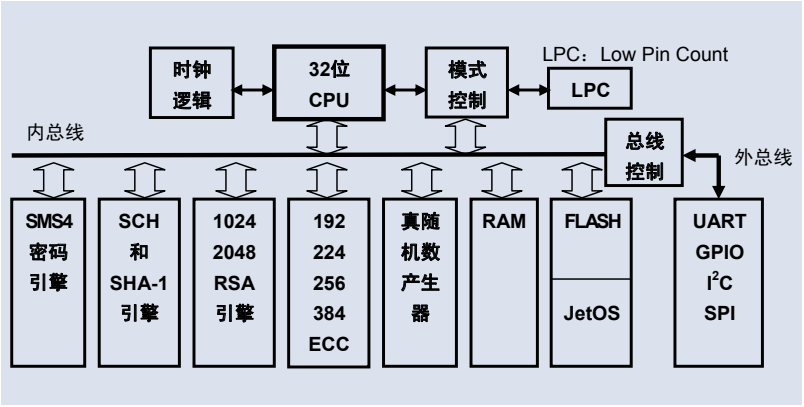


图3 J3210芯片结构

J3210芯片的资源如下：

- 32位SPARC CPU；
- 24KB的内部指令RAM，9KB的内部数据RAM；
- 128KB的FLASH存储器；
- 1024、2048位的RSA密码引擎；
- 192、224、256、384位的ECC密码引擎；
- 中国商用对称密码SMS4引擎；
- 中国商用哈希函数SCH引擎；
- SHA-1引擎；
- 真随机数产生器；
- I/O接口：LPC、I2C、SPI、UART、GPIO、JTAG。

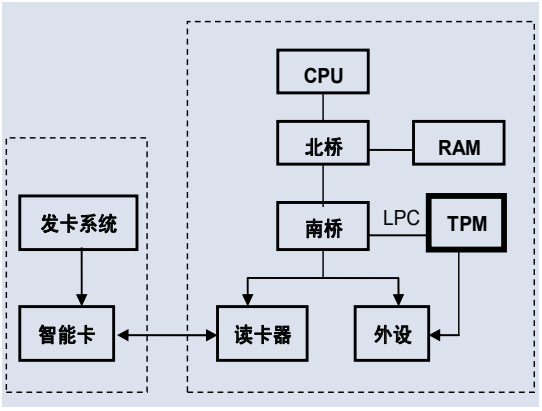


图4 一种可信计算机结构

国内可信计算平台

可信PC机

瑞达公司研制出一种新型的可信计算机，其可信平台模块芯片结构如图4所示。它采用带数据恢复的链式信任链，而且信任链延伸到应用，确保开机时信任链管辖范围之内的软件无病毒；采用了智能卡，用于用户身份认证和安全管理；用可信平台模块控制I/O口，安全可控。

除了瑞达公司外，联想、长城、方正和浪潮等公司也都在积极开发自己的可信计算机。

我国正在制定可信计算平台（PC机和服务器）的技术标准。

可信PDA

PDA是一种手持式移动计算平台，由于其安全性长期没有得到重视，因而存在严重的安全问题。第一，手持式设备容易丢失，丢失后被冒用、泄密；第二，使用闪速（FLASH）存储器，数据易被篡改，因此常受病毒的攻击；第三，采用无线通信，容易泄露信息。因此，应当采取措施确保PDA的安全。

在国家863计划项目的支持下，武汉大学研制出我国第一款可信PDA，其结构如图5所示。它具有以下可信机制与安全功能：（1）基于指纹识别的用户身份认证；（2）SD卡（Secure Digital Memory Card）全加密；（3）带数据恢复的星型信任模型；（4）TSS软件接口；（5）安全增强的操作系统；（6）无线通信加密与认证；（7）可信网络连接；（8）可控GPS（Global Position System，全球定位系统）定位。

可信服务器

瑞达公司和浪潮公司都在开发自己的可信服务器。由于服务器在技术上比PC机要复杂得多，因此我国在可信服务器方面的进展要比可信PC机滞后。

可信计算平台测评

可信计算产品已经开始走向应用。我国的政策规定信息安全产品必须经过测评认证才能投入实际应用。因此，必须对可信计算平台进行测评。

国际上，德国波鸿大学对可信平台进行模块测试，发现主流的可信平台模块在不同程度上都存在与标准不符合的问题。盖尔盖伊•托特（Gergely Tóth）指出：将白盒测试和Fuzzing技术相结合，发现OpenTC项目中的TSS的若干缺陷（Bug）和远程溢出安全漏洞。我国信息安全国重点实验室开展了可信密码模块（Trusted Cryptography Module，TCM）标准符合性测试研究。

在国家863计划项目的支持下，武汉大学研制出我国第一个可信计算平台的测评软件系统。图6给出可信计算平台测评软件系统结构。测评系统的技术路线是，以可信计算的理论和技术为基础，以国际和国家规范和标准为依据，以平台可信特征为测评重点进行测评。测评的目标是测评被测系统的可信性和安全性。主要测试对象是可信平台模块、信任链和可信支撑软件TSS。

实验测试对象有HP nc6400、HP nc6230、IBM ThinkPad R61以及部分国内可信计算机。

实际测试表明，目前无论是国外还是国内的可信计算机都没有完全符合相应的技术规范。但是，可信计算机的技术进步是明显的，早期的可信计算机产品基本上都没有信任链，后期的产品在信任链与技术规范的符合率方面大大提高。例如，HP nc6400与可信计算组织规范的符合率达到81.2%。现在仍然有一部分可信计算机没有信任链。

测评研究与实验证明，在我国开展对可信计算机的测评研究与实测认证是十分必要和迫切的。我国政府应当加大这方面的投入，加强测评认证的管理。

可信软件

近年来，随着软件规模的不断扩大，其内部结构越来越

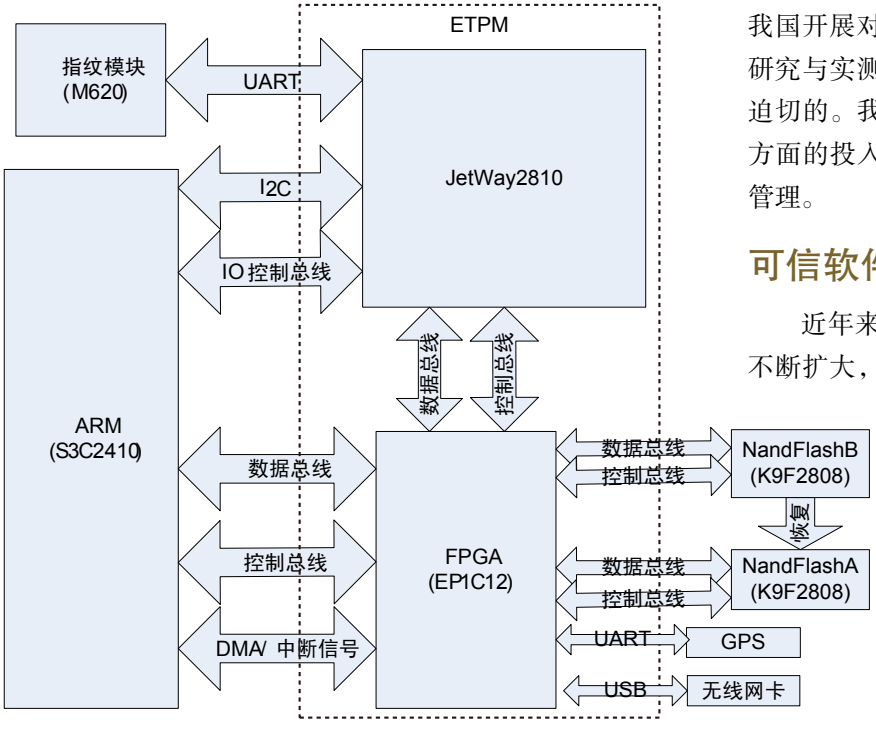


图5 可信PDA结构

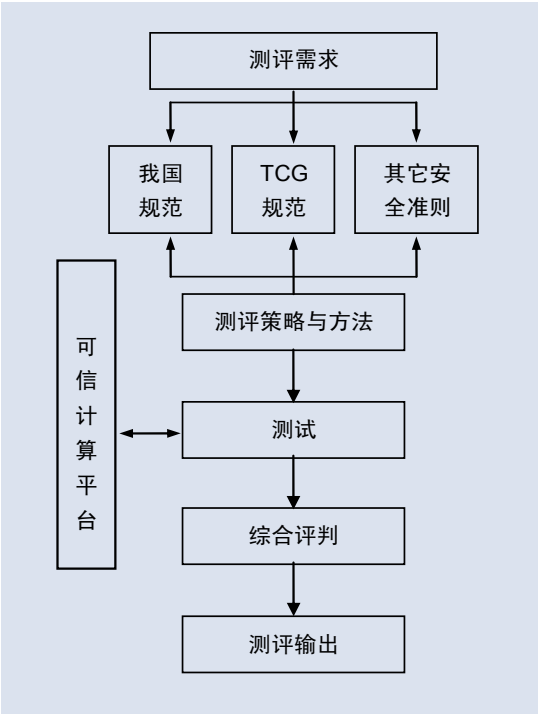


图6 可信计算平台测评软件系统结构

复杂，应用环境越来越开放，这些因素使得人们更加关注软件的可信性问题。学术界对可信软件有着不同的理解和认识，有些学者强调软件的正确性，有些学者强调软件的可靠性，有些学者强调软件的安全性。我们则强调可信性，即强调可靠性与安全性的结合。总之，各方面的研究共同促进了可信软件的发展。

可信基础软件

我们通常把操作系统、编译器和数据库称为计算机基础软件。其中，操作系统是计算机系统资源的管理者和调度者；编译器编译产生可执行代码；数据库对计算机系统的数据实施管理和处理。显然，它们的可信性是系统可信的重要基础。

操作系统和数据库的安全性很早就得到重视，并已经有广泛的研究。相比之下，编译器的安全性研究则起步较晚。在国家自然科学基金“可信软件重大专项”的支持下，我们对可信编译进行了研究。

编译器作为重要的系统软件，其可信性对于整个计算机系统的可信具有重要意义。如果编译器不可信，则很难保证其它软件的可信性。软件的可信性很大程度上依赖于程序代码的可信性，影响软件可信性的主要因素包括来自软件内部的代码缺陷、代码错误、程序故障以及来自软件外部的病毒、恶意代码等。因此，从代码角度来保证软件的可信性是实现可信软件的重要途径之一。

可信编译的目标就是从编译的角度保证软件的可信性，主要包括两方面含义，一方面，必须保证编译器自身是可信的。即必须保证整个编译操作的可信性，保证编译器在编译过程中不会给编译处理对象带来任何安全性问题，防止恶意攻击者通过修改编译器，在编译过程中对代码的原始语义进行篡改，影响程序代码本身的可信性；另一方面，必须保证编译器编译所得程序可执行代码是可信的，即编译器必须保证，通过其编译生成的程序代码是安全和可靠的。我们将满足以上两方面要求的编译器称为可信编译器。

编译器自身的可信性

编译器本身是一个可执行程序，同样会遭受攻击，造成编译器自身的不可信。编译器自身的不可信因素有两类，一类是同普通程序一样感染了病毒或木马，运行编译器时会出现破坏计算机数据、泄露信息、窃取密码等常见病毒发作现象；另一类是篡改编译器编译行为，使编译器在编译过程执行某种特定目的的操作。例如，在代码生成时在目标文件中插入恶意代码。

编译器自身的可信性主要是指其编译过程的正确性、安全性和可靠性。我们知道，编译器是一个很复杂的程序。目前，保证编译过程安全的主要手段仍然是依靠大量的测试。此外，形式化方法是目前研究者公认最有效的保证系统可信性的证明方法，因为它能够从数学的角度为可信性提供严密的证明。一般认为，

通过形式化验证的系统具有较高的可信性。目前，大多数情况下的形式化方法只适用于对程序源代码进行检测。我们认为，更好的方法是将形式化方法用于编译器本身。

编译生成可执行代码的可信性

可信编译器应保证编译所得的可执行代码是可信的，从而确保系统所运行程序的安全和可靠。我们拟通过在传统编译操作的基础上加入代码安全性加强机制、代码可信性验证机制及可执行代码保护机制等三种机制，来保证编译所产生代码的可信性。

代码安全性加强机制 该机制主要用于识别和处理程序中常见的一些安全漏洞。目前已提出许多针对程序常见安全漏洞的编译处理技术，具有代表性的如针对缓冲区溢出攻击的StackGuard方法等。

代码可信性验证机制 该机制不可能解决所有的代码安全性问题。对于可信性要求较高的程序代码，必须通过形式化方法对其进行可信性验证。因此，我们提出在代码安全性加强机制对代码进行安全加强之后，通过代码可信性验证机制对代码的可信属性进行验证，对未通过验证的非可信代码进行报警或其它处理。这样，通过代码安全性加强和可信性验证相结合的方法保证编译生成可执行代码的可信性。

可执行代码保护机制 为了防止攻击者对可信编译器最终生成的可执行代码进行恶意攻击或修改，可信编译器在完成编译之后，对可执行代码实施保护机制，保护编译所得可执行代码的完整性、秘密性和可用性，从而确保系统最终执行代码的可信运行。

我们对可信编译系统的总体框架进行了研究设计，如图7所示。

可信软件工程

众所周知，软件工程是从软件的整个生命周期的各个阶段采取措施，确保软件的质量。传统的软件工程的质量标准主要指软件的正确性和可靠性。软件的安全性显然也是一种重要的软件质量指标。可信软件工程就是从软件的整个生命周期的各个阶段采取措施，确保软件的可信性。

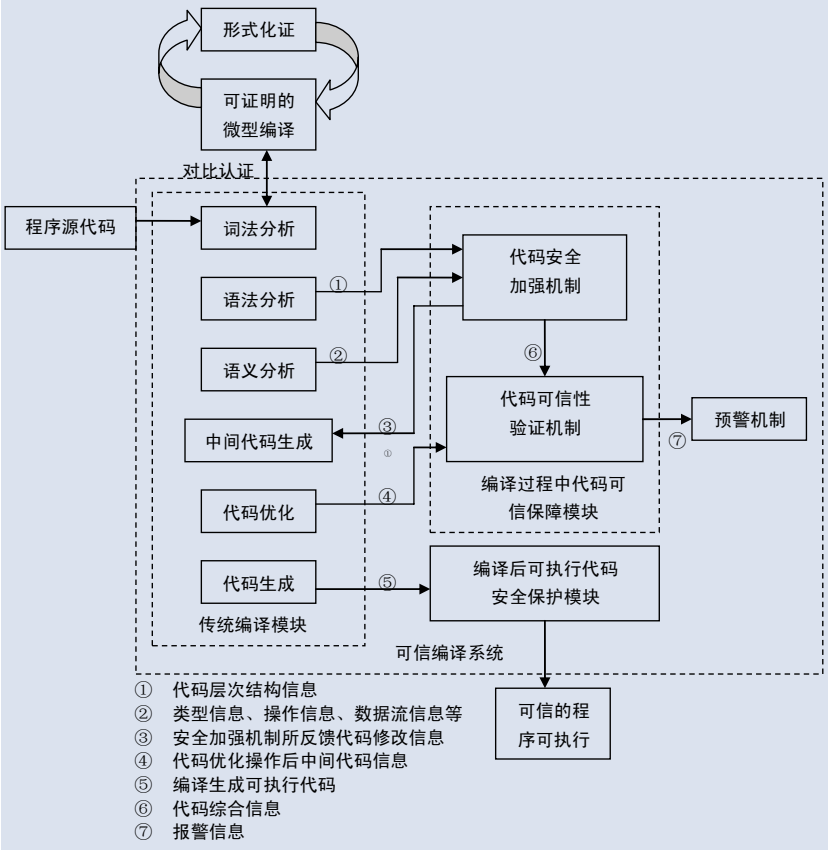


图7 可信编译系统框架

可信软件工程已经成一个重要的研究方向。其主要研究包括：软件可信性度量的理论与方法、可信程序设计方法学以及可信软件开发方法学等。

软件可信性度量的理论与方法

目前，可信计算中的软件可信性度量是按数据完整性度量来进行的，不是真正的软件动态可信性度量。因此，它只能确保软件的静态可信，而不能确保软件的动态可信。于是，如何进行软件的动态可信性度量，就成为软件质量确保的关键。软件的动态可信性是指当软件运行时所表现出来的行为可信性，既包括可靠性，也包括安全性。从基于数据完整性到基于行为完整性，把确保软件可信性的研究向前推进了一步。我们已经开展了基于软件行为完整性的软件可信性研究，并取得了一些成果。

可信软件开发方法学

可信软件的开发过程模型 软件开发是一个复杂的过程，其中需求分析、设计和测试仍是目前工程上保障软件可信性的重要阶段，但仅靠各阶段中的方法和技术仍不能满足高可信软件开发的需要。根据可信计算中信任链的概念，软件开发过程在理想（不出错）的情况下也可视为一条信任链，因为根据软件的开发过程，如果能保证开发过程中每一阶段的工作结果是可信的，而且其可信性可用形式化方法给予验证，则软件开发得到的最终结果即软件也是可信的。因此，需要研究能适应各阶段的统一的形式化方法和验证技术，保证各阶段工作结果的可信性。

软件行为描述语言和语义模型 软件行为的可信与软件的可信是密切相关的。从主体和客体的角度出发，软件行为可分为单一主体行为、伴侣主体行为及群体的行为等多种行为模式，为了能准确描述这些模式，就需要用严格的语法形式来定义这些模式，从而建立严格的描述软件行为的形式语言。不过，仅用形式化方法建立描述软件行为的形式语言是不够的。只有明确了行为关系的应用范围或者为这些行为关系明确了对象领域，这些语言符号表达的行为（模式）才有确定的语义。根据行为描述的对象领域的语义要求，可对表达行为模式的语言符号用逻辑语义、代数语义和指称语义的方法来建立语义模型。形式语言和相应的语义模型奠定了软件可信的形式验证方法的基础。

可信软件的验证方法 形式化验证是在形式化描述的基础上建立软件系统及其性质的关系，即分析系统是否具有所有期望性质的过程。基于信任链概念的可信软件开发过程的形式化验证虽然是分阶段进行的，但它们都是在前述的行为描述语言和语义模型框架下统一进行的。模型检验将是这些验证的主要技术，但由于模型检测技术存在“状态空间爆炸”问题，因此如何通过分阶段和阶段内的抽象分解方法来缓解这一问题是一个重要的课题。

基于构件的软件系统可信管理 基于软构件设计软件是一种重要的软件设计方法。在这里，软构件成为软件的基本部件，如同一座大楼的各种预制件和砖瓦。如果要确保“大楼”的质量，首先要有好的“预制件”和“砖瓦”。但是只有好的“预制件”和“砖瓦”，并不一定能保证一栋大楼的质量好。因此，首先要研发可信软构件的理论与技术，在此基础上再研究利用这些可信软构件设计构成可信软件系统的理论与技术。

理论上，首先建立可信管理的整体抽象模型，模型的各个功能部分综合起来应该从整体上支撑起整个应用的可信管理；其次建立构件可信属性元描述模型，分析对于可信构件在适配时需要的可信描述信息，例如构件的角色、采用的安全策略、自身安全级别、要求与之适配的构件安全级别等等；最后建立构件可信性的度量模型以及软件系统所采取的可信管理策略。

可信程序设计方法学

合理的程序设计可以避免诸如缓冲区溢出

等安全漏洞。目前，这方面已经有一些研究，但是还属于一种设计经验，缺少一般性的设计方法与理论。需要研究安全程序设计的一般性理论与方法。

安全程序设计不仅与程序设计方法有关，还与程序设计语言、编译等编程环境有关。如何设计出正确的程序，已经有从设计方法、程序设计语言和编译等方面共同确保的一整套有效方法。但是如何设计出安全的程序，还没有从设计方法、程序设计语言、编译等方面共同确保的一套有效方法。因此，这是需要重点研究的。

可信网络连接

虽然可信网络连接具有安全性、开放性和系统性等优点，但是可信网络连接仍然具有一些局限性。

安全性局限于完整性 可信网络连接基于完整性对终端进行可信验证，但完整性只能保证信息的来源可信与未被修改，并不能保证信息的内容可信和软件的动态可信。因此可信网络连接并不能完全保证接入终端的平台可信。

单向性 可信网络连接的出发点是保证网络的安全性，因此该架构没有考虑如何保护终端的安全。终端在接入网络之前，除了要提供自身的平台可信性证据之外，还应该具有对接入网络进行可信性评估，否则无法保证从网络中获取的服务可信。

缺乏安全协议支持 可信网络连接架构中，多个实体需要进行信息交互，如可信网络连接客户端与可信网络连接服务器之间、可信网络连接客户端与IMC之间、可信网络连接服务器与IMV之间、IMC与IMV之间都需要进行大量的信息交互，但是可信网络连接架构本身并没有给出相应的安全协议，只是简单地介绍了如何进行消息的传递。

缺乏网络接入后的安全保护 可信网络连接只是在终端接入网络的过程中对终端进行了平台评估与完整性验证，在终端接入网络之后并没有相应的措施对网络和终端进行保护。

我国可信计算工作小组（2005年1月成立，隶属于信息安全技术标准化委员会）通过分析可信计算组织的可信网络连接架构，认为其实质是一个二元结构，在网络访问层和完整性评估层都存在安全隐患，因此我国可信计算标准采用的可信网络连接架构是三元结构：通过引入一个策略管理器作为可信第三方，对可信网络连接架构中的所有实体进行管理；而且不只在网络访问层采用三元结构，还要在可信网络连接架构的各个层次都采用三元结构；所采用的技术必须是安全的，并且是具有国家自主产权的，要站在国家的利益上保护国家的信息资源。我国的可信网络接入控制体系结构的特点和创新性在于增加的策略管理器对访问请求者和访问控制器进行管理，在实现访问请求者和访问控制器之间的双向用户身份鉴别和双向平台可信性评估（包括双向平台凭证鉴别和双向平台可信性校验）过程中充当可信第三方的角色；访问请求者和访问控制器相互验证可信性，从网络连接顺序上看：访问请求者（可信）访问控制器（可信）可信网络，从而实现了信任链在网络上的传递；证书有效性验证和平台可信性校验都由策略管理器集中实现，简化了证书有效性验证机制和平台可信性校验机制，同时消除了证书有效性无法验证的安全隐患；只需进行一次会话密钥协商，主密钥不会在网络上传输，从而简化了密钥协商复杂性并增强了安全性等等。

我们对可信网络连接的架构及其关键技术进行了研究，并按照TNC1.2规范实现了基于可信平台模块的可信网络连接整体架构及各个接口，并在此基础上实现了客户端与服务器端的双向证明，做到了可信计算组织提出的实体接入网络时的平台配置及环境的度量和报告，体现了行为可信的思想，将信任链延伸到了应用和网络。在此

基础上，我们对可信网络传输与可信数据共享进行了一些研究。在可信传输方面，除了继续采用密码保护之外，通过对传输协议进行扩展，为传输的每一个数据报增加可信标签，用于传输路径上的信息定位、服务质量等功能。在可信资源共享方面，借助访问控制理论与安全多方计算的理论，设计层次化、跨可信域的、基于可信硬件的访问控制方法，达到主体对客体的安全访问，实现资源的可信共享。

可信计算发展中存在的一些问题

目前，可信计算已经成为世界信息安全领域中的一个新潮流。但是，目前可信计算发展还存在一些需要研究解决的问题。

理论研究相对滞后

在可信计算领域，国内外都处于技术超前于理论的状况。至今没有公认的可信计算理论模型。

可信度量是可信计算的基础。但是，目前缺少有效的软件动态可信性度量的理论与方法。信任链的理论需要进一步完善，如信任的传递理论，特别是信任在传递过程中的损失度量理论与方法。

理论来源于实践，反过来又指导实践。没有理论指导的实践是不能持久的。目前可信计算的技术实践已经取得长足的发展，因此应当在可信计算的实践中丰富和发展可信计算的理论。

一些关键技术尚待攻克，应当坚持持续不断的技术进步

实际测评表明，无论是国外还是国内的可信计算机产品都没能完全实现可信计算组织的PC技术规范。其原因之一是可信计算的一些关键技术尚未攻克，如I/O保护等。

另外，随着可信计算的发展和应用，原有的技术规范会暴露出一些问题，对于这些问题应当坚持改进。可信计算组织的技术规范版本不断升级，就是一种很好的做法。

CCF高级会员赵有健荣获中国青年科技奖

从中国科协获悉，CCF高级会员、清华大学计算机系赵有健教授荣获第11届中国青年科技奖。他是由CCF推荐的第2位获此荣誉的会员。此前，CCF高级会员、中国科学院自动化研究所谭铁牛研究员获第9届中国青年科技奖。

中国青年科技奖是在钱学森提议下，由中央组织部、人事部、中国科协设立的，目的是选拔培养优秀青年科技人才，促进青年科技工作者奋发进取、健康成长。评选对象为40岁以下从事自然科学和交叉科学的青年科技工作者，每2年评选1次，每届获奖人数不超过100名。

赵有健

CCF高级会员。清华大学教授。长期从事高速计算机网络体系结构的研究和高速网络设备的研制，在IPv6核心路由器的技术创新和研制方面做出突出贡献，曾获得国家科技进步二等奖和2006年CCF王选奖一等奖。

缺少操作系统、网络、数据库和应用的可信机制配套

目前，可信计算组织给出了可信计算硬件平台的相关技术规范和可信网络连接的技术规范，但还没有关于可信操作系统、可信数据库、可信应用软件的技术规范。网络连接只是网络活动的第一步，连网的主要目的是数据交换和资源公享，在这方面缺少可信技术规范。我们知道，只有硬件平台的可信，没有操作系统、数据库、网络和应用的可信，整个系统还是不安全的。

缺少安全机制与容错机制的结合

目前，国际可信计算领域存在以可信计算组织为代表的强调信息安全的流派和以容错专家为代表的容错流派，他们都为可信计算做出了贡献。但是用户需要既安全又可靠，因此两个流派应当结合，提供给用户既安全又可靠的可信计算机。

可信计算的应用较少

目前，国内外都推出了不少可信计算产品，并投入了一些实际应用。但是总的说来，应用的范围和规模都还很小。只有实际应用多了，为用户解决了实际问题，在应用中得到用户的欢迎，可信计算才能说是取得了真正的成功。

结语

目前，可信计算已经成为世界信息安全领域的一个新潮流。可信计算技术是一种新的行之有效的信息系统安全技术。与普通计算机相比，可信计算机的安全性大大提高。但可信计算机也不是百分之百安全，它不可能解决所有的信息安全问题，我们也不应当要求它解决所有信息安全问题。把可信计算技术与其它信息安全技术结合起来，我们将更有效地解决信息安全问题。

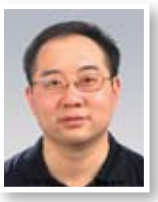
我国在可信计算领域起步不晚，水平不低，成果可喜，目前已经站在国际可信计算领域的前列。我们应当抓住机遇发展可信计算事业，建立信息安全体系，确保我国的信息安全。■

张焕国

CCF高级会员。武汉大学教授。主要研究方向为信息安全、可信计算、容错计算。
liss@whu.edu.cn

何炎祥

CCF理事、教育专委会副主任。武汉大学教授。主要研究方向为可信软件、分布并行处理。
yxhe@whu.edu.cn



赵　波

CCF高级会员。武汉大学副教授。主要研究方向为可信计算。
zhaobo@whu.edu.cn

彭国军

CCF会员。武汉大学讲师。主要研究方向为可信计算。
guojpeng@whu.edu.cn

严　飞

CCF会员。武汉大学讲师。主要研究方向为可信计算。

余发江

CCF会员。武汉大学讲师。主要研究方向为可信计算。