中国科学 E 辑: 信息科学
2007 年 第 37 卷 第 2 期: 129~150
http://www.scichina.com

《中国科学》杂志社
SCIENCE IN CHINA PRESS

信息安全综述*

沈昌祥[1] 张焕国[2**] 冯登国[3] 曹珍富[4] 黄继武[5]

(1. 海军计算技术研究所, 北京 100841; 2. 武汉大学计算机学院, 武汉 430072; 3. 中国科学院软件研究所, 北京 100080; 4. 上海交通大学计算机学院, 上海 200031; 5. 中山大学信息技术学院, 广州 510275)

摘要 21 世纪是信息的时代. 信息成为一种重要的战略资源, 信息的获取、处理和安全保障能力成为一个国家综合国力的重要组成部分. 信息安全事关国家安全、事关社会稳定. 因此, 必须采取措施确保我国的信息安全. 近年来, 信息安全领域的发展十分迅速, 取得了许多新的重要成果. 信息安全理论与技术的内容十分广泛, 但由于篇幅所限, 这里主要介绍密码学、可信计算、网络安全和信息隐藏等方面的研究和发展.

关键词 信息安全 密码学 可信计算 网络安全 信息隐藏

1 引言

21 世纪是信息的时代. 一方面, 信息技术和产业高速发展, 呈现出空前繁荣的景象. 另一方面, 危害信息安全的事件不断发生, 形势是严峻的. 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[1].

信息安全主要包括以下 4 个侧面: 信息设备安全、数据安全、内容安全和行为安全. 信息系统硬件结构的安全和操作系统的安全是信息系统安全的基础, 密码、网络安全等技术是关键技术. 只有从信息系统的硬件和软件的底层采取安全措施, 从整体上采取措施, 才能比较有效地确保信息系统的安全[2].

为什么信息安全的问题如此严重呢? 从技术角度来看, 主要有以下一些原因:

1. 微机的安全结构过于简单. 20 世纪 70 年代, 由于集成电路技术的发展, 产生了微机.

微机被称为个人计算机(personal computer). 由于是个人使用的计算机, 不是公用的计算机, 一是为了降低成本, 二是认为许多安全机制不再必要, 所以就去掉了许多成熟的安全机制, 如存储器的隔离保护机制、程序安全保护机制等. 于是, 程序的执行可以不经过认证, 程序可以被随意修改, 系统区域的数据可以随意修改. 这样, 病毒、蠕虫、木马等恶意程序就乘机泛滥了[3].

收稿日期: 2006-12-19; 接受日期: 2007-01-04
国家自然科学基金资助项目(批准号: 60373087, 60673071, 60572155)

* 本文的引言和可信计算部分由张焕国撰写, 密码学部分由曹珍富撰写, 网络安全部分由冯登国撰写, 信息隐藏部分由黄继武撰写, 并由沈昌祥定稿.

** 联系人, E-mail: liss@whu.edu.cn

2. 信息技术的发展使微机又成为公用计算机. 在应用上, 微机已不再是单纯的个人计算机, 而变成了办公室或家庭的公用计算机. 可是由于微机去掉了许多成熟的安全机制, 面对现在的公用环境, 微机的安全防御能力就显得弱了.

3. 网络把计算机变成网络中的一个组成部分. 网络的发展把计算机变成网络中的一个组成部分, 在连接上突破了机房的地理隔离, 信息的交互扩大到了整个网络. 由于 Internet 网络缺少足够的安全设计, 于是置于网络世界中的计算机, 便危机四伏. 难怪人们说: “如果上网, 你所受到的安全威胁将增大几倍. 而如果不上网, 则你所得到的服务将减少几倍”. 又由于网络协议的复杂性, 使得网络协议的安全证明和验证十分困难. 目前人们只能证明和验证一些简单的网络协议, 所以, 无法避免在网络协议中存在安全缺陷. 反言之, 即使网络协议是正确的, 也不能确保百分之百安全. 正确的协议也可被利用进行攻击. 攻击者完全可以根据哲学上“量变到质变”的原理, 发起大量的正常访问, 耗尽计算机或网络的资源, 从而使计算机瘫痪. 著名的 DoS 攻击就是明证[4].

4. 操作系统存在安全缺陷. 操作系统是计算机最主要的系统软件, 是信息安全的基础之一. 然而, 因为操作系统太庞大(如, Windows 操作系统就有上千万行程序), 致使操作系统都不可能做到完全正确. 操作系统的缺陷所造成的功能故障, 往往可以忽略. 如, 当 Windows 出现死机时, 人们按一下复位键重新启动就可以了. 但是, 如果操作系统的缺陷被攻击者利用, 则造成的安全后果却不能忽略[5].

2 密码学的研究与发展

信息安全离不开密码学. 作为信息安全的关键技术, 密码学可以提供信息的保密性、完整性、可用性以及抗抵赖性. 密码学主要由密码编码学和密码分析学两部分组成, 其中密码编码学的主要任务是研究对信息进行编码以实现信息隐蔽, 而密码分析学主要研究通过密文获取对应的明文信息. 密码编码学与密码分析学相互对立, 又相互依存, 从而推动了密码学自身的快速发展[6,7]. 当前, 密码学的研究主要是基于数学的密码理论与技术. 现代密码学的研究可大致分为 3 类: Hash 函数、对称密码(又称为私钥密码)和非对称密钥(又称为公钥密码)[8,9]. 下面, 我们将分别介绍这 3 类密码体制的研究现状和发展趋势.

2.1 Hash 函数的研究

密码学 Hash 函数(也称为杂凑函数)将任意长的输入消息串变化成为固定长度的输出串, 这个输出串称为该消息的 Hash 值(也称为杂凑值). 这里, 我们设 $y=h(x)$为一个 Hash 函数, 它需要满足以下条件: (1) 输入的 x 的长度是任意的, 输出的 y 的长度是固定的; (2) 对于给定的输入 x, 计算输出的 Hash 值 y 容易; 反过来, 对于给定的 Hash 值 y, 找出输入 x, 使得 $y=h(x)$在计算上不可行; (3)找出两个不同的输入 x 和 x', 即 $x \neq x'$, 使得 $h(x) = h(x')$在计算上不可行; 给定一个输入 x, 找出另一个不同的输入 x', 即 $x \neq x'$, 使得 $h(x) = h(x')$在计算上不可行.

Hash 函数的主要用途在于提供数据的完整性校验和提高数字签名的有效性, 目前国际上已提出了许多 Hash 函数的设计方案. 这些 Hash 函数的构造方法主要可分为以下 3 类: (1) 基于某些数学难题如整数分解、离散对数问题的 Hash 函数设计; (2) 基于某些对称密码体制如 DES 等的 Hash 函数设计; (3) 不基于任何假设和密码体制直接构造的 Hash 函数[8]. 其中第 3 类 Hash 函数有著名的 SHA-1, SHA-256, SHA-384, SHA-512, MD4, MD5, RIPEMD 和 HAVAL 等等.

在 2004 年的美国密码会议上, 山东大学王小云教授发表的题为《对 MD4, MD5, HAVAL-128, RIPEMD 等 Hash 函数的碰撞攻击》的学术报告是密码学 Hash 函数研究方向上的一个里程碑[10]. 这份报告对一些国际上通行的 Hash 函数给出了快速寻找碰撞攻击的方法. 之后, 在 2005 年欧洲密码和美国密码会议上, 王小云进一步发表了他们对 Hash 函数研究的新进展[11−14]. 今天, 研究和设计更安全的 Hash 函数已经成为国内外密码学家的热点课题.

2.2　私钥密码的研究

对于一个密码体制来讲, 如果使用的加密密钥和解密密钥相同, 或者虽然不相同, 但是可以由其中的任意一个很容易地推导出另外一个, 那么这个密码体制称为单密钥的对称密码, 又称为私钥密码.

分组密码是一种典型的私钥密码. 如, 美国数据加密标准 DES, IDEA 算法, Skipjack 算法, Rijndael 算法等等. 分组密码设计的关键在于如何寻找一种算法, 使得在密钥的控制下可以从一个足够大且足够"好"的置换子集合中, 简单而又快速地挑选出一个置换. 根据一个好的分组密码应当是既难破译又容易实现的, 这需要满足以下两个条件: (1) 加密函数 $E_k(.)$和解密函数 $D_k(.)$要求容易计算; (2) 如果 y 为 x 经过密钥 k 作用生成的密文, 即 $y=E_k(x)$, 那么从方程 $y=E_k(x)$ 或者 $x=D_k(y)$中求出密钥 k 是计算上不可行的.

随着分组密码设计的研究不断深入, 分组密码的分析技术也得到了快速的发展. 到目前为止, 已经有多种分组密码分析技术被讨论. 这些分析技术主要包括强力攻击、差分密码分析、差分密码分析的推广、线性密码分析、线性密码分析的推广、差分-线性密码分析等等. 在国际上, 美国国家标准技术研究所在2001年11月26日正式公布了新的数据加密标准(AES)[15]. 在美国之后欧洲启动了 NESSIE(new European schemes for signatures, integrity, and encryption)计划和 ECRYPT (European network of excellence for cryptology)计划, 制定了一系列的密码算法, 促进了密码的研究和应用. 在国内, 国家"八六三"计划也将制定密码的标准化问题列入了议程.

目前, 分组密码的重点研究方向为新型密码的设计、密码体制的软件优化、硬件实现和专用密码芯片的设计等.

张焕国、覃中平将密码学与演化计算结合起来, 借鉴生物进化的思想, 提出了演化密码的概念和用演化计算设计密码的方法. 并在分组密码 S 盒、Bent 函数、Hash 函数、随机序列的演化设计方面进行了有意义的研究[16−18].

除分组密码之外, 流密码也是一种重要的私钥密码. "一次一密"密码在理论上是绝对安全的这一结论使人们感到, 如果能以某种方式仿效"一次一密"密码, 则将得到保密性很高的密码. 长期以来, 人们以流密码仿效"一次一密"密码, 从而促进了流密码的研究和发展. 与分组密码相比, 流密码的理论与技术相对比较成熟. 流密码是世界各国重要领域的主流密码, 对信息安全发挥了极大的作用. 在流密码的设计方面, 除了移位寄存器序列、非线性组合序列、非线性过滤序列和钟控序列等方法外, 近年来人们将混沌序列引入流密码, 并取得了可喜的研究成果[19]. 国内的丁存生、肖国镇等教授在流密码研究领域做出了突出的贡献[20].

2.3　公钥密码的研究

对于一个密码体制来讲, 如果加密和解密的能力是分开的, 即加密和解密分别使用两个

不同的密钥实现, 并且不可能由加密密钥(公钥)推导出对应的解密密钥(私钥), 那么这个密码体制称为非对称密码, 又称为公钥密码.

自从 1976 年公钥密码的思想提出以来[21], 国内外密码学家设计了许多优秀的公钥密码体制, 其中著名的体制包括: 1978 年 Rivest 等提出的 RSA 公钥体制[22]; 1978 年 Merkle 与 Hellman 提出的基于背包问题的 MH 背包体制[23], 1979 年 Rabin 提出的 Rabin 体制[24], 1985 年 ElGamal 提出的 ElGamal 公钥体制[25], 1987 年 Koblitz 和 Miller 提出椭圆曲线密码公钥体制[26], 以及基于代理编码理论的 MeEliece 体制[27]和基于有限自动机理论的公钥密码体制[28]等等. 公钥密码除了公钥密码体制之外, 还包括数字签名技术[29]. 著名的数字签名有 RSA 签名、Rabin 签名、ElGamal 签名、Schnorr 签名[30]和美国国家数字签名标准 DSS[31]. 由于数字签名可以提供信息的鉴别性、完整性和不可否认性, 因此, 随着实际应用的需要, 特殊的数字签名也被广泛的提出. 主要包括: 代理签名[32]、盲签名[33]、可验证的加密签名[34]、不可否认签名[35]、前向安全签名[36]、密钥隔离签名[37]、在线/离线签名[38]、门限签名[39]、聚合签名[34]、环签名[40]、指定验证者签名[41]、确认者签名[42], 以及它们各种变型签名等等[43].

公钥密码虽然具有许多优点, 但是公钥密码的公钥认证和证书管理相当复杂. 例如目前流行的基于目录的公钥认证框架 X.509 证书框架的建立和维护异常复杂, 且成本昂贵[44]. 1984 年, Shamir 为了简化证书管理, 绕开了基于目录的公钥认证框架的束缚, 建设性地提出了基于身份的公钥密码系统的思想[45]. 在这种公钥密码体制的密钥生成过程中, 公钥直接为实体的身份信息, 例如唯一的身份证号码、电子邮件地址等等, 因此基于身份的公钥密码体制可以很自然地解决公钥与实体的绑定问题. 在 Shamir 提出基于身份的签名方案后, 基于身份的加密方案却在很长时间内没有被提出. 直到 2001 年, Boneh 和 Franklin 基于双线性配对技术提出第一个实用的基于身份的公钥密码体制[46]. 此后, 双线性配对技术成为构造基于身份密码体制和基于身份数字签名方案的主流, 出现了许多优秀的成果[47].

虽然基于身份的密码简化了 CA 公钥证书的管理, 但是由于它需要一个可信的私钥生成器(PKG)为所有用户生成私钥, 一旦 PKG 的安全性出现问题, 那么整个基于身份的密码系统将会处于瘫痪状态. 因此, 研究 PKG 的安全性以解决密钥托管问题是基于身份密码中的一个亟待解决的问题. 目前, 为了保证 PKG 的安全性, 通过门限密码技术提出了分布式 PKG 密钥生成[48]; 为了解决密钥托管问题, 无证书的密码体制也在 2003 年正式提了出来, 并在近几年得到了广泛的研究[49]. 南湘浩教授提出的组合公钥(CPK)方案[50]具有一定的优势, 已经得到广泛的关注.

公钥密码学是一种复杂的系统, 其工作环境充满了敌意, 很容易遭受来自外部、内部的各种攻击. 然而在公钥密码的初期, 人们对于各种攻击方式缺乏理性的认识, 使得人们对于公钥密码体制的安全性的认识受到了很大的局限. 例如, 人们最初考虑的攻击都带有典型的“教科书式”的形式. 之后, 人们逐渐意识到了通过形式化的方法去设计和分析公钥密码的重要性. 当前, 研究可证安全的公钥密码方案已经成为现代密码学的一个主流课题[7, 9].

2.4 可证明安全的研究

可证明安全性(主要从计算复杂性理论的角度来考虑密码方案的安全性)是近年来公钥密码学领域里的一个研究热点. 简单地说, 可证明安全其实是一种“归约”的方法, 它首先确定密码方案所需要达到的安全目标, 然后根据攻击者的能力去定义一个攻击者模型, 并指出这个

攻击者模型与密码方案安全性之间的归约关系. 比如某个密码方案是基于 RSA 问题假设的, 那么可以通过攻击者模型去分析方案的安全性: 如果攻击者可以在多项式时间里以一个不可忽略的概率去攻击密码方案, 那么通过归约推导, 可以构造出另外一个攻击者以另外一个不可忽略的概率去解决 RSA 问题. 由于 RSA 问题在选取一定安全参数条件下是安全的, 因此我们可以从归约矛盾中反推出这个密码方案是安全的. 可证明安全性目前主要涉及公钥密码体制、数字签名以及密钥协商协议三方面.

对于公钥密码体制来讲, 攻击者模型中攻击者的攻击目标主要有以下几种: 我们最容易想到的是公钥密码体制的单向性安全, 即仅知道一些公开信息, 攻击者不能对一个给定的密文 c 恢复其对应的明文 m. 然而在很多应用场合, 仅仅考虑密码体制的单向性是不够的, 我们需要对密码体制的安全性提出更高的要求. 1982 年 Goldwasser 和 Micali 在这方面做出了开创性工作, 将概率引入了密码学, 提出了"语义安全"的定义[51]. 语义安全又称多项式时间不可区分安全性, 它主要基于以下场景: 考虑一个二阶段的攻击者 $A=(A_1, A_2)$, 刚开始的时候 A_1 在明文空间里挑选出长度相等的两个消息 m_0 和 m_1. 之后, 通过随机抛币得到比特 $b\in\{0,1\}$, 加密其中的消息 m_b, 并将加密的密文 c 交于 A_2. A_2 猜测密文 c 所对应的明文消息并返回比特 b 的猜测结果 b'. 通过定义 $Adv(A)=2\Pr[b'=b]-1$ 为任何多项式时间攻击者 A 的猜测优势, 如果 $Adv(A)$是可忽略的, 那么密码体制为语义安全的. 除语义安全之外, 1991 年 Dolev 等提出另外一个安全性概念——非延展安全性[52]. 对于这种安全性的攻击是指, 当给定一个密文 c 时, 攻击者试图构造出一个新的密文 c' 使得密文 c 和 c'所对应的明文 m 和 m'是意义相关的. 非延展安全性无疑是重要的. 然而, 由于非延展问题的计算本质, 对它们进行形式化处理非常困难. 另外, 在攻击者模型中, 根据攻击者在攻击过程中所获取的不同有用信息, 攻击者的攻击方式可分为选择明文攻击、有效性检验攻击、明文检验攻击、选择密文攻击等[53].

对于数字签名方案来讲, 在攻击者模型中, 攻击者根据实际应用的场合主要考虑 3 种攻击目标: (1)完全攻击. 攻击者经过攻击之后可以获得签名者的私钥, 显然, 这种攻击最为严重, 危害最大; (2)通用性伪造. 攻击者经过攻击之后可以构造出一个有效的算法以很高的成功概率对消息进行伪造签名; (3)存在性伪造. 攻击者经过攻击之后可以提供一个新的消息-签名对[54]. 存在性伪造所对应的安全级别称为存在性不可伪造. 虽然在大多数场合下, 由于输出的消息很有可能是没有任何意义的, 存在性伪造似乎看起来并不显得那么危险. 然而, 一个数字签名方案如果是存在性可以伪造的, 那么它本身就不可以保证签名者的真实身份. 2002 年, 更高要求的强存在性不可伪造概念被提出[55]. 另一方面, 在攻击者模型中, 对于一个攻击者来讲, 他可以利用尽可能多的信息资源去进行签名伪造, 因此, 根据攻击者所掌握的信息不同, 攻击者的攻击方式有: 已知公钥攻击、已知消息攻击和适应性选择消息攻击[53].

对于密钥协商协议来讲, 攻击者模型中定义的攻击者可以通过预先定义的一些预言机询问以控制所有的通信, 其中 Execute 预言机询问用于建模被动攻击; Send 预言机询问用于建模主动攻击; Reveal 预言机询问建模已知会话密钥攻击; Corrupt 预言机询问建模前向安全和密钥泄露伪造攻击. 最后, 通过 Test 询问建模密码协商的语义安全性. 协议的安全性模型 BR93 最初由 Bellare 和 Rogaway 在 1993 年提出[56]. 随后, 其他的安全性模型, 包括 BR95[57], BPR2000[58]和 CK2001[59]等. 在亚洲密码 2005 会议上, Choo 对这些模型之间的关系进行了深入的研究[60]. 关于可证安全的协议可参见文献[61].

在当前公钥密码学可证安全性研究领域里, 最为流行的证明方法为在随机预言机模型下

的安全性证明. 随机预言机模型是由 Bellare 和 Rogaway[62]在 1993 年基于 Fiat 和 Shamir 建议[63]的基础上提出的, 它是一种非标准化的计算模型. 在这个模型中, Hash 函数作为随机函数, 对于每一个新的查询, 将得到一个均匀随机的应答. 随机预言机模型在构建可证安全密码方案时, 系统中的各个角色共享随机预言机完成操作. 当体制设计完成之后, 再用实际的 Hash 函数将此随机预言机替换. 虽然随机预言机模型下的安全性证明非常有效, 但是随机预言模型证明的有效性还存在争议. 比如, 1998 年 Canetti 等[64]给出了一个在随机预言机模型下证明是安全的数字签名方案, 但在随机预言机的实例中却并不安全, 因此, 当前的可证安全性证明研究一方面继续基于随机预言模型进行证明, 另一方面也追求在不基于随机预言机条件下的标准模型下的证明. 1998 年, Cramer 和 Shoup[65]设计了第一个在标准模型下可证明安全的实际有效的公钥密码体制. 2004 年开始, 其他基于双线性配对技术在标准模型下可证安全的公钥密码体制[66,67]被不断地深入研究与发展.

除了现在广泛使用的基于数学的密码外, 人们还向非数学密码领域进行探索, 如量子密码[68]和 DNA 密码[69]等. 目前国内外在量子密钥分配实验方面的通信距离已突破 100 公里.

2006 年我国政府公布了自己的商用密码算法, 这是我国密码发展史上的一件大事. 这必将促进我国商用密码科学研究和应用的繁荣.

3 可信计算的研究与发展

在信息安全的实践中, 人们逐渐认识到, 大多数安全隐患来自于微机终端, 因此必须确保源头微机的信息安全. 而这必须从微机的芯片、硬件结构和操作系统等方面综合采取措施. 由此产生出可信计算的基本思想.

3.1 可信计算的发展

3.1.1 可信计算的出现

(1) 彩虹系列. 1983 年美国国防部制定了世界上第一个《可信计算机系统评价准则》TCSEC (trusted computer system evaluation criteria)[70]. 在 TCSEC 中第一次提出可信计算机(trusted computer)和可信计算基 TCB (trusted computing base)的概念, 并把 TCB 作为系统安全的基础.

1984 年美国国防部在推出了 TCSEC 之后, 作为补充又相继推出了可信数据库解释 TDI (trusted database interpretation)[71]和可信网络解释 TNI (trusted network interpretation)[72].

这些文件形成了彩虹系列信息系统安全指导文件.

(2) 彩虹系列的意义和局限. 在彩虹系列中第一次提出可信计算机和可信计算基的概念. 多年来彩虹系列一直成为评价计算机系统安全的主要准则, 至今对计算机系统安全有重要的指导意义.

然而由于历史的原因, 随着信息科学技术的发展, 彩虹系列也呈现出如下的局限性:

(a) 主要强调了信息的秘密性, 而对完整性、真实性考虑较少;

(b) 强调了系统安全性的评价, 却没有给出达到这种安全性的系统结构和技术路线.

3.1.2 可信计算的高潮

(1) TCPA 和 TCG 的出现. 1999 年, IBM, HP, Intel 和微软等著名 IT 企业发起成立了可信计

算平台联盟 TCPA (trusted computing platform alliance). TCPA 的成立, 标志着可信计算高潮阶段的出现. 2003 年 TCPA 改组为可信计算组织 TCG (trusted computing group), 标志着可信计算技术和应用领域的进一步扩大. TCPA 和 TCG 的出现形成了可信计算的新高潮. TCPA 和 TCG 已经制定了关于可信计算平台、可信存储和可信网络连接等一系列技术规范[73].

(2) TCG 可信计算的意义.

(a) 首次提出可信计算机平台的概念, 并把这一概念具体化到服务器、微机、PDA 和手机, 而且具体给出了可信计算平台的体系结构和技术路线.

(b) 不仅考虑信息的秘密性, 更强调了信息的真实性和完整性.

(c) 更加产业化和更具广泛性. 目前国际上(包括中国)已有 200 多家 IT 行业著名公司加入了 TCG. IBM, HP, DELL, NEC, GATEWAY, TOSHIBA, FUJITSU, SONY 等公司都研制出自己的可信 PC 机(台式机或笔记本机). ATMEL, INFINEON, BROADCOM, NATIONAL SEMICONDUCTOR 等公司都研制出自己的可信平台模块(TPM)芯片.

(3) 欧洲的可信计算. 欧洲于 2006 年 1 月启动了名为“开放式可信计算(open trusted computing)”的可信计算研究计划[74],有 23 个科研机构和工业组织参加研究.

(4) 可信计算的其他流派. 目前, 除了 TCG 的可信计算外, 还有另外两个可信计算流派.

① 微软流派. 尽管微软是 TCG 的发起单位, 但是微软却又独立提出了代号为 Palladium 的可信计算计划[75]. 微软用的是 Trustworthy computing, 而没有使用 Trusted computing. Intel 对微软的 Palladium 计划给予支持, 宣布了支持 Palladium 计划的 LaGrande 硬件技术, 并计划推出采用 LaGrande 技术的新一代奔腾处理器[76]. 后来, 微软又将这一计划改名为 NGSCB (next generation secure computing base).

微软将推出新一代操作系统 VISTA. VISTA 支持可信计算机制, 这将掀起可信计算的新高潮.

② 容错流派. 容错计算是计算机领域中一个重要的分支. 1995 年法国 Jean-Claude Laprie 和美国 Algirdas Avizienis 提出可信计算(dependable computing)的概念. 容错专家们自 1999 年将容错计算会议改名为可信计算会议(PRDC)后, 便致力于可信计算的研究. 他们的可信计算更强调计算系统的可靠性、可用性和可维性, 而且强调可信的可论证性[77].

我们认为在可信计算发展过程中, 不同的团体和学者从不同的角度来研究问题, 是很正常的事情, 是学术研究繁荣的表现. 随着可信计算技术的发展, 不同学派将会逐渐融合趋同.

3.2　中国的可信计算事业

我国在可信计算领域起步不晚, 水平不低, 成果可喜[78].

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 月通过国家密码管理局主持的技术鉴定. 鉴定指出: 这“是我国第一款自主研制的可信计算平台”. 它在系统结构和主要技术路线方面与 TCG 的规范是一致的, 在有些方面有所创新, 在有些方面也有差异. 这一成果获得 2006 年国家密码科技进步二等奖. 这一产品被国家科技部等四部委联合认定为“国家级重点新产品”. 目前, 已在我国政府、银行、军队等领域得到实际应用[79,80].

2004 年 6 月在武汉召开了中国首届 TCP 论坛. 2004 年 10 月在解放军密码管理委员会办公室和中国计算机学会容错专业委员会的支持下, 在武汉大学召开了第一届中国可信计算与信息安全学术会议. 2006 年 10 月, 在河北大学召开了第二届中国可信计算与信息安全学术会议.

2005 年联想集团的“恒智”芯片和可信计算机相继研制成功. 同年, 北京兆日公司的 TPM 芯片也研制成功. 这些产品也都通过国家密码管理局的鉴定和认可.

此外, 同方、方正、浪潮、天融信等公司也都加入了可信计算的行列. 武汉大学、中国科学院软件研究所等高校和研究所也都开展了可信计算的研究.

武汉大学、华中科技大学与 HP 公司合作进行了基于可信计算平台增强网格安全的研究, 其研究成果得到国际同行的好评[81].

我国各级政府都大力支持可信计算的研究、开发和应用.

至此, 中国的可信计算事业进入了蓬勃发展的阶段.

3.3 可信计算的基本思想与主要技术路线

3.3.1 可信计算的目标和基本思想

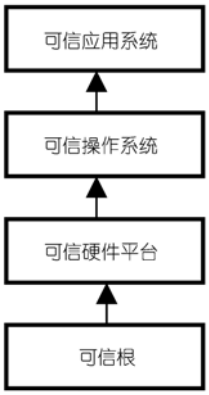

图 1 可信计算机系统

TCG 认为, 可信计算平台应具有数据完整性、数据安全存储和平台身份证明等方面的功能. 一个可信计算平台必须具备 4 个基本技术特征: 安全输入输出(Secure I/O)、存储器屏蔽(memory curtaining)、密封存储(sealed storage)和平台身份的远程证明(remote attestation). 可信计算产品主要用于电子商务、安全风险管理、数字版权管理、安全监测与应急响应等领域[73].

可信计算的基本思想是: 首先构建一个信任根, 再建立一条信任链, 从信任根开始到硬件平台, 到操作系统, 再到应用, 一级认证一级, 一级信任一级,把这种信任扩展到整个计算机系统, 从而确保整个计算机系统的可信.

一个可信计算机系统由可信根、可信硬件平台、可信操作系统和可信应用系统组成(如图 1 所示).

3.3.2 可信的概念与属性

(1) 可信的概念. 关于可信目前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:

TCG 用实体行为的预期性来定义可信: 一个实体是可信的, 如果它的行为总是以预期的方式达到预期的目标[73]. 这一定义的优点是抓住了实体的行为特征, 符合哲学上实践是检验真理的唯一标准的基本原则.

ISO/IEC 15408 标准定义可信为: 参与计算的组件、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 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, 而且这种可信赖还是可论证的[77].

我们给出自己的观点: 可信≈安全+可靠. 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[78].

IEEE 编辑出版了专门的可信计算汇刊: IEEE Transactions on Dependable and Secure Computing. 可见我们的观点与 IEEE 可信计算汇刊的观点是一致的.

(2) 信任的属性. 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.

信任具有二重性, 既具有主观性又具有客观性.

信任不一定具有对称性, 即 A 信任 B 不一定就有 B 信任 A.

信任可度量. 也就是说信任的程度可以测量, 可以划分等级.

信任可传递, 但不绝对, 而且在传播过程中有损失.

信任具有动态性, 即信任与与环境(上下文)和时间等因素相关.

(3) 信任的获得方法. 信任的获得方法主要有直接和间接两种方法. 设 A 和 B 以前有过交往, 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, 在这种情形下, 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 有过直接的交往经验, 我们称之为间接信任值, 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形, 这时便产生了信任链.

3.3.3 信任的度量与模型

目前, 关于信任的度量理论与模型主要有基于概率统计的信任模型[82,83]、基于模糊数学的信任模型[84]、基于主观逻辑的信任模型[85]、基于证据理论的信任模型[86]和基于软件行为学的信任模型[87]等. 但是目前的这些模型都还需要进一步优化, 朝着既能准确刻画客观事实, 又尽量简单实用的方向发展. 值得特别提出的是, 应当着重研究软件可信性的度量模型, 可信计算迫切需要这方面的理论支持.

3.3.4 信任根和信任链

信任根和信任链是可信计算平台的最主要的关键技术之一.

信任根是系统可信的基点. TCG 认为一个可信计算平台必须包含 3 个信任根: 可信测量根 RTM(root of trust for measurement)、可信存储根 RTS(root of trust for storage)和可信报告根 RTR(root of trust for reporting). 而信任根的可信性由物理安全和管理安全确保.

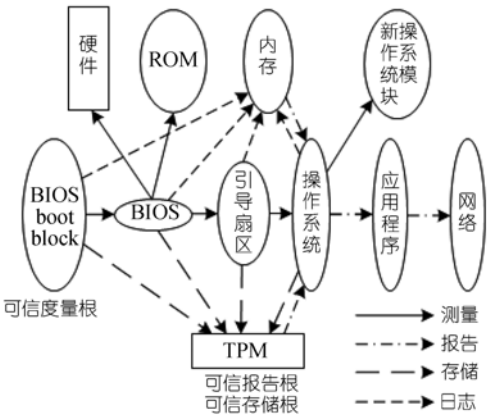

图 2　TCG 可信 PC 的信任链

信任链把信任关系从信任根扩展到整个计算机系统. 在 TCG 的可信 PC 技术规范中, 具体给出了可信 PC 中的信任链, 如图 2 所示. 我们可以看出: 这个信任链以 BIOS Boot Block 和 TPM 芯片为信任根, 经过 BIOS→OSloader→OS. 沿着这个信任链, 一级测量认证一级, 一级信任一级, 以确保整个平台的系统资源的完整性.

3.3.5 可信测量、存储、报告机制

可信测量、存储、报告机制是可信计算的另一个关键技术. 可信计算平台对请求访问的实体进行可信测量, 并存储测量结果. 实体询问时平台提供报告.

应当指出, 根据图 2 所进行的可信测量只是系统开机时的系统资源静态完整性测量, 因此只能确保系统开机时的系统资源静态完整性. 这不是系统工作后的动态可信测量, 因此尚不能确保系统工作后的动态可信性. 然而, 由于软件可信测量理论与技术的限制, 目前, 无论是国外还是国内的可信计算机都还未能够完全实现动态可信测量、存储、报告机制.

3.3.6 可信计算平台

TCG 不仅提出了可信服务器、可信 PC 机、可信 PDA 和可信手机的概念, 而且具体给出了技术规范.

可信 PC 是已经产品化的可信计算平台, 其主要特征是在主板上嵌有可信构建模块 TBB. 这个 TBB 就是可信 PC 平台的信任根, 它包括用于可信测量的根核 CRTM (core root of trust for measurement)和可信平台模块 TPM (trusted platform module)以及它们同主板之间的连接.

3.3.7 可信平台模块 TPM

可信平台模块 TPM 是一种 SOC 芯片, 它是可信计算平台的信任根(可信存储根和可信报告根), 其结构如图 3 所示. 它由 CPU、存储器、I/O、密码协处理器、随机数产生器和嵌入式操作系统等部件组成. 完成可信度量的存储、可信度量的报告、密钥产生、加密和签名、数据安全存储等功能.

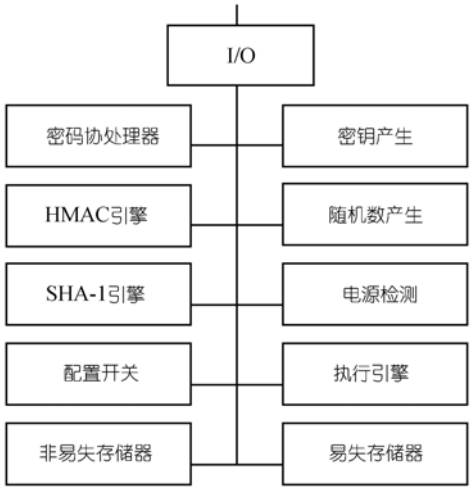

图 3 TCG 的 TPM 框图

必须注意: TPM 是可信计算平台的信任根. 中国的可信计算机必须采用中国的根芯片, 中国的根芯片必须采用中国的密码.

3.3.8 支撑软件

TSS (TCG software stack)是可信计算平台上 TPM 的支撑软件. TSS 的作用主要是为操作系统和应用软件提供使用 TPM 的接口.

TSS 的结构可分为内核层、系统服务层和用户程序层.

内核层的核心软件是可信设备驱动 TDD 模块, 它是直接驱动 TPM 的软件模块, 由其嵌入式操作系统所确定. 系统服务层的核心软件是可信设备驱动库 TDDL 和可信计算核心服务模块 TCS, 其中 TDDL 提供用户模式下的接口, TCS 对平台上的所有应用提供一组通用的服务. 用户程序层的核心软件是可信服务提供模块 TSP. TSP 给应用提供的最高层的 API 函数, 使应用程序可以方便地使用 TPM.

工作的流程如下: 应用程序将数据和命令发给应用 API 函数 TSP, TSP 处理后通过 TCS 再传给 TDDL. TDDL 处理后传给 TDD. TDD 处理并驱动 TPM. TPM 给出的响应, 反向经 TDD, TDDL, TCS, TSP 传给应用.

有了 TSS 的支持, 不同的应用都可以方便地使用 TPM 所提供的可信计算功能.

3.3.9　可信网络连接 TNC

TNC (trusted network connect)的目的是确保网络访问者的完整性. TNC 的结构分为 3 层. 网络访问层: 从属于传统的网络互联和安全层, 支持现有的如 VPN 和 802.1X 等技术, 这一层包括 NAR (网络访问请求)、PEP (策略执行) 和 NAA (网络访问管理) 3 个组件. 完整性评估层: 这一层依据一定的安全策略评估 AR(访问请求者)的完整性状况. 完整性测量层: 这一层负责搜集和验证 AR 的完整性信息.

TNC 通过网络访问请求, 搜集和验证请求者的完整性信息, 依据一定的安全策略对这些信息进行评估, 决定是否允许请求者与网络连接, 从而确保网络连接的可信性.

虽然 TNC 可确保网络连接的可信性向可信网络方面迈出了重要的一步, 但是网络根本目的在于数据交换和资源共享, 没有数据交换和资源共享方面的可信是远远不够的.

3.4　目前可信计算发展中存在的一些问题

目前可信计算已经成为国际信息安全领域中的一个新潮流. 但是, 目前可信计算发展中还存在一些必须研究解决的问题[78].

1. 理论研究相对滞后.

无论是国外还是国内, 在可信计算领域都处于技术超前于理论, 理论滞后于技术的状况. 可信计算的理论研究落后于技术开发. 至今, 尚没有公认的可信计算理论模型.

可信测量是可信计算的基础, 但是目前尚缺少软件的动态可信性的度量理论与方法.

信任链技术是可信计算平台的一项关键技术, 然而信任链的理论, 特别是信任在传递过程中的损失度量尚需要深入研究, 以便把信任链建立在坚实的理论基础之上.

理论来源于实践, 反过来又指导实践. 没有理论指导的实践最终是不能持久的. 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.

2. 一些关键技术尚待攻克.

目前, 无论是国外还是国内的可信计算机都没能完全实现 TCG 的 PC 技术规范. 如, 动态可信度量、存储、报告机制, 安全 I/O 等.

3. 缺少操作系统、网络、数据库和应用的可信机制配套.

目前 TCG 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, 这方面尚缺少可信技术规范. 只有硬件平台的可信, 没有操作系统、网络、数据库和应用的可信, 整个系统还是不安全的[88,89].

4. 缺少安全机制与容错机制的结合.

安全可靠是用户对可信计算的希望, 因此必须坚持安全与容错相结合的技术路线, 目前这方面的研究还十分缺乏.

5. 可信计算的应用需要开拓.

可信计算的应用是可信计算发展的根本目的. 目前可信 PC 机、TPM 芯片都已经得到实际应用, 但应用的规模和覆盖范围都还不够, 有待大力拓展.

3.5　可信计算的研究领域

现阶段的可信计算热潮是从可信 PC 平台开始的, 但是它涉及的研究和应用领域却要广泛得多. 可信计算的理论、关键技术和应用应当是研究的重点[78].

1. 关键技术.

① 可信计算的系统结构: 可信计算平台的硬件结构, 可信计算平台的软件结构.

② TPM 的系统结构: TPM 的硬件结构, TPM 的物理安全, TPM 的嵌入式软件.

③ 可信计算中的密码技术: 公钥密码, 对称密码, HASH 函数, 随机数产生.

④ 信任链技术: 完整的信任链, 信任链的延伸.

⑤ 信任的度量: 信任的动态测量、存储和报告机制.

⑥ 可信软件: 可信操作系统, 可信编译, 可信数据库, 可信应用软件.

⑦可信网络: 可信网络结构, 可信网络协议, 可信网络设备, 可信网格.

2. 理论基础.

① 可信计算模型: 可信计算的数学模型, 可信计算的行为学模型.

② 可信性的度量理论: 软件的动态可信性度量理论与方法.

③ 信任链理论: 信任的传递理论, 信任传递过程中的损失度量.

④ 可信软件理论: 可信软件工程方法学, 可信程序设计方法学, 软件行为学.

3. 可信计算的应用.

4 网络安全的研究与发展

网络安全主要包括两部分, 即网络自身的安全性和网络信息的安全性, 本节主要关注网络信息的安全性. 国内外学术界和企业界围绕网络的安全需求主要对网络内容安全、网络认证授权、防火墙、虚拟专用网、网络入侵检测、网络脆弱性检测、安全接入、安全隔离与交换、安全网关、安全监控与管理、网络安全审计、恶意代码检测与防范、垃圾邮件处置、应急响应等方面进行了研究, 并研发了大量的相关网络安全产品, 初步形成了一个产业. 可以预测, 基于网络的安全技术是未来信息安全技术发展的大趋势. 本节主要从公开密钥基础设施、入侵检测系统、网络应急响应、网络可生存性、可信网络 5 个方面概述了网络安全的研究现状及发展趋势[90−96].

4.1 公开密钥基础设施

公开密钥基础设施(PKI)技术是一种能够解决网络环境中信任与授权问题的重要技术, 包括身份的真实性、数据的机密性、文件的完整性、行为的不可否认性等. 近几年, 产业界、学术界和政府部门对 PKI 技术的研究与应用都给予了高度关注. 世界大型信息产业公司如 IBM, MICROSOFT, BALTIMORE, CERTCO, RSA, FUJITSU, MITSUBISHI 等都有 PKI 产品. 中国的很多信息产业公司如吉大正元、上海维豪、济南得安等也都有自主的 PKI 产品. 我国学术界如信息安全国家重点实验室也对 PKI 标准、PKI 体系结构、PKI 自身安全技术、交叉认证技术等进行了系统研究并取得了一批先进的技术成果. 我国国家标准化组织积极推进 PKI 标准的研究与制定, 并已经发布了一批相关标准和规范.

国内外学术界和产业界已经在信任及信任验证机制(包括信任模型、信任策略、验证机制等)、密钥管理技术(包括 CA 及用户的公、私密钥对产生、存储、备份、恢复等技术)、证书管理技术(包括证书库技术、证书和密钥对的作废和自动更换技术)、PKI 安全核心部件(包括不同规模的 CA 系统、RA 系统和 KM 系统等)、PKI 技术产品(包括各种各样的 PKI 应用终端系统, 如电子钱包、电子邮件、电子公章等应用终端)、CA 交叉认证技术和弹性、入侵容忍 CA 技术

等方面取得了一批创新性和实用性成果. 值得一提的是, “十五”期间中国在 PKI 关键技术研究与应用方面也取得了突破性进展, 取得的技术成果能够满足在大型网络环境下对 PKI 技术的实际需求, 并成功应用于政府、军队和金融等国家重要部门.

PKI 是解决网络环境下信任与授权问题的关键, 特别是在电子商务和电子政务系统中有着广阔的应用前景. PKI 的发展呈现出以下四大趋势:

1) 应用化趋势. 随着电子政务和电子商务的应用, 在当前情形下, PKI 仍是解决不信任的网络环境下的信任与授权问题的最佳选择, 必然会得到广泛应用. 但对应用和验证模式等问题仍需进行进一步研究和探讨.

2) 标准化趋势. PKI 的广泛应用必将造成互连、互通和互操作问题, 除了技术解决方案外, 标准是解决互连、互通和互操作问题的重要措施.

3) 集成化趋势. 与生物特征识别、基于身份的公钥密码、可信计算平台、入侵容忍 CA 和自适应 CA 等新技术和新应用的融合.

4.2　网络入侵检测系统

入侵检测系统(IDS)包括基于网络的 IDS 和基于主机的 IDS 两大类, 本节主要关注基于网络的 IDS. 网络 IDS 能够帮助网络系统快速发现网络攻击的发生, 扩展了系统管理员的安全管理能力, 提高了信息安全基础结构的完整性. 它从网络系统中的若干关键点收集信息, 并分析这些信息, 观察网络中是否有违反安全策略的行为和袭击的迹象.

国内外产业界和学术界对 IDS 进行了大量系统深入的研究, 并形成了大量的实用产品, 我国很多信息产业公司如联想、启明星辰、南大苏富特等都有自主的 IDS 产品, 很多研究机构都研制了 IDS 原型系统并发表和出版了大量学术论文和著作.

1990 年在分布式系统上开始采用入侵检测技术, 网络入侵检测技术诞生. 加州大学戴维斯分校的 Heberlein 等人开发出了 NSM(network security monitor). 该系统第一次直接将网络流作为审计数据来源.

1992 年由美国空军、国家安全局和能源部共同资助的分布式入侵检测系统(DIDS)的研究取得了进展. DIDS 集成了 Haystack 和 NSM 两种已有的入侵检测系统, 综合了两者的功能, 并在系统结构和检测技术上进行了改进. DIDS 由主机监视器、局网监视器和控制器组成, 分析引擎是基于规则的专家系统. DIDS 采用分布的数据采集和分布的数据分析, 但核心数据分析是集中控制的.

1994 年, Crosbie 和 Spafford 提出利用自治代理(autonomous agents)以便提高 IDS 的可扩展性、可维护性、效率和容错性.

1996 年 Stanford-Chen 为了解决入侵检测系统的可扩展性提出了 GRIDS(graph-based intrusion detection system)系统, 该系统对大规模自动或协同攻击的检测很有效. GRIDS 使用图形描述大规模网络中网络行为, 针对大范围的网络攻击比较有效. 其缺陷在于只是给出了网络连接的图形化表示, 而具体的入侵判断仍需人工完成.

1998 年至今, 这一阶段在检测方向上的新理论不多, 更偏重于检测算法的改进. 检测算法的改进集中在基于网络的入侵检测、分布式入侵检测、基于智能代理的入侵检测、神经网络和基因算法等几个领域. 为了提高 IDS 产品、组件及与其他安全产品之间的互操作性, 这一阶段人们开始高度重视 IDS 的标准化工作.

1998 年, 美国国防高级研究计划署(DARPA)制定了通用入侵检测框架(CIDF), 其最早由加州大学戴维斯分校安全实验室主持起草工作. CIDF 主要介绍了一种通用入侵说明语言(CISL), 用来表示系统事件、分析结果和响应措施. 为了把 IDS 从逻辑上分为面向任务的组件, CIDF 试图规范一种通用的语言格式和编码方式以表示在组件边界传递的数据. CIDF 所做的工作主要包括 4 部分: IDS 的体系结构、通信体制、描述语言和应用编程接口(API). 同时, CIDF 定义了通用入侵规范语言(CISL), 描述入侵行为. CIDF 在系统扩展性和规范性上比较有优势.

IDS 经过 20 多年的发展, 虽然已经取得了很大的进展, 但面对网络技术的迅猛发展和攻击行为的日益复杂, 暴露出许多不足, 仍需进一步深化和拓展. IDS 的发展呈现出以下三大趋势:

1) 迎合实际应用的发展趋势. 大量高速网络技术如 ATM、千兆以太网等相继出现, 如何实现宽带高速网络环境下的实时入侵检测已经成为面临的现实问题; 为了适应大规模分布式的检测需求, 仍需进一步研究大规模分布式检测技术与方法.

2) 标准化趋势. IDS 的大规模应用必然要求提高 IDS 产品、组件及与其他安全产品之间的互操作性, 标准化是未来 IDS 发展的必然趋势.

3) 向入侵防御系统(IPS)方向发展的趋势. IPS 是 IDS 的一个发展方向, 产业界已经从 2003 年开始陆续推出了 IPS 产品, 而把 IDS 功能当作 IPS 运行时可选的一种模式, 从而 IPS 逐渐替代了 IDS, 成为入侵检测类产品的主打产品. IPS 是对 IDS 的包容和覆盖, 同时具备了像防火墙一样的保护能力. IPS 可以有效解决与防火墙联动时延的问题, 减少联动产生的副作用.

4.3 网络应急响应

随着网络技术及相关技术的发展, 原先采取的传统的、静态的安全保密措施已不足以抵御计算机黑客入侵及有组织的信息手段的攻击, 必须建立新的安全机制, 于是在 1989 年美国国防部资助卡内基-梅隆大学, 为其建立了世界上第一个“计算机应急小组(CERT)”及其协调中心(CERT/CC). CERT 的成立标志着信息安全由静态保护向动态防护的转变.

1989 年美国国防部成立 CERT/CC 之后不久, 美国陆海空三军和国防部、国家安全局及国防通信局相继成立了应急组织, 接着美国联邦调查局、能源部、商业部、航空航天局等重要部门也陆续成立了应急处理机构. 到目前为止, 美国国防部、联邦政府各部门及各大企业, 已经建立了 50 多个计算机应急组织, 在美国国家基础设施保护委员会及其协调委员会的协调下, 已经形成覆盖全国的应急网络.

欧洲、大洋洲、北美和亚洲许多国家和地区, 特别是发达国家都已相继建立了信息安全应急组织. 根据美国和澳大利亚应急组织的提议, 于 1990 年 11 月成立了国际“计算机事件响应与安全工作论坛”(FIRST)组织. 此外, 亚太国家和地区也成立了“亚太事件响应协调组织”(APSIRC). 建立信息安全应急组织, 完善信息安全保障体系, 加强国际合作, 已成为信息安全领域的国际潮流.

我国已经从各种层面建立了很多应急处理组织, 如 1999 年 5 月成立的中国教育和科研网计算机应急小组(CCERT), 2000 年 10 月组建的“国家计算机网络应急技术处理协调中心”(简称 CNCERT/CC). CNCERT/CC 是在信息产业部互联网应急处理协调办公室的直接领导下, 组织国内计算机网络安全应急组织进行国际合作和交流的机构. 它负责协调我国各计算机网络安全事件应急小组(CERT), 共同处理国家公共电信基础网络上的安全紧急事件, 为国家公共电

信基础网络、国家主要网络信息应用系统以及关键部门提供计算机网络安全的监测、预警、应急、防范等安全服务和技术支持, 及时收集、核实、汇总、发布有关互联网安全的权威性信息. 目前, 国内很多科研机构、大专院校、以及企事业单位也都积极参与到网络应急响应的研究行列. 在体系结构方面已经形成了经典的 PDCERF 方法学, 即准备、检测、抑制、根除、恢复和跟踪 6 个阶段; 在核心工具方面已经开发了大量的实用产品与系统.

虽然学术界和产业界都对应急响应进行了广泛深入的研究, 也取得了很多优秀成果, 但有许多问题仍需要深化研究.

1) 应急响应体系研究. 包括应急响应组织体系、应急响应技术体系和应急响应支援体系等.

2) 技术标准研究与制订. 应急响应标准化工作是应急响应体系通信协调机制的基础, 同时也是应急响应联动系统正常运作的基础. 应急响应标准化工作是围绕着安全事件流进行的, 即安全事件从发生一直到消除的整个过程, 包括网络安全事件的发现、上报, 对安全事件分析、归类, 安全事件的传递、分析、决策, 联动响应, 安全事件备案等. 如应急响应流程标准、安全事件分类标准、网络安全事件报告格式标准, 安全事件描述和交换格式标准.

3) 实验环境建设. 建设实验环境是解决应急响应体系实际应用研究的必然需求, 一个典型的小型化并能充分模拟和描述大规模网络特征的硬件实验环境再配合以相应的软件模拟, 可以提供一个理论研究的实践平台和应用研究的验证环境.

4) 核心工具开发. 应急响应核心工具开发是建设应急响应体系的关键技术环节, 主要包括: 信息共享与分析中心 ISACISAC, 大型网络安全事件协同预警定位与快速隔离控制, 安全事件预案系统, 大规模网络安全状态模拟平台, 联动系统, 备份与恢复系统.

4.4　网络可生存性

网络可生存性(survivability)的目标是在网络系统遭受攻击、失效或出现事故时, 能够及时地完成其任务的能力. 可生存能力的基本思想是即使在入侵成功后, 系统的重要部分遭到损害或摧毁时, 系统依然能够完成任务, 并能及时修复被损坏的服务能力. 网络可生存性理论的研究已成为网络安全的一个新的研究热点, 许多组织和研究机构都在进行着这方面的工作. 弗吉尼亚大学和 Portland 大学正在合作开展“关键基础设施保护的信息可生存性”工程研究, 包括关键基础设施的可生存性评测、军用和民用基础设施研究及可生存性体系结构工程等. 目前该理论还很不成熟, 许多问题没有解决, 缺乏深入的理论研究和可实施性研究.

网络可生存性主要突出系统必须具有 4 个关键特性: 抵抗能力(resistance)、识别能力(recognition)、恢复能力(recovery)以及自适应能力(adaptation). 网络可生存能力的提出, 突破了狭隘的传统安全观念, 使人们意识到安全不是靠纯粹的技术打造, 它将计算机安全与风险管理结合在一起, 共同来保护系统, 最大限度地减少来自攻击、失效和事故对系统的影响. 可生存能力有一个很明确的、以服务为核心的保护对象, 即使攻击已造成网络系统一定程度上的损害, 仍然要保证网络系统基本服务的持续.

网络可生存性理论的核心是对无边界系统的可生存性理论的研究. 无边界系统强调的是一个系统中的所有参与者都无法获得关于这个系统的完整、准确的信息. 现实中的计算机大规模互联网络, 乃至电信网、电力网等均符合这个条件. 网络计算环境的趋势是向无限网络基础结构发展. 无限网络中没有统一的管理机构控制它的组成部分. 在这个网络中, 每个参与者对

整体的看法是不全面的, 必须信任和依赖于临近的参与者提供的信息, 而且不能在它的范围外行使控制权. 这就要求我们突破传统的方法, 建立起一整套适应于在信息不全面、不准确的条件下, 对系统的生存性进行分析的方法, 以及在缺乏相互间协调的情况下, 进行相互间合作的方法.

目前, 网络可生存性理论的主要研究内容有:

1) 可生存网络分析方法. 对大规模网络系统生存能力进行分析, 包括分析对系统生存能力的威胁, 进而找出降低风险的方法, 如系统中的敏感的服务; 具有强抵抗力、识别能力和恢复能力的构架元素; 具有强生存能力的系统架构等.

2) 紧急算法(emergent algorithms). 紧急算法是用来研究无边界系统在平时和受到各种类型的攻击和破坏时, 其生存性的表现情况. 应当具有不同于传统意义下的分级或者分布式算法的特征, 算法的研究方式应当类似于自然过程的研究方法, 如生物系统、经济系统等. 紧急算法应当适应于无法获得完全的和准确的信息, 没有中央控制部分、分级结构以及单独的、可区分的漏洞信息的情形. 同时, 紧急算法还要考虑到在没有相互协调的基础上的相互合作. 这些都是传统理论所无法解决或是难以解决的.

3) 可生存系统模拟研究. 由于无边界系统的特殊性, 现有的模拟方法将不能够完全适用于无边界网络, 需要我们进一步开发新的模拟方法.

4) 相应软件及工具的开发. 包括能够在网络中采集信息的代理软件和硬件, 网络安全事件预警、定位和隔离的软件, 系统环境模拟工具.

总体来讲, 我国政府部门、学术界和产业界都高度重视网络安全的研究, 形成了系列实用化成果, 但仍有许多问题需要进一步深化和拓展, 应特别加强以下几个方面的研究:

1) 网络应急响应. 从实际出发, 加强网络应急响应体系和技术标准的研究, 实验环境的建设, 核心工具的开发.

2) 网络可生存性(survivability). 网络可生存性理论已成为网络安全的一个新的研究热点, 目前该理论还很不成熟, 许多问题没有解决, 缺乏深入的理论研究和可实施性研究.

3) 移动和无线网络安全. 研究移动和无线网络的安全体系结构、安全策略、安全机制、安全管理、安全监控和安全评估方法等.

4.5 可信网络

随着网络的广泛应用和攻击技术的发展, 使得分散、孤立、单一的网络安全防御技术已无法对付越来越狡猾的攻击. 如果说过去的网络以追求高效率为主要目标的话,今天的网络则应能提供高可信的服务. 可信性成为衡量网络服务质量的重要标准. 于是, 近年来在国际上出现了可信网络这一新的研究方向. 可信网络的主要特征是具有安全性、可生存性和可控性[88]. TCG 提出了可信网络连接的技术规范 TNC, 向网络可信迈出了可喜的一步[73]. 可信网络是一个具有挑战性的研究课题, 必定会吸引众多的学者加入研究.

5 信息隐藏的研究与发展

信息隐藏(information hiding)是一门既古老又年轻的学科. 信息隐藏可以分为隐蔽信道技术和多媒体信息隐藏技术.

5.1　隐蔽信道

隐蔽信道可以进一步分为阈下信道(sbliminal channel, 也称为潜信道)[97]和隐信道(covert channel). 阈下信道是建立在公钥密码体制的数字签名和认证上的一种隐蔽信道, 其宿主是密码系统. 在阈下信道中的发送端, 阈下信道信息在一个密钥的控制下进行随机化, 然后在嵌入算法的作用下嵌入公钥密码系统的输入或输出参数. 在接收端, 系统在实现数字签名中的签名验证过程后, 提取算法完成了收方对阈下消息的提取. 除接收者外, 任何其他人均不知道密码数据中是否有阈下消息存在[98].

至今, 人们已经提出了多种阈下信道的构造办法. 这些方法基本上是建立在基于离散对数困难问题和椭圆曲线离散对数问题的数字签名系统上的. 研究的焦点主要集中在阈下信道的容量、阈下信道的安全性和新的阈下信道的设计上.

隐信道是在公开信道中建立起来的一种进行隐蔽通信的信道, 为公开信道的非法拥有者传输秘密信息. 隐信道可以分为隐蔽存储信道(covert storage channel)和隐蔽时间信道(covert timing channel)[99]. 在隐蔽存储信道中, 一个进程将信息写入存储点而通过另一个进程从存储点读取. 在隐蔽时间信道中, 一个进程将自身对系统资源(例如 CPU 时间)的使用进行调制以便第二个进程可以从真实反应时间中观察到影响, 以此实现消息的传递. 二者的主要区别是信息调制的方式的不同. 隐信道的主要研究问题包括: 隐信道的构造、隐信道的识别方法、隐信道的带宽估计方法、隐信道的消除等.

5.2　多媒体信息隐藏

多媒体信息隐藏[100]是以多媒体信号作为宿主载体, 利用多媒体数据的数据冗余(redundancy)和人们的听/视觉冗余来隐藏秘密信息的技术. 从听、视觉科学和信号处理的角度, 信息隐藏可以视为在强背景(原始图像/语音/视频等)下叠加一个弱信号(隐藏的信息). 由于人的听觉系统(HAS)和视觉系统(HVS)分辨率受到一定的限制, 只要叠加的信号幅度低于 HAS/HVS 的感知门限, HAS/HVS 就无法感觉到信号的存在. 因此, 通过对原始图像/语音/视频做有限制的改变, 就有可能在不改变听觉/视觉效果的情形下嵌入一些信息. 由于待嵌入的信息总可以转化为二进制序列, 因此, 嵌入的秘密信息的形式可以是多种多样的, 包括随机序列、数据、文字、图像/图形、语音/音频、视频等.

根据应用场合对隐藏信息的不同需求, 信息隐藏技术可分为隐写术(steganography)[101]和数字水印(digital watermarking)[102]两个主要分支. 隐写术可以进一步分为秘密隐写和普通隐写. 前者着重于信息伪装以实现秘密信息的传递, 后者解决信息的隐含标识. 类似地, 数字水印也可以分为鲁棒水印和脆弱水印. 前者用于多媒体的版权保护而后者用于内容认证. 依据隐藏协议, 信息隐藏还可分为无密钥信息隐藏、私钥信息隐藏、公钥信息隐藏.

对信息隐藏的基本要求包括: 稳健性(robustness)、不可检测性(undetectability)、信息隐藏容量(capacity)、计算复杂性等. 其中, 稳健性、不可检测性(包括听/视觉系统的不可感知性和统计上的不可检测性)和信息隐藏容量是信息隐藏的 3 个最主要的因素. 从技术实现的角度, 这 3 个因素互相矛盾, 因此, 对不同的应用需求, 需要有所侧重. 对于秘密隐写, 需要重点考虑不可检测性; 普通隐写则要求有较大的信息隐藏容量; 鲁棒水印对稳健性有特别高的要求; 脆弱水印对稳健性的要求则有双重性: 对恶意篡改脆弱而对正常的信号处理过程鲁棒. 除了可见水印外, 不可检测性应该是多媒体信息隐藏技术的共同要求.

安全性和稳健性将是目前多媒体信息隐藏走向应用的关键问题. 对于秘密隐写, 其安全性体现在如何对抗统计检测; 而隐写分析[103]则是如何有效检测低隐藏量下的秘密信息. 对于数字水印, 防止非法检测/篡改等安全问题和水印抵抗以几何攻击为代表的恶意攻击是急需解决的技术.

秘密信息的隐藏空间和隐藏方式是多媒体信息隐藏算法的两个基本要素. 秘密信息的隐藏空间称为嵌入工作域. 根据工作域, 多信息隐藏算法主要可分为两类: 时域/空域的方法[104]和变换域的方法[105]. 时域/空域方法把(处理后的)秘密信息直接嵌入到多媒体信号的时域/空域格式中. 由于听/视觉系统的特点, 直接嵌入时域/空域的信号幅度相对较低, 因而隐藏信号的稳健性通常较差. 变换域的方法是先对作为宿主载体的多媒体信号进行某种形式的数学变换(通常采用正交变换), 再将(处理后的)秘密信息嵌入到变换系数中, 之后再完成反变换. 常用于信息隐藏的正交变换有离散小波变换(DWT)、离散余弦变换(DCT)、离散 Fourier 变换(DFT)等. 由于正交变换/反变换具有将信号能量进行重新分布的特点, 变换域的方法可以将嵌入到变换系数的隐藏信号能量在时域/空域中进行扩散, 从而有效解决隐藏信息不可检测性与稳健性的矛盾. 类似于其他的压缩域处理技术, 可以把秘密信息直接嵌入到压缩域系数中而避免解压缩-再压缩运算, 这称为压缩域信息隐藏方法, 它是变换域方法的一种特殊形式.

不论是时域/空域的方法还是变换域的方法, 都需要进行数据的嵌入. 这由嵌入公式来实现. 有两种经典的嵌入方法: 叠加嵌入[105]和映射嵌入. 在叠加嵌入中, 待嵌入的数据作为弱信号用叠加的方式嵌入到宿主的时域/空域或变换域系数中. 在检测端, 通过最优检测和估值理论来设计检测器, 以提取隐藏的信号. 在映射嵌入中, 宿主信号的系数被映射函数映射到由嵌入比特确定的特征值, 隐藏数据的提取通过映射函数来确定. 最低有效位(LSB)替换和量化索引调制(QIM)[106]是典型的映射嵌入方式. 映射嵌入在实现隐藏信息的盲检测方面具有明显的优点.

至今, 在多媒体信息隐藏领域开展的研究工作包括信息隐藏基本理论与方法、信息隐藏的数字水印算法、隐写分析和数字水印攻击方法、信息隐藏协议、信息隐藏的应用等. 信息隐藏的应用领域包括隐蔽通信、多媒体版权保护、多媒体认证、信息的隐含标注等. 由于其在军事、安全、工业界广泛的应用前景, 它作为一类新的信息安全技术, 正在得到人们越来越密切的关注.

参 考 文 献

1 沈昌祥. 关于加强信息安全保障体系的思考. 信息安全纵论. 武汉: 湖北科学技术出版社, 2002
2 张焕国, 王丽娜, 黄传河, 等. 信息安全学科建设与人才培养的研究与实践. 全国计算机系主任(院长)会议论文集. 北京: 高等教育出版社, 2005
3 Pfleeger C P, Pfleeger S L. Security in Computing. 3rd Editon. NJ: Prentice Hall, 2003
4 孟庆树, 王丽娜, 傅建明, 等(译). 密码编码学与网络安全——原理与实践(第四版). 西安: 电子工业出版社, 2006
5 卿斯汉, 刘文清, 温红予. 操作系统安全. 北京: 清华大学出版社, 2004
6 Schneier B. Applied Cryptography, Protocols, Algorithms and Source Code in Co New York: John Wiley & Sons, 1996.
7 Mao W. Modern Cryptography: Theory and Practice. NJ: Prentice Hall PTR, 2003
8 冯登国. 国内外密码学研究现状及发展趋势. 通信学报, 2002, 23(5): 18—26
9 曹珍富, 薛庆水. 密码学的发展方向与最新进展, 计算机教育, 2005, 19—21
10 Wang Xiaoyun, Feng Dengguo, Lai Xuejia, et al. Collisions for hash functions MD4, MD5, HAVAL-128 and RIPEMD. Cryptology ePrint Archive: Report 2004/1999, Aug. 2004

11 Wang Xiaoyun, Lai Xuejia, Feng Dengguo, et al. Cryptanalysis of the hash function MD4 and RIPEMD. In: Advance in Cryptology-Eurocrypt'05, LNCS 3494. Berlin: Springer-Verlag, 2005. 1—18

12 Wang Xiaoyun, Yu Hongbo. How to break MD5 and other hash functions. In: Advance in Cryptology – Eurocrypt'05, LNCS 3494. Berlin: Springer-Verlag, 2005. 19—35

13 Wang Xiaoyun, Yu Hongbo, Yin Yiqun Lisa. Efficient collision search attacks on SHA-0. In: Advance in Cryptology – Crypto 05, LNCS 3621. Berlin: Springer-Verlag 2005. 1—16

14 Wang Xiaoyun, Yin Yiqun Lisa, Yu Hongbo. Finding collisions in the full SHA-1. In: Advance in Cryptology –Crypto 05, LNCS 3621. Berlin: Springer-Verlag, 2005. 17—36

15 Federal Information Processing Standards Publication (FIPS 197) Advanced Encryption Starndard (AES), Nov. 26, 2001

16 张焕国, 冯秀涛, 覃中平,等. 演化密码与 DES 的演化研究. 计算机学报, 2003, 26(12): 1678—1684

17 孟庆树, 张焕国, 王张宜, 等. Bent 函数的演化设计, 电子学报, 2004, 32(11): 1901—1903

18 Zhang Huanguo, Wang Yuhua, Wang Bangju, et al. Evolutionary Random number Generator Based on LFSR. Wuhan University Journal of Natural Science, 2007, 12(1): 179—182

19 罗启彬, 张键, 周颉. 混沌密钥序列的复杂性分析. 密码学进展——CHINACRYPT'2006. 北京: 中国科学技术出版社, 2006

20 Ding C S, Xiao G Z, Shan W J. The stability theory of stream ciphers. LNCS 561, Berlin: Springer-Verlag, 1991

21 Diffie W, Hellman M E. New directions in cryptography. IEEE Trans Inform Theor, 1976, iT-22(6): 644—654

22 Rivest R L, Shamir A, Adleman L. A method for obtaining digital signatures and public key cryptosystems. Comm ACM 1978, 21: 120—126

23 Merkle R C, Hellman M E. Hiding information and signatures in trap dorr knapsacks. IEEE Trans Inform Theor, 1978, 24(5): 525—530

24 Rabin M O. Digitalized signatures and public key functions as intractable as factorization. Technical Report LCS/TR212, Cambridge MA(1979), MIT

25 ElGamal T. A public key cryptosystem and signature scheme based on discrete logarithms. IEEE Trans Inform Theor, 1985, IT-31(4): 469—472

26 Koblitz N. Elliptic curve cryptosystem. Mathematics of Computation, 1978, 48: 203—209

27 McEliece R J, Miller. A public key cryptosystem based on algebraic coding theory. DSN Progress Rep. 42-44, Jet Propulsion Lab, 1978, 114—116

28 陶仁骥, 陈世华. 一种有限自动机公开钥密码体制和数字签名, 计算机学报, 1985 8(6): 401—409

29 曹珍富. 公钥密码学. 哈尔滨: 黑龙江教育出版社, 1993

30 Schnorr C P. Efficient identification and signature for smart cards. J Cryptography, 1991, 4(3): 161—174

31 NIST, Digital Signature Standard (DSS). Federal Information Processing Standards Publication 186

32 Mambo M, Usuda K, Okamoto E. Proxy signatures: Delegation of the power to sign messages. IEICE Trans Fundam, 1996, E79-A(9): 1338—1354

33 Chaum D. Blind signatures for untraceable payments. In: Crypto'82. New York: Plenum Press, 1993. 199—203

34 Boneh D, Gentry C, Lynn B, et al. Aggregate and verifiably encrypted signatures from bilinear maps. In: advances in Cryptography – Eurocrypt 2003, LNCS 2656. Berlin, Springer-Verlag, 2003. 416—432

35 Chaum D, Antwerpen H van. Undeniable signatures. In: CRYPTO'89, LNCS 435.Berlin: Springer-Verlag, 1989, 212—216

36 Bellare M, Miner S. A forward-secure digital signature scheme. In: CRYPTO'99, LNCS 1666. Berlin: Springer-Verlag, 1999, 431—448

37 Dodis Y, Katz J, Xu S,et al. Strong Key-Insulated Signature Schemes. In: Public Key Cryptography - PKC 2003, LNCS 2567. Berlin: Springer-Verlag, 2003. 130—144

38 Shamir A, Tauman Y. Improved online/offline signature schemes. In: Proceedings of Advances in Cryptology: Crypto'01, LNCS 2139. Berlin: Springer-Verlag, 2001, 355—367

39 Desmedt Y. Society and group oriented cryptography: A new concept. In: Crypto'87, LNCS 293. Berlin: Springer-Verlag, 1988. 120—127

40 Rivest R, Shamir A, Tauman Y. How to leak a secret. In: ASIACRYPT 2001, LNCS 2248. Berlin: Springer-Verlag, 2001. 552—565
41 Jakobsson M, Sako K, Impagliazzo R. Designated verifier proofs and their applications. In: EUROCRYPT'96, LNCS 1070. Berlin: Springer-Verlag, 1996.143—154
42 Chaum D. Designated confirmer signatures. In: Eurocypt'94, LNCS 950. Berlin: Springer-Verlag, 1995, 86–91
43 Wang G, Bibliography on signatures. Available at: http://icsd.i2r.a-star.edu.sg/staff/guilin/bible.htm
44 ITU-T, Rec. X.509 (revised) the Directory-Authentication Framework. 1993, International Telecommunication Union, Geneva, Switzerland
45 Shamir A. Identity-based cryptosystems and signature schemes. In: Advances in Cryptography – Crypto'84, LNCS 196, Berlin: Springer-Verlag, 1984. 47—53
46 Boneh D, Franklin M. Identity-based encryption from the Weil pairing. SIAM, J Comput, 2003, 32(3): 586—615
47 Barreto P S L M. The Pairing-Based Crypto Lounge. http: //paginas. terra.com.br/informatica/paulobarreto/ pblounge.html
48 Baek J, Zheng Y. Identity-Based Threshold Decryption, Practice and Theory in Public Key Cryptography-PKC'2004, Singapore(SG), March 2004, LNCS 2947. Berlin: Springer-Verlag 2004. 262—276
49 Al-Riyami S S, Paterson K G. Certificateless public key cryptography. Advances in Cryptology - Asiacrypt'2003, LNCS 2894. Berlin: Springer-Verlag, 2003, 452—473
50 南湘浩. CPK 标识认证. 长沙: 国防工业出版社, 2006
51 Goldwasser S, Micali S. Probabilistic Encryption. J Comput System Sci, 28(3): 270–299.
52 Dolev D, Dwork C, Naor M. Non-malleable Cryptography. SIAM J on Computing, 2000, 30(2): 391—437
53 Pointcheval D. Provable Security for Public Key Schemes. http://www.di.ens.fr/~pointche/pub.php?reference=Po04
54 Goldwasser S, Micali S, Rivest R. A digital signature scheme secure against adaptive chosen-message attacks. SIAM J Comp, 1988,17(2): 281—308
55 An J, Dodis Y, Rabin T. On the security of joint signature and encryption. In: Advances in Cryptology-EUROCRYPT'02, LNCS 2332. Berlin: Springer-Verlag, 2002. 83—107
56 Bellare M, Rogaway P. Entity Authentication and Key Distribution. In: Advances in Cryptology - Crypto 1993, LNCS 773. Berlin: Springer-Verlag, 1993, 110–125
57 Bellare M, Rogaway P. Provably secure session key distribution: The three party case. In: 27th ACM Symposium on the Theory of Computing. New York: ACM Press, 57—66
58 Bellare M, Pointcheval D, Rogaway P. Authenticated Key Exchange Secure Against Dictionary Attacks. In: Advances in Cryptology-Eurocrypt 2000 LNCS 1807. Berlin: Springer-Verlay, 2000. 139—155
59 Canetti R, Krawczyk H. Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels. In: Advances in Cryptology – Eurocrypt 2001 LNCS 2045. Berlin: Springer-Verlag, 2001. 453—474
60 Choo K K R, Boyd C, Hitchcock Y. Examining Indistinguishability-Based Proof Models for Key Establishment Protocols. In: Advances in Cryptology - Asiacrypt 2005, LNCS 3788. Berlin: Springer-Verlag 585—604
61 Choo K K R. Provably Secure Mutual Authentication and Key Establishment Protocols Lounge. http://sky.fit.qut.edu.au /~choo/lounge.html
62 Bellare M, Rogaway P. Random oracles are practical: a paradigm for designing efficient protocols, In: Proc. Of the 1st ACM Conference on Computer and Communication Security, New York: ACM Press, 1993. 62—73
63 Fiat A, Shamir A. How to prove yourself: {Practical} solutions to identification and signature problems. In: Advances in Cryptology——Crypto '86. Berlin: Springer-Verlag, 1986. 186—194
64 Canetti R, Goldreich O, Halevi S. The random oracle methodology, revisited. In: Proceedings of the 30th Annual Symposium on the Theory of Computing (STOC'98). New York: ACM Press, 1998. 209—218
65 Cramer R, Shoup V. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In: Advance in Cryptology- Crypto'98, LNCS 1462. Berlin: Springer-Verlag, 1998. 13—25
66 Water B. Efficient Identity-Based Encryption Without Random Oracle. Advances in wyptology CRYPTO 2004 LNCS 3152. Berlin: Springer-verlag, 2004. 443—459

67 Boneh D, Boyen X. Short signatures without random oracles. In: Advance in Cryptology- Eurocrypt'04, LNCS 3027. 2004. 56—73

68 Zeng Guihua. Quantum Identity Authentication Without Lost of Quantum Channel. 密码学进展——CHINACRYPT '2004. 北京: 科学出版社, 2004

69 肖国镇, 卢明欣. DNA 计算与 DNA 密码. 工程数学学报, 2006, 23(1): 1—6

70 Department of Defense Computer Security Center. DoD 5200.28-STD. Department of Defense Trusted Computer System Evaluation Criteria [S]. USA: DOD, December 1985

71 National Computer Security Center. NCSC-TG-021. Trusted Database Management System Interpretation [S]. USA: DOD, April 1991

72 National Computer Security Center. NCSC-TG-005. Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria [S]. USA: DOD, July 1987

73 Trusted Computing Group. TCG Specification Architecture Overview [EB/OL]. [2005-03-01]. https: //www. trustedcomputinggroup. org/

74 The Open Trusted Computing (OpenTC) consortium. General activities of OpenTC [EB/OL]. [2006-3-1]. http: //www. opentc. net/activities/

75 Microsoft. Trusted Platform Module Services in Windows Longhorn [EB/OL]. [2005-4-25]. http: //www. microsoft. com/resources/ngscb/

76 Intel Corporation. LaGrande Technology Architectural Overview [EB/OL]. [2004-5-1]. http: //www. intel. com/technology/security/

77 Avizienis A, Laprie J C, Randell B, et al. Basic concepts and taxonomy of dependable and secure computing. IEEE Trans Dependable Secur Comput, 2004, 1(1): 11—33

78 张焕国, 罗捷, 金刚, 等. 可信计算研究进展, 武汉大学学报(理学版), 2006. 52(5): 513—518

79 张焕国, 毋国庆, 覃中平, 等. 一种新型安全计算机, 第一届中国可信计算与信息安全学术会议论文集: 武汉大学学报(理学版), 2004, 50(S1)

80 张焕国,刘玉珍,余发江, 等, 一种新型嵌入式安全模块. 第一届中国可信计算与信息安全学术会议论文集: 武汉大学学报(理学版), 2004.50(1)

81 Yan Fei,Zhang Huanguo,Sun Qi,et al. An Improved Grid security infranstructure by trusted computing. Wuhan University Journal of Natural Science, 2006, 11(6)

82 Patel J, Luke T W T, Jennings N R, et al. A Probabilistic Trust Model for Handling Inaccurate Reputation Sources. In: Trust Management, Third International Conference, iTrust 2005. Paris, 2005.23-26: 193—209

83 Beth T, Borcherding M, Klein B. Valuation of thust in open network. In: Proceeding of the European Symposium on Research in Security(ESORICS). Brighton: Springer-Verlag, 1994, 3—18

84 唐文, 陈钟. 基于模糊集合理论的主观信任管理模型研究软件学报, 2003, 14(8): 1401—1408

85 Audun Jøsang. An Algebra for Assessing Trust in Certification Chains. The proceedings of NDSS'99, Network and Distributed System Security Symposium, The Internet Society, San Diego, 1999

86 袁禄来, 曾国荪, 王伟. 基于 Dempster-Shafer 证据理论的信任评估模型, 武汉大学学报(理学版), Vol.52, No.5, 2006.

87 屈延文. 软件行为学, 电子工业出版社, 2004

88 林闯, 彭雪海. 可信网络研究, 计算机学报, 2005. 28(5)

89 陈火旺, 王戟, 董威. 高可信软件工程技术, 电子学报, 2003, 31(12): 1933—1938

90 Anderson J P. Computer security technology planning study. ESD-TR-73-51, Vol.II, Electronic Systems Division, Air Force Systems Command, Bedford, MA, USA

91 冯登国. 网络安全原理与技术. 北京: 科学出版社. 2003 年 9 月

92 Shim S S Y, Gong L, Rubin A D et al. Securing the high-speed internet. IEEE Computer, 2004, 37(6): 33—35

93 Enz C C, El-Hoiydi A, Decotignie J, et al. WiseNET: an ultralow-power wireless sensor network solution. IEEE Computer, 2004, 37(8): 62—70

94 Carle J, Simplot-Ryl D. Energy-efficient area monitoring for sensor networks. IEEE Computer, 2004, 37(2): 40—46

95 冯登国. 国内外信息安全技术研究现状及发展趋势. 中国计算机科学技术发展报告 2005. 北京: 清华大学出版社, 2006. 236—256

96 Feng Dengguo, Wang Xiaoyun. Progress and Prospect on Information Security Research in China. J comput sci tech, 2006, 21 (5): 740—755

97 Simmons G J. The prisoner's problem and the sbliminal channel. Advances in Cryptology: Proceedings of CRYPTO'83. NY:Plenum Press 1984. 51—67

98 王育民, 张彤, 黄继武, 等. 信息隐藏技术——理论与应用. 北京: 清华大学出版社, 2006

99 A guide to understanding covert channel analysis of trusted systems. National Computer Security Center. NCSC-TG-030.

100 Petitcolas F A P, Anderson R J, Kuhn M G. Information hiding — A survey. Proc IEEE, 1999, 87(7): 1062—1078

101 Anderson R J, Petitcolas F A P. On the Limits of Steganography. IEEE J Selected Areas Commun, 1998 16(4): 474—481

102 Swanson M D, Kobayashi M, Tewfik A H. Multimedia data embedding and watermarking technologies. Proc IEEE, 1998, 86(6): 1064—1087

103 Johnson N F, Jajodia S. Steganalysis of images created using current steganography software. In: Proc of 2nd International Workshop on Information Hiding. LNCS 1525, 1998. 273—289

104 Bender W, Gruhl D, Morimoto N, et al. Techniques for data hiding, IBM System J, 1996, 35(3/4): 313—337

105 Cox I J, Killian J, Leighton F T, Shamoon T, Secure spread spectrum watermarking for multimedia IEEE Trans Image Process, 1997, 6(12): 1673—1687

106 Chen B Wornell G W. Quantization index modulation: A class of provably good methods for digital watermarking and information embedding. IEEE Trans Inform Theory, 2001, 47(4): 1423—1443