可信计算与网络安全

王振宇 / 中关村可信计算产业联盟

【摘　要】随着信息技术的迅猛发展和互联网的普及，以及移动互联、物联网、大数据、云计算、工业互联网等新型场景的迅速推广，信息传播的速度、广度和实时性都达到史无前例发展。信息化应用已经深入国家与社会的各个方面，同时也带来大量的不良信息以及恶意的网络行为，因此信息系统的安全保障能力已成为一个国家综合国力和经济竞争力的重要组成部分。要确保信息系统的安全，必须从信息系统底层做起从硬件做起，从体系结构上进行安全设计，由此催生了我国可信计算技术的产生和发展。本文将围绕可信计算做具体介绍。

【关键词】信息安全　可信计算3.0　关键技术　主动免疫

1 引言

网络空间的安全与人类社会休戚相关。在人类社会中，信任是人们相互合作和交往的基础，如果我们确定对方不可信，就不会与其合作和交往。人们也是通过相信甲，甲又相信乙，这样一个人相信一个人完成对事情的管理和掌控。可信计算就是把人类社会成功的管理经验用于计算机信息系统和网络空间。从广义的角度，可信计算为用户（包括网络用户和应用用户）提供了一个更为宽广的安全环境，它从安全体系的角度来解决安全问题，确保用户的安全执行环境，突破传统被动防御，打补丁杀病毒的方式，为计算机建立起自己免疫系统，是一套整体考虑的先进安全管理技术。

2 可信计算的由来

可信计算是信息科学发展结果，在早期的大型机时代系统内建了安全架构，对执行代码、数据进行了隔离，对资源、用户等进行了分配和权限设定。而随着计算机的发展，个人PC逐渐取代了大型机，在这个过程中个人PC为了减少成本去掉了大型机原有的安全机制，如任务隔离、内存保护、环境隔离、权限控制等。原有的安全架构被简化了，而外围环境却变得日益复杂，不安全因素越来越多。原来的计算机网络和业务系统相对封闭风险较小，而近些年来互联网的发展和推广使得每一个终端去接触互联网的机会大大增加，原先很多封闭的业务系统也与互联网有了交集，随之而来的安全隐患也就更多。传统安全防护依赖于防火墙、杀毒软件和IDS“老三样”产品，这种外围被动的防护方式存在全保障能力欠缺、自身安全机制容易被篡改和旁路、管理分散不能构成整体防御等问题，传统安全的外围被动防护方式并不足以应对新形式下的安全问题，近年来的重大安全事件印证了这一点。

与此同时，随着网络技术的发展，

信息化系统架构已经由点式孤立松散耦合的基础架构，演进成为具有分布式大规模协同特性的海量计算、动态可重构的移动计算以及无处不在的普适计算等多种组织形态，而安全性、可信性技术缺失已经成为当今信息化进一步飞跃式发展的重大障碍。为了跨过这一障碍，国际上对可信计算的讨论越来越广泛，可信计算产品的数量越来越多，像微软、因特尔、IBM、HP等国际巨头都在不断推进可信计算技术，深化可信计算产品。由于对安全性、可信性技术的需求是国际性的也是全方位的，信息系统已经渗透到了人们工作生活中的各个领域，随着国际巨头对安全性的宣传，以及对可信计算产品的推广活动，使得可信计算再次成为热点走到公众面前。

3 可信计算解决的问题

目前大部分网络安全系统主要由防火墙、入侵检测、病毒防范等组成。这种常规的安全手段只能在网络层、边界层设防，在外围对非法用户和越权访问进行封堵，以达到防止外部攻击的目的。由于这些安全手段缺少对访问者源端—客户机的控制，加之操作系统的不安全导致应用系统的各种漏洞层出不穷，其防护效果正越来越不理想。此外，封堵的办法是捕捉黑客攻击和病毒入侵的特征信息，而这些特征是已发生过的滞后信息，属于“事后防御”。随着恶意用户的攻击手段变化多端，防护者只能把防火墙越砌越高、入侵检测越做越复杂、恶意代码库越做越大，误报率也随之增多，使得安全的投入不断增加，维护与管理变得更加复杂和难以实施，信息系统的使用效率大大降低，而对新的攻击毫无防御能力。近年来，“震网”“火焰”“Mirai”“黑暗力量”“WannaCry勒索病毒”等重大安全事件频频发生，显然，传统防火墙、入侵检测、病毒防范等“老三样”封堵查杀的被动防御已经过时，网络空间安全正遭遇严峻挑战[1]。

安全防护手段在终端架构上缺乏控制，这是一个非常严重的安全问题，难以应对利用逻辑缺陷的攻击。目前利用逻辑缺陷的漏洞频繁爆出，如“幽灵”“熔断”，都是因为CPU性能优化机制存在设计缺陷，只考虑了提高计算性能而没有考虑安全性。由这种底层设计缺陷导致的漏洞难以修补，即使有了补丁其部署难度也是越来越大。幽灵、熔断的补丁部署后会使性能下降30%。补丁难打、漏洞难防已经是当前信息安全防御主要问题之一。

可信计算正是为了解决计算机和网络结构上的不安全，从根本上提高安全性的技术方法，可信计算是从逻辑正确验证、计算体系结构和计算模式等方面的技术创新，以解决逻辑缺陷不被攻击者所利用的问题，形成攻防矛盾的统一体，确保完成计算任务的逻辑组合不被篡改和破坏，实现正确计算。

4 可信计算的定义

可信计算的定义是指计算运算的同时进行安全防护，使计算结果总是与预期一样，计算全程可测可控，不被干扰。可信计算是一种运算和防护并存的主动免疫的新计算模式，具有身份识别、状态度量、保密存储等功能，类似人体的免疫系统，及时识别“自己”和“非己”成份，从而

破坏与排斥进入机体的有害物质[2]。

5 可信计算的核心思想

网络空间由于其开放性，允许两个网络实体未经过任何事先的安排或资格审查，就可以进行交互。这就导致我们在进行交互时有可能对对方实体一无所知。对方实体可能是通过这次交互来破坏我们数据的恶意程序，也可能是一个已经被黑客控制了的计算平台，还可能是企图诈取我们钱财的人或组织等。如果我们无法判断对方实体是否可信就贸然交互，很可能造成巨大的损失。

为解决这个问题，我们需要找到一种方法，这种方法能够让用户判断与自己交互的实体是否可信，进而确保网络空间的安全。这就是可信计算的基本出发点。可以说可信计算就是把人类社会成功的管理经验用于计算机信息系统和网络空间，具体而言，就是首先在计算机系统中建立一个信任根，信任根的可信性由物理安全、技术安全、管理安全共同确保；再建立一条信任链，从信任根开始到硬件平台、操作系统、应用，一级度量认证一级，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[3]。

6 可信计算的关键技术

可信计算主要有两个核心技术，一个是信任根技术，一个是信任链技术。信任根是我们信任的起点源头，在系统结构上，以硬件形式构建于整机中，通过建立度量机制，保证系统完整性、身份可信性、安全存储和可信存储，实现主动防御；信任链是我们传递信任的方法，从信任根开始，一级验证一级，一级信任一级，使源头信任传递到应用系统和整个网络，保证系统可信可控，实现综合防范。

可信计算防御产品主要由硬件信任根（TPCM）、可信软件基（软件核心）、密码支撑（TCM）和管理中心（集中管理）构成。

7 主动免疫的防护效果

目前，我们所使用的计算机体系结构在设计时只追求计算速度，并没有考虑安全因素，如系统任务难以隔离、内存无越界保护等。这直接导致网络化环境下的计算服务存在大量安全问题，如配置可被篡改、恶意程序被植入执行、利用缓冲区溢出攻击、非法接管系统管理员权限等。可信计算采用运算和防御并行的双体系架构，在计算运算的同时进行安全防护，使计算结果总是与预期一样，计算全程可测可控，不被干扰[4]。

可信计算能够实现计算机体系结构的主动免疫。就像人体免疫一样，能及时识别“自己”和“非己”成分，使漏洞不被攻击者利用。云计算、大数据、物联网、工业系统等新型信息技术应用都需要可信免疫体系作为基础支撑，确保操作行为、资源配置、数据存储和策略管理的可信，以达到攻击者进不来、非授权者重要信息拿不到、窃取保密信息看不懂、系统和信息篡改不了、系统工作瘫痪不成和攻击行为赖不掉的防护效果。如果有可信机制，“震网”“火焰”“心脏出血”等恶意代码可不杀自灭。

8 可信计算适用的环境

可信计算产品及解决方案重点应用于

等级保护系统、保密系统、军事系统等领域，以主动防御的方式，从根本上解决国家关键基础设施、重要信息系统、涉密信息系统、军队应用系统所面临的安全威胁。同时，可信计算技术可在云计算、物联网、工业控制系统等新技术领域进行延伸，形成针对特定领域的可信计算产品和解决方案，为用户系统构建完整的主动防御体系，满足我国信息化建设的安全需求。

工业控制系统。2010年“震网”病毒事件破坏了伊朗核设施，震惊全球。这标志着网络攻击从传统“软攻击”阶段升级为直接攻击电力、金融、通信、核设施等核心要害系统的“硬摧毁”阶段。应对APT已成为确保国家关键基础设施安全，保障国家安全、社会稳定、经济发展、人民生活安定的核心问题。

三网融合。电信网、广电网和互联网三网融合后，信息安全风险将主要来自于网络开放性、终端复杂性、信息可信性等方面。信息量急剧增加，信息内容控制将对信息保密防范技术提出更高要求。终端智能化和移动等多接入方式，使其将面临更复杂的攻击。另外，大规模的用户数量将给监管带来重大挑战。也存在原有法律与三网融合新要求相冲突的问题，应建立新的监管体制和法律体系。

物联网。物联网将传感、通信和信息处理整合成网路系统。把物品与互联网连接起来，实现智能化识别、定位、跟踪监控和管理，这必然会成为影响社会稳定、国家安全的重要因素之。物联网运用大量感知节点（智能设备和传感器），将成为窃取情报、盗窃隐私的攻击对象，而且庞大节点以集群方式连接将对网络通信的依赖更加敏感，对分布式的物联网核心网络的管理平台安全性、可信性要求更高。另外，物联网对数据传输的安全性和身份认证的可信性提出了更高的要求。

云计算。云计算是一种能够动态伸缩的虚拟化资源，通过网络以服务的方式提供给用户的计算模式，用户不需要知道如何管理那些支持云计算的基础设施，其安全风险在于：由不可控、不可信的云经营商统管IT资源和计算基础设施，以及更大规模异构共享和虚拟动态的运营环境难以控制。如何保证云中IT资源安全、用户隐私保护以及云计算环境的可信可靠，已成为云计算进一步发展的关键因素。另外，制定相应的云计算法律法规，明确用户和运营商法律责任也是发展云计算必不可少的环节。

9 结语

云计算、大数据、物联网、工业系统等新型信息技术应用都需要可信免疫体系作为基础支撑，确保操作行为、资源配置、数据存储和策略管理的可信，推动信息化的发展。

参考文献

[1] 沈昌祥. 用主动免疫可信计算 3.0 筑牢网络安全防线营造清朗的网络空间 [J]. 信息安全研究 , 2018, 4(04):282~302.

[2] 沈昌祥、左晓栋 . 网络空间安全导论 [M]. 北京：电子工业出版社 ,2018.

[3] 张焕国、赵波 . 可信计算 [M]. 武汉：武汉大学出版社 ,2016.

[4] 沈昌祥，张焕国，王怀民，等 . 可信计算的研究与发展 [J]. 中国科学：信息科学，2010(02):139~166.