可重构信息安全系统研究综述

肖 玮[1,2],陈性元[1,3],包义保[1]
(1. 解放军信息工程大学密码工程学院,河南郑州 450000;2. 空军航空大学基础基地,吉林长春 130022;
3. 密码科学技术国家重点实验室,北京 100000)

摘 要: 传统安全计算提供固定的安全服务能力,无法根据环境和安全需求的变化灵活配置,导致安全管理复杂,软硬件资源重复利用率低. 可重构安全计算为提升系统灵活性、适应性和可扩展性提供了新的手段. 本文阐述了可重构安全计算的发展历程,初步研究了其内涵与意义,提出了可重构安全计算的概念模型,并详细论述了其中的关键技术及其研究现状,最后分析了可重构安全计算的发展趋势. 可重构信息安全系统是新型计算与信息安全技术融合的必然产物,必将为信息安全技术提供更广阔的应用空间.

关键词: 可重构信息安全系统; 可重构安全计算; 灵活性; 适应性
中图分类号: TP393 **文献标识码:** A **文章编号:** 0372-2112 (2017)05-1240-09
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2017.05.030

Review of Research on Reconfigurable Information Security System

XIAO Wei[1,2], CHEN Xing-yuan[1,3], BAO Yi-bao[1]
(1. *Cryptography Engineering College of the PLA Information Engineering University, Zhengzhou, Henan* 450000, *China*;
2. *Flight Fundamental Training Base, Aviation University of Air Force, Changchun, Jilin* 130022, *China*;
3. *State Key Laboratory of Cryptology, Beijing* 100000)

Abstract: Traditional security computing provides fixed security service capability, making it impossible to reconfigure the security system based on changes in the network environment and security needs. Therefore, its adaptive capacity is poor and its security management becomes complicated. Besides, the ratio of hardware reuse is low. Reconfigurable security computing provides a new method to improve the flexibility, adaptability and extensibility of the system. This paper describes the development of reconfigurable security computing, preliminarily studies on its connotation and significance, puts forward its concept model and discusses the key technology and its research status in detail. What's more, the development trend of reconfigurable secure computing is analyzed. Reconfigurable information security system integrates the new computing and information security technique. It is the inevitable development trend and will provide a broader application for information security technology.

Key words: reconfigurable information security system; reconfigurable security computing; flexibility; adaptability

1 引言

随着信息安全技术的迅猛发展,新的应用环境、安全威胁与安全需求都要求安全系统具有灵活的自适应能力与柔性安全服务提供能力. 早在2007年美国发布的《联邦网络空间安全及信息保障研究与发展计划(CSIA)》中曾明确指出,可重构和可升级的安全系统是下一代先进系统和体系结构的主要研究领域之一. 近年来,可重构技术[1]、软件自定义网络[2~4]、可重构网络[5,6]等技术发展迅速,为研究可重构信息安全系统奠定了的技术和理论基础. 可重构信息安全系统是新型计算与信息安全技术融合的必然产物,必将为信息安全技术提供更广阔的应用空间.

本文对可重构信息安全系统以及由此而延伸出的可重构安全计算及其研究领域进行了全面分析,指出可重构安全计算的未来发展方向.

2 可重构安全计算的产生与意义

2.1 通用计算、专用计算与可重构计算

传统的以冯·诺依曼(Von Neumann)架构为基础

收稿日期:2015-12-30;修回日期:2016-08-22;责任编辑:马兰英
基金项目:国家"863"高技术研究发展计划基金(No.2012AA012704);国家自然科学基金(No.61502531)

的通用计算(General purpose computing)具有实现方式灵活,通用性强,容易实施和修改,成本投入低廉等特点,但是其性能和功耗并不理想,缺乏对并行处理等高性能计算的支撑. 与通用计算相对应的是以专用集成电路(Application Specific Integrated Circuit, ASIC)为基础的专用计算(Application specific computing),它可以根据应用的特性优化所选择的计算架构,采用数据驱动方式,无需指令集,执行速度快,功耗低,但存在一旦部署功能固定,设计周期长,一次性工程投入成本过高等缺点,只能应用于一些对性能要求特别高的环境中. 以特定领域处理器(Domain Specific Processor, DSP)为基础的特定领域计算(Domain specific computing)在性能上较通用计算具有明显改善,但灵活性弱于通用计算.

对于可重构计算,目前没有严格的定义,学术界比较认可的定义是:在软件的控制下,根据应用的需要,利用系统中的可重构资源重新构造计算平台,使其接近软件的灵活性(Flexibility)和专用硬件电路的高性能(Efficiency). 可重构计算系统(Reconfigurable System)在性能、功耗、灵活性和适应能力等关键指标之间取得更好的平衡,填补了通用计算和专用计算之间的空白,如图 1 所示. 可重构计算不使用指令集,不受指令流驱动的约束,一旦配置完成,即以类似专用计算仅受数据流驱动的方式运行,其能效比非常好. 随着微电子技术和大规模集成电路技术的不断发展,以及电子设计自动化(Electronic Design Automation, EDA)技术的发展,以"具有充足硬件资源"的计算环境为基本出发点的可重构计算将成为冯·诺依曼体系结构以外的另一种主流计算架构.

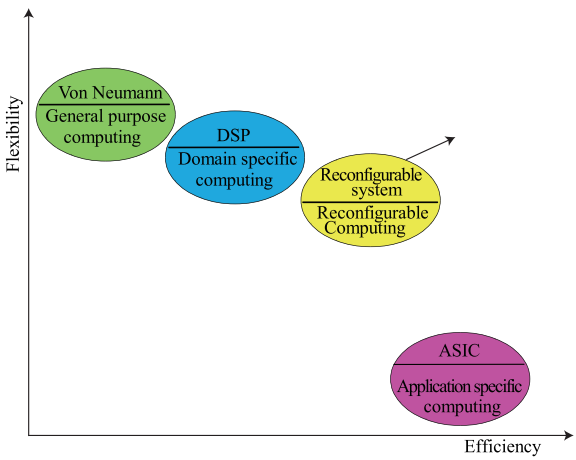

图1　常见计算体系结构的比较

2.2　可重构安全计算的产生

传统安全计算存在两方面的不足:(1)传统安全机制和现代信息系统所需要的安全服务之间存在着一系列的矛盾,如提供安全服务的安全机制的"静态性"和安全服务需求的"动态性"之间的矛盾,以及安全保护机制部署的固定性和信息系统运行环境的动态性之间的矛盾;(2)信息系统规模的不断扩大,复杂性不断增加,对安全保护机制的性能提出越来越高的要求,使得采用单纯的硬件或软件都无法解决这些问题,促使人们积极考虑采用重构思想解决安全计算中的一系列棘手问题.

近年来,在新型计算架构、软件工程及可重构软件系统研究方面所取得的巨大进步,促使以自适应软件、可重构软件、可重构网络、SDN 等为代表的可重构系统发展迅速,这使信息安全研究人员相信,用可重构思想可有效解决安全计算面临的安全性、高性能、灵活性、适应性、可编程性以及可定制性等方面的挑战,可重构安全计算应运而生. 可重构安全计算是在计算体系与架构、大规模集成电路、软件工程的深入发展和直接推动下出现的,其发展过程如图 2 所示. 由图 2 可以看出,可重构安全计算综合运用可重构计算技术和可重构软件技术解决信息安全领域存在的深层次问题,必将对信息安全理论和技术的发展产生深远影响.

2.3　可重构安全计算的内涵

将可重构计算思想应用到安全系统建设和管理中,构建可重构信息安全系统,为信息安全开辟了全新的研究领域,是信息安全领域发展的重要发展方向. 所谓可重构信息安全系统,是指能够根据应用环境及其变化情况进行动态配置,从而安全高效地运行的信息安全系统. 可重构安全计算为可重构信息安全系统的构建提供了强有力的"核",是指以可重构硬件和软件为基础构建起来的安全计算架构,它能够根据计算环境及其变化情况,调整其内部组织结构,形成最适合当前安全需求的软硬件计算架构,从而达到增强安全适应性、灵活性和提高安全系统性能的目的.

可重构安全计算与以通用 CPU 为基础的传统安全计算存在着巨大的不同. 首先,它们所依据的计算模型和体系结构不同. 传统的安全计算以冯·诺依曼体系结构为基础,而可重构安全计算以可重构软件和可重构硬件计算模型为基础来实现安全机制. 其次,它们的应用和管理模式及思路不同. 传统的安全计算以静态的"一般化"的配置应对千变万化的安全需求,安全机制必需成体系部署、管理与使用,而对于可重构安全计算来说,则更强调可以根据环境的特点与安全需求的变化,重构出"个性化"的安全服务,减少冗余,提高效率,管理的重点在于重构过程所需各类信息以及对重构结果正确性和安全性的验证等. 再次,它们所使用的编程模式和工具链不相同. 可重构安全计算需要充分利用软硬件资源可重构的特点,根据应用环境与安全

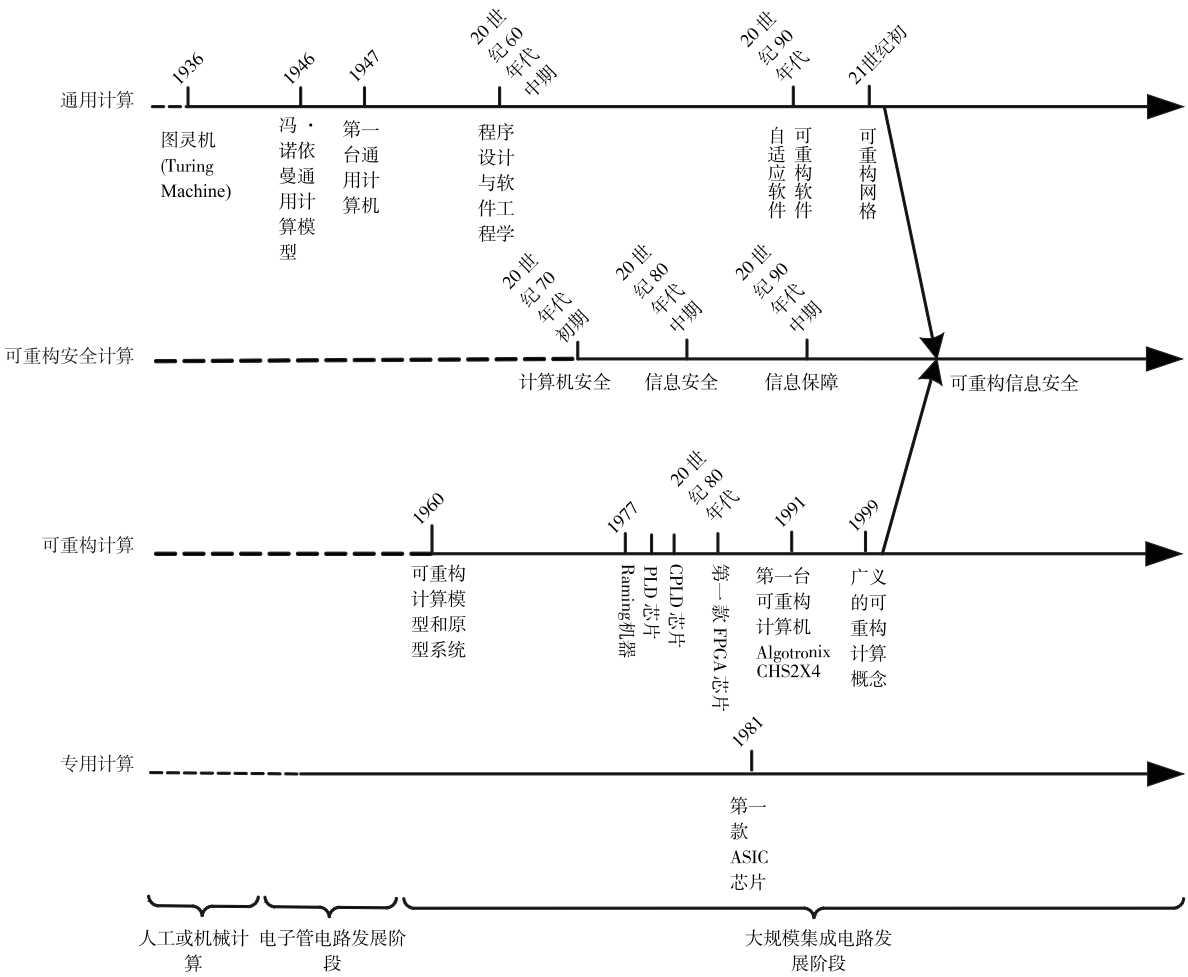

图2 可重构安全计算发展脉络

需求选择恰当的架构,因而对编程模式、编译工具都有着和传统安全计算不同的要求. 由此可见,可重构安全计算与传统安全计算存在着巨大差别,一系列新的理论和技术问题亟待解决,这使得可重构安全计算成为国际前沿研究领域.

2.4 可重构安全计算的研究意义

可重构安全计算所具有的优良特性,使得它成为信息安全领域新的支撑性技术,为柔性构建信息安全系统、适应信息安全需求动态变化、增加信息安全应急响应能力、提升信息安全系统服务水平都具有重要的意义.

可重构安全计算可为面向不同应用环境、不同安全需求的信息安全系统柔性构建提供新的支撑. 在我国信息化建设中,不同行业、不同信息系统、不同应用场合,存在着不同的信息安全需求与安全保密强度要求. 而目前的信息安全保障体系建设中,虽然出台了一系列信息安全保障体系建设的法规与制度,但是信息化管理人员面对众多庞杂的信息安全产品仍感到无从下手、无法配置、体系化建设困难、管理难度大,无法根据不同的信息安全需求与安全保密强度要求,重构出所需要的信息安全系统. 究其原因,主要是目前的信息安全系统或产品存在着灵活性和性能上的瓶颈,不具备高可信安全系统的重构能力,无法“个性化”地反映信息安全系统的实际需要,因而部署困难,使用复杂,效率低下,这严重阻碍了信息安全技术的应用和发展.

可重构安全计算可为应对信息系统安全威胁、提升信息安全应急响应能力提供新手段. 我国是信息化发展速度最快国家之一,但信息系统安全保护能力依然薄弱. 一方面,与安全技术发展总是滞后于安全威胁的客观事实有关,另一方面,与安全系统建设普遍采用一般化的信息安全保护技术,不能针对具体应用环境进行定制,安全服务冗余大,运行效率低,且不具备自适应、自配置、自管理及自治愈等快速反应能力有关,在出现信息安全事件后,不能根据具体情况对安全体系进行自动或有人工干预的重构与调整,导致安全事件造成的损失无法及时得到弥补.

可重构安全计算是促进信息安全领域发展的重要催化剂,具有巨大的发展空间和潜力. 可重构安全计算对信息安全保护模型、技术体系、编程和实现模式、应用与管理模式、部署方式等方面都将产生深远的影响. 然而,国内外目前在可重构安全计算方面已经开展的研究主要集中于可重构密码算法实现、可信计算平台 TPM 实现、安全协议性能加速、软件工程中的可重构安全软件设计等方面. 这些研究主要集中在可重构计算本身以及利用可重构计算实现部分的信息安全技术,虽然为可重构安全计算提供了基础,但是还远远不足以支撑起整个的技术体系. 例如,整体上应当采用什么样的结构,采用什么样的应用和管理模式等,还鲜有研究.

3　可重构安全计算研究的概念模型

可重构信息安全系统需要可重构计算(硬件)和通用计算(软件)的协同配合,共同构建起安全、高效、灵活、适应性强和按需定制的信息安全保障系统. 本文给出一个可重构安全计算概念性模型,如图 3 所示.

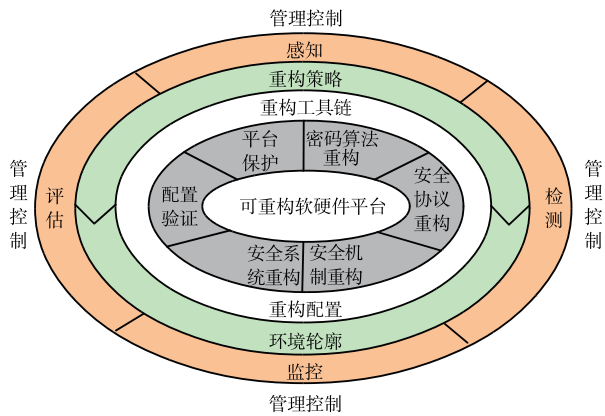

图3　可重构安全计算概念模型

该概念模型各部分功能分别如下:

(1)管理控制. 可重构安全系统的管理控制对整个系统的所有组件进行全面的管理和控制,是实现可重构安全系统各组件协调一致工作以及快速反应的基础.

(2)重构信息获取. 包括感知、监测、监控和评估等组件,通过感知计算环境和状态发生的变化,判断未来对计算环境安全状况的影响;通过检测与监控系统中随机发生的异变或故障,发现系统本身因重构或其它操作而出现的脆弱性漏洞;通过量化评估系统性能和安全状况,为系统重构提供重构依据.

(3)重构策略. 当环境轮廓参数或安全需求发生变化时,由重构策略分析组件从中提取出安全需求,根据重构策略库匹配输入的安全需求,从中获得所有待执行的重构策略.

(4)重构工具链. 重构工具链根据重构策略生成重构配置,并对重构配置的正确性和安全性进行验证,防止出现错误配置和不安全配置. 重构工具链主要包括软硬件划分与调度、配置自动生成、配置验证、配置编译与综合等工具.

(5)重构实施. 重构实施组件负责将由重构工具链生成的重构配置流恰当的部署到软硬件基础平台上. 可重构安全系统主要实施密码算法重构、安全协议重构、安全机制重构和系统级重构等内容. 在重构配置流注入到可重构安全计算环境之前,以及在重构后的计算环境中,均需要对重构配置进行静动态分析和安全性验证,确保其正确性和安全性.

(6)重构软硬件基础平台. 为可重构安全系统提供基础的软硬件平台,同时提供完整的软硬件安全保护,如重构配置流的安全保护、防恶意注入和修改等.

4　可重构安全计算研究进展与现状

可重构安全计算还没有形成完整的技术体系,但由图 3 所示的概念模型可见,它涉及到密码算法可重构技术、安全协议可重构技术、可重构可信计算技术、安全系统重构技术、重构正确性和安全性验证和证明等领域,下面将就这些领域进行一些讨论.

4.1　可重构密码算法

可重构安全系统中所涉及的密码算法重构,是指根据计算环境对密码算法的实际需要,在可重构软硬件平台上,现场按需静态或动态地构造出所需要的密码算法. 密码算法是典型的数据驱动型计算,它对输入的数据和密钥进行诸如混乱和扩散等各种变换,达到保护数据机密性和完整性的目的. 为了实现高性能的密码运算通常采用专用密码芯片,但其存在代价高昂,依赖厂商,部署固定等缺陷. 利用可重构计算方法来实现密码算法,在部署或运行时根据环境的需要对硬件进行重构,获得相应的密码算法,可极大提高芯片的灵活性、可扩展性和使用效率.

国外从 1999 年就开始可重构密码系统的研究,取得了很多成果. 2003 年,美国马萨诸赛大学的电子计算机工程系 Elbirt 和德国波鸿大学的 Paar 提出了一种针对分组密码运算的硬件可重构密码体系结构 COBRA[7,8],如图 4,该结构由 16 个粒度为 32 位的可重构功能单元按 4×4 阵列排列,支持 VLIW 计算模式;每个可重构功能单元由多个 32 位的可重构元素组成;COBRA 结构的行与行之间由粒度为 8 的交叉开关网络互连,通过不同的配置,可以调整互连结构实现不同的密码算法.

Fronte 等人[9]提出了 Celator 可重构密码体系结

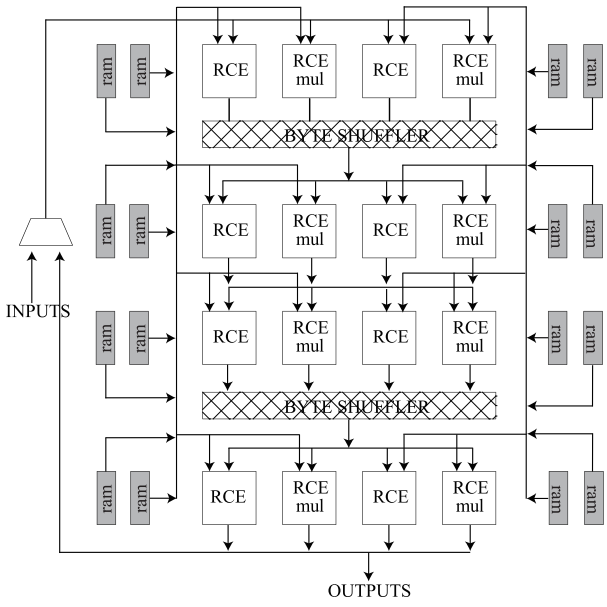

图4 COBRA可重构密码阵列体系

构. Ravi 等人[10]提出了基于 GPP(通用目标处理器)的定制密码处理器. 此外,还有加州大学的 Garp[11]结构、麻省理工大学的 Matrix[12]结构、惠普实验室的 CHESS[13]结构、Worcester Polytechnic 学院的 Smart-Cell[14]结构、德国凯撒斯劳滕大学的 KressArray 结构[15]等都是面向专用领域的典型可重构结构.

国内一些大学针对密码处理的可重构体系结构也进行了深入研究,取得了一定的成果. 国防科技大学提出并设计了可重构层次互连密码处理结构 RHCA[16]. 北京科技大学研制了 RELOG_DIGG[17]可重构密码系统. 解放军信息工程大学研制了分组密码、序列密码与公钥密码多款可重构密码芯片[18]. 清华大学研制了 GREP[19]通用可重构处理器,支持密码算法动态重构.

研究密码算法的重构主要关注密码算法的重构粒度、密码处理可重构架构、密码算法的动态重构[20~25]、参数化密码算法可重构设计[26,27]等方面. 研究人员正努力寻找密码算法的一般性架构,通过对密码算法一般性结构进行分析、提取和参数化配置,形成专用的粗粒度可重构元,可有效降低密码算法重构时配置生成和验证的复杂度,缩短重构配置注入和生效的时间. 对于密码算法在可重构硬件平台上的实现,目前主要集中于静态重构,只考虑到加解密的性能,忽略了重构所需时间,无法应用于动态重构的环境. 对于动态跨算法的重构目前研究还比较缺乏.

4.2 可重构 TPM

信息系统中的硬件平台和操作系统是安全的基础,只有从硬件和软件底层整体上采取措施,才能有效地确保信息系统的安全,正是这一思想推动了可信计算的产生和发展. TPM 是一种植于计算机内部为计算机提供可信根的芯片,可以为可信计算平台提供远程证明、会话密钥绑定、数据封装与解封等服务. TCG 明确指出 TPM 仅提供具有基本密码运算和安全功能的最小集合. 由于 TPM 只支持很少的密码算法,且其安全性完全取决于 TPM 厂商,使得它无法适用于一些特定的应用环境. 此外,目前 TCG 组织发布的 TPM 规范过于刻板,只能用于安全等级较低的环境中. 因此,有必要对 TPM 进行扩展,使其具有更好的适应性. 用可重构计算思想实现具有动态性和适应性的 TPM,可为各项应用提供更多、更广泛、更可靠的安全功能. 目前,已有学者就这一问题上进行了有益探索. Thomas Eisenbarth 等人[28]针对 TPM 的可扩展性和灵活性设计要求,给出了一种动态可重构可信计算架构,如图 5,该架构能够提供最小功能的可信计算基,还具备密码运算加速、动态更新/升级、安全性独立于生产厂商等特性. 但该方法只是对 TPM 部分功能的小范围修改,不是对 TPM 功能或其组件的重构,尽管如此,这也是对可重构 TPM 的一个有益探索.

Benjamin Glas 等人[29]提出了一种可重构可信平台系统架构,利用 FPGA 动态可重构技术实现可信计算的所有安全特性. Sunil 等人[30]提出了基于 FPGA 的可持续的可信平台模块(STPM),可以保证安全更新 TPM 加密引擎而不损害系统的可信性.

上述研究表明,使用可重构安全计算思想实现 TPM 具有下列优势:(1) 使信任链移植到硬件层更加容易.(2) 可根据环境升级和更新 TPM 的功能.(3) 提供独立于厂商的可信性. 因此,从目前的研究成果来看,基于可重构计算的可信 TPM 研究思路,对研究可信安全系统重构具有很大的启发性意义. 然而可重构 TPM 研究还处于初步阶段,对于如何构建可重构的 TPM,如何保证重构后 TPM 的可信性及其它安全属性,

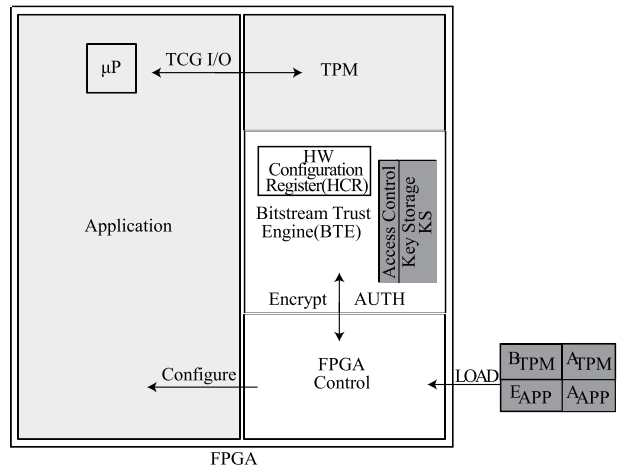

图5 可重构TPM体系

还需要深入的探讨.

4.3　可重构安全协议及系统

构建可重构信息安全系统离不开各种类型的可重构组件,典型的有可重构网络系统、可重构防火墙、可重构安全协议等. 可重构网络是可重构安全计算重要的平台,文献[31 ~ 37]对可重构网络的相关技术进行了深入研究,协议重构和协议栈重构是近几年可重构网络系统研究的主流方向,热点是动态协议重构,其难点和重点在于协议栈的体系结构、重构的在线触发、协议在线评价及优化等方面.

防火墙技术虽然历经多年的发展,但在性能、安全性、价格以及抵抗新型网络攻击的能力等方面还存在诸多不足. 传统的软件防火墙价格低廉,灵活性强,但是性能一直不够理想,且安全性不高于操作系统,容易遭受网络攻击;传统的硬件防火墙通过硬件化使用频率较高的模块来加速性能,但价格昂贵,部署固定,面对新的网络攻击反应能力不足. 因此,防火墙向可重构方向发展是明智的选择. 文献[38 ~ 43]利用软硬件协同可重构技术实现防火墙,在性能和灵活性之间取得较好平衡. 但这些研究主要关注于防火墙的性能和局部重构能力,而对分布式防火墙重构方法的研究还比较缺乏,这阻碍了以防火墙为代表的网络安全组件的进一步发展.

在现代分布式网络环境中,比较常用的安全协议主要有 PPTP、L2TP、IPSec、SSL/TLS、HTTPS、SET 等,种类繁多,数量庞大,使得安全管理与配置变得十分复杂,不利于安全系统的建设和发展. 安全协议可重构技术可以有效缓解上述问题. 文献[44 ~ 49]采用软硬件协同和部分动态重构技术实现安全协议,有效提高了安全协议的性能. 目前安全协议的研究主要关注性能和灵活性的提高,在增强安全协议主动防御能力和效能重构方面还缺乏重构方法、重构配置生成及安全性验证方面的研究.

4.4　重构配置的分析与验证

可重构信息安全系统只有在配置到具体环境或运行时才能确定其功能. 为确保系统安全性,应该具有针对具体应用环境及运行时场景对重构配置进行静态和动态分析的能力,以判断它是否具备指定的属性,需要解决以下一系列的问题:(1)从本地或远端下载而来的配置是否可信,是否执行既定的行为. (2)动态配置加载将使系统的执行过程发生变换,变换后的可重构系统是否还继续保持其安全性. (3)重构配置的来源事先并不确定,只有在重构配置注入系统时才可能对其进行分析,这要求具有运行时动态安全验证的能力.

针对上述问题,研究人员提出了众多的研究思路和解决方案. 例如,典型地,FPGA 配置流的可信验证问题通常依赖于厂商的支持,即由厂商在 FPGA 芯片内置入可信的加解密硬件电路和密钥来实现对配置流的验证. 这种方法的缺点是必需完全信任 FPGA 芯片生产厂商. 为了解决这一问题,Chaves 等人基于 HASH 方法提出了一种灵活的配置可信验证方法[50],根据正确的配置流不会对 FPGA 芯片之外的区域进行重构且必需和 FPGA 芯片的内在特征一致的特性,提出了一种根据配置流所产生的行为来判断其可信性的方法. 文献[51 ~ 54]对配置流可信性分析与验证方法进行了进一步讨论. 这些讨论虽然能够部分解决 FPGA 配置流的可信问题,但都无法支持运行时动态重构和验证. 文献[55]给出了一种适用于运行时动态重构的重构配置安全性验证方法. 以“携带证明式编程”方法(PCC,Proof-Carrying Code)为基础,编写重构配置的同时,形式化地构造出针对重构配置的安全性证明,并和重构配置安全地绑定起来一同发布. PCH 方法对安全系统的动态重构进行了有益尝试,但是存在构造重构配置可信性证明困难这一缺点,使得 PCH 方法对重构配置的生成过程要求极高,需要进一步研究.

由于传统的软件静、动态分析与验证技术[56]并不完全适用于可重构信息安全系统,其配置的分析与验证是非常困难的. 因此,重构配置的安全性分析与验证技术,尤其是动态重构的安全验证研究,是可重构安全计算中一个重点与难点问题.

5　可重构安全计算的发展趋势

可重构安全计算对信息安全的发展有着直接的推动作用,但相关理论和技术目前还不成熟,在以下几方面需要深入研究.

(1)可重构安全计算架构与模型研究. 可重构安全系统涉及密码算法、安全协议与安全机制等内容,是一项复杂的系统工程,只有对种不同架构与模型的充分比较和分析,才能设计出系列化可重构安全计算架构,为不同应用环境、不同安全需求、不同安全威胁下的安全系统重构提供支持.

(2)安全软件可重构技术. 主要包括可重构安全软件架构描述方法、安全软件可重构模型、安全软件动态重构方法等. 重点关注重构时机选择、重构配置生成、重构对系统的影响等内容,为安全机制重构提供基本理论、方法与技术.

(3)密码算法动态重构及其通用体系结构研究. 主要关注重构时机的选择、动态重构配置生成的复杂性、重构的效率等方面. 可重构密码算法体系结构的研究主要关注“如何用一种可重构的密码算法架构,能够高效支持各种不同的密码算法的能力”.

(4)可重构可信计算基研究. 主要关注于“如何将

可重构思想应用于可信计算,研制具有灵活性、可扩展性的可重构 TPM、TNC 及其它可重构可信安全系统",主要研究可重构可信计算基的基本构成、可信计算基的动态重构方法,以及重构状态下可信状态安全迁移等内容.

(5)安全协议重构技术研究. 这方面的研究将逐渐由基于可重构计算平台的密码协议实现向密码协议可重构的计算平台演变. 主要关注"安全协议形式化描述方法,安全协议可重构元的提取技术,以及安全协议动态更换方法"等内容.

(6)重构配置静动态分析和形式化验证技术研究. 主要关注于"如何根据具体的场景对重构配置进行正确性和安全性分析,判断其是否符合指定的安全属性和功能目标";需要研究如何将仿真、测试等传统的静态分析方法,以及模型检验、定理证明等形式化验证方法扩展到可重构安全计算环境中;特别地,需要针对可重构安全系统动态性和实时性特点,研究具有实时性和可靠性的可重构安全系统验证方法,这是重构配置形式化验证研究的重点和难点.

(7)可重构安全计算工具链的研究. 工具链对可重构安全计算的应用前景有着直接的影响. 好的工具链是可重构安全计算技术正确实施的有力保障. 然而,目前专门针对这方面的高性能工具还比较缺乏,也缺少相关研究成果.

(8)可重构安全计算软硬件平台的安全防护技术. 可重构安全计算平台不同于传统的安全计算平台,主要在于其"可重构"的特点,使得平台自身的安全威胁增多. 目前,如何保护可重构硬件平台已经成为国际国内研究的热点和难点问题.

参考文献

[1] Estrin G,Bussell B,Turn R,Bibb J. Parallel processing in a restructurable computer system[J]. IEEE Transactions Oil Electronic Computers,1963,12(6):747 – 755.

[2] 张朝昆,崔勇,唐翯祎,等. 软件定义网络(SDN)研究进展[J]. 软件学报,2015,26(1):62 – 81.
Zhang Chaokun,Cui Yong,Tang He-yi,et al. State-of-the-art survey on software-defined networking (SDN)[J]. Journal of Software,2015,26(1):62 – 81. (in Chinese)

[3] Nunes BAA, Mendonca M, Nguyen XN, Obraczka K, Turletti T. A survey of software-defined networking:Past, present,and future of programmable networks[J]. IEEE Communications Surveys and Tutorials, 2014, 16(3): 1617 – 1634.

[4] Software-Defined networking research group (SDNRG)[EB/OL]. http://irtf.org/sdnrg,2013.

[5] 兰巨龙,程东年,胡宇翔. 可重构信息通信基础网络体系研究[J]. 通信学报,2014,35(1):128 – 139.
LAN Ju-long,CHENG Dong-nian,HU Yu-xiang. Research on reconfigurable information communication basal network architecture[J]. Journal on Communications,2014,35(1):128 – 139. (in Chinese)

[6] 兰巨龙,邢池强,胡宇翔,等. 可重构技术与未来网络体系架构[J]. 电信科学,2013,29(8):16 – 23.
Lan Julong,Xing Chiqiang,Hu Yuxiang,et al. Reconfiguration technology and future network architecture[J]. Telecommunications Science,2013,29(8):16 – 23. (in Chinese)

[7] Elbirt A J. Reconfigurable computing for symmetric-key algorithms[D]. Massachusetts,USA:Electrical and Computer Engineering Department, University of Massachusetts Lowell,2002.

[8] AJ Elbirt. Instruction-level distributed processing for symmetric-key cryptography[A]. In:International Parallel and Distributed Processing Symposium (IPDPS03)[C]. Nice, France 2003. 78.

[9] Fronte D, Perez A, Payrat E. Celator: A multi-algorithm cryptographic co-processor[A]. In Proceedings of the International Conference on Reconfigurable Computing and FPGAs (ReConFig'08)[C]. IEEE Computer Society,Los Alamitos,CA,2008. 438 – 443.

[10] Ravi S,Raghunathan A,Potlapally N,et al. System design methodologies for a wireless security processing platform [A]. Proceedings of the 39th annual Design Automation Conference[C]. New Orleans, Louisiana, USA: ACM, 2002. 777 – 782.

[11] Hauser J R,Wawrzynek J. Garp:A MIPS processor with a reconfigurable coprocessor[A]. Proceedings of Field-Programmable Custom Computing Machines[C]. Los Alamitos,CA,USA:IEEE,1997. 12 – 21.

[12] Mirsky E,DeHon A. MATRIX:a reconfigurable computing architecture with configurable instruction distribution and deployable resources[A]. IEEE Symposium on FPGAs for Custom Computing Machines[C]. Napa, CA, USA:IEEE,1996. 157 – 166.

[13] Marshall,Alan,et al. A reconfigurable arithmetic array for multimedia applications[A]. Proceedings of the 1999 ACM/SIGDA seventh international symposium on Field programmable gate arrays[C]. New York, USA: ACM, 1999. 135 – 143.

[14] Liang C,Huang X. SmartCell:An energy efficient coarse-grained reconfigurable architecture for stream-based applications[J]. EURASIP Journal on Embedded Systems, 2009(1):1 – 15.

[15] Hartenstein R,Herz M,Hoffmann T. Mapping applications onto reconfigurable kressArray[A]. Proceedings of 9th

International Workshop on Field Programmable Logic and Applications[C]. Berlin, German: Springer LNCS 1673, 1999. 385 – 390.

[16] 姜晶菲. 可重构密码处理结构的研究与设计[D]. 长沙: 国防科技大学,博士论文,2007.

[17] 曲英杰. 可重组密码逻辑的设计原理[D]. 北京:北京科技大学. 2002.

[18] 杨晓辉. 面向分组密码处理的可重构设计技术研究[D]. 郑州:中国人民解放军信息工程大学. 2007.

[19] Wang Y, Liu L, Yin S, et al. On-chip memory hierarchy in one coarse-grained reconfigurable architecture to compress memory space and to reduce reconfiguration time and data-reference time[J]. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2014, 22(5): 983 – 994.

[20] Bossuet L, Grand M, Gaspar L, et al. Architectures of flexible symmetric key crypto engines—a survey: From hardware coprocessor to multi-crypto-processor system on chip[J]. ACM Computing Surveys (CSUR), 2013, 45(4):41.

[21] Granado-Criado J M, Vega-Rodríguez M A, Sánchez-Pérez J M, et al. A new methodology to implement the AES algorithm using partial and dynamic reconfiguration[J]. INTEGRATION, the VLSI journal, 2010, 43(1): 72 – 80.

[22] Francisco Fons, Mariano Fons, Enrique Cantó, Mariano López. Deployment of run-time reconfigurable hardware coprocessors into compute-intensive embedded applications[J]. Journal of Signal Processing Systems, 2012, 66(2):191 – 222.

[23] Pérez O, Berviller Y, Tanougast C, et al. The use of runtime reconfiguration on FPGA circuits to Increase ihe performance of the AES algorithm implementation[J]. Journal of Universal Computer Science, 2007, 13(3): 349 – 362.

[24] Ismaili Z E A A, Moussa A. Self-partial and dynamic reconfiguration implementation for AES using FPGA[J]. International Journal of Computer Science Issues, 2009(2):33 – 40.

[25] Hori Y, Satoh A, Sakane H, et al. Bitstream encryption and authentication using AES-GCM in dynamically reconfigurable systems[A]. International Workshop on Security[C]. Berlin, German: Springer, 2008. 261 – 278.

[26] Le Masle A, Luk W, Eldredge J, et al. Parametric encryption hardware design[A]. International Symposium on Applied Reconfigurable Computing[C]. Berlin, German: Springer, 2010. 68 – 79.

[27] Öksüzoglu E, Savas E. Parametric, secure and compact implementation of RSA on FPGA[A]. 2008 International Conference on Reconfigurable Computing and FPGAs[C]. Los Alamitos, California, USA: IEEE, 2008. 391 – 396.

[28] Eisenbarth T, Güneysu T, Paar C, et al. Reconfigurable trusted computing in hardware[A]. Proceedings of the 2007 ACM workshop on Scalable trusted computing[C]. New York, USA: ACM, 2007. 15 – 20.

[29] Glas B, Klimm A, Sander O, et al. A system architecture for reconfigurable trusted platforms[A]. Proceedings of the conference on Design, automation and test in Europe[C]. New York, USA: ACM, 2008. 541 – 544.

[30] Malipatlolla S, Feller T, Shoufan A, et al. A novel architecture for a secure update of cryptographic engines on trusted platform module[A]. 2011 International Conference on Field-Programmable Technology (FPT)[C]. Piscataway, NJ, USA: IEEE, 2011. 1 – 6.

[31] Conte A, Anquetil L P. Design for application protocol stack framework[A]. IEEE International Conference on Communications[C]. New Orleans: IEEE, 2000. 565 – 570.

[32] Stefan B. Ken M, Brian W. Application-compliant networking on embedded systems[A]. Proc of 5th IEEE International Workshop on Networked Appliances Manchester[C]. Piscataway, NJ, USA: IEEE, 2002. 53 – 58.

[33] Moon J T, Kim J S, Kim J B, et a1. A hardware implementation of distributed network protocol[J]. Computer Standards and Interfaces, 2005, 27(3): 221 – 232.

[34] 蔡衍文,陈天洲,吴朝晖. 面向通信设备的网络协议构件化[J]. 计算机应用究,2004,21(12):253 – 256.
Cai Yan-wen, Chen Tian-zhou, Wu Zhao-hui. Component-based Network Protocols on Communication Device[J]. Application Research of computers, 2014, 21(12): 253 – 256. (in Chinese)

[35] Casado R, Bermudez A, Duato J, et a1. A protocol for deadlock-free dynamic reconfiguration in high-speed local area networks[J]. IEEE Trans on Parallel and Distributed Systems, 2001, 12(2): 115 – 132.

[36] Casado R, Bermudez A, Quiles F J, et a1. Influence of network size and load on the performance of reconfiguration protocols[A]. IEEE International Symposium on Network Computing and Applications[C]. Cambridge, IEEE, 2001. 46 – 57.

[37] Casado R, Bermudez A, Duato J, et a1. Performance evaluation of dynamic reconfiguration in high-speed local area networks[A]. Proceedings of 6th International Symposium on High-Performance Computer Architecture[C]. Toulouse, IEEE, 2000. 85 – 96.

[38] Jedhe G S, Ramamoorthy A, Varghese K. A scalable high throughput firewall in FPGA[A]. 16th International Sym-

posium on Field-Programmable Custom Computing Machines [C]. Los Alamitos, CA, USA: IEEE, 2008. 43 – 52.

[39] Lee T K, Yusuf S, Luk W, et al. Compiling policy descriptions into reconfigurable firewall processors [A]. 11th Annual IEEE Symposium on Field-Programmable Custom Computing Machines, 2003 [C]. Los Alamitos, CA, USA: IEEE, 2003. 39 – 48.

[40] Kai Zhang, Xiaoming Ding, Ke Xiong, Shuo Dai. RSS: A reconfigurable security system designed on NetFPGA and virtex5-LX110T [A]. 1st European NetFPGA Developers Workshop [C]. Oxford, UK: University of Cambridge, 2010.

[41] Tan T H, Ooi C Y, Hau Y W, et al. Remote dynamically reconfigurable platform using NetFPGA [A]. 2014 IEEE International Symposium on Circuits and Systems (ISCAS) [C]. Piscataway, NJ, USA: IEEE, 2014. 1239 – 1242.

[42] Tan T H, Ooi C Y, Marsono M N. rrBox: A remote dynamically reconfigurable network processing middlebox [A]. 2015 25th International Conference on Field Programmable Logic and Applications (FPL) [C]. London, UK: Imperial College, 2015. 1 – 4.

[43] Bossuet L, Fischer V, Gaspar L, et al. Disposable configuration of remotely reconfigurable systems [J]. Microprocessors and Microsystems, 2015, 39(6): 382 – 392.

[44] Qi Y, Fong J, Jiang W, et al. Multi-dimensional packet classification on FPGA: 100 Gbps and beyond [A]. 2010 International Conference on Field-Programmable Technology (FPT) [C]. Piscataway, NJ, USA: IEEE press, 2010. 241 – 248.

[45] Salman A, Rogawski M, Kaps J P. Efficient hardware accelerator for IPSec based on partial reconfiguration on Xilinx FPGAs [A]. 2011 International Conference on Reconfigurable Computing and FPGAs [C]. Piscataway, NJ, USA: IEEE, 2011. 242 – 248.

[46] Wang H, Bai G, Chen H. A gbps IPSec SSL security processor design and implementation in an FPGA prototyping platform [J]. Journal of Signal Processing Systems, 2010, 58(3): 311 – 324.

[47] Isobe T, Tsutsumi S, Seto K, et al. 10 Gbps implementation of TLS/SSL accelerator on FPGA [A]. 2010 18th International Workshop on Quality of Service (IWQoS) [C]. Piscataway, NJ, USA: IEEE, 2010. 1 – 6.

[48] Hamilton M, Marnane W P. Implementation of a secure TLS coprocessor on an FPGA [J]. Microprocessors and Microsystems, 2016, 40(2): 167 – 180.

[49] Paul R, Chakrabarti A, Ghosh R. Multi core SSL/TLS security processor architecture and its FPGA prototype design with automated preferential algorithm [J]. Microprocessors and Microsystems, 2016, 40: 124 – 136.

[50] Chaves R, Kuzmanov G, Sousa L. On-the-fly attestation of reconfigurable hardware [A]. 2008 International Conference on Field Programmable Logic and Applications, FPL 2008 [C]. Heidelberg, Germany: Kirchhoff Institute for Physics, IEEE, 2008. 71 – 76.

[51] Kastner R, Huffmire T. Threats and challenges in reconfigurable hardware security [R]. California Univ San Diego La Jolla, Dept of Computer Science and Engineering, July 2008.

[52] Drimer S, Kuhn M G. A protocol for secure remote updates of FPGA configurations [A]. International Workshop on Applied Reconfigurable Computing [C]. Berlin German: Springer, 2009. 50 – 61.

[53] Huffmire T, Brotherton B, Callegari N, et al. Designing secure systems on reconfigurable hardware [J]. ACM Transactions on Design Automation of Electronic Systems (TODAES), 2008, 13(3): 44.

[54] Saar Drimer. Volatile FPGA design security-a survey [EB/OL]. http://www.cl.cam.ac.uk/sd410, 2008. 1 – 42.

[55] Drzevitzky S, Kastens U, Platzner M. Proof-carrying hardware: Towards runtime verification of reconfigurable modules [A]. 2009 International Conference on Reconfigurable Computing and FPGAs [C]. Piscataway, NJ: IEEE, 2009. 189 – 194.

[56] Silva V D, Kroening D, Weissenbacher G. A survey of automated techniques for formal software verification [J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2008, 27(7): 1165 – 1178.

作者简介

肖 玮 女, 1979 年出生, 博士研究生, 讲师, 主要研究方向为网络与信息安全、可重构安全计算.

陈性元(通讯作者) 男, 1963 年出生, 博士, 教授, 主要研究方向为网络与信息安全等. E-mail: chxy302@vip.sina.com