



基于安全基片的可重构网络安全管控机制^{*}

陈 杰, 刘建伟, 王蒙蒙, 何双羽, 毛 剑

(北京航空航天大学电子信息工程学院 北京 100191)

摘 要:对下一代互联网安全体系架构进行了分析探讨,重点研究了已有网络体系架构的特点及面临的安全挑战,界定了可重构网络体系的安全目标,并提出了基于安全基片的可重构网络安全管控机制。同时,给出了安全基片定义以及基于安全基片的可重构网络安全模型,并对多级安全等级的安全服务构造、基于安全基片动态构建安全服务等可重构网络安全管控的关键环节进行了深入阐述。

关键词:下一代互联网设计;可重构网络;安全基片;动态安全模型

doi: 10.3969/j.issn.1000-0801.2014.07.004

Security Substrate Based Security Management and Control Mechanism of Reconfigurable Network

Chen Jie, Liu Jianwei, Wang Mengmeng, He Shuangyu, Mao Jian

(School of Electronic and Information Engineering, Beihang University, Beijing 100191, China)

Abstract: The next generation internet security architectures were analyzed and the characteristics and security challenges of the existing network were studied. The security goals of reconfigurable network were defined, and the “security substrate” based security management and control mechanism of reconfigurable network was presented. The definition of “security substrate” was given and the corresponding reconfigurable networks security model was illustrated. The construction of security services with multilevel security structure and security service establishment process via “security substrate” were put forward, which were key components of the security management and control architecture of reconfigurable network.

Key words: next generation internet design, reconfigurable network, security substrate, dynamic security model

1 引言

作为目前的基础网络体系,互联网是迄今为止运行经验最为丰富的网络,也是全球投资最大的网络。互联网以其网络的开放性、技术的创新性、信息传播的交互性而广泛渗透到社会各个领域。随着人们对互联网的规模、功能和性能等方面的需求越来越高,以 IPv4 为核心技术的互联网面临着日趋严峻的挑战^[1]。由于当前网络内在的能力

与结构对业务需求的适应性差,导致其对融合、泛在、质量、安全、扩展、可管可控、移动等的支持能力低下,不能从根本上满足提供泛在的信息服务、支持多样化和全方位的网络业务、保证高质量的通信效果、确保信息交互的安全可信、实施有效的管理控制等迫切需求^[2]。

互联网从诞生到现在已经发展了 40 多年,在设计之初,由于当时各种背景所限,其体系结构的设计基础是“分组交换”技术、“端到端透明”和“最大努力交付”等理念^[3]。

^{*} 国家重点基础研究发展计划(“973”计划)基金资助项目(No.2012CB315905),国家自然科学基金资助项目(No.61272501)



同时因为诞生之初的互联网应用于一个封闭的可信环境,所以根本没考虑现在开放的不可信环境的安全问题。目前互联网的安全问题十分突出,主要表现为:中间节点对传输数据分组的来源不验证、不审计,导致地址、身份被假冒,垃圾信息泛滥,大量的入侵和攻击行为无法跟踪,难以溯源;用户个人信息或者关键数据在网络上存储和传输都会面临风险,互联网中的数据系统、业务系统常常遭到攻击,各层漏洞层出不穷。这些安全脆弱性出现在互联网的设计、实现、运行和管理的各个环节。为了从根本上解决这些问题,下一代互联网及其应用的研究引起了世界各国的普遍关注,相继启动了一系列的重大研究计划与项目。研究人员希望在下一代互联网中解决目前互联网在扩展性、高性能、实时性、移动性、安全性、易管理和经济性等方面存在的重大技术问题。参加文献[4]指出下一代互联网的研究应该充分体现可控、可信、可管的特点。参考文献[5]认为可信的下一代互联网应具有如下特性:

- 实现系统和信息的保密性、完整性、可用性;
- 真实性,即用户身份、信息来源、信息内容的真实性;
- 可审计性,即网络实体发起的任何行为都可追踪到实体本身;
- 私密性,即用户的隐私是受到保护的,某些应用是可匿名的;
- 抗毁性,在系统故障、恶意攻击的环境中,能够提供有效的服务;
- 可控性,指对违反网络安全政策的行为具有控制能力。

国家科学技术部于2012年部署国家重点基础研究发展计划(“973”计划)项目“可重构信息通信基础网络体系研究”,用于研究基于可重构技术的新型网络体系架构,其中一项重要的研究内容就是针对可重构网络的安全管控机理与结构的研究与设计。下面将围绕可重构网络安全管控机制展开详细介绍。

2 下一代互联网设计中的安全管控机制

在过去的10年中,为了解决现有网络的不足之处,美国、欧盟、日本以及我国的研究机构在政府的大力推动下,纷纷开展未来网络体系架构的研究,其中比较有影响力并且在安全管控方面涉及较多的主要有以下几个项目。

2.1 NDN

NDN(named data networking)(2010–2013年)^[6–8]是由美国国家科学基金会(NSF)FIA(future internet architecture)

项目资助,由加州大学洛杉矶分校、帕罗奥多研究中心(PARC)、华盛顿大学、伊利诺大学香槟分校等12个组织合作研究。NDN项目致力于使互联网可以不考虑内容存储所在的物理位置,直接提供面向内容的功能。NDN将通信模式从关注“在哪里”,如地址、服务器、端系统,转变为关注“是什么”,即用户和应用关注的内容。

根据NDN体系结构遵循的设计原则:所谓的“细腰”结构是原互联网爆炸式增长的关键因素,NDN将保持沙漏型的体系结构,但其安全性必须内置在体系结构中,这与当前互联网安全采用事后补救式的机制不同,后者并不能满足当前敌意持续增长的环境。传统网络聚焦网络连接的安全,关注连接到何处和如何连接,而NDN则是基于内容的安全。内容的发布者在发布内容时产生一个映射 $M(N, C, \text{sign}(N, C))$,接收者则可验证内容和映射。在NDN体系结构的安全和隐私属性保护机制中,每个NDN分组的名字用一个数字签名和分组的内容绑定。这个基础特性提供数据完整性和原始认证,支持信任和起源通过分组签名者和它的源(例如个人和组织)之间的映射。命名和签名的内容也为构建安全应用打下坚实的基础,但是这引出了两个核心安全需求:实现具有良好成本效益的细粒度签名操作和设计功能性的有效的信任管理基础模型。NDN虽然提供了新的、基础的且强有力的机制来验证内容和确定起源,但是恶意的和有害的内容如垃圾邮件(例如来自恶意软件),也可能起源于一个合法的内容源且拥有合法的数字签名。

2.2 XIA

XIA(expressive internet architecture)^[9,10]是由NSF FIA项目资助,由卡内基梅隆大学、威斯康星大学麦迪逊分校、波士顿大学、杜克大学合作研究。XIA项目致力于构建一种未来互联网体系结构,具有以下特点:可信、支持长期演化的多种应用模型、支持长期的技术革新、支持不同网络参与方的显示接口。XIA体系结构具有内在安全性、支持丰富的通信实体集和保持当前网络的“细腰”结构。参考文献[11]中首次提出支持路由控制、路由失效隔离、端到端通信的信息显式可信的互联网体系结构SCION(scalability, control, and isolation on next-generation network)。SCION的设计原则是:基于域的隔离机制,划分路由控制平面为不同的独立域;交互、可控的路由选择,源和目的地之间联合选择路径;端到端通信的显式信任和小可信计算基(small trusted computing base)。

SCION 定义了自治域 (autonomous domain, AD) 作为自主管理的单元, 包括传输自治域和端自治域。基于地理拓扑或管理关系的大型核心网络可以被划分成若干个自治域。SCION 将自治域划分为层次结构的可信域 (trust domain, TD), 提供基于域的隔离属性。一个可信域可以是数个共享相同的商业契约、文化、法律法规和技术协议的自治域的集合, 具有一致的信任根、公共路由策略和自治域间的互审计性。可信域的内核也可作为其所包含的所有自治域的信任根, 基于该信任根可以在可信域内各自自治域之间执行一致的安全策略。良好的设计原则使 SCION 具有较强的安全性和可生存性等内在特质, 进而避免了像当前互联网这样通过使用零散式的补充协议作为安全补丁的方式。同时 SCION 假设作为在可信域中信任锚点的少数顶层的互联网服务提供商 (ISP) 数量并不太多, 达到了小可信计算基的设计目标, 降低了系统的复杂度。

2.3 AKARI

AKARI 项目是由日本通信技术国家研究所 (national institute of communication technology, NICT) 发起和研究的。AKARI 中关于网络安全的定义是: 保护网络通信、设备、信息、服务和资源, 以抵抗各种恶意行为如未授权的修改、破坏、信息泄露、干扰、伪造和假冒。AKARI 项目研究人员提出的下一代网络安全通用架构^[12,13]中, 将安全需求在数据平面和控制平面中分为 3 个级别: 设备安全、基础设施和服务安全。一个网络应该提供的安全服务包括身份管理、身份验证、机密性、完整性、隐私、不可否认性、可审计性、访问控制、可恢复性和授权等, 其中 AKARI 项目研究人员认为身份管理、隐私和可恢复性对下一代网络是必不可少的。

2.4 SDN

2007 年, 作为斯坦福大学 Clean State 在企业网安全方面的一个子项, 斯坦福大学的 Casado M 等人提出了 SANE 网络架构和 Ethane 网络架构, 用于提供企业网络中的安全管理^[14]。后来由于这种技术本身的优势和相应的技术推广, 这种网络架构不断发展, 而后被重新命名为软件定义网络 (software defined networking, SDN), 并被认为是替代传统层次网络架构、解决当前和未来网络爆炸性需求的一种革新技术。SDN 基于控制和转发相分离的思路, 实现了网络和业务的可编程, 促进了网络的虚拟化和 IT 化以及硬件的归一化, 为降低建设成本、运维难度和业务响应时间奠定了基础。目前产业界成立了中立的开放网络基金会 (Open Networking Foundation, ONF), 包括德国电信、Facebook、

Google、微软、Verizon、Yahoo 等在内的 41 家公司参与推动 SDN 有关的产品、标准化和市场形成。

对 SDN 的架构^[15]进行分析可知, SDN 中的安全问题^[16]主要集中在控制平面和应用平面及其中间的接口。

(1) 控制平面

集中化的控制平面承载着网络环境中的所有控制流, 是网络服务的中枢机构, 其安全性直接关系到网络服务的可用性、可靠性和数据安全性, 是 SDN 安全首先要解决的问题。控制平面的安全问题包括网络监听、地址欺骗、DDoS 攻击和病毒、蠕虫及木马攻击。

(2) 应用平面

应用平面将通过应用提供各种复杂的网络服务, 安全问题也将随之而来。应用平面的主要安全问题包括应用的授权、认证、隔离以及策略冲突的消解^[17]。

综上, 虽然上述几个影响力较大的下一代网络设计项目都取得了初步的成果, 其或多或少也针对网络安全管控方面有所考量, 但由于未来网络的安全机制和网络需求与架构密切相关, 所以目前还并没有产生具体的安全管控机制或安全参考模型。

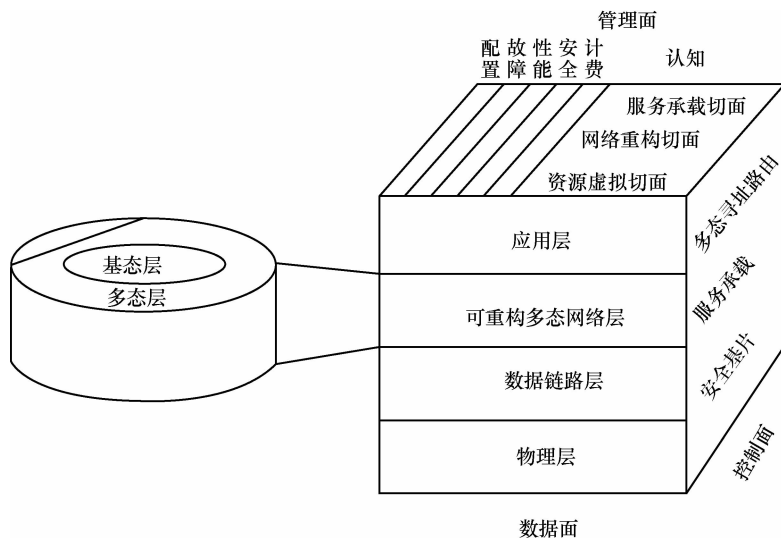
3 可重构网络安全管控

3.1 可重构网络体系结构

当前信息网络依赖的基础互联传输能力是制约整个信息网络总体功能的结构性瓶颈, 当前网络内在的能力与结构对业务需求的适应性差, 导致其对融合、泛在、质量、安全、扩展、可管可控、移动等的支持能力低下, 使得业务需求与网络基础能力之间的差距愈发显著。以应对上述挑战为切入点, 信息工程大学的兰巨龙等人^[18]提出了“可重构网络”思想并建立可重构信息通信基础网络体系, 在此基础上提出网络元能力理论、多态寻址路由机制、网络重构机理和安全可管可控机理, 以达到支持目前业务和未来新业务的不同服务质量需求, 功能灵活扩展, 满足泛在互联、融合异构、可信可管可扩需求。其网络体系功能结构如图 1 所示。

可重构网络的核心特征是其内在结构的时变性, 即由时变的结构驱动时变的服务能力, 最终实现网络服务对应用要求和特征的动态适配, 从“一致满足”应用要求的时变信道出发, 具有包含“渐变跟随”、“着眼整体”、“隐性隔离”和“自主驱动”特征的柔性可重构重要内涵^[19]。

可重构信息通信基础网络体系设计采用自顶向下方

图1 可重构网络体系功能参考模型^[18]

法,将泛在互联、服务质量保证、融合异构、安全可信、可管可扩等功能内嵌到网络体系结构中,以达到为不同业务提供满足其根本需求的、可定制的基础网络服务的目的,主要技术手段是通过增强 OSI 7 层网络参考模型中网络层和传输层的功能以解决目前 IP 网络层的功能瓶颈。

3.2 可重构网络安全挑战

可重构网络继承了目前互联网所面临的一些安全威胁,包括地址欺骗、身份伪造、拒绝服务攻击、非法入侵以及恶意代码等各种攻击。但是由于可重构网络与目前互联网有着网络体系结构上的不同,解决可重构网络安全可管可控问题面临着不同的挑战。

(1)网络集中管控的结构增加了中心节点被攻击的风险

可重构网络是以增加网络体系结构的复杂度来提高网络基础数据传输能力,其对网络的管控方式更加灵活、管控能力更强,但这种复杂度的增加必然需要集中的决策和优化,这在增加网络的管控开销的同时也会形成大大小小的功能节点。通过这些中心节点能实现网络功能的集中管控,但也面临着更多的风险。这里更多的风险,一方面是指攻击者会更愿意攻击中心节点;另一方面是指一旦中心节点被攻破,造成的破坏更大。

(2)动态变化的网络结构破坏了传统安全域的边界

可重构网络通过网络结构的自组织、功能的自调节和业务的自适应更好地适配承载业务的需求,其网络结构具有内在时变性,这意味着可重构网络的拓扑结构、节点状态、安全策略都是动态变化的,在这种情况下,传统的构建于具有明确边界的安全域之上的安全机制将不再适用。所

以在可重构网络体系中,需要设计新的符合可重构网络特征的安全机制。

(3)安全即服务的模式要求安全管控机制具备更高的顽健性

不同于传统互联网零散、修补式的解决安全管控问题的思路,可重构网络在设计之初就考虑要将安全管控机制内嵌到网络体系之中,这使得安全机制可以作为网络的基本服务提供给网络的使用者,即安全即服务模式。安全即服务的优点是极大地提高了可重构网络的安全性,可以为网络业务提供充分适配且全面的安全服务。传统互联网中常常通过部署第三方安全设备来实现一些安全机制,即使网络可用性被破坏,这些安全机制仍可能有效;而在可重构网络中一旦网络服务的可用性被破坏,比如受到拒绝服务攻击则会造成安全管控机制的失效。所以需要可重构网络安全管控机制具备更高的顽健性,难以轻易被破坏。

3.3 可重构网络安全目标

可重构网络安全管控在于解决安全功能简单叠加、不能满足系统复杂安全要求的问题,创立基于重构的安全基片逻辑,构建面向业务应用、内嵌的基于安全基片的安全管控机制,一方面使可重构网络为用户提供具有内置安全的网络服务;另一方面使可重构网络从体系架构设计层面支撑可管可控安全需求。

可重构网络安全管控的基本思路基于以下几点。

(1)提供充分且适配的安全服务的能力

目前的网络业务由于没有细分安全性需求,从而导致或者完全忽略可能存在的安全问题,或者盲目追求高安全

性而耗费大量网络资源,最终都违背了为用户提供安全、有效服务的网络设计初衷。因此,构建针对不同应用场景和用户需求、具有多级安全强度的安全服务,以实现网络安全需求的充分满足与合理适配,是设计可重构网络安全管控机制的关键。

(2) 基于全局一致性的安全管控能力

可重构网络需要进行全局性的规划和优化,有利于实现对网络的一致控制,提高网络资源利用效率以及网络的安全性。可重构网络还需要提供更方便、灵活的管理手段,对网络运行的各个方面实施全面、高效的管理,并无缝、高效地解决可控性问题。

即除信息安全外,还可以综合考虑网络应用性能、负载均衡等多方面的需求。SDN 提供了将信息安全与网络可用性、容灾备份等统一考虑的技术手段。

(3) 具备安全态势分析和动态调整的能力

从理论上讲,根本上消除网络的脆弱性、企图设计并实现一个绝对安全的网络体系结构是不切实际的。既需要从可重构网络体系结构设计上考虑足够的能应对已知安全威胁的安全机制,如必须提供可信任的网络服务,确保网络地址及其位置的真实可信、网络对象可识别和已知的网络攻击可防范等,也需要具备必要的容错机制,实现入侵容忍、网络恢复、攻击源追踪定位等功能。

4 基于安全基片的可重构网络安全管控机制

4.1 安全基片

安全基片的概念及其构建机理是安全管控体系设计的核心环节,基于安全基片可以构造针对不同应用场景和用户需求、具有多级安全强度的安全服务,以实现网络安全需求的充分满足与合理适配。下面介绍可重构网络安全基片及相关概念的定义。

(1) 安全基片(security substrate, SS)是针对共性安全与管控特征要求而构造的基本安全要素和功能的总和,是实现网络安全管控机制动态可重构的功能基础,基于安全基片构造多级安全等级安全服务,进而更加灵活地满足具体的安全业务的不同安全需求。

(2) 安全元能力(security atomic capability, SAC)是指能提供基本安全要素和功能的实体单元,通过安全元能力的有序重组可以为构建安全服务提供功能单位。通过对现有网络安全机制中所涉及的具体安全技术进行分析归纳,同时结合可重构基础网络的特性,将形成安全元能力的安

全要素的粒度确定在能独立完成一定安全功能的安全协议一级,如认证协议、密钥分配协议、密钥协商协议和具体的加密算法等。

(3) 安全元服务(security atomic service, SAS)是指由多种安全元能力聚类为一种“安全机制”,并由这些安全机制来保障提供的“安全服务”。

(4) 安全服务链(security service chain, SSC),节点上的安全元能力动态有序地组合成具有一定顺序的安全元能力序列,当这些有序组合在一起的安全元能力能够供具体的安全时,即称为安全服务链。安全服务链是节点提供安全服务的逻辑和功能结构。安全服务链是一类特殊的服务链,其功能和结构与其他业务服务链相似,由公共部分和特定部分组成,公共部分是使用该服务链的安全业务都要使用相同的安全元能力;特定部分则由于业务安全需求的不同,服务链的构建过程中或考虑元能力的参数不同,或考虑组合顺序不同等原因,出现多个不同分支。

(5) 安全服务路径(security service pathway, SSP),根据上层业务的不同,安全需求网络可定制安全服务路径,安全服务路径是一种网络拓扑结构,其依据节点上安全基片可提供的安全元能力是否能满足相应的业务安全需求,结合路由和安全服务链构建一条最优路径,满足上层业务的安全需求。

4.2 基于安全基片动态构建安全服务

安全服务构建机制需要能满足可重构基础网络的差异化业务、多级安全需求、动态结构重组和安全功能动态重构的性能要求,以实现“服务承载网业务承载需求充分满足、网络安全需求合理适配”的构建目标。作为基础通信网络,不同承载业务的安全需求以及网络的安全态势和网络资源使用情况皆在动态变化,因此可重构基础网络中的安全服务也必须是动态可重构的,借鉴现有信息系统安全模型由安全策略、防护、检测、响应和恢复共同构成完整安全体系的思想,并基于安全基片作为功能基础,将安全服务的构建过程设计为动态调整的迭代过程,并在此过程中融合了业务安全需求分析、网络安全态势感知、安全方案适配、可信路径构建、安全服务链构建、安全服务动态调整等机制,以实现可重构网络安全服务的动态构建需求。

在融合了业务安全需求分析、网络安全态势感知、安全方案适配、可信路径构建、安全服务链构建、安全服务动态调整等机制的基础上,设计安全服务构建流程,如图2所示,将可重构网络安全服务构建过程划分为5个步骤。

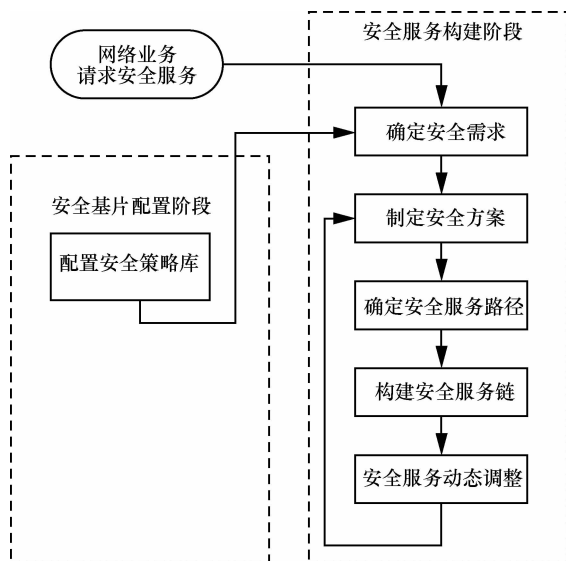


图2 安全服务构建流程

(1) 确定安全需求

为了实现针对上层安全服务提供充分且适度的安全服务,首先需要准确描述安全服务的安全需求,业务安全需求由网络智能感知和业务需求驱动共同确定。对上层业务安全需求和网络安全态势的智能感知是可重构网络的一项基本特性,是实现安全服务可重构、资源自配置、能力自调整的前提,包括业务类型分析和网络安全态势分析等,业务类型可通过协议解析、数据流量分析获得;安全态势分析需运用网络流量分析、入侵检测、安全审计等技术。在网络智能感知的基础上,业务需求驱动同样重要,从用户角度判断用户信息资产的“价值”,由用户主动定制其对数据机密性、完整性或隐私保护等安全机制的需求会较为准确。

(2) 制定安全方案

基于具体业务安全需求和当前网络安全态势,根据网络安全策略库,决定提供何种安全服务以及该安全服务的安全等级级别,进而确定所需要的具体安全机制和安全技术。选择何种安全服务以及各安全服务的强度级别需要综合考虑业务的安全需求和当前网络安全态势,即所确定的安全方案需要在应对当前网络安全威胁的基础上满足业务安全需求。针对业务相同的安全需求,如果当前网络面临的安全风险较大,则需选择更高安全等级级别的安全服务;反之,则可以适度选择较低安全等级级别的安全服务,节约网络资源。

(3) 确定安全服务路径

根据安全方案的具体要求,结合路由策略、网络节点

安全基片状态和可用资源等信息综合决策,确定提供安全服务的安全服务路径,确定安全服务路径经过的所有节点及需要其提供的安全服务。安全方案中规定了构建安全服务所必需的安全技术及其具体配置,接下来需要确定由哪些节点来提供这些安全服务,这个过程可以理解为是在对网络节点可提供的安全元能力和可用资源(计算资源、存储资源、带宽资源)进行认知、分析的基础上,综合考虑数据分组转发可达性以及网络节点行为的信任值等约束条件的路由建立过程。

(4) 构建安全服务链

安全服务路径经过的所有节点根据安全方案重构安全基片,构建安全元服务进而构建安全服务链,建立安全服务路径。确定某网络节点是安全服务路径中的节点,则开始根据该节点的实时资源使用情况进行安全元服务的重构。

重构分为以下几种情况:

- 具备所需安全元能力,则直接构建安全服务链;
- 目前不具备所需安全元能力,但通过重构可以具备该元能力且可用资源满足实现重构的条件,执行安全元能力的重构过程,进而构建安全服务链;
- 目前不具备所需安全元能力,虽然通过重构可以具备该元能力但目前节点资源不满足实现的条件,则通过网络级的重构,释放该节点部分资源以满足重构条件,执行安全元能力的重构过程,进而构建安全服务链。

(5) 安全服务动态调整

考虑到可重构网络的动态特征,在安全业务执行过程中,可能出现网络拓扑的动态变化、安全态势的动态变化、网络资源的动态变化,需要对这些变化进行感知,并反映到网络控制层面,必要时须对安全方案进行调整,重新进行第(2)~(4)步。需要实现网络安全态势感知、网络资源变化感知以及节点资源的释放,网络资源变化感知需要确定安全业务承载过程中网络资源的变化情况,比如是否有网络节点宕机,是否出现网络流量拥塞,是否有新的资源加入网络而且利用新的资源可以更好地提供安全服务等。节点资源释放是指在某一项安全服务执行完成后的一段时间内,节点上的某些元能力不再被其他安全服务所需要,则释放该元能力所占用的资源,优化网络资源的利用情况。

5 结束语

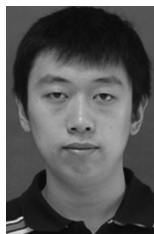
本文对下一代互联网尤其是可重构网络的安全管控

机制的目标和构建机制进行了研究探讨。具体通过研究分析下一代互联网体系架构设计中安全管控的重要性,对已有的几个下一代互联网体系设计项目中的安全管控机制进行分析总结。重点研究可重构网络体系架构的特点及其面临的安全挑战,对可重构网络体系的安全目标进行了界定,并对安全基片、多级安全强度的安全服务、安全服务路径等概念进行了定义。最后提出了基于安全基片的可重构网络安全管控机制,并详细说明了多级安全强度安全服务构造和基于安全基片构建多级安全强度安全服务的流程。本文提出的安全服务构建流程能够满足可重构网络动态、充分、适配地支持网络业务的差异性的安全需求,为应对构建可重构网络安全管控机制的安全挑战提供了一种可行的方案。

参考文献

- 1 吴建平,吴茜,徐恪.下一代互联网体系结构基础研究及探索. 计算机学报, 2008, 31(9):1536~1548
- 2 兰巨龙,邢池强,胡宇翔等.可重构技术与未来网络体系架构. 电信科学, 2013, 29(8):16~23
- 3 Day J. Patterns in Network Architecture: A Return to Fundamentals, Edition I. Prentice Hall, 2007
- 4 林闯,任丰原.可控可信可扩展的新一代互联网. 软件学报, 2004(12):1815~1821
- 5 Jain R. Internet 3.0: ten problems with current internet architecture and solutions for the next generation. Proceedings of Military Communications Conference (MILCOM 2006), Washington, DC, USA, 2006
- 6 Named data networking. <http://www.named-data.net/>, 2012
- 7 The NDN Project Team. Named Data Networking (NDN) Project. NDN Technical Report NDN-0001, October 2010
- 8 DiBenedetto S, Gasti P, Tsudik G, *et al.* ANDaNA: anonymous named data networking application. Proceedings of 19th Annual Network & Distributed System Security Symposium, San Diego, CA, USA, February 2012
- 9 Han D S, Anand A, Dogar F, *et al.* XIA: efficient support for evolvable internetworking. Proceedings of NSDI'12, San Jose, CA, USA, April 2012
- 10 Anand A, Dogar F, Han D S, *et al.* XIA: an architecture for an evolvable and trustworthy internet. Proceedings of the Tenth ACM Workshop on Hot Topics in Networks (HotNets-X), Cambridge, MA, USA, November 2011
- 11 Zhang X, Hsiao H C, Hasker G, *et al.* SCION: scalability, control, and isolation on next-generation networks. Proceedings of IEEE Symposium on Security and Privacy, Oakland, USA, May 2011
- 12 Hirabaru M, Inoue M, Harai H, *et al.* AKARI architecture conceptual design for new generation network. NICT AKARI Project Report. http://www.nict.go.jp/en/photonic_nw/archi/akari/4otfsk00000dgfsp-att/4otfsk00000dggej.pdf, 2007
- 13 Teraoka F. Redesigning layered network architecture for new generation networks. Proceedings of FutureNet II, GLOBECOM'09, Honolulu, Hawaii, December 2009
- 14 Casado M. Architectural support for security management in enterprise networks. Doctoral Dissertation, Stanford University, 2007
- 15 ONF. Software-Defined Networking: the New Norm for Networks. ONF White Paper, 2012
- 16 王淑玲,李济汉,张云勇等. SDN 架构及安全性研究. 电信科学, 2013, 29(3):117~122
- 17 Hartman S, Wasserman M, Zhang D. Security Requirements in the Software Defined Networking Model. IETF Draft (draft-hartman-sdnsec-requirements), 2013
- 18 兰巨龙,程东年,胡宇翔.可重构信息通信基础网络体系研究. 通信学报, 2014, 35(1):128~139
- 19 程东年,汪斌强,王保进等.网络结构自调整的柔性内涵初探. 通信学报, 2012(8):214~222

[作者简介]



陈杰,男,北京航空航天大学电子信息工程学院博士生,主要研究方向为 Ad Hoc 网络安全、下一代互联网安全机制。



刘建伟,男,博士,北京航空航天大学电子信息工程学院教授、博士生导师,主要研究方向为网络与信息安全、通信网络安全、密码学、信道编码技术。

王蒙蒙,女,北京航空航天大学电子信息工程学院博士生,主要研究方向为网络安全、密码学。

何双羽,男,北京航空航天大学电子信息工程学院博士生,主要研究方向为网络安全、密码学。

毛剑,女,博士,北京航空航天大学电子信息工程学院讲师,主要研究方向为 Web 应用行为分析与信任管理、云存储数据完整性验证。

(收稿日期:2014-06-22)