

从层次角度看网络空间安全技术的覆盖领域

方滨兴

(哈尔滨工业大学, 黑龙江 哈尔滨 150001)

摘要: 网络空间安全是涉及计算机科学与技术、信息与通信工程、控制科学与工程、密码学等学科的交叉学科, 具有明确而深入的学科内涵。给出了网络空间安全的定义, 提出了网络空间安全的层次模型, 并系统地梳理了目前网络空间安全学科中的八大研究领域在设备层、系统层、数据层和应用层所面临的主要研究问题和相关技术, 包括信息安全、信息保密、信息对抗、云的安全、大数据、物联网安全、移动安全和可信计算等。为进一步凝练网络空间安全的技术体系和学科方向提供了指导和借鉴。

关键词: 网络空间安全; 层次模型; 学科内涵; 信息安全; 信息对抗

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2015.00001

A hierarchy model on the research fields of cyberspace security technology

FANG Bin-xing

(Harbin Institute of Technology, Harbin 150001, China)

Abstract: Cyberspace security is an interdisciplinary subject involved with computer science and technology, information and communication engineering, control science and engineering and cryptography. It has an explicit and in-depth discipline connotation. First, the concepts of cyberspace security were advanced, and the definition was given. Then, a hierarchy model of cyberspace security was proposed. Based on the model, the details technologies of eight research fields of cyberspace security including information security, information secrecy, information countermeasure, cloud security, big data, IOT security, mobile security, and trustable computing were presented. New guidance and experience for the research in cyberspace security could be taken as.

Key words: cyberspace security; hierarchy model; discipline connotation; information security; information countermeasure

1 引言

为实施国家安全战略, 加快网络空间安全人才培养, 国务院学位委员会、教育部于2015年6月决定增设“网络空间安全”一级学科^[1], 于2015年10月决定增列“网络空间安全”一级学科博士学位授权点^[2], 这对于我国加快网络空间安全人才队伍建设和核心技术的自主创新具有重要意义。

美国国家安全54号总统令和国土安全23号

总统令中对网络空间 (cyberspace) 的定义是^[3,4]:

“网络空间是连接各种信息技术基础设施的网络, 包括互联网、各种电信网、各种计算机系统、各类关键工业设施中的嵌入式处理器和控制器。还涉及人与人之间相互影响的虚拟信息环境。”该定义强调网络空间是大范围连接的网络, 这种说法有一定的局限性, 导致物理隔离的网络、ad hoc网络等局域连接的网络不包含在网络空间中。

本文对网络空间的定义是: “网络空间就是

所有由可对外交换信息的电磁设备作为载体，通过与人互动而形成的虚拟空间，包括互联网、通信网、广电网、物联网、社交网络、计算机系统、通信系统、控制系统等。”首先，定义强调的“信息交换”不仅包括全局范围连接，也包括局域连接。因此，网络空间包括了局域连接的网络。其次，定义强调的“由电磁设备作为载体”明确了信息交换的途径，即通过电磁设备交换信息。因此，声音、化学、生物交换信息不属于网络空间的范畴。最后，定义强调的“与人互动而形成的虚拟空间”说明网络空间区别于陆、海、空、天的物理空间，是一个用于解决人的问题的虚拟空间。

在此基础上，本文首先提出了四横八纵的网络空间安全技术的覆盖领域，该体系纵向上分为设备层、系统层、数据层和应用层4个层次，横向上覆盖了信息安全、信息保密、信息对抗、云的安全、大数据、物联网安全、移动安全和可信计算8个主要领域；然后，分别介绍了在每个领域在不同层次所面临的安全问题及对应的安全技术；最后给出了结论。

2 网络空间安全的层次模型

网络空间中的任一信息系统或系统体系自

底向上可分为设备层、系统层、数据层和应用层4个层次，每个层次都面临着不同的安全问题，相应地形成了网络空间安全的4层次模型，如图1所示。设备层的安全应对在网络空间中信息系统设备所面对的安全问题；系统层的安全应对在网络空间中信息系统自身所面对的安全问题；数据层的安全应对在网络空间中处理数据的同时所带来的安全问题；应用层的安全应对在信息应用的过程中所形成的安全问题。

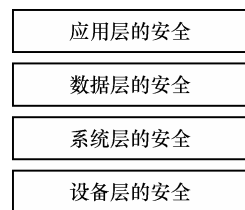


图1 网络空间安全的4层次模型

网络空间安全的研究领域主要包括信息安全、信息保密、信息对抗、云的安全、大数据、物联网安全、移动安全、可信计算领域。其中，信息安全是核心和根本，其他领域是信息安全向外的延伸。围绕这8个领域，本文归纳总结了网络空间安全的4层次模型面临着的安全问题及相应的安全技术，分别如图2和图3所示。

应用层的安全	有害信息	信息汇聚	制造舆论	恶意滥用	隐私挖掘	控制渗透	支付冒充	信誉不实
数据层的安全	信息篡改	密码破解	情报窃取	操作抵赖	数据混乱	隐私泄露	电话窃听	非法程序
系统层的安全	黑客攻击	远程木马	僵尸网络	平台攻击	运行干扰	传输干扰	传输阻塞	软件故障
设备层的安全	设施损毁	辐射泄密	电磁破坏	平台崩溃	设备失效	电子干扰	终端被攻	有害信息
	信息安全	信息保密	信息对抗	云的安全	大数据	物联网安全	移动安全	可信计算

图2 网络空间安全模型中的安全问题

应用层的安全	内容安全	脱密验证	传播对抗	可控的云	服务确保	控制安全	应用安全	信任可控
数据层的安全	数据安全	新型密码	情报对抗	可信的云	数据确保	信息确保	通信安全	可信证明
系统层的安全	运行安全	网络防窃	网络对抗	安全的云	系统确保	传输安全	信道安全	软件确保
设备层的安全	物理安全	干扰屏蔽	电子对抗	可靠的云	稳定确保	探针安全	终端安全	硬件可靠
	信息安全	信息保密	信息对抗	云的安全	大数据	物联网安全	移动安全	可信计算

图3 网络空间安全模型中的安全技术

3 设备层的安全

信息安全领域在设备层主要面临物理设备损毁的安全问题,例如“911 恐怖袭击导致 IT 公司消失”事件。针对设备损毁问题,应当关注物理安全,物理安全是对网络与信息系统物理装备的保护,例如生存性技术、容错技术、容灾技术、冗余备份技术等。

信息保密领域在设备层主要面临辐射泄密的安全问题,例如侧信道攻击。电磁辐射是指计算机电子线路在运行中所出现的电平翻转形成了交变电磁场,其能量形成了电磁波在空间进行传播。应该关注干扰屏蔽技术以防止辐射泄密。

信息对抗领域在设备层主要面临电磁破坏的安全问题,例如激光枪、高能炸弹、电磁炸弹。事实上,信息对抗是能量的对抗,具体包括维持我方使用与控制的能力,抵挡敌人阻碍我方使用的手段以及妨碍敌人达到相同目的的方式。针对电磁破坏,应该关注电子对抗技术,例如电子防护技术、电子攻击技术以及电子作战支援技术等。

云安全领域在设备层主要面临平台崩溃的安全问题,即云的不可靠性,例如大规模平台宕机、服务中断等。在设备层面实现可靠的云是物理安全灾备问题的一个实例化,可采用多副本冗余的方法保证云平台的容灾性,例如,复云的概念——云服务商之间建立接口互相备份,按照实际使用的情况结算。

大数据领域在设备层主要面临设备失效的安全问题。大数据的数据量大和传统意义上的数据量大有区别的,后者要求每条数据是精准的、不可缺失的;而前者关注的是非线性的数据,数据是可缺失的。针对大数据的设备失效问题,要重点关注数据保障技术,它解决的问题不是传统意义上严格的灾备,数据不需要完全恢复,允许在不影响大数据计算的前提下,缺失某些数据。

物联网安全领域在设备层主要面临电子干扰的安全问题。物联网的物理支撑是传感器,电子电磁波干扰会造成传感器网络以及其他传输通道的安全问题。针对上述问题,应该关注物联网的探针安全技术,例如干扰控制技术、安全路由技术、入侵检测技术等。

移动安全领域在设备层主要面临终端被攻击的安全问题。移动终端是移动互联网的重要载体,移动终端逐渐由通信工具向个人的信息处理中心转变,这使得移动终端成为新的安全热点。移动终端的智能化,带来了非法篡改信息、非法访问、病毒和恶意代码等新的安全问题。因此,需要关注移动终端安全技术,涵盖终端自身安全性、终端防泄密和终端运行维护管理等。

可信计算领域在设备层主要面临底层设备故障引起的安全问题。为解决此问题,提高提供可信计算服务的硬件实体可靠性,包括元器件可靠性、设备可靠性和系统可靠性。以可信赖平台模块(TPM, trusted platform module)为核心提供可信硬件平台,并作为可信计算平台的信任根,建立一级信任一级的信任链。

4 系统层的安全

信息安全领域在系统层面主要面临针对系统的黑客攻击,例如安全漏洞的恶意利用、非法控制系统、系统资源消耗等。黑客攻击导致运行环境出现安全问题,则需要研究运行安全。运行安全是指对网络与信息系统的运行过程和运行状态的保护,主要涉及对网络与信息系统的可控性、可用性等信息安全属性的保护,主要的保护方式有风险分析、安全策略、入侵防护、入侵检测、应急响应、系统恢复等。

信息保密领域在系统层面主要面临远程木马攻击造成的网络窃密问题。网络窃密是指未经信息持有人授权,通过网络攻击手段窃取秘密信息,以达到个人目的、经济利益、政治或军事优势等。秘密信息包括个人信息、敏感信息、专有信息等。远程木马通过网络从代码的角度去窃密信息,因此,在系统层应关注网络防窃技术。

信息对抗领域在系统层面主要面临僵尸网络攻击问题。黑客利用蠕虫等手段在互联网中数百到数十万台计算机上植入僵尸程序以便达到暗中操控的目的,这些被操控的计算机构成的网络被称作僵尸网络。针对僵尸网络,应该关注网络对抗技术,例如基于蜜罐密网对僵尸网络的监测技术、计算机网络防卫技术等。

云安全领域在系统层主要面临针对平台的攻

击问题。应对云平台攻击，需要构建安全的云，保证不让用户受到外来的攻击、保证用户的信息不被外界所窃取或篡改、保证用户的程序不被外界所劫持，主要防护技术包括云身份认证与访问控制、云风险评估、虚拟运行环境安全等。

大数据领域在系统层面主要面临运行干扰引发的安全问题。由于计算量大、数据量大，当某个计算节点中断服务时，就需要通过摆动、浮动等方式转移计算任务，此时计算的可靠性就成为了关键问题。相对应地，应该关注系统确保技术，以保证大数据计算的可靠性。

物联网安全在系统层主要面临传输干扰引发的安全问题。物联网多元化、异构化的网络环境加剧了数据传输环节的脆弱性，例如，针对传播环节的中间人攻击，攻击者拦截通信双方的通话，使通信的两端认为他们正在通过一个私密的连接与对方直接对话。针对传输干扰，应该关注物联网的传输安全技术防御干扰和欺骗，例如安全认证技术、安全数据融合技术等。

移动安全领域在系统层主要面临传输阻塞所引发的安全问题。移动终端的通信依靠运营商的基站，攻击者可以通过攻击基站，使其阻塞，进而中断基站服务，例如，运营商之间的拒绝服务攻击，就是向某基站大量地发送数据，将其资源占满，使其提供正常服务。针对上述问题，应该关注移动互联网的信道安全技术，例如终端与基站之间的安全通信协议和标准等。

可信计算领域在系统层主要面临软件故障所造成的安全问题。软件故障会导致系统崩溃，为此，需要关注可信计算的软件确保技术，软件确保是使软件在收到恶意攻击的情形下依然能够继续正确运行及确保软件在授权范围内被合法使用的思想，主要技术包括软件可信建模、程序安全性分析以及软件运行监控等。软件确保由信息确保发展而来，未来将进一步发展为系统确保、服务确保，最终成为实体确保。

5 数据层的安全

信息安全领域在数据层主要面临数据冒充、数据篡改、数据劫持等信息篡改的安全问题。相应地，应该关注数据安全技术。数据安全是指对

信息在数据收集、处理、存储、检索、传输、交换、显示、扩散等过程中的保护，使得在数据处理层面保障信息依据授权使用，不被非法冒充、窃取、篡改、抵赖。数据安全主要涉及对机密性、真实性、完整性、不可否认性、可用性等信息安全属性的保护。主要技术包括针对信息丢失的数据备份技术、针对信息窃取的加密保护技术、针对信息篡改的完整性检查技术、针对信息抵赖的数字签名技术、针对信息冒充的身份认证技术以及针对数据丢失的数据备份技术等。

信息保密领域在数据层主要面临通过暴力破解密码来非法侵入系统并获取私密信息等安全问题。暴力破解本质上是算法层面的对抗，常用的办法有字典攻击和彩虹表，前者通过逐一尝试字典中的各种明文字符串进行密码破解，后者利用彩虹表进行散列值反查明文。针对上述安全问题，应该关注新型密码的设计和实现。

信息对抗领域在数据层面主要面临情报窃取的安全问题。攻击者往往通过密码破解、绕过认证以及加密机制破解等方式达到信息窃取的目的，并最终演化为没有硝烟的情报战争。赢得情报战争的胜利，需要关注情报对抗技术。情报对抗是指敌我双方为获取对方情报和破坏对方搜集己方情报，向对方宣传虚假信息、以掩饰己方军事意图而进行的各种对抗活动，主要包括信息窃取、军事谋略、行动保密。

云安全领域在数据层面主要面临操作抵赖的安全问题。为防止操作抵赖需要建立可信的云，保证租户在云中的程序不被其他租户或云服务商所篡改和分析，保证租户在云中的数据不被其他租户或云服务商所篡改和窃取。可信的云的研究可从可信云框架、数据安全、审计和权限分割等几方面展开。

大数据领域在数据层面主要面临数据混乱所造成的安全问题。大数据在数据层面存在着海量的混乱数据，有价值的信息与噪声数据混杂在一起，导致数据无法被有效利用，例如网络水军散布的虚假言论。针对数据混乱问题，应该主要关注大数据的数据确保技术，建立数据的甄选机制，将有价值的信息从混乱的数据中区分出来，进而解决大数据的可信问题。

物联网领域在数据层面主要面临隐私泄露的安全问题。相应地,应该关注物联网的信息确保技术,主要包括数据的隐私保护和访问控制技术。隐私保护是使个人或物体等实体不愿被其他人获取的隐私信息得到应有的保护,隐私信息主要包括数据信息、位置信息。访问控制是按用户身份来限制用户对某些信息的访问或限制对某些控制功能的使用。

移动安全领域在数据层面主要面临电话窃听的安全问题。电话窃听内容包括移动终端之间的音视频数据和文本数据,其本质是数据传输过程中出现的数据篡改问题。针对此问题,应该关注通信安全技术,建立端对端的安全通信。这类技术仍属于传统的信息安全技术范畴,但要考虑终端移动所带来的特殊需求,例如端对端加密、身份替换等。

可信计算领域在数据层面主要面临非法程序所带来的数据不可信问题。数据可信是一种观念性的概念,涉及到数据来源可信、数据传输途径可信、数据处理过程可信等多个方面。要解决非法程序造成的数据不可信问题,需要关注可信证明技术,建立程序的鉴别体系,确定程序的可信性,涉及的主要技术包括加密签名技术、数据溯源技术、数据访问控制技术、数据使用控制技术等。

6 应用层的安全

信息安全领域在应用层主要面临有害信息传播的安全问题。有害信息包括谣言、暴力渲染、欺诈、色情诱惑等。有害信息的传播本质上是内容安全问题,由此,应该关注内容安全的相关技术。内容安全是对信息在网络内流动中的选择性阻断,以保证信息流动的可控能力,主要涉及信息的可控性、可用性等。相关技术包括文本特征抽取、字符串匹配、信息过滤与封堵等。

信息保密领域在应用层主要面临信息汇聚所引发的信息泄露问题。攻击者通过汇聚公开发布内容,利用大数据手段从中挖掘用户隐私。针对此问题,应该关注脱密验证技术,通过归纳学习、机器学习、统计分析等方法得到数据对象间的内在特性,据此分别在数据发布层面和数据查询层面建立脱密验证体系。

信息对抗领域在应用层主要面临制造舆论的安全问题。信息对抗在应用层关注的是舆情、心理,美国称之为传播对抗。中国最早称之为心理战,目前包括心理战、法律战和舆论战。为全面掌控舆情,应对新媒体引发的新问题,应该关注传播对抗技术,主要包括舆情的发现与获取、舆情的分析与引导、舆情的预警与处置等。

云安全领域在应用层主要面临云平台恶意滥用所造成的安全问题。攻击者能够利用云平台进行拒绝服务攻击,利用云平台进行僵尸网络攻击等。针对云的恶意滥用,需要在应用层实现可控的云,即云平台不会被利用作为攻击工具,保证在云平台中的程序不是恶意程序,保证在云平台中的用户可以被追溯责任,保证在云平台中的用户没有害人的能力。可控的云涉及的主要技术包括检测和预防云上木马传播、防御云做DDoS攻击、防御云做有害信息传播等。

大数据领域在应用层主要面临隐私挖掘所造成的信息泄露问题。隐私泄露是大数据特性引发的特有的安全问题,大数据在应用层其他安全问题都能够在其他领域找到。没有大数据之前,信息呈现碎片化,且相对安全。大数据的出现导致攻击者能够从海量的数据中挖掘出用户感兴趣的信息,获得更高层次的知识和规律,进而获取用户的隐私信息。针对隐私挖掘,需要关注大数据的服务确保技术,必须建立隐私保护体系,否则,大数据就是一把双刃剑。

物联网安全领域在应用层主要面临恶意渗透所造成的失控问题。物联网的核心应用是控制,物理信息系统将信息和物理环境相结合的目的就是以远程的、可靠的、实时的、安全的、协作的方式控制物理实体。工业控制系统产品越来越多地采用通用协议、通用硬件和通用软件,通过各种方式与互联网等公共网络连接,病毒、木马等威胁正在向工业控制系统扩散。由此,应该关注物联网的控制安全技术,主要技术包括控制安全保障体系、控制安全框架模型、控制安全异常发现等。

移动安全在应用层主要面临支付冒充的安全问题。伴随网购消费的快速发展,网上支付日益普及,随之而来的网上支付冒充的安全问题也备

受关注。移动终端病毒或木马的侵袭、支付软件自身存在的漏洞，很可能造成支付隐患。同时，移动支付追求便捷的用户体验，导致了支付安全性的降低。针对上述问题，应该关注移动终端的应用安全技术，针对不同操作系统，从应用自身和平台安全策略入手，保障应用安全。

可信计算在应用层主要面临信誉不实所引发的安全问题。可信计算在设备层实现硬件可靠，在系统层实现软件确保，在数据层证明程序可信。那么，在应用层要解决的就是信任缺失的问题，要做到信任可控，其中，应用的信任度是应用的行为表现符合主体（使用者）预期的程度，应用的可控度是主体对应用行为表现的限制能力。由此，应该关注信任可控技术，主要包括应用级完整性保障技术、应用异常检测技术和应用信任协商技术等。

7 结束语

本文基于网络空间安全层次模型，系统地梳理了目前的网络空间安全技术体系。从层次的角度来看，物理层的安全主要研究能量对抗，系统层的安全主要研究代码对抗，数据层的安全主要研究算法对抗，应用层的安全则根据不同应用研究不同的内容。从领域的角度来看，信息安全包括物理安全、运行安全、数据安全、内容安全；信息保密包括干扰屏蔽、网络防窃、新型密码、脱密验证；信息对抗包括电子对抗、网络对抗、情报对抗、传播对抗；云的安全包括可靠的云、安全的云、可信的云、可控的云；大数据包括稳

定确保、系统确保、数据确保、隐私确保；物联网安全包括探针安全、传输安全、信息确保、控制安全；移动安全包括终端安全、信道安全、通信安全、应用安全；可信计算包括硬件可靠、软件确保、可信证明、信任可控。

参考文献：

- [1] 国务院学位委员会，教育部. 关于增设网络空间安全一级学科的通知(学位[2015]11号)[R/OL]. http://www.moe.gov.cn/jyb_xxgk/moe_1777/moe_1778/201511/t20151127_221423.html.
Academic Degree Commission of the State Counter, the Ministry of Education. Notice concerning establishing cyberspace security as a first level discipline([2015]11)[R/OL]. http://www.moe.gov.cn/jyb_xxgk/moe_1777/moe_1778/201511/t20151127_221423.html.
- [2] 关于开展增列网络空间安全一级学科博士学位授权点工作的通知(学位[2015]39号)[R/OL]. http://www.moe.gov.cn/jyb_xxgk/moe_1777/moe_1778/201511/t20151127_221424.html.
Notice concerning developing cyberspace security first level discipline doctorate authorization([2015]39)[R/OL]. http://www.moe.gov.cn/jyb_xxgk/moe_1777/moe_1778/201511/t20151127_221424.html.
- [3] National security presidential directive 54/homeland security presidential directive 23 (NSPD-54/HSPD-23)[EB/OL]. <https://epic.org/privacy/cybersecurity/EPIC-FOIA-NSPD54.pdf>.
- [4] The comprehensive national cybersecurity initiative[EB/OL]. <https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative>.

作者简介：



方滨兴（1960-），男，江西万年人，博士，哈尔滨工业大学教授，中国工程院院士，主要研究方向为网络安全、信息安全、并行处理、互联网技术等。