DOI:10.3969/j.issn.1009-6868.2016.01.003
网络出版地址:http://www.cnki.net/kcms/detail/34.1228.TN.20151204.1604.002.html

网络空间安全体系及关键技术

Security Architecture and Key Techniques of Cyberspace

张应辉/ ZHANG Yinghui[1]
郑东/ ZHENG Dong[1]
马春光/ MA Chunguang[2]
(1. 西安邮电大学 通信与信息工程学院,陕西 西安 710121;
2. 哈尔滨工程大学 计算机学院,黑龙江 哈尔滨 150001)
(1. School of Telecommunication and Information Engineering, Xi'an University of Posts and Telecommunications, Xi'an 710121, China;
2. College of Computer Science, Harbin Engineering University, Harbin 150001, China)

中图分类号:TN929.5 文献标志码:A 文章编号:1009-6868 (2016) 01-0010-004

摘要: 提出一种新型立体式网络空间安全体系结构,新结构有助于实现立体式网络空间安全防御体系,克服了传统线性防御体系只能应对单一性安全威胁的缺点。在新的体系结构中,网络空间中的节点分布于所有层次之中,且每一层的活动支撑着其他层的活动,并对整个网络空间产生影响。此外,针对所提出的立体式网络空间安全体系结构,结合当前的热点应用,指出了立体式网络空间安全防御体系应采取的关键技术。

关键词: 网络空间;立体式安全体系;信息安全

Abstract: A novel three-dimensional security architecture of cyberspace is proposed. This architecture has contributed to the construction of the three-dimensional security defensive system of cyberspace, and it overcomes the disadvantage of tackling only unitary security threats in the traditional linear defense system. In the proposed architecture, each node is involved in all layers in cyberspace, and the events in a layer affect other layers and thus affect the whole cyberspace. In addition, considering the proposed three-dimensional security architecture, security techniques suitable for the three-dimensional security defensive system are pointed out. These techniques are based on the current hot applications in practice.

Key words: cyberspace; three-dimensional security architecture; information security

网络空间[1]一词最早出现在美国科幻小说中,在故事中主角将自己意识感知的世界称为网络空间。随着时代的发展,网络空间被赋予了很多新的含义。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、各种计算机系统及人与人之间相互影响的虚拟环境。

网络不仅是一个消息的载体和媒介,它还改变了我们周围的一切,并悄悄地改变着我们的思维[2]。从某种程度上讲,人们所处的环境,都被赋予了网络和信息的属性[3]。因此,我们可以认为网络空间安全[4]的核心是信息安全。如今,信息技术以及其工业应用迎来了前所未有的繁荣,信息安全问题也变得越来越突出。此外,科学与技术的发展给信息安全带来了新的挑战,利用量子[5]与DNA计算,许多现存的公钥加密系统变得不再安全,网络空间的安全问题变得越来越严峻。

收稿日期:2015-10-23
网络出版时间:2015-12-04

1 网络空间安全分析

在给出网络空间安全体系结构之前,我们首先对网络空间的安全性进行分析。

1.1 传统意义上的网络空间安全范畴

1.1.1 物理电子设备安全

物理电子设备是我们存放消息数据的载体,从这个意义上讲,对于其安全性的考虑,不仅包括硬件电子设备在硬件上的不被恶意损毁和盗取,也应包括用户存放于上面的数据不应被人为地通过物理手段窃取或者删除。如何保证存放数据的物理设备有一定的灾备能力,如何从毁坏的设备中恢复用户的数据等问题都非常重要。此外,旁路攻击[6]中利用电磁信号变化、电位变化等,通过统计学恢复加密数据明文的攻击手段也属于此范畴。

1.1.2 应用层与系统层安全

应用层与系统安全主要是指当用户的数据在计算机系统中储存的时候,系统和应用层是安全可靠的。这里的安全威胁主要来自于不可信系统,或者恶意应用软件。

1.1.3 网络安全

传统意义上的网络安全是如何保障网络互连互通安全。网络互连指的是将不同的网络通过连接设备连接形成一个巨大的网络,或者是为

了便于管理，将一个更大的网络划分为几个子网，而网络互通是指建立各个子系统共享资源的环境，网络互连比网络互通更易实现。为了实现网络互连，一般使用中继器、网桥、路由器等设备，而为了实现网络互通，必须考虑各个子系统之间数据交流协调同步问题，同时需要设置各个子系统之间硬件和软件的参数等。如何在网络空间上安全传播，不被恶意窃听和修改，便成了重中之重。网络传播过程的安全，也不仅仅指的是传播链路上的安全，还应包括提供网际传输链路的服务提供商在硬件和软件上，不被恶意攻击，链路可以畅通无阻。针对网络的常见攻击手段有拒绝服务攻击、中间人攻击等。

1.1.4 人员管理安全

网络管理人员是网络空间的一个至关重要的组成部分，管理人员依靠专业知识规划、监督、控制着网络资源的使用以及网络中的各种活动，从而使得网络的安全性能达到最优化。因此，从信息技术角度上解决网络安全问题的同时，我们必须加强对网络网络管理人员的监督以及管理。网络管理人员对网络安全的威胁不仅包括管理人员的监守自盗、擅权越权等非法操作，更包括安全意识薄弱、管理环节不健全等潜在威胁。所以我们要采取切实可行的措施，制订更加严格的管理制度，不断提高和加强网络管理人员的管理水平以及安全意识。

1.2 新形势下的网络空间安全范畴

近几年，随着智能移动终端的普及，人们的生活与网络联系更为密切。因此，除了4个传统意义上的安全考虑之外，新的形势下还有很多新的网络空间安全问题。这里所谓的新形势是指：在当代新技术不断涌现，各领域高度融合的前提下，网络空间安全所展现出来的新局面。新形势之所以新，是因为：

（1）所处层次的复杂化。如果不考虑人员层的管理安全，以往的安全问题出现的时候，所处层次往往比较单一，比如上述提到的XcodeGhost事件，就出现在编译环境和由该环境生成的代码中，属于应用层范畴。但是新形势下的网络空间安全往往是跨区域、跨层次的。

（2）表现形式的多元化。传统安全问题表现形式较为单一，比如个人隐私，在传统的思维模式里，用户可以根据自己意愿对所持有数据进行公开。但是在大数据时代，数据挖掘技术和机器学习学习技术能从用户已公开的数据中嗅探出用户不愿意公开的数据，隐私的表现形式已经不仅仅是自己不愿意公开的数据，更广泛地分布在已经公开的碎片数据中。

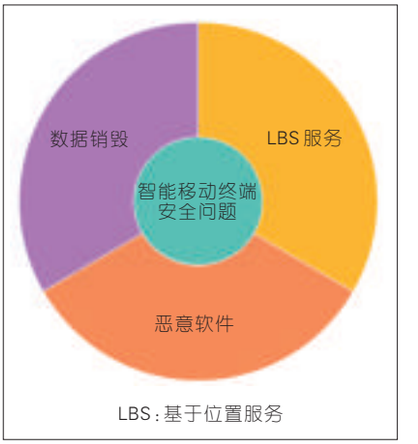
（3）涉及技术的多样化、新型化。比如下面提到的物联网技术，它涵盖了材料技术、生物技术、通信技术等，每个环节都有新的安全指标和挑战。很多技术在以往的安全关键技术中都是很少涉及的，比如材料技术。涉及到安全问题的一个典型例子就是最近逐渐兴起的可编程材料技术，工程师可根据需求对材料进行编程，改变材料结构。那么，我们可以断言，距离材料型病毒诞生的一天也不远了。

可以看出，新形势下的安全问题是对传统问题的延续与补充，传统问题所表达的安全基准在新形势下也同样适用。新形势下的安全问题很可能是若干传统安全问题的交集。下面我们就结合当下的热点应用，阐述新形势下的安全问题。

1.2.1 智能移动终端安全

近年来，手机等智能移动终端迅速发展，很多安全问题也随之暴漏出来，如图1所示，具体包括：

（1）恶意软件。智能终端的恶意软件和PC端的恶意软件具有同样的危害。从所属层次上来说，终端恶意软件仍然属于应用层和系统层层面，



▲图1 智能移动终端安全

但是由于移动终端的存储能力和计算能力有限，终端恶意软件多以后门、木马的形态存在。所以，终端恶意应用正逐渐向网络层过渡。

（2）基于位置服务[7]。基于位置服务是指通过运营商或者外部设备获取移动终端设备位置信息的服务。如何保证一个基于位置服务提供商是可信的，不会将用户的位置信息暴漏给其他第三方，是值得考虑的一个问题。基于位置的服务是网络层、应用层与物理设备层的相互交叉的产物。

（3）数据销毁。当更换手机或硬盘时，人们会把旧的设备格式化，以清除数据，避免信息泄露。数据销毁则是需要物理设备层、应用层与系统层协调工作。

1.2.2 可穿戴设备安全

近几年还有一些其他类型嵌入式系统和可穿戴设备的安全性也引起了人们的重视。常见的可穿戴设备是指那些具有部分计算能力，与智能移动设备相辅使用的便携式设备。这些设备多以手表、鞋子、帽子等形式存在，边缘化的还有一些服装、书包、配饰等。然而，在2015年的HackPWN安全极客狂欢节上，有白帽子黑客向组委会递交了一个小米手环的漏洞，通过该漏洞，黑客可以完全接管小米手环的控制权。要

想解决可穿戴设备安全问题，应该从物理设备层与系统层进行考虑。

1.2.3 云计算安全

云计算[8]在近几年受到了学术界、产业界和政府等的共同关注。云计算的安全主要包括：

（1）虚拟化安全。虚拟化技术在信息系统中发挥着极其重要的作用，它可以降低信息系统的操作代价、改进硬件资源的利用率和灵活性。但随着虚拟技术的广泛运用，其安全问题越来越受到人们的关注。

（2）云存储安全。云存储可以为用户提供海量的存储能力，而且可以减少成本投入。然而，由于对数据安全性的担忧，仍然有很多用户不愿意使用云存储服务。如何保证用户所存储数据的私密性，完整性等都是云存储安全的范畴。

1.2.4 物联网安全

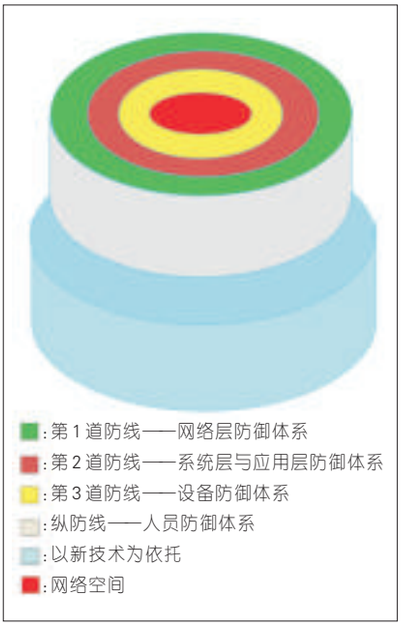
物联网[9]被视为继计算机、互联网和移动通信之后的第3次技术革命和信息产业浪潮，它广阔的行业前景和潜在的巨大市场规模受到了各国政府和研究者的极度重视。物联网涵盖了材料技术、生物技术、计算机技术、电子技术、通信技术，打破了行业之间的界限，实现了通信从人与人向人与物，甚至于物与物之间拓展。然而，也正因为如此，物联网的安全才更加具有挑战性。

1.2.5 量子计算机对传统密码学算法带来的挑战

随着科学的进步与发展，诞生了很多新兴的技术，如量子计算机技术。量子计算机的诞生，可能对传统意义上的密码学构成威胁，其特点是计算能力非比寻常，将在现有计算能力上实现指数增长。目前来说，量子计算机还处于萌芽期，不具备可操作性，而且实验性量子计算机也不足以对传统加密算法发起攻击，但是随着政府资金的大量投入，理论和实践活动的开展，实用性量子计算机或许随时都会诞生。传统密码算法[10-11]所依赖的大整数分解，椭圆曲线以及离散对数问题在大规模量子计算机面前，会变得不堪一击。

2 网络空间安全体系结构

随着中国在电子银行、电子商务和电子政务方面的进一步发展，网络空间安全形势也越来越严峻，急需构建新型网络空间安全防御体系，从传统线性防御体系向新型立体式网络空间防御体系发展。传统线性防御体系只能应对某一层内的单一性安全威胁，而新型网络空间防御体系必须能够实现立体化的安全防域，即该网络空间中的节点分布于所有域之中，网络空间中的所有活动支撑着其他域中的活动，并且其他域中的活动同样能够对网络空间产生影响。立体式网络空间安全体系如图2所示。



▲图2 立体式网络空间安全防御体系

2.1 第1道防线——网络层防御体系

网络防御层[12]是保证信息数据在网络传输过程中的坚固堡垒与屏障。防御模式不仅包括传统意义上的虚拟专用网络（VPN）、防火墙等。而且为了确保网络互连互通安全，需要加强对网络互连互通设备的安全设置，比如中继器、网桥、路由器等等。在新兴技术的支持下，网络层安全如虎添翼。服务器可以通过固化在用户终端的安全模块，对用户的网页浏览行为进行管控，确保用户所浏览的网页没有受到钓鱼网站的劫持冒用。同时，用户之间的会话在逻辑上是加密的，并且会话密钥的分享方式是安全可靠的。

2.2 第2道防线——系统层与应用层防御体系

系统层与应用层防御是针对于软件而言的，在系统最先开始编译的时候，就可以将一些安防软件、病毒检测软件内嵌到系统中，尤其是在软件开源的大趋势下，我们完全有能力将安防体系作为系统模块的一部分，固化在操作系统本身的结构中。面向的对象，包括一些底层是Linux嵌入式系统的可穿戴设备，以及拥有开源优势的安卓手机系统，都可以被这个防御思维有针对性地进行改造。在用户接入系统的时候，通过系统将对所有的用户进行约束与管控：通过在终端上部署防病毒客户端，有效控制病毒的感染与传播，依托于大数据云计算平台，进行终端和网络病毒查杀，以保证计算终端配置和软硬件信息不被恶意病毒修改。通过主机对终端硬件如磁盘、外接设备等的安全监控，可以实现移动存储介质的安全接入，控制终端用户对核心系统的读写等。

2.3 第3道防线——设备层防御体系

设备层防御体系是从硬件上构建的防御体系，从最底层打牢网络空间的基石。通过改良硬件的基础设施，在硬件最初被设计的时候，就将其安全功能考虑进去，必要时候可以在芯片中内嵌一些安全算法，布控一些安全防御设备，包括反窃听、反旁路攻击等。合理规划安排硬件安装

过程中的每一个环节，对硬件的操作进行软件上或者物理上的监控。确保在设备层面构成网络空间的第3道防线。

2.4 纵防线——人员防御体系

建设人员防御体系的核心是建设合理的人员管理体系。对人员的安防意识进行有针对性的强化，同时加强道德品质建设，对于具有专业能力的计算机从业人员进行正确疏导，避免误入歧途。加强法律的威慑力与约束能力，加强安防软件硬件的基础设施建设，加快落实实名制，在实名制的基础上引入生物特征识别机制，加大网络犯罪的犯罪成本。人员的管理穿插在防御体系的每一个环节中，因此非常值得关注。

3 网络空间安全关键技术

3.1 智能移动终端恶意代码检测技术

针对智能移动终端恶意代码而研制的新型恶意代码检测技术，是在原有PC机已有的恶意代码检测技术的基础上，结合智能移动终端自身的特点而引入的新技术。从检测方法上，可分为动态监测和静态检测。因为智能移动终端自身的计算能力有限，手机端恶意代码检测往往需要云查杀辅助进行。与手机数据销毁相对应，手机取证[13]也有着极为重要的应用。手机取证是打击犯罪的重要手段之一。在手机取证中，手机的SIM卡、内外存设备，以及手机所对应的服务提供商都是手机取证的重要环节。

3.2 可穿戴设备安全防护技术

3.2.1 生物特征识别技术

英特尔首席执行官的科在2014年的CES预热演讲中强调，英特尔将推出“Intel Security”品牌，用安全领军可穿戴设备。讲话中还提到，英特尔将把生物特征识别技术应用于可穿戴设备中。生物特征识别技术指的是用生物体本身的特征对一个人进行身份验证，这其中的一些技术，比如指纹识别技术，已经被用户们所熟知。除此之外，近年来又新兴了如步态识别、脸像识别、多模态识别技术的新一代生物特征识别技术。可穿戴设备可以对用户的身份进行验证，如果验证不通过将不予提供服务。

3.2.2 入侵检测与病毒防御工具

保证可穿戴设备安全的另一个重要思路就是在设备中引入入侵检测与病毒防护模块。由于可穿戴设备中本身的计算能力非常有限，所以，嵌入在可穿戴设备中的入侵检测或者病毒防护模块只能以数据收集为主，可穿戴设备通过网络或者蓝牙将自身关键节点的数据传递到主控终端上，再由主控终端分析出结果，或者通过主控终端进一步转递到云平台，最终反馈给可穿戴设备，实现对入侵行为或者病毒感染行为的发觉与制止。

3.3 云存储安全技术

3.3.1 云容灾技术

利用物理上隔离的两台设备以及一些特殊的算法，实现资源的异地分配。当有一台或者数台物理设备被意外损毁，用户仍然可以通过储存在其他设备上的冗余信息恢复出原数据。比较有代表性的就是基于Hadoop的云存储平台，其核心技术是分布式文件系统（HDFS）。在硬件上，云容灾技术不依赖具体的某一台物理设备，并且不受地理位置的限制，使用非常方便。未来应进一步考虑效率更高、更稳定的云容灾技术。

3.3.2 可搜索加密与数据完整性校验技术

用户可以通过关键字搜索云端的密文数据。新的可搜索加密技术应该关注关键词的保护，支持模糊搜索，即允许用户在搜索的时候输入错误，同时还要支持多关键词检索，并对服务器返回的结果进行有效性验证。此外，为了实现数据的完整性验证，使得用户并不需要去完全下载自己存储在云端的数据，而是基于服务器提供的证明数据和自己本地的小部分后台数据。未来新的完整性审计技术应该支持用户对数据的更新，同时保证数据的机密性。

3.3.3 基于属性的加密技术

基于属性的加密[14]是一种非常有吸引力的密码学原语，支持一对多加密模式。在基于属性的加密系统中，用户向属性中心提供属性列表信息或者访问结构，属性中心返回给用户私钥。数据拥有者选择属性列表或者访问结构对数据进行加密，把密文外包给云服务器进行存储。在基于属性的环境中，由于不同的用户可以拥有相同的属性信息，因此可以具有一样的解密能力，从而导致属性撤销和密钥滥用的追踪问题。未来基于属性的加密技术应同时考虑密钥滥用的追踪和属性撤销机制。

3.4 后量子密码

现代密码学是建立在计算复杂性理论基础之上的。然而，量子计算机的高度并行计算能力，可以将相应的困难问题化解为可求解问题。以量子计算复杂度为基础设计的密码系统必然具有抗量子计算的性质，从而有效地增强了现代密码体制的安全防护。未来量子密码的研究主要还应关注实用的量子秘钥分发协议。此外，编码密码技术也具有抵抗量子算法攻击的优点，是信息技术领域不可缺少的重要技术之一。未来的研究可以关注基于编码的加密技术、基于编码的数字签名技术等。

4 结束语

随着计算机网络技术的快速发

展，网络空间安全正面临着前所未有的发展机遇与挑战。通过分析传统线性结构防御体系以及传统的网络空间安全问题，结合当今严峻的新型网络空间安全威胁，我们提出一种新型立体式网络空间安全体系结构。新结构有助于实现立体式网络空间安全防域体系，并克服了传统线性防御体系只能应对单一性安全威胁的缺点。此外，我们还详细介绍了网络空间安全的基本范畴，并结合当前的热点应用，指出了立体式网络空间安全防御体系应采取的安全措施。

参考文献

[1] CLARK D D, WROCLAWSKI J, SOLLINS K R, et al. Tussle in Cyberspace: Defining Tomorrow's Internet [J]. IEEE/ACM Transactions on Networking, 2005, 13(3):462–475. doi: 10.1109/TNET.2005.850224

[2] 王晟, 虞红芳, 许都. 可信网络中安全、可控可管及可生存技术研究[J]. 中兴通讯技术, 2008, 14(1): 36–41

[3] NALEWAJSKI R F. Elements of Information Theory [J]. Perspectives in Electronic Structure Theory, 2011, 294(3–4): 371–395

[4] SCHWALM K T, SCHWALM K T. National Strategy to Secure Cyberspace [J]. Technical Report, AFRL–IF–RS–TR–2006–266, 2006, 1–27

[5] STEANE A M. How to Build a 300 bit, 1 Gop Quantum Computer [J]. Quantum Information & Computation, 2004, 7(3): 171–183

[6] 张阳, 陈开颜, 李雄伟,等. 基于差异度的密码芯片旁路攻击研究[J]. 通信学报, 2015, 3 (03): 100–105

[7] 唐科萍, 许方恒, 沈才樑. 基于位置服务的研究综述[J]. 计算机应用研究, 2012, 12(12): 4432–4436

[8] SINGH B, DHAWAN S, ARORA A, et al. A View of Cloud Computing[J]. Communications of the ACM, 2013, 53(4): 50–58

[9] 朱洪波, 杨龙祥, 于全. 物联网的技术思想与应用策略研究[J]. 通信学报, 2013, 5(5): 31–31

[10] ZHANG Y Q, WANG X Y. A Symmetric Image Encryption Algorithm Based on Mixed Linear–Nonlinear Coupled map Lattice [J]. Information Sciences, 2014, 273: 329–351

[11] 郑东, 赵庆兰, 张应辉. 密码学综述[J]. 西安邮电大学学报, 2013, 18(6): 1–10

[12] MANATHA G S, SHARMA S C. Network Layer Attacks and Defense Mechanisms in MANETS– A Survey [J]. International Journal of Computer Applications, 2010, 27 (1): 529–535

[13] ANDROULIDAKIS I. Mobile Phone Forensics [M]. Mobile Phone Security and Forensics. US: Springer, 2012: 75–99

[14] SHI Y, ZHENG Q, LIU J, et al. Directly

作者简介

张应辉，西安邮电大学通信与信息工程学院讲师、硕士生导师；主要研究方向为公钥密码学、云存储安全；目前主持国家自然科学基金；获得公开国家发明专利7项，其中授权2项，发表学术论文30余篇。

郑东，西安邮电大学通信与信息工程学院教授、博士生导师，西安邮电大学无线网络安全技术国家工程实验室主任；主要研究方向为基于编码的密码学、云存储安全；主持或参与了多项国家级研究课题，包括国家科技攻关项目、国家“863”计划项目等；出版学术专著2部，发表学术论文100余篇。

马春光，哈尔滨工程大学计算机学院教授、博士生导师；主要研究方向为信息安全与隐私保护、物联网等；主持完成了国家自然科学基金、教育部博士点基金等；获黑龙江省国防科技进步一等奖1项等，出版学术专著2部，发表学术论文60余篇。