

涌现视角下的网络空间安全挑战

屈蕾蕾 肖若瑾 石文昌 梁彬 秦波

(中国人民大学信息学院 北京 100872)

(llqu@ruc.edu.cn)

Cybersecurity Challenges from the Perspective of Emergence

Qu Leilei, Xiao Ruojin, Shi Wenchang, Liang Bin, and Qin Bo

(School of Information, Renmin University of China, Beijing 100872)

Abstract The security in the cyberspace undoubtedly belongs to emergent properties in nature. This kind of emergent properties brings about severe challenges to cybersecurity. A number of efforts of research on emergent phenomena related to the security in the cyberspace have been seen both home and abroad. Up till now, a lot of significant results have been achieved by this kind of research. However, people's knowledge of emergence in cybersecurity is still far from sufficient. For this situation, the challenges to cybersecurity are observed systemically from the perspective of emergence to promote the development of innovative ideas and theories in cybersecurity. At first, fundamental concepts of emergence in cybersecurity are revealed based on the original meaning of emergence in systems science. Secondly, challenges of emergent security to the cyberspace are explored with consideration to attacks, vulnerabilities, and defenses. Then, the state-of-the-art of research on the emergence of security in the cyberspace is analyzed in a way that it has been divided into three categories, which include descriptive research, directive research, and operational research. Finally, with the focus on fundamental theories, basic models, and practical tools, discussions are made to answer the question about how to further the study in the future in the field of emergent security in the cyberspace.

Key words cybersecurity; emergence; systems science; simulation; epidemiological models; systems theoretic based design

摘要 网络空间的安全性属于涌现属性,该属性给网络空间安全带来了严峻的挑战。国内外已有不少研究者关注网络空间安全的涌现现象,迄今已取得不少成果。然而,人们对网络空间安全涌现性的认识还非常不足。针对这一状况,从涌现性的视角对网络空间安全挑战进行全面考察,旨在促进网络空间安全新思想、新理论的发展。首先,从系统科学中的涌现性的本意出发,揭示网络空间安全涌现性的基本思想;其次,从攻击、漏洞和防御3个角度,考察网络空间中存在的涌现式安全挑战;然后,按描述性、指导性和操作性3种类型,分析网络空间安全涌现性研究的发展状况;最后,从基础理论、基本模型和实用工具3个方面,讨论开展未来工作的基本途径。

收稿日期:2019-06-11;修回日期:2019-09-03

基金项目:中国人民大学科学研究基金项目(中央高校基本科研业务费专项基金资助)(19XNH119)

This work was supported by the Fundamental Research Funds for the Central Universities, and the Research Funds of Renmin University of China (19XNH119).

通信作者:石文昌(wenchang@ruc.edu.cn)

关键词 网络空间安全;涌现性;系统科学;模拟;传染病模型;基于系统理论的设计

中图法分类号 TP309

涌现性(emergence)是网络空间安全所具有的天然属性^[1-3],换言之,网络空间的安全性是一种涌现属性.不正确认识和充分了解涌现属性就不可能妥善解决网络空间的安全问题^[4-5].

涌现现象在自然界和现实社会中随处可见.涌现性的通俗解释是整体大于部分之和.涌现属性的概念在生物学、物理学、经济学和社会学等领域都得到很好的应用.涌现现象在网络空间中也客观存在,随着物联网(Internet of things, IoT)等的发展,涌现现象的出现更加频繁和明显,使人们在网络空间中面临的挑战(包括安全挑战)变得更加严峻^[6-7].

若想获得对网络空间安全涌现性的认知,就需要尝试从涌现的角度考察网络空间安全问题.目前,对于复杂系统的涌现性,尽管仍然没有“完美”的解决方案^[1],但是研究人员已经提出了不少可以在一定程度上分析、控制乃至利用涌现性的理论和工具,比如用于复杂网络中病毒传播建模的传染病模型^[8]和基于系统理论的系统设计与分析模型^[9]等.这些模型和工具在分析和控制涌现现象方面有着很好的表现,在多个科学领域都得到了广泛的应用^[9-13].

认识网络空间安全的涌现性不仅有助于解决某些具体的安全问题,还有助于建立网络空间安全科学的理论基础.长久以来,由于网络空间甚至计算机系统的复杂性,人们很难做到对系统的威胁与漏洞有足够充分的了解.因此导致在攻防博弈中,防御者总是处于“建立系统→被攻破→打补丁→再次被攻破”的循环中(即所谓的cyber cycle),始终处于被动地位^[14].如何才能化被动为主动、从设计之初就建立“安全的”系统呢?不少研究者^[14-21]达成了一个基本共识,即建立网络空间安全科学(science of cybersecurity).他们认为,应当在科学方法的指导下开展网络空间安全研究,获取具有普适性的结论与思想,而不能总像从前那样“头痛医头,脚痛医脚”(即“ad hoc”办法)^[16-21].如果网络空间安全能够遵循科学的发展道路,那就有希望科学地分析和预测网络空间的行为,从而从根源上防止漏洞的产生和抵御攻击事件的破坏^[22].

那么,如何才能建立网络空间安全科学呢?引入和借鉴其他成熟的科学领域的理论和研究成果是一个很好的思路,得到了很多研究者^[1,14,17-23]的认可.备受关注的思想和方法有形式化方法^[17,20]、系统

科学方法^[1,18,23]和实验科学方法^[17,19-20]等.其中,蕴含在系统科学之中的复杂性理论表现得尤为突出.因为,借鉴复杂性理论在分析和解决系统复杂性问题方面的大量研究与成果,也许有助于在分析和解决网络安全的复杂性、设计“安全”的系统、打破cyber cycle等方面有所突破,从而为网络安全科学的建立奠定良好的基础^[14,23-24].

近些年来,网络空间安全领域已有不少研究人员^[1,18,22-30]意识到了复杂性理论特别是涌现理论对于网络空间安全研究的重要性,试图将一些复杂性科学领域已有的研究模型和工具引入安全领域.例如,将传染病模型应用于对恶意软件传播机制的研究^[31-37]、扩展工程安全(safety)模型以用于解决网络安全(security)的问题^[38-42],取得了一定的效果.这些工作揭示了开展网络空间安全涌现性相关研究的重要意义和良好前景.

然而,与复杂的网络空间和严峻的涌现式安全挑战相比,人们对网络空间安全涌现现象的认识仍然处于初级阶段,还需要更多的新思想、新理论去解决更多更复杂的网络空间安全涌现性问题.而且,已有的工作也大多局限于解决特定的涌现问题,未能就网络安全的涌现性及其相关问题研究给出系统化、体系化的诠释,尚缺乏复杂系统研究所需拥有的“全局观”.针对这种局面,本文从涌现现象的视角对网络空间安全挑战以及已有的应对方法进行系统化的研究和梳理,分析存在的不足,并提出未来的研究方向.

1 网络空间安全的涌现性

为研究网络空间的涌现式安全问题,必须了解涌现式安全性的基本思想,这个任务的完成应该从涌现性的本意及其发展状况入手.

1.1 网络空间安全涌现性研究

如果网络空间安全问题有规律可循,那么应对起来一定会更加得心应手.提及一般规律,自然会想起系统科学,因为,系统科学对自然界和现实社会中的一般现象以及事物发展的一般性规律进行研究,寻找最具普适性的规律.系统科学研究与很多其他科学领域的研究密切相关,例如,医学中的群体免疫^[43]、生物学中的种群进化^[44]、物理学中的统计力

学^[45]等。这些方面的研究既是系统科学理论的源泉也得益于系统科学理论的发展,尤其是其中的复杂性理论。相比之下,系统科学理论的作用在网络空间安全领域还没有得到充分发挥^[1]。但另一方面,网络空间是复杂的,具有复杂系统的很多特性,涌现性就是其中之一,复杂系统理论理应在网络空间中发挥更多的积极作用,特别是在应对棘手的安全问题方面。

网络空间是一个遍及全球的大型复杂系统,其中的安全涌现现象随处可见:从恶意软件传播到DDoS(distributed denial of service)攻击^[46-47],从跟踪网络的隐私获取能力到口令重用所带来的巨大危害。不难看出,涌现性这一特性给网络空间安全研究带来了巨大的影响和挑战。物联网、云计算、普适计算的发展给网络空间增添了大量的新型设备和新型交互方式,使得网络空间的复杂程度进一步提升。同时,大数据和人工智能技术的发展赋予了很多设备更强的学习和交互能力,使得设备的行为变得更加难以预料。以智能家居场景为例,在该场景中,用户家中装有大量可以获取隐私信息的物联网设备,尽管我们也许可以确保每个设备只获得它应当获得的信息(当然,这已很难做到),但是我们很难确保多个设备不会“串通”起来通过它们已有的信息分析出它们本不该获得的隐私信息。这样的行为就属于典型的涌现行为,在实际攻击发生之前,我们很难对其做出预测并提前部署防御措施,自然就更别提解决了。

现有的网络空间安全技术手段和解决方法大多集中关注单个节点的安全分析与防护,很少关注“交互”所带来的安全问题,就更别说系统化地研究安全问题了。当然,必须承认,这些方法的确很出色地解决了某些安全问题,比如说检测软件漏洞和防止病毒入侵,但是一旦遇到稍大规模的系统,这些方法就力不从心。进一步而言,面对当前日益严峻的网络空间安全态势,考虑到网络空间安全天然的复杂性,现有的安全解决方案在处理大规模系统安全问题和遏制漏洞利用及网络攻击事件方面显得十分乏力^[23]。

针对传统手段的不足,目前在网络空间安全领域已有一些研究者^[1,18,25-30,48]提出可以借鉴和引入以涌现为代表的复杂性科学研究思想,帮助解决传统安全方法无法解决的系统安全问题。早在20世纪90年代就有研究者^[49-50]意识到复杂网络的固有属性(小世界、无标度等)可能会对安全研究造成的影响;2010年之后,陆续有一些研究提出从涌现的角度研究跟踪网络、DDoS攻击、洋葱路由以及口令重

用现象^[1,28,51]等;在2015年以后,出现了一波利用系统化设计思路和方法尝试“控制”网络空间安全涌现现象(涌现威胁)的“热潮”^[13,29,33,37,52-53]。这些工作提出了进行网络空间安全涌现性研究的一些思路和方法,也展现了进一步研究的前景。但是,与网络空间中浩如烟海的涌现现象相比,这方面的研究还远远不足。总的来说,在网络空间安全领域,涌现现象及其相关的研究依然没有得到足够的重视。毕竟,借鉴以涌现性为突出特征的复杂性的研究思想和成果不仅可以帮助解决一些长久以来的疑难问题,还能够帮助建立网络空间安全科学。

许多研究者^[1,17-18,20,23,30]认为,引入以复杂性理论为代表的系统科学理论是建立网络空间安全科学的重要条件。以科学理论为支撑,有助于寻找解决安全问题的根本之道,“设计”出安全的系统,而不再总是处于攻防博弈中的被动地位^[14]。在复杂系统研究的众多方向之中,涌现性研究对于安全领域而言具有更为特别的意义。因为现有工作难以排除的漏洞和难以防御的攻击很大程度上就是从系统各个组件之间的复杂交互之中形成的涌现效应^[1]。从这一点上讲,我们认为,涌现性研究在网络空间的系统的整个生命周期^[54]中都具有极为显著的积极意义,有助于从系统生命周期的各个环节着手应对涌现式安全威胁的破坏。另外,已有工作^[27]也表明,在网络空间中,可以利用涌现特性进行安全防御,也就是说,可以为系统打造具有涌现效应的安全防御能力。

总而言之,无论是对学术研究还是对实际系统开发,研究网络空间安全中的涌现现象都有着十分重要的积极意义。为了能更好地帮助理解涌现现象研究的重要思想,下面结合涌现概念的形成与发展探讨在安全领域研究涌现现象的思路和方向。

1.2 涌现概念的形成与发展

若要对涌现属性有一个初步的认知,很有必要了解复杂系统。从字面意义上来看,“复杂系统”通常意味着一个比其他系统更难以描述和理解的系统,这种系统往往:1)含有大量组件;2)各组件之间存在大量复杂交互^[44,55-57]。上述2点确实是复杂系统的重要特征与必要条件,但是还不够充分。事实上,系统科学领域并没有就复杂系统的严格定义达成共识^[44]。然而,这也并不意味着我们对于辨别复杂系统束手无策,长久以来的相关研究总结了复杂系统的一些行为特征,可以作为复杂系统的判据。复杂性理论和非线性科学的先驱 Holland^[44]认为复杂系统具有4个典型的行为特征:

1) 自组织性(self-organization).在没有中心控制结构的情况下,系统会自主地形成一定的模式(pattern),比如鸟群和鱼群的形成.

2) 混沌行为(chaotic behavior).初始条件的微小改变会对系统的行为造成极大的改变,这就会使得人们很难以预料系统最终的走向,比如说多变的天气就是一个很典型的示例.

3) “肥尾”行为(“fat-tailed” behavior).一般意义上所认为的小概率事件的发生往往比我们预想的更为频繁,例如各种经济、政治、生态上的灾难性事件.

4) 适应性交互(adaptive interaction).复杂系统中的元素根据周围环境的改变对自身行为做出适应性改变,例如股市交易中的股民根据股价的变化买进或卖出.

虽然没有出现在复杂系统的上述行为特征列表上,但涌现性是复杂系统中最重要的特征之一.正如复杂系统本身的定义一样,涌现性也没有一个被广为接受的正式定义^[58],复杂性科学研究的不同阶段、不同方向对它有不同的解释.一部分研究者^[59]认为,涌现性实质上就是一种“整体大于部分之和”的过程和行为,即系统中各个组件之间的交互使得整个系统产生了不能靠组件的简单加总来得到的特征和行为.根据文献[60]的总结,涌现现象可归结为具有以下特征的微-宏观效应(micro-macro link)现象:系统局部组件之间的交互产生了新的系统全局行为,即由微观效应产生了新的宏观现象.而文献[61-62]则认为涌现性就是那些无法通过系统模型得出和理解的特征和行为.这些定义的出发点不同,理解的角度也不一样,但是却都可以归结到一个点:涌现性是一种全局的、系统的特征,是不能通过简单分析系统单个组件得到.

当然,本文无意参与涌现性定义的学术争论.考虑到各种定义之间也有共通之处,本文综合Simon^[59,63]和Holland^[44]的看法,即涌现性指的是:1)系统组件的交互使得系统产生了组件的简单加总所无法得到的行为;2)这种行为可以从复杂系统层级结构的角度加以解释,某一层级的聚合成为上一层级的涌现属性的“基础材料”.但是我们同样也发现,使用这种定义作为涌现性的判据还是存在过于粗粒度的问题,仍然需要一些更加细化的判据来判断系统的涌现现象.为此,从上述定义出发,我们采纳文献[27,60,64]等所提出的涌现现象判据,并将其总结为5条判据:

1) 可加性判据.系统的整体涌现特征不是其组件特征的简单加总.

2) 新奇性判据.系统整体涌现特征与其组件具有的特征属于完全不同的种类.

3) 可演绎性判据.无法根据系统单个组件的特征推导和预测出系统的整体涌现特征.

4) 系统出现宏观构型或已有宏观构型发生改变.

5) 当系统网络拓扑的度分布特征满足幂律分布时,认为系统达到自组织临界状态,此时涌现发生.

上述判据中的第5条判据与其他4条判据是有区别的,它涉及到涌现性的一个重要特征,即幂律分布.由此可见,涌现性的一些典型特征可以帮助我们判断涌现现象的发生.我们通过图1总结了涌现性的一些常见特征.为了更加直观地体现网络空间安全的涌现性,我们在图1中提供了这些特征在网络空间安全中的映射.

1.3 涌现性研究的现状与意义

通过1.2节对涌现性概念的分析,我们可以发现,涌现性往往意味着“出乎意料”,即系统产生了计划外的行为,超出了设计、开发、运行和维护人员的控制范围.这就体现了研究涌现性的意义所在,如果能透过现象看本质,了解产生涌现现象的背后机理,就有希望在问题发生时很快找到问题的来源,也能通过预测系统的行为预防问题的产生,还可以控制涌现现象发生的程度,甚至还有可能利用涌现性来“设计”出我们想要的涌现现象.

那么,如何着手研究本就非常复杂的涌现现象呢?文献[61]认为可以从定义、要素、应用和限制4个方面入手,并提供了一些研究指导.首先基于不同的反馈类型和因果关系对已有的涌现现象进行分类,这有助于了解涌现现象发生的背后机理.也可以从这些已有的现象中归纳出涌现性的一些要素,从而对在什么样的情况下会发生涌现现象有一个大致的了解.尽管很难拥有类似物理学中的微积分那样强有力的研究和预测工具,但还是可以基于已有的分类对涌现性进行一定程度的度量,还可以基于涌现性要素对系统将要出现的涌现行为做出大致的判断.这样,就可以试着通过微观、底层、组件的行为“设计”出宏观、高层、整体的涌现行为,也可以着力控制那些负面的涌现现象与行为.当然,涌现性的研究与应用也是有边界的,必须对涌现性研究与应用的适用场景与范围有足够的了解,才能确保在合适的场景使用合适的工具.下面对涌现性的应用作进一步介绍.

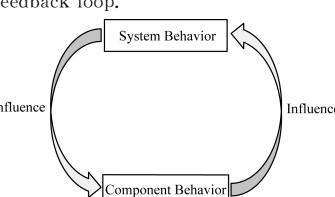
Characteristic	Interpretation	Examples in Daily Life	Examples in Cybersecurity
Power-law Distribution (also known as Scale-free Networks)	1) Mathematical treatment: The probability density function of variable x is $f(x)=\alpha x^{-r}$ ($\alpha > 0, r > 0$) 2) Another treatment: The scales of most individuals are small, and only a few individuals have enormous scales.	1) Zipf's law: In the natural language corpus, the number of occurrences of a word is inversely proportional to its ranking in the frequency table. 2) Matthew effect: The stronger is getting stronger, and the weaker is getting weaker.	1) Degree distribution: Only a few nodes have a high degree (these nodes are often called Hub), and others only have a small degree. The attacker only needs to focus on those Hub nodes to gain control of the network. 2) Preferential linking: Newly added network nodes will also be preferentially linked to those Hub nodes, making the importance of the Hub nodes even more enhanced.
Feedback Loop (also known as Micro-Macro Link)	Component behaviors affect system behaviors and are influenced by system behaviors, vice versa, which creates a feedback loop.		Stock market: The buying/selling behaviors of investors make a big difference in the stock price. But in reverse, the rise and fall of the stock price will significantly affect the decision-making behaviors of investors. Tor: On the one hand, since the anonymity that it provides depends significantly on the number of users, the user's decisions about whether to use can affect the degree of anonymity. On the other hand, the degree of anonymity also affects users' choices about whether to use it.
Nonlinearity	If we consider the system behavior we care about as a dependent variable $f(x)$, as the independent variable x changes, $f(x)$ must change rapidly in a nonlinear manner.	Biological virus propagation: As the number of infected people increases, the infection rate and range will grow increasingly, and the number of newly infected people per unit of time shows a typical non-linear growth characteristic.	Computer virus propagation: As for the Internet, because of the high connectivity and the nonexistent need for physical "contact" of network nodes, computer viruses spread much faster and more widely than biological viruses.
Distributed Control	Systems that exhibit typical emergent phenomena often do not have central control nodes. For them, control is often dispersed to a significant number of nodes (components), which means greater autonomy.	Biosphere: Obviously, there is no central control in the biosphere that controls the behavior of each organism so that each organism can act on its own.	Password system: As a typical human-centered computer system, there is no control in the password system for human users.

Fig. 1 The characteristics of emergence and typical examples

图1 涌现的特征及示例

涌现性的应用主要可分为设计和控制。“设计”通常意味着“设计我们想要的涌现现象”。在系统的设计过程中,系统组件(微观)的特征与行为是已知的,我们所要做的就是基于这些已知的微观要素来“设计”出我们想要的涌现现象。这个问题涉及到微-宏观效应(micro-macro link)问题,事实上,这个问题称得上是涌现性研究中最核心也是最困难的问题。尽管仍然没有确切的解决方案,但是研究者^[60-61,65]在思路和方向上基本达成了共识:结合自顶向下(top-down)的系统设计方法和自底向上(bottom-up)的仿真模拟实验方法,通过不断地进行循环迭代实验来达到最终的目的。在具体的施行过程中,研究和设计者应当始终坚持“全局观”,始终把想要获得的涌现现象作为系统设计的目标,通过分析这个目标找到相关联的系统组件,然后对这些组件的特征和行为进行设计和控制;紧接着进入仿真

模拟阶段,通过仿真模拟平台运行这个系统,检查系统的整体行为是否符合预期设计目标,如果不符的话,再对组件的行为进行修改,一直循环以上过程直到满足预期。

与“设计”相反的是,“控制”一般意味着“控制我们不想要的涌现现象”。而与“设计”类似的是,“控制”同样也很困难,因为涌现现象天生具有不可预测性。但是,尽管完全控制和预测是不可能的,但是仍然可以通过理论分析与仿真模拟对系统的涌现行为做出大致判断,至少可以判断会有什么程度、属于哪个分类的涌现现象,有利于提前部署相应的防护措施,控制危害的规模。以全球气候系统为例,我们无法精确地预测天气情况,但是至少可以做出大致的判断,这样也就能在台风来临之前告知公众尽快撤离。同样,可以在大规模计算机病毒蔓延之前告知用户尽快安装防病毒软件。

总而言之,尽管涌现性的作用不是万能的,它具有特定的适用性^[61],但是考虑到人类目前对于复杂世界的了解十分有限,涌现性研究仍然是深入了解和适应世界发展的强有力途径。

2 现实挑战

根据关键特征及其在安全研究中的意义,我们将涌现视角下的安全挑战分为3种类型:攻击、漏洞和防御。下面结合现实案例进行考察和分析。

2.1 攻击

涌现式攻击意味着攻击能力是一种涌现效应。也就是说,一个攻击系统的组件不具有这种攻击能力,但是当多个组件“协作”起来构成整体攻击系统

时,该系统就会产生出一种“不同寻常”、“意想不到”的攻击能力,其典型代表是DDoS攻击的破坏能力^[66-68]和病毒(恶意软件)^[34-35,69-72]的感染传播能力。

如果将发动DDoS的网络视为一个系统,那么网络中的单个设备就是构成系统的组件。在这样的系统中,单个设备所能产生的流量是极为有限的,甚至是微不足道的;可以造成大规模网络瘫痪的DDoS攻击能力是由大量设备的复杂通信和交互而产生的整体效应,即涌现效应(见图2所示)。事实上,即使我们对每个组件的所有软硬件都进行透彻的分析,也很难由此预料到攻击效果。尤其是随着通过社交网络等新型网络进行控制和通信的DDoS变种相继出现,实时处理和提前防御此类攻击变得更难以进行。

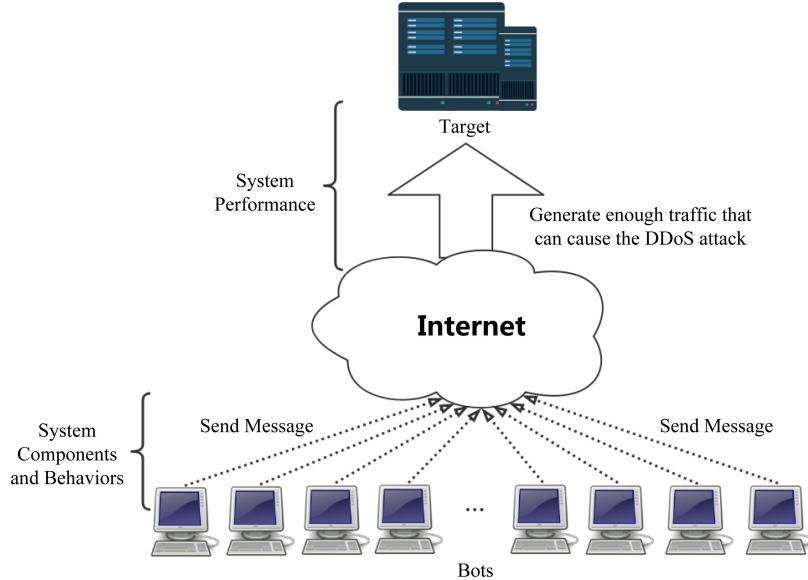


Fig. 2 Emergent DDoS attacking capabilities

图2 涌现式DDoS攻击能力

与DDoS的攻击能力相似的是,病毒(恶意软件)的感染传播能力也是一种典型的涌现现象。在这种场景下,组件是单个具有网络通信能力的设备(网络节点),而系统则是这些节点通过互联所构成的复杂网络。层出不穷的大规模病毒攻击事件告诉我们,由于互联网高度互联的特性,计算机病毒的传播速率远比我们想象得更快,影响范围也远比我们想象得广;而且,另一方面,这种特性也使得群体免疫这种常在公共卫生领域中被提及的概念很少出现在计算机病毒领域^[1]。另外,除了互联网之外,目前已有的研究表明,P2P(peer to peer)网络、移动电话网络等其他网络中的恶意软件也表现出类似的涌现性质^[69,72-73]。

作为复杂系统的典型代表,包括以上网络在内的复杂网络具有多种典型的非线性性质,因此,计算机病毒在网络上的传播动力学是难以用传统的线性模型来描述的。在实际场景中,这种涌现式感染传播能力给安全人员带来了极大的挑战:一方面,由于群体免疫的缺乏,很难通过在小部分节点上部署防御措施来达到控制病毒传播的目的;另一方面,与生物学或者医学中的“病毒”不同,大多数类型的计算机病毒在传播过程中无需节点之间实际“接触”,传播极为迅速,留给我们的反应时间十分短暂,甚至可以说没有。

从以上关于DDoS攻击和病毒传播的例子中我们可以看到,由于其天然的大规模、难检测、难控制

和难防御的特性,涌现式攻击的确是目前网络空间安全领域亟待解决的难题。

2.2 漏 洞

当我们谈及攻击时,一般指的是来自系统外部的恶意行为(这里我们不考虑可能由内部节点发动的内部攻击(insider attack)).但攻击的得逞一定有2方面的原因:1)攻击者的能力;2)被攻击系统的漏洞。如果系统本身没有漏洞,那么攻击也就无从谈起。而很多时候,我们害怕的不是漏洞,而是“意料之外”的漏洞,因为这常常意味着我们没有有效的应对措施。不幸的是,涌现式漏洞就属于这类漏洞中既难以预测又难以应对的。下面通过互联网、跟踪网络和口令系统中的3个例子来阐释涌现式漏洞给安全人员带来的严峻考验。

在20世纪90年代互联网刚刚兴起之时,就已经有大量的数学和物理学家^[45,49-50,74]对互联网的复杂网络特性进行了研究。根据他们的研究成果,最适合用来对互联网进行建模的模型远非被广为接受的随机模型。事实上,互联网不是“随机”形成的,也不是“公平”的,它体现出典型的无标度(scale-free)特性,这对安全的影响非常显著。无标度其实可以等同于幂律分布(power-law distribution),如图3所示。在无标度网络中,节点的度分布是非常不均匀的,只有极少数的hub节点拥有很高的度,绝大多数的点只有很小的度,而且新加入的节点也会以极大的概率优先连接到这些hub节点上。在某种意义上,占据网络节点数量极小一部分的hub节点却主导了整个网络的运行^[75-76]。这也就意味着,如果攻击者想要攻击整个网络,他不需要花费很大的代价,只需要集中力量攻击其中一小部分节点就可以。事实上,大量研究^[45,49]的确表明,复杂网络对节点的随机失效(failure)具有显著的健壮性,但在面对有目的性的

攻击(attack)时,却比我们预想的更加脆弱。在这一场景下,如果将设备节点看作组件,将互联网看作系统,那么由节点之间的通信与交互产生的涌现效应既可以出现在hub节点,也可以出现在包含hub节点的无标度网络结构,还可以出现在应对攻击的脆弱性中。

尽管也被称为“网络”,跟踪网络的涌现式漏洞却跟互联网有些不同之处。理想的跟踪网络应当对用户的意愿和隐私有足够的尊重和保护,即参与其中的用户(tracker)能够实现彼此的实时定位和跟踪,而不能够获得其他不在这一网络中的用户(non-tracker)的位置信息。但在实际运行过程中,前者是基本功能要求,而后者却难以实现。根据文献[51],在机会跟踪网络(opportunistic tracking networks)中,如果网络中有足够的设备节点(tracker)对非网络成员(non-tracker)的流量进行嗅探并将其位置报告给一个中央控制结构,那么这个中央控制机构就很有希望获知其他非网络成员(non-tracker)的位置信息。这种涌现效应产生自跟踪网络成员(tracker)之间复杂的通信和交互,也受到诸如所在区域的人口密度、城市规划以及跟踪网络规模大小等因素的影响。然而,尽管涌现式跟踪能力受到各种环境因素的制约,不是100%确定能够产生,但只要这一漏洞存在,就会对用户隐私造成极大的威胁。

上述2个例子都跟网络有关,但事实上,涌现式漏洞不仅存在于网络中,很多系统中都有它的身影,比如我们几乎每天都要接触的口令系统。长久以来,口令机制的安全性被大量安全人员所诟病,其中服务端漏洞的代表是口令数据库的脆弱性,而用户端漏洞的代表是口令重用现象的普遍性^[77-79]。下面从涌现的角度考察口令重用现象的出现和危害。

首先,为什么口令重用现象属于涌现现象?这就要从记忆口令的困难程度和人类记忆能力的限度开始说起。一方面,记忆口令的难度绝不是一个关于口令数量的线性函数,因为我们不仅要记忆口令本身,还要记忆口令和账户的搭配关系,后者显然是一个随着账户数量扩大而呈指数型爆炸增长的过程^[80]。另一方面,为了安全起见,我们总是建议用户设置足够“随机”和复杂的口令^[81],而事实上,普通人类记忆这类毫无关联的字符串的记忆能力是有限的^[59];而且,若要为每个账户设置不同的足够“强”的口令,那么随着账户数量增长而增长的口令数量又给用户带来了新的困扰,即记忆中的这些口令会互相干扰^[82-83](大多数人都有过在尝试登录不常用

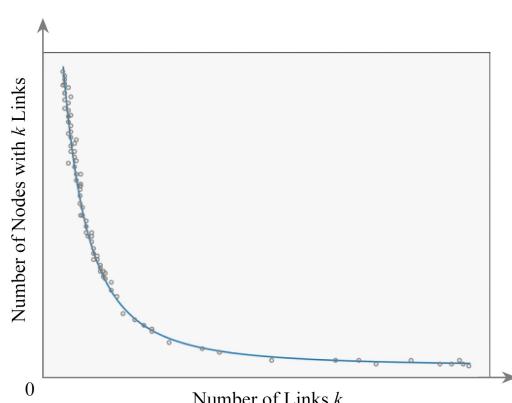


Fig. 3 Power-law distribution

图3 幂律分布

账户时不断试错的经历).面临着巨大的记忆挑战和自身有限的记忆能力,足够“智能”的人类想出了解决办法,即重用口令.在这种情况下,若把单个口令系统看作一个组件,那么所有的口令系统就可以被视为一个整体(系统),比较独特的一点是,这些组件的交互(相互干扰)是在人脑中进行的,口令重用现象就由这些交互产生的涌现现象.

其次,不仅口令重用属于涌现现象,它的危害也具有典型的涌现属性.当用户在多个口令系统中重用同一个口令时,这些系统间就产生了一种微妙的联系,即它们彼此依赖,总体的安全性变成了最弱的那个系统的安全性^[77,81],可以形式化地表达为

$$S_{\text{all-systems}} = \min\{S_{\text{system 1}}, S_{\text{system 2}}, \dots, S_{\text{system } n}\},$$

其中, S 代表系统的安全性.

一旦其中一个系统的用户口令数据被泄露,那么该用户在其他系统中的账户也危在旦夕.更糟糕的是,对于单个口令系统而言,攻击者甚至可以通过控制极少量的用户账户进而获得整个系统的控制权.举个最简单也最极端的例子,重用口令的用户恰好是某个系统的管理员,这个例子看似极端,实则并不罕见,系统的管理员常常做出一些匪夷所思的事情.总而言之,口令重用呈现出典型的“多米诺效应”和“蝴蝶效应”特点,即单个系统单个用户账户的泄露可能会导致一系列难以想象的后果,这种非线性性是涌现现象的典型表现.

总的来说,涌现式漏洞经常来源于系统的某些固有属性所带来的局限性,这种局限性在系统设计之初就隐含在系统的架构中,但是未能被设计者发现.令人遗憾的是,往往只有大规模攻击事件的发生才能让我们意识到漏洞的存在及其严重性.

2.3 防 御

近年来,随着涌现现象和网络空间安全 2 方面研究的逐渐深入,利用涌现特性部署安全防御措施

的研究受到关注,例如用于检测无线传感器网络中的节点复制(node replicas)的算法 Discard^[52]和基于 agent 的 DDoS 协同防御机制^[27].下面首先简要介绍 Discard 算法的相关内容.

无线传感器网络属于典型的自组织网络.由于设计目标和成本所限,该网络中节点的安全性很差,其节点之间通信所基于的协议非常简单,给攻击者留下了可乘之机.在无线传感器网络中,复制节点指的是攻击者通过某种手段获取某个设备节点的访问权,进而获取该节点的全部内容,这样,可以在另一台相似设备上复制该节点的全部内容并把该复制设备部署到原节点所处的网络中去,达到冒充身份、扩大控制范围的目的.为了更有效地检测复制节点,文献[52]提出可以利用复杂网络涌现现象研究中的经典模型——传染病模型.它把传染病模型很好地嵌入到网络节点的通信协议中,提出了 Discard 算法.在该算法中,单个节点是不具有“全局目标”的,它只会跟周围的节点“交流”自己所知道的信息,复制节点的识别能力是由大量节点之间的交互作用形成的涌现结果.

除了类似 Discard 这种从涌现的角度去设计的算法之外,安全领域其实还有很多传统的防御措施也具有涌现性质,只不过以前很少有人从涌现的角度去理解和认识它们.这类防御措施的典型例子有:洋葱路由的匿名性^[84-86]、自组织网络中的建立信任^[22,48,87]、安全多方计算^[58,88-93]、共识机制^[94-95]等.

在洋葱路由中,如图 4 所示,整个洋葱路由网络是一个整体,而单个通信节点则属于组件.当只有很少人使用洋葱路由时,其所能提供的匿名性是十分有限的.而随着使用人数的增多,网络节点之间交互的数量和复杂度呈非线性快速增长,洋葱路由所能提供的匿名性和它的优越性开始逐渐涌现^[1].

由于在自组织网络中不存在任何来自外部或者

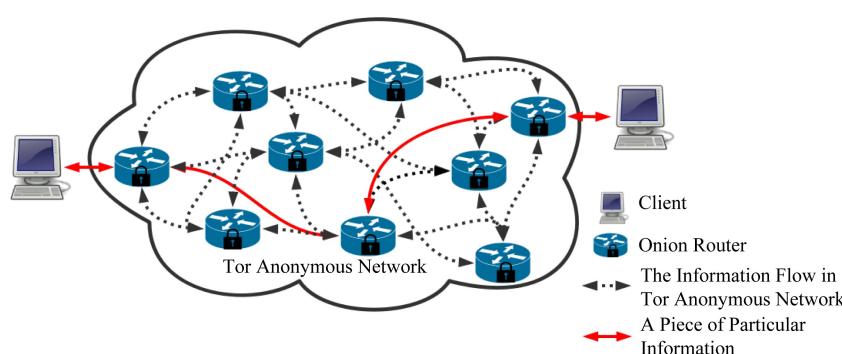


Fig. 4 Tor

图 4 洋葱路由

内部的控制,所以所有的网络节点都没有“全局目标”,它们只关心自己的状态以及与邻居的交互^[96].然而,正是这种没有“全局观”的简单交互与协作使得信任链和安全路由得以涌现,这也就是群智能(swarm intelligence)的一种体现^[48].从这个角度来说,安全多方计算和共识机制的涌现性也是如此——组件之间的简单交互使得安全状态得以涌现.在安全多方计算中,涌现作用是对数据机密性的保护;而在共识机制中,涌现结果是一致性共识.

上述涌现式防御机制极其有力地说明了将涌现性研究引入安全领域的意义所在:可以基于组件的交互“设计”出系统的整体安全性质,使得系统趋向我们想要的安全状态.当然,由于网络空间的复杂性,设计或者理解涌现式安全防御方案都具有相当大的挑战性.

3 应对方法

涌现性给网络空间安全带来的挑战并不意味着我们束手无策.目前已有不少出色的工作从涌现性的视角研究、分析以及应对网络空间安全问题出发,本节对较有代表性的工作进行总结和介绍.我们首先对这一领域的发展脉络进行梳理,然后根据研究的主题与内容分为描述性、指导性和操作性3类进行介绍.

3.1 发展历程

这一领域的研究可追溯到20世纪90年代.文献[97]给出了无边界系统(网络)(unbounded systems或unbounded networks)中生存性(survivability)的定义:在攻击、故障、事故等事件发生时,系统(网络)仍能及时完成目标和任务的能力.这是一种典型的整体属性,也是一种涌现属性,因为它无法由系统的组件呈现,也无法通过组件的性质推导得出.显然,这种属性跟安全联系十分密切,这类研究可以看作是网络空间安全涌现性研究的雏形.

进入21世纪,不断扩张并渗透人类生活的互联网引起了复杂网络研究者们的重视.起初的主流观点认为互联网是随机网络的代表,后来随着研究的逐渐深入,研究者们^[45,49-50,74]在其中发现了无标度(幂律分布)、层级结构、聚类效应等特性.这表明互联网实质上不是“随机”生成的,而是典型的复杂网络.而且,研究人员们^[45,49]也表示,以无标度为代表的上述复杂网络固有属性对于安全研究有重要的意义.

互联网的快速发展使得计算机病毒开始流行起来.受生物学、医学和公共卫生领域在生物病毒防治方面的经验启发,研究者们^[31-36]陆续将生物病毒传播中的传染病模型引入计算机病毒传播的研究中.相关的研究不仅仅局限于传统的互联网,实际上,由于人类个体的移动性所带来的影响,与节点位置基本固定的传统互联网相比,移动网络(比如蓝牙网络、移动电话网络等)中的病毒传播与生物病毒传播更为相似^[31-35].所以,这方面的研究非常关注移动网络中的病毒传播.

进入2010年以后,围绕网络空间安全涌现性的研究开始逐渐引起更多研究者的关注,越来越多的出色工作进入人们的视野,例如Husted等人^[28,35,51]、Leveson等人^[98-100]和Xu等人^[101-104]的工作.

Husted等人^[28,35,51]一直致力于探索由普适计算和物联网环境中大量设备之间的交互作用所形成的涌现式漏洞和攻击形式,跟踪网络中的涌现式用户隐私威胁和移动网络中的涌现式蠕虫病毒传播能力是他的主要关注点和切入点.他提出可以使用基于agent的仿真建模方法对机会跟踪网络的涌现式威胁进行研究,也可以使用传染病模型对移动网络中的蠕虫传播动力学进行一定的建模和分析,从而建立解决该类问题的基本思路.在文献[1]中,基于已有在跟踪网络和移动网络2方面的研究成果,他给出了网络空间安全涌现性的概念和意义,并结合该领域的实际情况讨论分析了一些具有代表性的涌现现象.特别重要的是,他还指出,基于agent的仿真模拟、传染病模型和基于系统理论的设计(systems theoretic based design)是网络空间安全涌现研究的有效途径.

传染病模型一般用于分析计算机病毒的传播动力学,有望帮助人们在病毒传播的早期及时部署有效的控制措施;基于agent的模拟常常可以帮助人们对系统进行测试,观察系统的涌现行为,根据模拟结果对组件进行适当的调整;相比于前2种途径主要关注“反应”和“调整”,基于系统理论的设计却有望让我们从系统设计之初就预防漏洞的产生.在基于系统理论的设计领域,典型的工具有STAMP(system-theoretic accident models and processes)和构建于其上的STPA(systems theoretic process analysis)^[98-99](在后文中,二者统一称为STAMP(STPA)).该工具是由美国麻省理工学院的Leveson等人^[98-100]设计的.该工具最初并不是为网络空间安全所准备的,而是用于解决工程安全问题,两者的区别在于前者

是 security 问题,而后者是 safety 问题.然而,由于大规模关键基础设施的数字化,安全(security)漏洞渐渐成为工程安全(safety)领域的新兴焦点.2007年,该团队中的 Laracy^[100]对 STAMP(STPA)进行了扩展,用以分析美国空中运输系统中可能出现的涌现式安全(security)威胁.2013 年文献[38]提出了 STPA-sec——一个用来识别和控制系统安全(security)漏洞的工具,这是一个里程碑式的事件.其后,除了该团队,越来越多的研究者致力于将以 STAMP(STPA)为代表的基于系统理论的设计思想引入网络安全领域,设计了诸如 STPA-SafeSec^[39] 和 STRIDE^[40] 等工具.

相比于 Husted 等人^[28,35,51] 和 Leveson 等人^[98-100]主要关注实验方法的运用,美国德克萨斯大学圣安东尼奥分校的 Xu 等人^[101-104]则侧重于通过

形式化的方法来进行网络安全动力学研究.2012 年他们研究了任意网络中 push-based 和 pull-based 这 2 种类型的计算机病毒的传播动力学^[101].2015 年他们提出了一种新的可能:当防御者使用类似于“white worms”的手段来“攻击”攻击者的时候(文中将其称为“active defenses”),网络空间的攻防博弈又会产生怎样的变化^[102].2018 年,他们的研究又深入了一步——当攻击者和防御者都采用了 2 种手段的时候(攻击:push-based 和 pull-based, 防御: preventive 和 reactive),根据他们的推导和证明,这种网络安全动力学场景在整个参数宇宙中都是稳定的^[103].

图 5 对上述发展历程进行了简要的总结和勾画.下面按照描述性、指导性、操作性的分类方法对相关研究进行更为全面和细致的介绍.

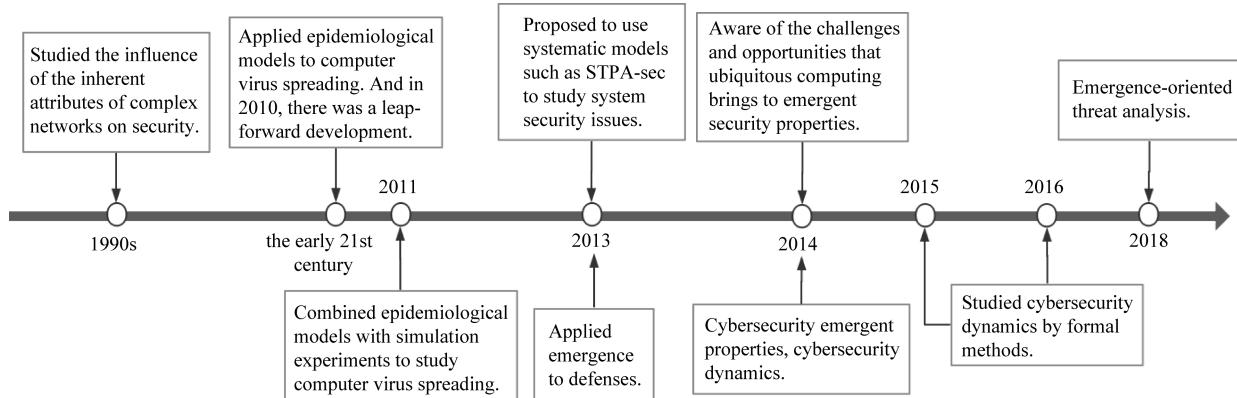


Fig. 5 History of the research on emergence in cybersecurity

图 5 网络空间安全涌现性研究发展历程

3.2 描述性的研究

我们把那些利用涌现理论来描述网络安全中的性质、行为和现象的研究称为描述性研究.这类研究往往不以提供明确的解决方法为目标,而是着眼于寻找崭新的思考问题的角度.下面从理论分析和形式化证明 2 个方面进行介绍.

3.2.1 理论分析

让我们按照“现象、定义、原理”的思路考察那些基于系统理论对网络安全涌现现象进行描述和分析的研究.

1) 现象

这类研究大多以举例和罗列的方式讨论典型的网络安全涌现现象,旨在寻找进一步研究的切入点,其中文献[1]的讨论较为全面,覆盖范围较广.根据文献[1],DDoS 的攻击能力、跟踪网络的隐私威胁、洋葱路由的匿名性、车联网系统对城市交通造

成的潜在威胁、弱口令和口令重用现象造成的安全威胁以及社交网络和比特币的价值都是网络安全中的涌现现象.另外,文献[58]简明扼要地讨论了网络安全动力学、扩展的 trace 属性框架(extended trace-property framework)以及密码学安全属性所蕴含的涌现性质.根据文献[26]的研究,作为复杂系统的典型示例,以信息物理系统(cyber-physical system, CPS)为组件构成的“系统的系统”CPSoS(cyber-physical systems-of-systems)能够明显地展示涌现性质,包括在死锁、分布式容错时钟同步(distributed fault-tolerant clock synchronization)、报警处理(alarm processing)等计算机系统经典问题中的体现.而文献[48]则将关注点放在自组织网络中,移动自组织网络中的信任、分布式传感器网络中的安全路由、动态联盟中的公共访问状态、移动自组织网络中基于群智能的安全路由等都是由网络节点间的交互作用

形成的涌现效应。

与上述综合性分析工作不同,文献[4, 28, 30-32, 105]主要关注某一个特定的涌现现象。根据文献[105],如果移动网络中的设备能够充分利用人类社交网络中的关系,那么,这些复杂的社交网络关系可以形成系统性能的涌现性效果。更具体地说,在容错网络中,能够提高路由协议的性能;就防火墙而言,可以有效地延缓病毒传播的速率。文献[28]主要关注2类涌现现象:机会跟踪网络中的隐私威胁和WiFi网络中的蠕虫传播能力。早在2006年文献[31]就探讨了蓝牙网络中蠕虫病毒的传播能力。随着智能手机的发展和流行,2014年文献[32]对已有的移动网络恶意软件传播模型进行了一次系统化的综述,可以为后续的研究提供一定的指导。文献[4]提出了更有概括性的观点:计算机集群安全(cluster security)是一种涌现属性。由于大规模、分布式和异质性的特点,计算机集群中存在着大量复杂交互,集群的安全属性无法通过对单个计算机的安全属性进行简单加总得到,这是涌现性的体现。

2) 定义

基于对网络空间安全领域大量涌现现象的观察和分析,文献[58]定义网络空间安全中的涌现行为:

“在网络空间中,如果一个系统拥有其低层组件所不具备的某种安全属性,那么,该安全属性蕴含着涌现行为。”

虽然这并不是国际上统一的正式定义,但它可以为进一步的研究提供借鉴。事实上,国际上也没有唯一的公认定义。每种定义都从某个角度揭示了网络空间安全涌现性的一定意义。

3) 原理

原理方面的研究工作侧重于通过模拟实验和数据分析等手段探究涌现现象的背后机理并找到一些重要的影响因素。

针对跟踪网络中的涌现式隐私威胁,文献[28, 51]采用仿真实验的方法对实际的跟踪网络环境进行了模拟,给出了该环境下实现有效跟踪的必要条件。特别地,他们可以根据这些条件量化跟踪网络中的涌现式隐私威胁。

文献[28]也在移动网络中的病毒传播动力学领域进行了探索——他们将传染病模型与仿真模拟实验相结合,发现了一些以病毒感染率为关键影响因素。文献[33]采用系统化、整体化的研究思路和方法对移动僵尸网络(mobile botnet)的进化过程和影响进行了研究。文献[34]则在探讨了设备和网

络的特征对移动网络病毒传播趋势造成的影响之后,提出了这类病毒利用上述特征进行迅速传播的原型系统,并基于该系统通过仿真模拟实验得出了病毒得以迅速传播的一些必要条件。

文献[36]的研究以真实数据为基础,通过对计算机病毒传播的真实数据进行分析,发现了互联网上计算机病毒传播的一般性规律——无论传染速率是多少,它都能在类似互联网这样的无标度网络上有效传播。

3.2.2 形式化证明

文献[101-104]采用形式化证明的方法对网络空间安全涌现性进行研究。它们首先采用形式化手段对某些特定的攻防情景进行严密的推导证明,继而得出一些推论,最后再通过仿真模拟实验的方式对这些推论进行检验。

文献[101]利用非线性动力系统方法研究了任意网络中2类不同病毒(push-based和pull-based)的传播动力学。当多种病毒同时在同一网络中传播时会出现怎样的情景,这些病毒甚至会互相攻击,试图夺取主动权。文献[104]对这一情景下的病毒传播动力学进行了研究。研究结果揭示了防御能力和网络连通性之间的关系,为部署防御措施提供了一定的指导。

文献[102-103]对攻防交互所造成的网络空间安全动力学场景进行了探讨。在文献[102]中,防御方被赋予了一种特殊的能力——可以利用“white worms”来达到对攻击者进行“攻击”的目的。理论推导和模拟实验结果表明,这种动力学场景表现出显著的发散和混沌特征,其涌现行为很难准确度量和预测。文献[103]的研究结果显得比较乐观,它主要探讨了2种攻击方式(push-based和pull-based)和2种防御方式(preventive和reactive)之间的攻防交互所形成的特殊网络安全动力学场景。研究结果表明,该场景在整个参数空间中都是稳定的、收敛的,而且在除了某种特殊情况的其他所有情况下都是指数收敛的(该特殊情况下是多项式收敛的)。

文献[106]基于形式化的方法证明了涌现属性的存在并分析了涌现属性是如何出现的,还提出了可用于帮助判断什么情况下会出现涌现属性的判断条件,给出了关于如何“设计”涌现属性的指导。

总的来说,基于严密的理论推导、数学证明以及精巧的仿真模拟实验,上述工作提供了很多非常具有参考意义的指导和建议。

3.3 指导性的研究

根据已有的观察和研究,可以就“网络空间安全涌现性研究应当如何进行”提出指导方案和建议,我们称这类工作为指导性研究。这类工作往往围绕以下6个核心问题展开探讨:研究目标和前景是什么;应当从哪些方面着手;遵循怎样的研究路线;应当引入哪些理论;可以利用哪些工具;进一步研究的困难与挑战是什么。下面沿着回答这些问题的思路对这类工作进行讨论。

文献[1-2]曾指出安全自身就是一种涌现属性。考虑到安全事件的难以预料性、安全环境的复杂性、敌手能力的难以预测性、人工科学的过于主观性等多种因素,对安全这一涌现属性进行度量显得格外困难^[30]。考虑到上述因素所带来的的复杂性,文献[5]认为涌现性质只有在一切部署完成后才会出现,且取决于具体实现方式,因此在设计阶段进行安全决策无法预测所有潜在的副作用,最好将网络空间安全视为一个社会实验来进行。文献[20]认为“难以度量”是阻碍网络空间安全成为一门科学的重要原因之一。目前,建立网络空间安全科学的必要性得到了越来越多的认可^[14-15,20-21],运用科学的方法分析和解决涌现式安全问题的意义日趋明显,这是传统的安全研究方法和手段难以胜任的^[22],必须寻求新的、足够智能的、有适应性的方法加以应对。

文献[15]认为可以从3个方面着手:基于不可信的部件建立可信的系统、建立更有“全局观”的入侵检测系统和DDoS防御系统、建立系统化的模型和设计框架等。文献[20]在“全局观”和系统化模型方面与文献[15]达成了共识,它认为可以在运用系统化思维的基础上考虑利用形式化的方法去解决“当多个部件组成一个系统时如何考虑系统的安全性”的问题。诚然,由组件交互所引起的涌现问题已经足够棘手,加上“人是系统的关键组成部分”,事情会变得更加麻烦。相对于机器,人的行为具有更大的不确定性,更加难以预测。如果为了避免麻烦,在设计系统时不把“人”这一关键组件纳入考虑范围,那该系统的设计显然难以充分反映现实情况,更不用说对未来的安全事件做出预测了^[22,30]。为了能够对包括人的因素在内的众多系统组件加强控制,确保系统正常运行,文献[14]提出可以将控制论引入安全研究,用于在设计系统时更好地限制系统的行为,以期从根源上预防安全漏洞的产生。另外,它也指出由于网络空间的复杂性和攻防双方天然的不对等,防御方始终处于“建立系统→被攻破→打补丁→再

次被攻破”的“cyber cycle”中,很有必要建立网络安全科学以打破这种格局。关于这一点,文献[18]认为网络安全的终极目标应该是实现一个面对不可预见的攻击仍然具有鲁棒性的防御系统,这样的系统可以随着环境的变化进行适应性的改变,还可以在遇到损害时进行自我修复;为实现这样的目标,很有必要让复杂性理论派上用场,复杂性科学有助于理解当今的网络空间及其与人类行为、社会规范和经济激励的联系,有助于建设更加安全的网络空间。

很多文献把同时含有计算机和人的系统称为“社会-技术系统”(social-technical system)。由于目前信息技术已经渗透到人类生活的方方面面,这种系统实质上属于网络空间的主流——毕竟系统设计出来就是给人类使用的,没有使用者的系统几乎不存在。而正如本节前文所述,难以预测的人类行为使得网络空间安全的复杂性进一步提升,为涌现现象提供了更多可能,给研究者带来了更多挑战。针对这一问题,包括文献[22,107]在内的多项研究提出应该拥抱系统化思维,应该借鉴复杂性理论的研究思路与方法。在这方面,文献[65]提供了很好的指引,它主要探讨了涌现性研究中的核心问题“微-宏观效应”的解决方案是否存在。基于对已有相关研究的归纳和总结,它提出了一套研究框架:1)定义系统目标;2)收集系统信息;3)自上而下地建立模型;4)计划仿真模拟实验;5)自下而上地进行仿真实验并收集数据;6)分析数据,然后得出结论。类似地,文献[108]提出了一套处理涌现问题的总体框架,文献[60]对多种面向涌现的系统设计方法和设计模式进行了比较分析,可以同文献[65]一起为涌现问题研究提供指导。

安全领域也已经有一些工作尝试提出研究网络空间安全涌现现象的研究路线与方案。比如,文献[4]针对计算机集群安全的涌现特性提出了一个关于如何部署防护技术的大致框架,该框架在很大程度上利用了已有的成熟技术,具有一定的参考价值。文献[109-110]的工作着眼于整个网络空间安全的动力学研究,其适用范围更广、与复杂性理论的联系也更为紧密。根据文献[109-110],安全性度量、网络空间第一性原理(first-principle)的建模与分析、数据分析、建立网络空间的系统化理论等研究都是开展网络空间安全动力学进一步研究的重要基础。

研究需要有工具支撑,文献[1]推荐了传染病模型、基于agent的仿真模拟、基于系统理论的设计

(systems theoretic based design) 三种工具。文献[32]对 3 种通用的传染病模型进行了对比。文献[22]认为基于 agent 的仿真模拟可用于对具有涌现行为的复杂系统进行建模, 可用于网络空间安全研究。文献[24]强调了系统化方法对于工程安全(safety)和网络空间安全(security)研究的重要性, 并对基于系统理论的实验工具 STAMP(STPA)及其在网络空间安全领域的衍生产品 STAMP-sec 和 STPA-sec 进行了介绍。文献[25]还对其他基于系统科学的研究工具进行了详细介绍。

必须看到, 尽管上述工作建立了一定的基础, 网络空间安全涌现现象研究依然困难重重, 比如, 如何在网络空间安全领域处理和解决系统的非线性性、组件之间的依赖性、系统行为的不确定性、人类因素的难以预测性等都是目前需要解决的难题^[110]。

3.4 操作性的研究

操作性的研究针对网络空间安全领域中的涌现问题设计实际可用的算法或工具。这些研究或者着力于分析、缓解、控制已有的涌现现象, 设计并实现分析工具; 或者探讨如何利用涌现特性实现检测攻击或者部署防御的目的, 设计检测或者防御算法。

3.4.1 分析和控制涌现现象

目前对网络空间安全涌现现象进行分析和控制的主流研究可大致分为 3 类: 1) 利用 STAMP(STPA) 进行系统化建模和分析; 2) 基于仿真模拟实验平台开展工作, 所用平台主要以多 agent 系统(multi-agent system, MAS)为主; 3) 主要包括面向涌现的威胁分析、保护架构、防御措施等。

1) 基于 STAMP(STPA)的研究

作为一种基于系统理论的系统设计工具, STAMP 事故分析模型(systems-theoretic accident model and processes)和以它为基础的 STPA 过程分析方法(systems-theoretic process analysis)最初用于解决工程安全问题^[9], 其中的安全(safety)主要指工程安全、人身安全、国家安全等。随着工控系统的逐渐信息化以及智能家居、无人驾驶、智慧城市等典型物联网系统的发展与流行, safety 与 security 的联系日趋紧密, 二者之间不再像过去那样泾渭分明——safety 会影响到 security, 比如节点劫持攻击; security 也会影响到 safety, 比如车联网的安全会影响乘车人的人身安全。由于 STAMP(STPA)在“设计安全的系统”方面的杰出表现, 越来越多的研究者致力于把它引入网络空间安全领域。

作为 STAMP(STPA)的开创者和设计者, Leveson 等人^[38]也意识到了这一研究方向的重要性。文献[38]提出了 STPA-sec, 它是 STPA 在网络空间安全(security)领域的扩展和应用, 它能够识别并且强制执行那些针对不安全控制措施的约束, 从而防止系统在面对外界干扰时受到攻击。作为 STPA 的后继者和衍生物, STPA-sec 的指导思想是:既然系统的设计者无法控制攻击者的行为, 不如将关注重心转移到控制漏洞的产生, 将所有安全问题的发生视为“控制的不足”, 它旨在为系统的设计师和分析者提供一个更加系统化的视角, 指导安全策略的设计。

STPA-sec 还催生了很多新的分析工具, 这些工具中的很大一部分是它的衍生物。文献[13]认为以前的 STPA 和 STPA-sec 都只关注损失, 没有关注隐私, 因此, 针对隐私领域特有的问题(比如开环控制), 它对 STPA-sec 进行了 2 方面的拓展:重新定义损失和获取隐私控制结构, 并实现了 STPA-Priv。考虑到已有的方案大多将 safety 和 security 问题分开处理而忽视了二者的联系, 文献[39]提出了 STPA-SafeSec, 将 safety 和 security 整合到一个框架里进行研究和分析。STPA-SafeSec 可以分析出由 safety 约束和 security 约束之间的依赖和交互所造成的问题与漏洞。文献[12]使用 STPA 对无人驾驶汽车进行安全性分析, 它能够在设计初期就发现涉及多个层面的问题, 从而防止安全隐患的产生。这些工作为如何在网络空间安全领域应用 STAMP(STPA)提供了一定的参考。

有些工具不是由 STAMP(STPA)衍生的, 但多少也受到了其设计思想的影响。针对信息物理系统(CPS)的特有安全问题, 文献[40]设计并实现了复杂系统分析工具 STRIDE, 它可用于 2 方面分析: 1) 单个系统组件可能涌现出什么类型的安全威胁; 2) 单个系统组件的一个漏洞如何使得整个系统的安全状态遭受威胁。着眼于与文献[39]类似的问题, 文献[41]提出了一种可以深度结合 safety 和 security 分析的技术模型 SAFE, 它可以清晰地记录系统的假设并且提高复杂软件驱动系统分析的可追踪性。文献[42]使用复杂系统安全性分析工具 CAST^[111]对遭受震网病毒攻击的核能源基础设施进行了安全威胁分析。实验结果表明, CAST 能够在系统设计阶段识别出针对特定 CPS 的安全威胁, 从而可以向 CPS 设计人员提供可用于提升 CPS 安全性的实用建议。

2) 基于仿真模拟实验平台的研究

作为研究涌现现象的重要工具,多 agent 系统(MAS)在诸多领域得到了广泛应用,也引起了网络空间安全领域的关注。

值得注意的是,很多时候研究者们会将传染病模型和多 agent 系统一同使用以对计算机病毒的传播动力学进行研究。一方面,使用传染病模型进行建模;另一方面,使用多 agent 系统进行仿真模拟,从而检验模型的适用性,同时观察系统会在仿真过程中涌现出什么样的性质。文献[69]提出一个事件驱动模拟器来模拟现实的恶意软件传播环境。文献[112]提出一种描述蓝牙网络蠕虫病毒传播动力学的细粒度分析模型,并使用仿真模拟的手段来对该模型进行分析评测,结果发现该模型能够以很高的准确率预测出蓝牙网络蠕虫的传播动力学。文献[34]通过仿真模拟实验的手段得出了一些量化的数据支持:可以造成传染病模型式传播的恶意软件所需要的移动设备数量和其他相关条件。

基于多 agent 系统的仿真模拟实验也在防御 DDoS 攻击、模拟攻防博弈等领域得到了应用。文献[113]做了一次重要尝试,将一个原用于对关键基础设施系统部件失效进行建模分析的多 agent 系统用于网络空间安全仿真模拟。文献[114]设计了一个基于 agent 的社会-技术系统模型,它是一种对节点之间的相互依赖所造成的影响进行分析和评估的方法,使复杂系统的分析者能够看到各个 agent 之间的交互以及依赖关系,从而可以对未来可能会发生的系统行为做出一定的预测。非常有趣的是,文献[115]提出了一个用于模拟“捉迷藏”游戏的多 agent 仿真模拟平台 Medusa,其研究者认为网络空间安全攻防博弈就是一个典型的“捉迷藏”游戏,可以基于该平台从“捉迷藏”的角度观察和研究多 agent 网络空间场景中的个体行为和系统涌现行为。针对 DDoS 的典型涌现属性,文献[27]建立了基于 agent 的 DDoS 协同防御仿真框架,并以 DDoS 协同防御涌现行为为目标,采用基于 agent 的方法建立 DDoS 协同防御体系模型。也就是说,利用防御系统的涌现行为达到防御 DDoS 的目标。

3) 其他面向涌现的防御研究

除了 STAMP(STPA)和基于多 agent 的仿真模拟实验工具,很多研究者从其他角度入手提出了很多实用的研究工具,例如文献[29,53]的工作。

文献[53]将工控系统视为信息物理系统(CPS)的典型例子,尝试用系统化的方法为其解决安全问

题。它提出的解决方案是一个多层的网络空间安全保护架构,具有灵活的结构和弹性智能,能够为工控系统制定网络空间安全保护策略。

文献[29]将关注点放在更大、更复杂的系统上——由多个 CPS 组成的系统 CPSoS,它提出了一种“面向涌现”的系统设计方法,能够为 CPSoS 威胁分析提供支持,以发现 CPSoS 中的涌现式安全威胁。

针对安全多方计算^[93]、恶意软件传播^[72,116-117]、手机组件通信^[118]等的涌现现象和其他相关内容^[119-120],研究者们也对相应的解决方案进行了探讨。

3.4.2 利用涌现进行防御

网络空间安全涌现性研究已从分析和控制涌现现象向前迈进了一步,即利用涌现特性来进行网络空间安全防御:一方面检测攻击,一方面部署防御,如文献[52,97,121]的工作。

在攻击检测方面,文献[52,121]的工作是有益的尝试。在移动无线传感器网络中,节点劫持攻击(node-capture attack)是很多进一步攻击的重要基础。由于无线传感器网络设备数量庞大、性能低、安全性差、无人看管的特性,攻击者很容易对某个设备节点进行劫持。一旦劫持成功,就有可能对其内容进行任意篡改,从而进一步发动女巫攻击、自我推荐攻击、诽谤攻击等形式的攻击。文献[121]提出了一种利用移动无线传感器网络的涌现性来检测节点劫持攻击的算法。在该算法中,单个节点只跟自己有限数量(常数)的“邻居”进行交互,但是最终整个网络的所有节点都能够知道哪一些节点已经被劫持了。也许是因为无线传感器网络的独有特性给涌现性研究带来了更多的机会和可能,文献[52]也将研究的重心放在了无线传感器网络中,它要检测的是节点复制攻击(node replicas attack)。为了达到有效的检测目的,它将流行病模型应用到了检测算法中,提出了一种分布式的、随机化的用于检测群部署(group-deployed)无线传感器网络中节点复制攻击的算法 Discard。与文献[121]的方案相似,该方案也催生了涌现属性,即攻击检测能力。

文献[97]尝试利用涌现特性进行防御部署,它首先对无边界系统(网络)中的生存性(survivability)给出了定义:在攻击、故障、事故等事件发生时,系统(网络)仍能及时完成目标和任务的能力。为了保证整体属性能从组件的交互中涌现出来,它着力于将涌现算法引入到无边界系统(网络)中,并给出实现该算法的方法和步骤。这些方法和步骤基本覆盖了包括邻居交互、分布式信息、协议、环境在内的

所有要素以及包括设计策略、实际考量、性能边界在内的所有步骤,具有重要的参考价值。

总而言之,从已有的工作中可以看出:网络空间安全涌现性研究已经形成了一定的规模,取得了很多重要的成果,但是,总的来说仍然不是一个足够成熟的研究领域,还有很大的发展空间。

4 未来研究方向

纵观当前的发展状况,下面探讨今后应该如何进一步从涌现的视角研究网络空间安全问题,讨论从理论基础、基本模型和实用工具3个方面展开。

4.1 理论基础

首先,既然是研究系统的涌现问题,那就必须从系统出发,必须拥有系统化思维,学会从系统、整体的角度思考问题。文献[20]指出,必须拥有系统化思维,才有可能解决由多个部件组合起来并相互作用所产生的新的安全问题。系统化思维在很多领域都受到了重视^[122-123],比如文献[123]用系统化的思维和模型解决工作场所人身安全的问题,其中有关系统化思维和层级结构的思想具有很好的参考价值。

要想正确认识并有效运用系统化思维,很有必要了解系统科学理论的基本思想,涵盖复杂性理论的系统科学理论在工程^[124]、医学^[125]等多个领域得到了广泛的应用。文献[23]指出,传统的安全设计与分析手段在遏制漏洞利用和网络攻击事件发生的范围和频率方面已经显得十分乏力,而基于复杂性理论的新方法却在理解和解决网络安全问题的根本原因方面显得非常有潜力。文献[18]也认为,由于可帮助人们加深对技术、人类、社会之间的复杂交互的理解,复杂性理论有望为网络空间安全研究提供重要的理论支撑。文献[126]介绍了如何利用系统科学理论解决实际系统中的问题并给出了一些思路和工具。虽然没有特别针对网络空间安全中的问题,但是思路、方法和工具都是通用的,能够在一定程度上为研究者提供参考。

作为复杂系统中的一种重要表现形式,复杂网络也在网络空间中占有极为重要的一席之地,因为,无论是传统的互联网,还是新型的物联网或软件定义网络(soft-defined network, SDN),其形式都是网络,属于复杂网络。所以,通过了解复杂网络的理论和研究模型、工具,可以增进对复杂网络的理解和认识,可以知道自组织网络是如何形成和发展的^[127],

可以分析复杂网络的层级结构^[74],可以获知复杂网络可能会涌现出哪些性质^[45],可以了解互联网这类典型复杂网络的复杂性体现在哪里^[49],也可以知道该用什么样的理论和模型来对特定的网络进行研究和分析^[127]等。这样一来,就能够分析什么样的网络拓扑才是最“安全”的^[45],也有可能在计算机病毒传播早期通过在关键节点上部署防御措施以防止病毒进一步扩散。

当然,在计算机病毒传播这个典型的网络空间安全案例中,起关键作用的不只有网络拓扑和防御措施,最核心的内容应当是网络空间安全动力学,即什么样的攻防交互会导致网络空间状态产生什么样的变化。文献[50]介绍了一些有关复杂网络动力学的研究。基于上述研究,文献[109]给出了网络空间安全动力学的概念,此后,其作者利用形式化证明的方法开展了进一步研究^[101-104],取得了非常不错的成果。

值得一提的是,形式化方法对于网络空间安全理论研究(包括涌现性在内)的重要性也得到了文献[17,128]等的认同。

4.2 基本模型

文献[127]介绍了一系列用于研究复杂网络进化特征的模型,并讨论了如何基于这些模型进行仿真分析。这些模型主要有:随机网络模型、小世界模型、无标度模型以及具有优先链接(preferential linking)的非无标度模型等。

上述模型都是比较通用的复杂网络动力学模型,就网络空间安全研究而言,其优点是具有一定的普适性,其缺点是缺乏网络空间安全的针对性。应对这种局面,一方面,3.2.2节提供的很多基于攻防交互的网络空间安全动力学模型可作借鉴;另一方面,相比于上述模型,用于研究病毒(包括生物病毒和计算机病毒)传播动力学的传染病模型(比如文献[8]中的模型)的应用历史更久远、应用范围也更广阔。早在2001年,基于传染病模型,文献[36]就发现了计算机病毒的传播规律,即无论传播速率是多少,计算机病毒都能在类似互联网这样的无标度网络上有效传播。随后,随着移动网络的逐渐兴起和飞速发展,文献[34-35,72,112,116]等将传染病模型应用到移动网络的病毒(恶意软件)传播动力学研究中,并取得了很好的成效。值得一提的是,传染病模型实际上也只是一个统称,还可以进一步细分为很多针对特定问题的小模型,关于这些小模型的种类和特征,可以在文献[32,70]中找到更多的细节。

除了传染病模型之外,还有一些其他的模型也能够提供一定的参考和辅助。比如文献[129]提出了一种度量系统复杂性的模型。有了这样的度量模型,就可以发现系统的结构,也就能够对涌现现象进行一定程度的量化。

4.3 实用工具

在 3.4.1 节中,我们已展示了一些基于多 agent 仿真模拟实验平台和 STAMP(STPA)及其衍生物的研究工作。这些工作的成果无疑表明,将上述 2 类工具应用于网络空间安全涌现性的研究是很有潜能的。因此,本节对这 2 类工具作更进一步的介绍。

在所有的多 agent 仿真模拟实验平台中,Repast^[130] 和 NetLogo^[131] 是被使用较多的 2 种。使用 Repast 时,可以基于它所提供的库函数进行创建、运行、展示和收集数据等所有与基于 agent 的模拟实验相关的操作,还可以根据需要对 agent 的行为进行编程。NetLogo 也具有类似的功能,它是一种多 agent 的编程语言和模拟实验环境,能够用于对复杂系统进行仿真实验研究。比较独特的是,它是一套开源的工具。由于功能的相似性以及二者的各有所长,二者的使用量基本处于势均力敌的状态。除了上述这些工具之外,文献[115]所设计的“捉迷藏”仿真模拟实验平台 Medusa 也可以作为一个候选工具。

关于 STAMP(STPA)在网络空间安全领域的衍生物,受到较多关注的应当是由原团队设计实现的 STAMP-sec(STPA-sec)^[38]。它主要针对系统的控制环节,能够识别出其中会导致安全漏洞的控制,并对这些控制施加约束。此外,解决类似问题的工具还有 STRIDE^[40] 和 CAST^[111]。另外,考虑到尽管 STPA 应用广泛,覆盖了包括海军^[10]、港口安全^[11]、无人驾驶^[12]、隐私保护^[13] 等在内的多个领域,但如何使用 STPA 很大程度上仍然是一个“具体问题具体分析”(ad hoc)的过程,没有严格的程序规范来对该分析过程进行指导。针对这个问题,文献[132]提出了一个很好的解决方案:首先,定义了 STPA 的形式化结构,并设计实现了一种基于该结构的系统化执行 STPA 分析的工具;其次,设计实现了使用上述分析工具所产生的结果来生成系统和软件需求的工具。这 2 种工具可以指导研究者如何使用 STPA。另外,致力于分析工程安全(safety)和网络空间安全(security)之间的联系与交互所导致的问题的工具 SAFE 和 STPA-SafeSec 能够将系统硬件组件的状态同它们的安全影响联系起来,从而可以在

事故发生时帮助安全人员更快定位到问题来源,更有针对性地解决问题。

根据文献[1]的观点,STAMP(STPA)及其衍生物对系统控制能力的要求比较高,比较适合军事、政府、工业这类层级结构和控制结构都很明确的场景,而面对很多控制力较弱的商用场景就会稍显乏力(比如消费者的行为就是很难以控制的一个重要因素)。因此,在使用这类工具的时候,应当更加注意其适用性。另外,期待未来会出现更多针对商用场景的系统化分析工具。

5 结语

本文以提升对网络空间安全涌现性的认识和促进新思想、新理论的发展为目标,讨论了在网络空间安全领域研究涌现现象的意义,并回顾了涌现理论自身的含义与研究状况;借助若干典型案例,从涌现性的视角对网络空间安全所面临的挑战进行了全面考察;简要地梳理了网络空间安全涌现性研究的发展历程,并按照研究的主题和深度对其进行了系统化的分类和阐释;围绕着“可以采用哪些理论、模型和工具开展进一步的研究工作”这一主题,分析了目前工作的不足并尝试提出了未来的发展方向。

诚然,本文的工作仍然处于网络空间安全研究的初级阶段。但是,我们希望该项工作能够激发对涌现式安全思想的共鸣,能够唤起对网络空间安全涌现性的重视。我们也希望该项工作的成果有助于系统地认识网络空间涌现式安全问题研究的发展状况和未来趋势,为今后的进一步研究和问题的解决建立良好的基础。

参 考 文 献

- [1] Husted N, Myers S. Emergent properties & security: The complexity of security as a science [C] // Proc of the 5th New Security Paradigms Workshop. New York: ACM, 2014: 1–14
- [2] McGraw G. Software security [J]. IEEE Security & Privacy, 2004, 2(2): 80–83
- [3] Ross R, McEvilley M, Oren J. Systems security engineering: Considerations for a multidisciplinary approach in the engineering of trustworthy secure systems, (NIST SP)-800-160 [R]. Gaithersburg, MD: National Institute of Standards and Technology, 2018

- [4] Yurcik W, Koenig G A, Meng Xin, et al. Cluster security as a unique problem with emergent properties: Issues and techniques [C] //Proc of the 5th LCI Int Conf on Linux Clusters. Champaign, IL: National Center for Supercomputing Applications, 2004: 18–28
- [5] Pieters W, Hadžiosmanović D, Dechesne F. Cyber security as social experiment [C] //Proc of the 5th New Security Paradigms Workshop. New York: ACM, 2014: 15–24
- [6] Zhang Zhikai, Cho M C Y, Shieh S. Emerging security threats and countermeasures in IoT [C] //Proc of the 10th ACM Symp on Information, Computer and Communications Security. New York: ACM, 2015: 1–6
- [7] Conti M, Li Qianqian, Maragno A, et al. The dark side (-channel) of mobile devices: A survey on network traffic analysis [J]. Piscataway, NJ: IEEE Communications Surveys & Tutorials, 2018, 20(4): 2658–2713
- [8] Brauer F. Compartmental models in epidemiology [M] // Mathematical Epidemiology. Berlin: Springer, 2008: 19–79
- [9] Leveson N. Engineering a Safer World: Systems Thinking Applied to Safety [M]. Cambridge, MA: MIT Press, 2011
- [10] Rokseth B, Utne I B, Vinnem J E. Deriving verification objectives and scenarios for maritime systems using the systems-theoretic process analysis [J]. Reliability Engineering & System Safety, 2018, 169: 18–31
- [11] Williams A D. Beyond a series of security nets: Applying STAMP & STPA to port security [J]. Journal of Transportation Security, 2015, 8(3/4): 139–157
- [12] Abdulkhaleq A, Lammering D, Wagner S, et al. A systematic approach based on STPA for developing a dependable architecture for fully automated driving vehicles [J]. Procedia Engineering, 2017, 179: 41–51
- [13] Shapiro S S. Privacy risk analysis based on system control structures: Adapting system-theoretic process analysis for privacy engineering [C] //Proc of the 2nd IEEE Security and Privacy Workshops (SPW). Piscataway, NJ: IEEE, 2016: 17–24
- [14] Adams M D, Hitefield S D, Hoy B, et al. Application of cybernetics and control theory for a new paradigm in cybersecurity [J]. arXiv preprint arXiv:1311.0257, 2013
- [15] Saydjari O S. Cyber defense: Art to science [J]. Communications of the ACM, 2004, 47(3): 52–57
- [16] Longstaff T, Balenson D, Matties M. Barriers to science in security [C] //Proc of the 26th Annual Computer Security Applications Conf. New York: ACM, 2010: 127–129
- [17] Schneider F B. Blueprint for a science of cybersecurity [R]. New York: Cornell University, 2011
- [18] Forrest S. The complex science of cyber-defense [C/OL] // Proc of the Annual Meeting of the American Association for the Advancement of Science. Washington, DC: American Association for the Advancement of Science, 2015 [2019-06-10]. https://www.researchgate.net/publication/267908003_The_Complex_Science_of_Cyber-Defense
- [19] Maxion R A, Longstaff T A, McHugh J. Why is there no science in cyber science: A panel discussion at NSPW 2010 [C] //Proc of the 1st New Security Paradigms Workshop. New York: ACM, 2010: 1–6
- [20] Evans D. Workshop report [C] //Proc of the NSF/IARPA/NSA Workshop on the Science of Security. Charlottesville, VA: University of Virginia, 2008: 1–8
- [21] Herley C, Van Oorschot P C. Sok: Science, security and the elusive goal of security as a scientific pursuit [C] //Proc of the 2017 IEEE Symp on Security and Privacy (SP). Piscataway, NJ: IEEE, 2017: 99–120
- [22] Such J M, Criado N, Vercouter L, et al. Intelligent cybersecurity agents [J]. IEEE Intelligent Systems, 2016, 31(5): 3–7
- [23] Armstrong R, Mayo J, Siebenlist F. Complexity science challenges in cybersecurity, SAND2009—2007 [R]. Albuquerque, NM: SAND National Laboratories, 2009
- [24] Young W, Leveson N. Inside risks—an integrated approach to safety and security based on system theory: Applying a more powerful new safety methodology to security risks [J]. Communications of the ACM, 2014, 57(2): 232–242
- [25] Kriaa S, Pietre-Cambacedes L, Bouissou M, et al. A survey of approaches combining safety and security for industrial control systems [J]. Reliability Engineering & System Safety, 2015, 139: 156–178
- [26] Kopetz H, Bondavalli A, Brancati F, et al. Emergence in cyber-physical systems-of-systems (CPSosS) [M] //Cyber-Physical Systems of Systems. Berlin: Springer, 2016: 73–96
- [27] Chuai Yingcai. Research on agent-based simulation DDoS collaborative defense [D]. Zhengzhou: PLA Information University, 2013 (in Chinese)
崔迎才. 基于 Agent 的 DDoS 协同防御仿真研究[D]. 郑州: 中国人民解放军信息工程大学, 2013)
- [28] Husted N W. Analysis techniques for exploring emergent vulnerabilities and attacks on mobile devices [D]. Bloomington, IN: Indiana University, 2014
- [29] Ceccarelli A, Zoppi T, Vasenev A, et al. Threat analysis in systems-of-systems: An emergence-oriented approach [J]. ACM Transactions on Cyber-Physical Systems, 2018, 3(2): No.18
- [30] Pfleeger S, Cunningham R. Why measuring security is hard [J]. IEEE Security & Privacy, 2010, 8(4): 46–54
- [31] Su Jing, Chan K K W, Miklas A G, et al. A preliminary investigation of worm infections in a bluetooth environment [C] //Proc of the 4th ACM Workshop on Recurring Malcode. New York: ACM, 2006: 9–16
- [32] Peng Sancheng, Yu Shui, Yang Aiming. Smartphone malware and its propagation modeling: A survey [J]. IEEE Communications Surveys & Tutorials, 2014, 16(2): 925–941
- [33] Lu Zhuo, Wang Wenye, Wang Cliff. On the evolution and impact of mobile botnets in wireless networks [J]. IEEE Transactions on Mobile Computing, 2015, 15(9): 2304–2316

- [34] Szongott C, Henne B, Smith M. Evaluating the threat of epidemic mobile malware [C] //Proc of the 8th IEEE Int Conf on Wireless and Mobile Computing, Networking and Communications (WiMob). Piscataway, NJ: IEEE, 2012: 443–450
- [35] Husted N, Myers S. Why mobile-to-mobile wireless malware won't cause a storm [C/OL] //Proc of the 4th USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET). Berkeley, CA: USENIX Association, 2011 [2019-05-24]. <https://www.usenix.org/legacy/event/leet11/tech/slides/husted.pdf>
- [36] Pastor-Satorras R, Vespignani A. Epidemic spreading in scale-free networks [J]. Physical Review Letters, 2001, 86(14): 3200–3203
- [37] Lu Zhuo, Wang Wenye, Wang Cliff. How can botnets cause storms? Understanding the evolution and impact of mobile botnets [C] //Proc of the 33rd IEEE Conf on Computer Communications. Piscataway, NJ: IEEE, 2014: 1501–1509
- [38] Young W, Leveson N. Systems thinking for safety and security [C] //Proc of the 29th Annual Computer Security Applications Conf. New York: ACM, 2013: 1–8
- [39] Friedberg I, McLaughlin K, Smith P, et al. STPA-SafeSec: Safety and security analysis for cyber-physical systems [J]. Journal of Information Security and Applications, 2017, 34(2): 183–196
- [40] Khan R, McLaughlin K, Laverty D, et al. STRIDE-based threat modeling for cyber-physical systems [C] //Proc of the 6th IEEE PES Innovative Smart Grid Technologies Conf Europe (ISGT-Europe). Piscataway, NJ: IEEE, 2017: 1–6
- [41] Procter S, Vasserman E Y, Hatcliff J. SAFE and secure: Deeply integrating security in a new hazard analysis [C] // Proc of the 12th Int Conf on Availability, Reliability and Security. New York: ACM, 2017: No.66
- [42] Nourian A, Madnick S. A systems theoretic approach to the security threats in cyber physical systems applied to Stuxnet [J]. IEEE Transactions on Dependable and Secure Computing, 2015, 15(1): 2–13
- [43] Rothman K J, Greenland S, Lash T L. Modern Epidemiology [M]. Philadelphia, Pennsylvania: Wolters Kluwer Health, 2008
- [44] Holland J H. Complexity: A Very Short Introduction [M]. Oxford, UK: OXFORD Univeristy Press, 2014
- [45] Albert R, Barabasi A L. Statistical mechanics of complex networks [J]. Reviews of Modern Physics, 2002, 74(1): 47–97
- [46] Villeneuve N, dela Torre J, Sancho D. Asprox reborn [EB/OL]. Cupertino, CA: Trend Micro Incorporated, 2013 [2019-06-30]. <http://www.trendmicro.it/media/wp/asprox-reborn-whitepaper-en.pdf>
- [47] Akritidis P, Chin W Y, Vinh T L, et al. Proximity breeds danger: Emerging threats in metro-area wireless networks [C] //Proc of the 16th USENIX Security Symp. Berkeley, CA: USENIX Association, 2007: 323–338
- [48] Gligor V. Security of emergent properties in ad-hoc networks (transcript of discussion) [C] //Proc of the 12th Int Workshop on Security Protocols. Berlin: Springer, 2004: 256–266
- [49] Newman M E J. The structure and function of complex networks [J]. SIAM Review, 2003, 45(2): 167–256
- [50] Boccaletti S, Latora V, Moreno Y, et al. Complex networks: Structure and dynamics [J]. Physics Reports, 2006, 424(4/5): 175–308
- [51] Husted N, Myers S. Mobile location tracking in metro areas: Malnets and others [C] //Proc of the 17th ACM Conf on Computer and Communications Security. New York: ACM, 2010: 85–96
- [52] Shashidhar N, Kari C, Verma R. The efficacy of epidemic algorithms on detecting node replicas in wireless sensor networks [J]. Journal of Sensor and Actuator Networks, 2015, 4(4): 378–409
- [53] Huang Shuang, Zhou Chunjie, Yang Shuanghua, et al. Cyber-physical system security for networked industrial processes [J]. International Journal of Automation and Computing, 2015, 12(6): 567–578
- [54] Royce W W. Managing the development of large software systems: Concepts and techniques [C] //Proc of the 9th Int Conf on Software Engineering. Piscataway, NJ: IEEE, 1987: 328–338
- [55] Holland J H. Hidden Order: How Adaptation Builds Complexity [M]. Cambridge, MA: MIT Press, 1995
- [56] Mantel H. On the composition of secure systems [C] //Proc of 2002 IEEE Symp on Security and Privacy. Piscataway, NJ: IEEE, 2002: 88–101
- [57] Waldrop M M. Complexity: The Emerging Science at the Edge of Order and Chaos [M]. New York: Simon and Schuster, 1993
- [58] Xu Shouhuai. Emergent behavior in cybersecurity [J]. arXiv preprint arXiv:1502.05102, 2015
- [59] Simon H A. The Sciences of the Artificial [M]. 3rd ed. Cambridge, MA: MIT Press, 1996
- [60] Jin Shiyao, Huang Hongbing, Fan Gaojun. Emergence-oriented research on multi-agent systems and its state of arts [J]. Chinese Journal of Computers, 2008, 31(6): 881–895 (in Chinese)
(金士尧, 黄红兵, 范高俊. 面向涌现的多 Agent 系统研究及其进展[J]. 计算机学报, 2008, 31(6): 881–895)
- [61] Fromm J. Ten questions about emergence [J]. arXiv preprint nlin/0509049, 2005
- [62] Fromm J. Types and forms of emergence [J]. arXiv preprint nlin/0506028, 2005
- [63] Holland J H. Emergence: From Chaos to Order [M]. Oxford, UK: OXFORD University Press, 2000
- [64] Auyang S Y. Foundations of Complex-system Theories: In Economics, Evolutionary Biology, and Statistical Physics [M]. Cambridge, UK: Cambridge University Press, 1998

- [65] Fromm J. On engineering and emergence [J]. arXiv preprint nlin/0601002, 2006
- [66] Pras A, Sperotto A, Moura G C M, et al. Attacks by “anonymous” wikileaks proponents not anonymous, TR-CTIT-10-41 [R]. Enschede, Netherlands: Design and Analysis of Communication Systems Group (DACS), 2010
- [67] Koliaris C, Kambourakis G, Stavrou A, et al. DDoS in the IoT: Mirai and other botnets [J]. Computer, 2017, 50(7): 80–84
- [68] Douligeris C, Mitrokotsa A. DDoS attacks and defense mechanisms: Classification and state-of-the-art [J]. Computer Networks, 2004, 44(5): 643–666
- [69] Fleizach C, Liljenstam M, Johansson P, et al. Can you infect me now: Malware propagation in mobile phone networks [C] //Proc of the 5th ACM Workshop on Recurring Malcode. New York: ACM, 2007: 61–68
- [70] La Polla M, Martinelli F, Sgandurra D. A survey on security for mobile devices [J]. IEEE Communications Surveys & Tutorials, 2013, 15(1): 446–471
- [71] Zhang Zhikai, Cho M C Y, Wang Chiwei, et al. IoT security: Ongoing challenges and research opportunities [C] //Proc of the 7th IEEE Int Conf on Service-oriented Computing and Applications. Piscataway, NJ: IEEE, 2014: 230–234
- [72] Ramachandran K K, Sikdar B. Dynamics of malware spread in decentralized peer-to-peer networks [J]. IEEE Transactions on Dependable and Secure Computing, 2010, 8(4): 617–623
- [73] Shang Yilun, Luo Weiliang, Xu Shouhuai. L-hop percolation on networks with arbitrary degree distributions and its applications [J]. Physical Review E, 2011, 84(3): 031113
- [74] Ravasz E, Barabási A L. Hierarchical organization in complex networks [J]. Physical Review E, 2003, 67(2): 026112
- [75] Barabási A L, Albert R. Emergence of scaling in random networks [J]. Science, 1999, 286(5439): 509–512
- [76] Barabási AL, Bonabeau E. Scale-free networks [J]. Scientific American, 2003, 288(5): 60–69
- [77] Ives B, Walsh K R, Schneider H. The domino effect of password reuse [J]. Communications of the ACM, 2004, 47(4): 75–78
- [78] Das A, Bonneau J, Caesar M, et al. The tangled Web of password reuse [C] //Proc of the 21st Network and Distributed System Security (NDSS) Symp. Reston, VA: Internet Society, 2014: 23–26
- [79] Seitz T, Hartmann M, Pfab J, et al. Do differences in password policies prevent password reuse? [C] //Proc of the 37th CHI Conf Extended Abstracts on Human Factors in Computing Systems. New York: ACM, 2017: 2056–2063
- [80] Florêncio D, Herley C, Van Oorschot P C. Password portfolios and the finite-effort user: Sustainably managing large numbers of accounts [C] //Proc of the 23rd USENIX Security Symp. Berkeley, CA: USENIX Association, 2014: 575–590
- [81] Florêncio D, Herley C, Van Oorschot P C. Pushing on string: The don’t care region of password strength [J]. Communications of the ACM, 2016, 59(11): 66–74
- [82] Chiasson S, Forget A, Stobert E, et al. Multiple password interference in text passwords and click-based graphical passwords [C] //Proc of the 16th ACM Conf on Computer and Communications Security. New York: ACM, 2009: 500–511
- [83] Meng Weizhi, Li Wenjuan, Jiang Lijun, et al. On multiple password interference of touch screen patterns and text passwords [C] //Proc of the 36th CHI Conf on Human Factors in Computing Systems. New York: ACM, 2016: 4818–4822
- [84] Snader R, Borisov N. A tune-up for Tor: Improving security and performance in the Tor network [C] //Proc of the 15th Network and Distributed System Security (NDSS) Symp. Reston, VA: Internet Society, 2008: 127–136
- [85] Chen Zhouguo, Pu Shi, Zhu Shixiong. Traceback technology for anonymous network [J]. Journal of Computer Research and Development, 2012, 49(S2): 111–117 (in Chinese)
(陈周国, 蒲石, 祝世雄. 匿名网络追溯溯源综述[J]. 计算机研究与发展, 2012, 49(S2): 111–117)
- [86] Dingledine R, Mathewson N, Syverson P. Tor: The second-generation onion router [C/OL] //Proc of the 13th USENIX Security Symp. Berkeley, CA: USENIX Association, 2004 [2019-06-10]. https://www.usenix.org/legacy/events/sec04/tech/full_papers/dingledine/dingledine_html/
- [87] Popa R A, Blumberg A J, Balakrishnan H, et al. Privacy and accountability for location-based aggregate statistics [C] //Proc of the 18th ACM Conf on Computer and Communications Security. New York: ACM, 2011: 653–666
- [88] Cramer R, Ivan B D, Nielsen J B. Secure Multiparty Computation and Secret Sharing [M]. Cambridge, UK: Cambridge University Press, 2015
- [89] Zhong Hong, Huang Liusheng, Luo Yonglong. A multi-candidate electronic voting scheme based on secure sum protocol [J]. Journal of Computer Research and Development, 2006, 43(8): 1405–1410 (in Chinese)
(仲红, 黄刘生, 罗永龙. 基于安全多方求和的多候选人电子选举方案[J]. 计算机研究与发展, 2006, 43(8): 1405–1410)
- [90] Ben-Efraim A, Lindell Y, Omri E. Optimizing semi-honest secure multiparty computation for the Internet [C] //Proc of the 23rd ACM SIGSAC Conf on Computer & Communications Security. New York: ACM, 2016: 578–590
- [91] Goldreich O. Secure multi-party computation [R/OL]. Rehovot: Weizmann Institute of Science, 1998 [2019-06-10]. https://www.researchgate.net/profile/Oded_Goldreich/publication/2934115_Secure_Multi-Party_Computation
- [92] Du Wenliang, Atallah M J. Secure multi-party computation problems and their applications: A review and open problems [C] //Proc of the 9th Workshop on New Security Paradigms. New York: ACM, 2001: 13–22

- [93] Ben-David A, Nisan N, Pinkas B. FairplayMP: A system for secure multi-party computation [C] //Proc of the 15th ACM Conf on Computer and Communications Security. New York: ACM, 2008: 257-266
- [94] Nasreen M A, Ganesh A, Sunitha C. A study on Byzantine fault tolerance methods in distributed networks [J]. Procedia Computer Science, 2016, 87: 50-54
- [95] Baliga A. Understanding Blockchain Consensus Models [M]. Pune, Maharashtra, India: Persistent Systems, 2017
- [96] De Wolf T, Holvoet T. Emergence versus self-organisation: Different concepts but promising when combined [C] //Proc of the 3rd Int Workshop on Engineering Self-organising Applications. Berlin: Springer, 2004: 1-15
- [97] Fisher D A, Lipson H F. Emergent algorithms: A new method for enhancing survivability in unbounded systems [C/OL] //Proc of the 32nd Annual Hawaii Int Conf on Systems Sciences, 1999 [2019-06-10]: <https://ieeexplore.ieee.org/abstract/document/772824>
- [98] Laracy J R, Leveson N G. Apply STAMP to critical infrastructure protection [C] //Proc of the 7th IEEE Conf on Technologies for Homeland Security. Piscataway, NJ: IEEE, 2007: 215-220
- [99] Leveson N G. Safety analysis in early concept development and requirements generation [C] //Proc of the Annual INCOSE Int Symp. San Diego, CA: International Council on Systems Engineering, 2018: 441-455
- [100] Laracy J R. A systems-theoretic security model for large scale, complex systems applied to the US air transportation system [D]. Cambridge, MA: Massachusetts Institute of Technology, 2007
- [101] Xu Shouhuai, Lu Wenlian, Xu Li. Push-and pull-based epidemic spreading in networks: Thresholds and deeper insights [J]. ACM Transactions on Autonomous and Adaptive Systems, 2012, 7(3): No.32
- [102] Zheng Ren, Lu Wenlian, Xu Shouhuai. Active cyber defense dynamics exhibiting rich phenomena [C] //Proc of the 2nd Symp and Bootcamp on the Science of Security. New York: ACM, 2015: No.2
- [103] Zheng Ren, Lu Wenlian, Xu Shouhuai. Preventive and reactive cyber defense dynamics is globally stable [J]. IEEE Transactions on Network Science and Engineering, 2018, 5 (2): 156-170
- [104] Xu Shouhuai, Lu Wenlian, Zhan Zhenxin. A stochastic model of multivirus dynamics [J]. IEEE Transactions on Dependable and Secure Computing, 2011, 9(1): 30-45
- [105] Miklas A G, Gollu K K, Chan K K W, et al. Exploiting social interactions in mobile systems [C] //Proc of the 9th Int Conf on Ubiquitous Computing. Berlin: Springer, 2007: 409-428
- [106] Zakinthinos A, Lee E S. Composing secure systems that have emergent properties [C] //Proc of the 11th IEEE Computer Security Foundations Workshop. Piscataway, NJ: IEEE, 1998: 117-122
- [107] Davis M C, Challenger R, Jayewardene D N W, et al. Advancing socio-technical systems thinking: A call for bravery [J]. Applied Ergonomics, 2014, 45(2): 171-180
- [108] de Haan J. How emergence arises [J]. Ecological Complexity, 2006, 3(4): 293-301
- [109] Xu Shouhuai. Cybersecurity dynamics [J]. arXiv preprint arXiv:1502.05100, 2015
- [110] Xu Shouhuai. Cybersecurity dynamics: A foundation for the science of cyber security [M] //Proactive and Dynamic Network Defense. Berlin: Springer, 2018: 1-31
- [111] Leveson N G. CAST analysis of the shell Moerdijk accident [R/OL]. Cambridge, MA: MIT Press, 2016 [2019-06-10]. <http://sunnyday.mit.edu/shell-moerdijk-cast.pdf>
- [112] Yan Guanhua, Eidenbenz S. Modeling propagation dynamics of bluetooth worms (extended version) [J]. IEEE Transactions on Mobile Computing, 2009, 8(3): 353-368
- [113] Cunningham C, Roque A. Adapting an agent-based model of socio-technical systems to analyze security failures [C] // Proc of the 17th IEEE Int Symp on Technologies for Homeland Security. Piscataway, NJ: IEEE, 2017: No.18
- [114] Charitoudi K, Blyth A J C. An agent-based socio-technical approach to impact assessment for cyber defense [J]. Information Security Journal: A Global Perspective, 2014, 23(4/5/6): 125-136
- [115] Tandon A, Karlapalem K. Medusa: Towards simulating a multi-agent hide-and-seek game [C] //Proc of the 27th Int Joint Conf on Artificial Intelligence and the 23rd European Conf on Artificial Intelligence. San Diego, CA: International Joint Conferences on Artificial Intelligence, 2018: 5871 - 5873
- [116] Magkos E, Avlonitis M, Kotzanikolaou P, et al. Toward early warning against Internet worms based on critical-sized networks [J]. Security and Communication Networks, 2013, 6(1): 78-88
- [117] Morales J A, Al-Bataineh A, Xu Shouhuai, et al. Analyzing and exploiting network behaviors of malware [C] //Proc of the 2nd Int Conf on Security and Privacy in Communication Systems. Berlin: Springer, 2010: 20-34
- [118] Octeau D, McDaniel P, Jha S, et al. Effective inter-component communication mapping in Android: An essential step towards holistic security analysis [C] //Proc of the 22nd USENIX Security Symp. Berkeley, CA: USENIX Association, 2013: 543-558
- [119] Blyth A. Understanding security patterns for socio-technical systems via responsibility modelling [C] //Proc of the 8th IEEE Int Symp on Service Oriented System Engineering. Piscataway, NJ: IEEE, 2014: 417-421
- [120] Datta A, Franklin J, Garg D, et al. On adversary models and compositional security [J]. IEEE Security & Privacy, 2010, 9(3): 26-32

- [121] Conti M, Di Pietro R, Mancini L V, et al. Emergent properties: Detection of the node-capture attack in mobile wireless sensor networks [C] //Proc of the 1st ACM Conf on Wireless Network Security. New York: ACM, 2008: 214–219
- [122] Underwood P, Waterson P. Systemic accident analysis: Examining the gap between research and practice [J]. Accident Analysis & Prevention, 2013, 55: 154–164
- [123] Carayon P, Hancock P, Leveson N, et al. Advancing a sociotechnical systems approach to workplace safety—developing the conceptual framework [J]. Ergonomics, 2015, 58(4): 548–564
- [124] Leveson N G. Rasmussen's legacy: A paradigm change in engineering for safety [J]. Applied Ergonomics, 2017, 59: 581–591
- [125] Anderson B R. Improving health care by embracing systems theory [J]. The Journal of Thoracic and Cardiovascular Surgery, 2016, 152(2): 593–594
- [126] Sterman J D. System dynamics modeling: Tools for learning in a complex world [J]. California Management Review, 2001, 43(4): 8–25
- [127] Dorogovtsev S N, Mendes J F F. Evolution of networks [J]. Advances in Physics, 2002, 51(4): 1079–1187
- [128] Cucker F, Smale S. On the mathematics of emergence [J]. Japanese Journal of Mathematics, 2007, 2(1): 197–227
- [129] Crutchfield J P. The calculi of emergence: Computation, dynamics and induction [J]. Physica D: Nonlinear Phenomena, 1994, 75(1/2/3): 11–54
- [130] Collier N. Repast: An extensible framework for agent simulation [J]. Natural Resources and Environmental Issues, 2001, 8: 17–21
- [131] Tisue S, Wilensky U. NetLogo: A simple environment for modeling complexity [C] //Proc of the 5th Int Conf on Complex Systems. Trieste, Italy: The World Academy of Sciences, 2004: 16–21

- [132] Thomas IV J P. Extending and automating a systems-theoretic hazard analysis for requirements generation and analysis [D]. Cambridge, MA: Massachusetts Institute of Technology, 2013



Qu Leilei, born in 1995. PhD candidate. Student member of CCF. Her main research interests include system security, science of cybersecurity, and human factors in cybersecurity.



Xiao Ruojin, born in 1998. Undergraduate. Her main research interests include system security and science of cybersecurity.



Shi Wenchang, born in 1964. PhD, professor, PhD supervisor. Distinguished member of CCF. His main research interests include cybersecurity, trusted computing, cloud computing, and operating systems.



Liang Bin, born in 1973. PhD, professor, PhD supervisor. His main research interests include program analysis, vulnerability detection, and Web security.



Qin Bo, born in 1977. PhD, associate professor, master supervisor. Her main research interests include pairing-based cryptography, data security and privacy, and VANET security.