网络空间安全初调研

刘迅

摘要：网络空间安全是一个相当广泛的领域，包含了传统意义上的信息安全，以及今年来兴起的、依托于网络的多种新技术方面的安全。作为网络空间安全专业的学生，在进入专业方向学习之前，对所学专业全貌有一个了解是十分必要的。本文结合网络空间安全领域两篇综述和作者本人的了解，从典型事件与学科优势两方面对网络空间安全领域进行了初步调研和总结。

引言：伴随着移动互联网在近十数年间的蓬勃发展，人类社会在机械化、电气化的阶段后，进入了信息化阶段。和之前任何一次工业革命不同，信息化革命彻底改造了人类社会的方方面面，信息技术全面渗透进人们的日常生活中。以手机为例，手机对于现代人俨然可以说是一种“体外器官”，离开了手机，等于告别了社交媒体、移动支付、健康码查验，在现代社会中近乎寸步难行。除了手机这一常见的技术产品以外，互联网、电信网、计算机系统、嵌入式处理器和控制器系统等机、物与人相互作用，构成了网络空间。对于这样一种庞大且深入我们生活的技术结构，其中的安全性是尤要着重考虑的。毕竟，我们在网络空间这一结构上倾注了太多。

1 领域典型事件

安全性的概念并不是孤立的，而是依托于其反面“不安全”。从行为上讲，也就是在“攻”与“防”的动态互动中，才能得到所谓“安全性”。

本节将选取网络空间安全领域的部分典型事件进行探讨，着眼于“攻”与“防”的对立双方。

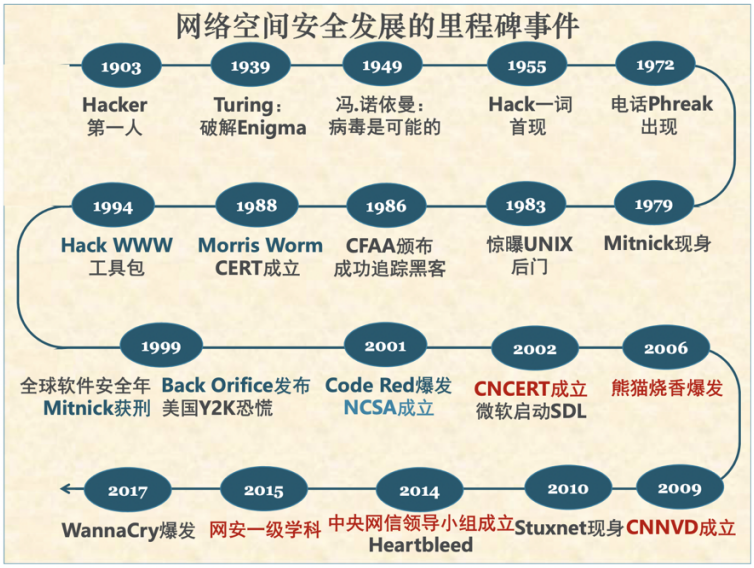

图 1：网络空间安全发展的里程碑事件　来源/邹维老师课件

1.1 WannaCry 勒索病毒

- 时间：2017 年 5 月 12 日

WannaCry 勒索病毒，是一种利用了 NSA 开发的永恒之蓝(EternalBlue)漏洞进行攻击的蠕虫。无论是勒索还是蠕虫病毒，它们都并不罕见，但在 WannaCry 之前的很长一段时间，勒索病毒只是零星出现。而借助永恒之蓝漏洞，WannaCry 实现了全球范围内的大规模感染、掀起了一场蠕虫风暴，对个人信息、经济生产乃至国家安全都造成了巨大挑战。

WannaCry“成功”的另一大因素，是因为它使用比特币作为赎金。在此之前，勒索者往往要费尽心思避免资金来源被警方追查。而通过比特币交易，勒索者几乎规避了赎金被追查的风险。

从“防”的角度看，WannaCry 事件犹如温水煮青蛙的过程中加入一瓢开水。WannaCry 一方面带来了全球的重大信息损失和财产损失，但另一方面同样让人们从美梦中惊醒，促使人们关注勒索软件等一系列网络安全问题。这也是付出沉重代价后所拥有的一些教训。

1.2 node-ipc 包供应链投毒

- 时间：2022 年 3 月 15 日

node-ipc 包是一个知名开发工具的依赖项，发布于 GitHub 网站，每周有百万下载量。俄乌战争期间，node-ipc 包作者以反战为名，借 node-ipc 包向俄罗斯和白俄罗斯的用户发起攻击。为了掩人耳目，源代码经过混淆，其行为是首先检测用户的 IP 段，如果检测为俄罗斯或白俄罗斯，则试图覆盖代码当前目录、子目录和父目录的所有文件。或许是包作者意识到他的行为已经严重违法，在随后的更新中，他去掉了文件覆盖的代码，转而在桌面上生成一个名为“WITH-LOVE-FROM-AMERICA”的“反战宣言”。

这起事件相当恶劣，对开源生态的信任根基有很大的负面影响。开源软件有大大小小一众依赖项，使用者完全不可能实时、全面地对所有代码进行审核，生态完全是建立在对其他开发者的信任上。而在众多依赖项构成的开源供应链上，如果有一个作者——无论是出于主观恶意还是政治动机——进行投毒攻击，对用户造成的影响都是不可估量的。

不过笔者在与学业导师包云岗老师交流后，对于这起事件的思考更深了一层。从表面上看，这起供应链投毒只有“攻”的一面，但事实上，投毒这件事情能被大众知晓，其中就蕴含了“防”的因素。

这起事件影响恶劣，主要源自于两个方面：首先，它在用户不知情的情况下覆盖用户的所有信息，是纯粹的破坏行为，这是恶劣的根本；其次，由于开源代码面向世界，所有开发者都可以对源码进行检查，因而这起破坏行为很快就被发现并公之于众，进而造成恶劣的社会影响。反过来想，如果这起投毒发生在闭源项目中，那么问题暴露的周期将会变得更长。在后一种情况下，没有造成恶劣影

响并非因为事件本身不恶劣，而仅是因为问题没有被暴露出来。从这个角度看，node-ipc 包投毒事件正是攻与防双方作用的结果。

1.3 随申码用户数据疑似泄露

- 时间：2022 年 8 月

网络流传截图显示，有人在网络上兜售“4850 万用户上海随申码”信息。

对此，上海市大数据中心回复

“数据不是我们泄露的”。

1.4 相关法律条例

网络空间安全作为一个不断更新的领域，立法实践是需要建立在一定的攻防基础上的，因此相对于攻防实践，免不了有时间上的延迟。面对移动互联网大幅普及的新环境出现的新问题，从 2016 年起，各国的相关法规条例陆续出台。有些是在原有条例基础上的更新，有些是对应新问题而制定的新法。

网络安全法，中国 2016 年 11 月 7 日颁布，自 2017 年 6 月 1 日施行。

数据安全法，中国 2021 年 6 月 10 日颁布，自 2021 年 9 月 1 日起施行。

个人信息保护法，中国 2021 年 8 月 20 日颁布，自 2021 年 11 月 1 日起施行。

GDPR，欧盟 2018 年 5 月 25 日出台，其中“被遗忘权”是欧盟法律中首次明确。

数字服务法案草案，欧盟 2020 年 12 月 15 日出台。

数字市场法案草案，欧盟 2020 年 12 月 15 日出台，以上两部法律意在明确数字服务提供者的责任并遏制大型网络平台的恶性竞争行为。

2 学科优势：横向与纵向

考虑网络空间安全专业的优势，可以从横向与纵向两个维度考虑。一方面是横向与其他学科对比，另一方面是纵向与之前的网络空间安全专业相对比。

2.1 横向对比

对比计算机科学与技术、人工智能这些同样接触计算机的专业，网络空间安全专业的特点和优势主要体现在以下三方面：其一是更加综合，其二是攻防互动的学科观点，其三是注重实践。

网络空间安全包括有硬件上的安全，有软件上的安全，有网络结构上的安全，具体到技术层面还有人工智能安全、大数据安全、量子计算安全等等。从事安全的前提当然是了解它是怎么运行的，毕竟不可能把研究对象完全当做一个黑箱，也就是首先要学习所要研究物体的运行原理。这意味着网安既不是“造轮子”，也不是“用轮子”，而是在一个了解原理的基础上“检查轮子”的角色。这同样意味着网安的学习更加综合，需要建立在计科、AI 的基础上，再更进一步研究对象的安全性。

不同于其他相对“静态”的学科，网络空间安全专业是在“道高一尺魔高一丈”的对抗中建立完善的。这提供了一种在攻与防中对立统一的学科观点，学习的过程也要求不能仅仅站在“遵守规则”的一方，而鼓励从多个角度思考，探索边界情况，寻找对抗的支撑点。

另一特点在于网络空间安全专业是和实际问题紧密联系的学科。所研究的问题、研究的方法和观点乃至实践的材料都建立在真实的攻防上。而实际的网络攻防实践日新月异，这也促使专业领域的研究和学习需要多实践、跟上最新攻防的脚步。

2.2 纵向对比

网络空间安全，从教学专业的角度上，正在得到越来越多的重视。2015 年，国务院学位委员会联合教育部下发文件，在“工学”门类下增设“网络空间安全”一级学科。[1]

而经过七年的教学积累，以及行业领域的实践积累，网络空间安全这样一个新兴的专业相较于以往，也逐渐沉淀、成熟下来。

结语：本文结合领域内的综述以及历来对网络空间安全领域的了解，总结而成了此篇报告。文章选取近年来网络空间安全领域的部分典型事件，讨论了 WannaCry 攻击对全球网络空间造成的沉重打击以及催生的大众网络空间安全意识、node-ipc 包供应链投毒事件背后蕴含着的攻防两方作用结果、影响较大的数据泄露事件以及在新环境攻防实践中的国内外相关立法。文章还结合笔者本人对网络空间安全专业的思考，讨论了专业在横向及纵向两个维度上的特点与优势。本文为笔者自身梳理学科思路提供了很好的机会，但一大缺憾在于缺少对网络空间安全领域的更具有广度的调研。

参考文献：

1. 张焕国等. 网络空间安全综述[J]. 中国科学:信息科学. 2016,46(02).
2. 沈昌祥等. 信息安全综述[J]. 中国科学 E 辑:信息科学. 2007,(02).
3. 杨玉国. 欧盟委员会公布《数字服务法案》 谷歌高层对法案提出质疑[N]. 国际在线. 2020-12-16.

[1] 在用筛选网页时间功能检索的过程中，并没有找到在 15 年之前，网络空间安全专业到底是归属于哪个一级学科。15 年前就已经有学校（如信息工程大学）开设网络空间安全学院，另有学校开设的是信息安全专业，并且不同学校信息安全归属的一级学科不同。或许在 15 年之前，网络空间安全专业在全国各校并没有统一。