



当前位置：首页 > 会员中心 > 会员资讯

网络安全建模辅助工具试运行絮语

网络安全建模辅助工具运行概念试验版今天上线了，这是由安天技术委员会威胁建模兴趣小组开发的在线服务的WEB工具，通过PC浏览器访问mbsse.antiy.cn，可以使用修订已经发布的网络安全模型，也可以建立自己的模型，可以支持工作组间的共享，由于人力所限，目前我们仅完善了对Chrome内核浏览器系统的支持。我们希望在可以期许的未来，给网安建模工作提供一个可用便利的软件支撑环境。但之所以称之为“运行概念试验版”而不是“测试版”，是因为我们深知距离工具的真正可用，还有很长的路要走。

关于建模工具

网络安全建模是网络安全工作中基于经验的汇聚所进行的范式提炼，是网络安全知识体系的上层建筑。借助优秀的模型和框架的辅助，网络安全工作者可更直观清晰，更有条理性地展开工作。模型是由对象、属性、关系、逻辑等要素组成的，但我们深感遗憾的是，大量优秀的网络安全抽象模型，缺乏配套的数据定义来支持计算、推理、关联分析，仍然是依靠人学习阅读理解使用的“认知成果”。尽管类似Office的SmartArt到Visio，能支持从简单到复杂模型的绘制，但这种绘图，没有将模型转化为一种可计算的知识结构；STIX、MITRE有价值地完成了一部分威胁和防御能力的形式化，包括数字工件本体的构建，但相对是一个窄带实践，并不适用于一些更宏观的模型。于是，我们有些不切实际的想象：是否能把网络安全基于文档和视觉理解上的建模工作，转化为既能满足交互操作和视觉理解，同时又满足模型的属性和数值定义，使之成为一个未来支持推理、计算的数据结构？当然，这是一个非常遥远的愿景，我们短时间内所想的，是一方面构建一个各种安全模型的“汇集地”，一方面尝试实现部分模型的数值、关系和逻辑定义。



图：在线建模辅助工具中的D3FEND (MITRE) 模型

关于网络安全知识工程与建模

网络安全的基础支撑工作，大体可以分成特征工程与知识工程两部分。

其中，**特征工程**支撑威胁检测引擎和安全产品、安全内核等的更新运行，是把复杂的威胁对抗转化为共性化、代价线性化的匹配和计算过程的基础工作，是网络安全自动化运行迭代的基本面；

而**知识工程**更多的是面向网络安全的维护者、运行者、操作者、开发者、决策者等角色，以人所能理解的文字、图表等信息形态来进行相关的知识传递。在非常长的时间内，我们更着重特征工程的运行效率和实际效果，更强调产生可部署的、自动化的运行价值；而知识工程则相对被视为一种更发散的、对体系性和系统要求不高的工作。

安天在这两个方向上都有较长时间的积累和努力：围绕安天反病毒引擎的持续规则升级，构建了以赛博超脑为基础设施的大规模对象分析和特征工程体系；同时安天CERT等团队，在恶意样本分析、APT事件分析、关键事件研判等方面进行知识成果生产，但这些工作和我们在特征工程运行的体系性相比，依然显得十分发散。

建模过程是为了理解事务和运行规律而进行抽象，建模方法可以在真实客观世界和认知世界之间建立起来一座桥梁。网络空间是一个复杂的、人工构造的世界，网络安全对抗更是一个复杂的过程。建模成为了我们认知这个世界的武器，过去二十多年来，各种系统建模、过程模型、威胁和风险模型、成熟度模型、能力模型的成果不断涌现。

在这些成果中，有的是其他领域的通用经典模型进入到网络安全领域，例如OODA环、PDCA环等——我们常说“闭环是一切具有指控特性与对抗特性的事物与过程的基本特征”；有的是经典概念在网络空间领域的移植变形，例如物理作战的杀伤链模型被移植到网络空间，产生了网空杀伤链、网空通用杀伤链、统一杀伤链、认知影响杀伤链等各种变体；各种成熟度模型则是根据网络安全建设和运营有阶段性特点，相对量化地提供了评价依据以及层级间的依赖关系；也有的模型是为相对碎片化的（甚至看起来杂乱无章的）经验知识找到了新的聚合方法，例如以ATT&CK为代表的威胁框架模型，将攻击的战术、技术与更细化的杀伤链的攻击战术阶段、目标相关联后，相比此前基于CAPEC的分类方法，体现出了更强的系统性。

可以看到，这些新涌现的模型既超越了原有的案牍知识中一般性的图表和清单，形成了更加系统、严谨、多维的知识组织结构，也在原有的基于特征工程所映射或表征的、条目化的安全知识（例如恶意代码命名等）之上，构建了在TTPs或者系统运行结构与机理层面的升维可能性，创造了特征工程体系与知识工程体系工作的连接点。我们做的并不是“绘图工具”。我们的关键目标是把每个模型的内在的逻辑关系和属性定义转化成一种可机读、可计算的结构，同时将其逻辑定义与显式定义解耦（这一点也是我们与Visio、Office SmartArt以及其他在线图表生成工具的最大差异）。

诚然，如果对网络安全模型的应用目标只是用于网络安全的方法培训，以及在各种文档中贴图、引用、印证，那么我们的尝试是没有任何意义的；但是，如果考虑到网络安全知识工程与特征工程的结合潜力，特别是以大模型平台为代表的AI技术对复杂知识的吸纳和生成能力，我们的工作就可能产生价值。大模型技术的成熟使得海量由自然语言所承载的、在以往需要人传承理解的知识转化为计算机生成内容乃至工作逻辑成为可能，但这种吸星大法既带来了“涌现性”，也带来了幻觉。

我们提出一种想象：由于建模结构远比自然语言叙述更为严谨和有约束力。在类似网络安全这种需要高度的严谨性的领域，是否能通过模型框架，为大模型的结果生成，提供更确定性的路径指引。或许当我们形成了足够的这种具有约束性的知识逻辑积累，就可以在未来约束“幻觉”的产生。我们同时认为，智能化带来的人机工程提升并不是单纯的把更多人能够完成的工作交给“机”来做——把海量的样本对象丢给机，或者把基于特征工程所形成的匹配、检测结果，通过更多的汇聚、关联、统计、加权、深度学习等方式，形成更整体的判断结果和预测以辅助人工决策。我们还要教会“机”更多的东西——把更抽象的知识转化为机器系统可以消费和理解的、辅助网络安全的规划、运营、分析的升维逻辑。

来源：安天集团

上一篇：刘东出席2023世界互联网大会乌镇峰会“数据治理推动全球数字经济发展论坛”并发表主旨演讲

下一篇：后会有「栖」，明年见