可能的艺术
THE ART OF THE POSSIBLE

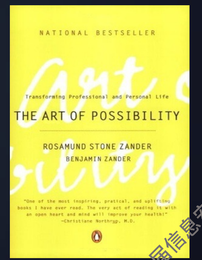
第16届信息安全高级论坛

美国2024RSA参会热点研讨
INFORMATION SECURITY FORUM 2024

谈谈RSA2024会议上的GenAI和Q-DAY问题

翟起滨

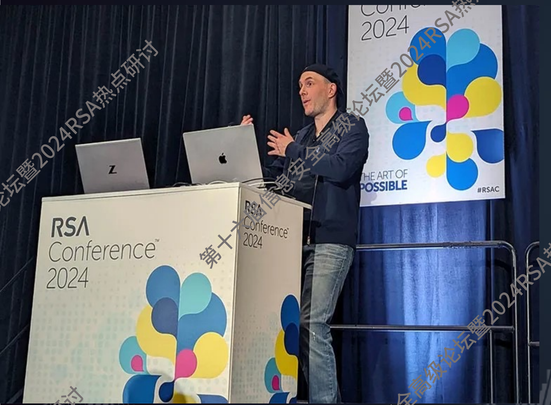
中国科学院信息工程研究所/北大软微学院



《可能的艺术》叙述一位心理学家和一位音乐家，将他们的各自的新颖想法融合在一起，创建一个快乐生活的计划。许多看似阻碍我们日常生活的情况可能只是基于我们随身携带的假设框架。围绕同一组情况绘制不同的框架，新的途径就会出现。GenAI和Q-DAY问题正是这种可能艺术在网络空间里的一种表现！

RSAC 2024，May 6, titled “How Large Language Models are Reshaping the Cybersecurity Landscape”

可 能 的 艺 术
THE ART OF THE POSSIBLE
第16届信息安全高级论坛
美国2024RSA参会热点研讨
INFORMATION SECURITY FORUM 2024



- Google 的 Elie Bursztein（1980 年 6 月 1 日出生于法国，法国计算机科学家和软件工程师。他目前是 Google 和 DeepMind AI 网络安全技术和研究负责人），在这个专题会议上他代表Google做出承诺（Google on the promise of large language models and cybersecurity），他演讲一开始就针对使用 GenAI 最令人担忧的是对手传播错误信息的能力，以及对手使用 GenAI 制作令人信服的网络钓鱼电子邮件的能力……

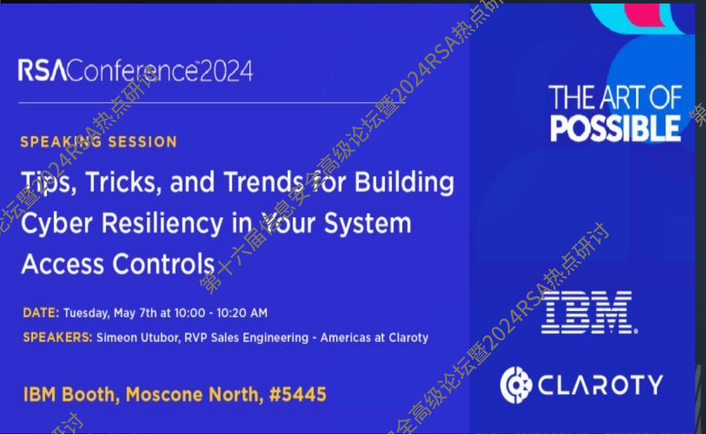
  他详细谈了Google 对 AI 技术中使用大型语言模型进行深入分析时存在的问题，演示了他们把网络安全统治权移交给 GenAI 来完成的一系列过程，比如零样本（Zero-Shot Learning，是一种能够在没有任何样本的情况下学习新类别的方法）内容审核识别和修复等任务时，所存在的难题；以及存储库中的开源代码，检测和修复攻击面中的软件漏洞等问题。他强调训练语言模型的泛化能力，综合人类的推理能力。这将使该技术能够对用户生成的内容进行分类，而无需人工审核。
- Bursztein 表示：“我知道解决好这些问题，不会像人们想象的那么快，至少需要几个月的时间。”
- 他最后强调：“在人工智能达到我们需要的可靠性和强大程度以充分发挥其潜力之前，还需要进行更多的研究和更多的创新。”“如果您还没有进入这个领域，希望 [RSA 会议] 能让您兴奋地进入这个领域，并开始考虑如何使用它。”

READY FOR Q-DAY? POST-QUANTUM CRYPTOGRAPHY AT RSA 2024

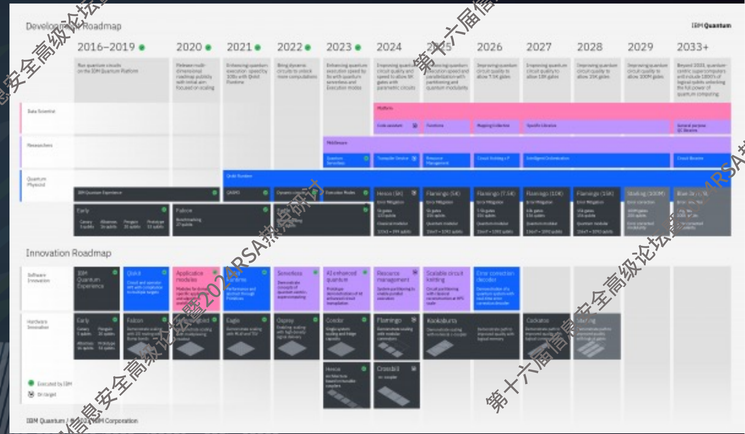
- InTechnology讲台中，**主持人Camille 与 Fortanix 首席 AI 官 Richard Searle 博士;Keyfactor首席安全官克里斯•希克曼（Chris Hickman）以及埃森哲量子安全工程师 Andrew Driscoll一起探讨了量子计算和后量子密码学,他们的对话涵盖了量子计算和后量子密码学的概述，探讨如何为后量子现实做好准备，以及量子计算机何时能真正的到来。**

- 对话的最后，讨论了量子计算何时推出以及组织如何调整准备时间的问题。Chris强调，现在是开始准备的时候了，组织应该像对待关键基础设施的任何其他元素一样对待密码学。安德鲁随后说明了具有破解现代加密能力的量子计算机可能已经存在，但如果由民族国家或组织将其用于高度敏感的目的而开发，它们的存在可能会被保密一段时间。

伟大的量子计算时代很快就会到来



- IBM在2023年12 月 4 日，宣布实现了133 量子位“Heron”（鹭）处理器QPU,他将以量子为中心的超级计算变为现实。准备在2025年，推出Kookaburra(笑翠鸟)处理器QPU，这将是一个具有量子通信链路的1386 量子位多芯片处理器，这就意味着以量子为中心的超级计算机时代就要到来。
- 互联网的安全问题是严格依赖于底层加密算法的可靠性。 然而，直到现在我们所有的基于认证和加密功能的应用程序大多数都基于 RSA公钥算法和有限域中的离散对数问题或椭圆曲线(ECC)的算术问题,而这些问题是经受不起量子计算机攻击的，也就是说，到了2025年，上面提到的那些密码学根基都会被破坏掉。



SandboxAQ于RSA2022会议前,5月11日， 在 Nature 上发表论文：立即把各部门使用的密码转型过渡到后量子密码；RSAC2024, 这家公司继续推进这个任务！

Google母公司 Alphabet在2022年3月22日剥离了其量子技术部门，成立了一家名为“Sandbox AQ”的初创公司。该公司已任命前谷歌首席执行官埃里克施密特（EricSchimdt）为董事长，量子技术专家杰克·希达里（Jack Hidary）为执行官，公司主要开发后量子密码技术。后量子密码学是北约和美国政府正在关注的一项技术。施密特说，量子技术和人工智能技术的融合已经在改变整个行业，加速科学发现，重新设想我们认为可能的事情。他进一步表示，Sandbox AQ的战略定位是在全球范围内领导这一转型，因为该公司专注于利用当今的高性能计算能力和新兴量子平台，来开发商业上可行的量子技术。

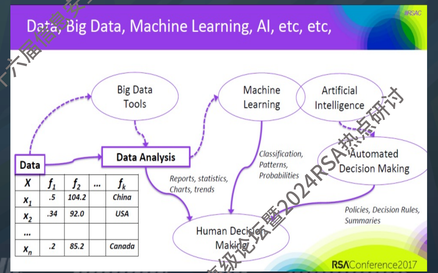
- 今天的生成式AI 技术和量子计算技术，早在 20 世纪初就引起科学家的兴趣和各式各样的构想，直到现在仅仅是技术上的一步步完善，理论上还没有更新的突破。
- 生成式 AI, 在 2020 年代爆发,且进入公众意识，但几十年来，生成式 AI 一直是我们生活的一部分，2022年：OpenAI 引入了 ChatGPT，这是 GPT-3 的前端，可生成复杂、连贯和上下文相关的句子和长篇内容以响应最终用户的提示。
- 当下，支持人工智能采用的密集型计算需求不断增加。然而，由于硬件的可用性、硬件的性能和功耗效率，当前的计算无法满足这种需求。解决这些问题的办法是量子计算芯片，量子计算机一旦问世，人工智能的新蓝图才真正展开。这也正是2022年谷歌的达人施密特把谷歌最有能力搞人工智能的技术人员组建AQ-sandboxes 的原因。我们对这个公司的前途，拭目以待……

Google was founded in 1998 by Larry Page(拉里.佩奇）and Sergey Brin（谢尔盖.布林）while they were Ph.D. students at Stanford University.

Google2012年用16000台电脑构置的神经网络一起找猫。

“RSA2015:Escaping Security’s Dark Ages”！

RSA2017会议给出口号：
Modern data control ,Intelligence led security



纽约时报记者Lewisy与Schmidt对话
“The Great AI. Awakening”

可 能 的 艺 术

THE ART OF THE POSSIBLE

第16届信息安全高级论坛

美国2024RSA参会热点研讨

INFORMATION SECURITY FORUM 2024

感谢聆听！