解读 Sectigo 2024 年预测四：人工智能-网络安全攻防双方的终极技术？

零信技术国际 SSL 证书战略合作伙伴 Sectigo 本月在其官网博客栏目发布了 2024 年数字安全领域的七大预测，笔者利用周末时间翻译并解读了这七大预测。

今天解读预测四：人工智能-网络安全攻防双方的终极技术？

笔者认同 Sectigo 的观点-网络安全防护需要人工智能，当然你也无法阻止黑客利用人工智能，这仍然符合传统网络安全攻防双方的“魔高一尺道高一丈”的魔咒。要想真正从魔咒解脱出来，笔者将从密码应用来保障网络安全的角度来解读这个问题。

首先，我们必须要理解为何攻击者要攻击系统，当然是为了获取有价值的数据。其次，我们必须搞清楚网络安全防护的最终目的是什么，当然是为了保护数据安全，而不是为了仅仅保护服务器安全，是为了保护数据的全生命周期安全，包括数据的收集、存储、使用、加工、传输、提供、公开等，这七个环节中的最重要的是数据传输安全，传输安全不做好，其他安全保护都是空中楼阁。

但是，目前的现状是大家只重视传统的服务器端保护，大家都用极致的技术，包括人工智能技术来保护数据在机房服务器里的安全，并没有做好数据的“在途”安全，数据离开了城堡，流通到用户端的通道并没有采用 HTTPS 加密，使得攻击者根本不用去攻击防卫森严的城堡，而只需坐等在数据流通的途中，就可以非常容易地打劫数据和篡改数据！这是传统安全防护理念的局限，而不管用了什么最先进的技术包括人工智能也没有用！

Sectigo 的观点是在欧美普遍实现了 HTTPS 加密的前提下的观点，当然也值得我国网络安全业界关注和思考。但是，我国的当务之急是要做好这个话题的基础工作—HTTPS 加密的普及使用，特别是商密 HTTPS 加密的普及应用，没有这个基础通信安全，其他安全攻防就失去了意义，因为你保护了业务系统的安全，只是保护了数据安全的一端，没有 HTTPS 加密就没有保护数据能安全地流动到用户端。这是数据安全的基础保护，必须普及实现数据在流通的每一个环节的 HTTPS 加密保护。

实现数据的“在途”安全的唯一可靠技术就是 HTTPS 加密，数据在全生命周期中的流通传输都必须是通过 https 加密通道流通。而要想实现所有系统的普及应用 HTTPS 加密，则必须采用自动化证书管理技术来自动化实现 HTTPS 加密，没有这个自动化是无法普及实现 HTTPS 加密的。

在我国，依据《密码法》，数据传输安全必须采用商密算法实现 HTTPS 加密，当然也必须

是自动化部署商密 SSL 证书来实现 HTTPS 加密自动化，只有这样才能可靠保障每个系统的每一个数据处理过程中的数据处于有效保护中，使得数据从生产到销毁的全生命周期都处于持续安全状态。这也是《数据安全法》所定义的“数据安全”要求，“通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。”

人工智能将一定是数字安全领域的终极防御手段之一，巧了，自动化证书管理技术的英文名称就是终极的英文单词 acme，也就是，人工智能是防御服务端安全的终极技术，而 HTTPS 加密自动化则是保障数据传输安全的终极技术，只有同时普及应用这两个终极技术才能保障数据的“在岸”安全和“在途”安全，才能真正保障用户数据的全面安全。

<下面请读者朋友仔细阅读原文译文>

在与时间的赛跑中，黑客和网络安全专业人士都在积极利用人工智能的力量。2024 年将决定人工智能是成为强大的威胁行为者，还是保护网络安全领域的最具影响力的新兴技术。

2024 年将是一个决定性的时刻—一个关乎人工智能(AI)命运的战场。人工智能是否会成为一个强大的威胁行为者，甚至能够胜过最复杂的网络安全措施，还是会成为最终的守护者，成为防御网络威胁浪潮的灯塔？ 这场决定性的对决将成为一场与时间的竞赛，黑客和网络安全专业人士都积极利用人工智能的力量来推进各自的目标。

当我们站在这个技术十字路口的门槛时，了解人工智能在网络安全中的作用至关重要。将人工智能融入数字防御领域，为黑客和安全专家之间古老的猫鼠游戏引入了新的维度。传统上用于破坏安全系统的工具现在被防御者用来预测、预防和响应网络威胁。

人工智能：威胁行为者

黑客始终处于技术创新前沿，他们并不回避采用人工智能来增强攻击的能力。能够实时学习和适应的自动化黑客工具对传统的网络安全措施构成了重大挑战。人工智能分析大量数据并以前所未有的速度识别漏洞的固有能力使恶意行为者占据了上风，使他们能够在防御者做出反应之前利用弱点。

生成式人工智能为新的人工智能计划打开了闸门，使得实施强大的人工智能信任、风险和安全管理能力的需求变得更加迫切。 - Gartner，2023

人工智能：防御灯塔

另一方面，网络安全专业人员越来越多地利用人工智能作为保护数字基础设施安全的力量倍增器。采用机器学习算法来检测发现潜在威胁的模式，从而实现主动防御措施。人工智能分析网络流量、识别异常和预测潜在违规行为的能力使安全团队能够领先网络犯罪分子一步。从本质上讲，人工智能已经成为网络安全人员在持续的数字霸权之战中不可或缺的盟友。

2024 年不仅是技术冲突的一年，也是意识形态冲突的一年。 人工智能是否可以被信任为数字领域的最终捍卫者，或者它被滥用的可能性是否超过了它的好处？答案在于在网络安全领域负责任地开发和部署人工智能。道德考虑、透明度和严格的监管对于确保人工智能在数字世界中发挥积极作用至关重要。

未知的技术领域

虽然人工智能使防御者能够增强其安全态势，但它也带来了一系列需要持续警惕的新挑战，必须承认人工智能能力的双重性。在网络安全中道德地使用人工智能需要一种微妙的平衡—最大限度地发挥其保护潜力，同时最大限度地减少意外后果的风险。

明年人工智能网络安全对决的高潮将塑造数字防御的未来。人工智能会成为一把双刃剑，既能防御又能攻击，还是会成为安全、有弹性的数字生态系统的关键？事关重大，其结果将影响全球各行各业和全社会。

2024 年：在威胁与防御的十字路口前行

2024 年人工智能与网络安全的交叉点将成为持续对抗网络威胁的关键时刻。这场冲突的结果将决定人工智能是数字安全领域的潜在威胁还是最终防御。当我们迈向这一技术前沿时，负责任地开发和合乎道德的人工智能部署对于利用其潜力造福人类和确保安全的数字未来至关重要。我们今天做出的决定将在未来几年内在网络空间的走廊中回响。

王高华

2023 年 12 月 25 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。