# 解读 Sectigo 2024 年预测三：深度伪造将破坏数字信任

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 年数字安全领域的六大预测，笔者利用周末时间翻译并解读了这六大预测。

今天解读预测三：深度伪造将破坏数字信任。

相信读者朋友对“深度伪造(Deepfake)”已经不陌生了，即使没有听说过这个名词，但一定刷到过各种外国名人讲一口流利的中文的视频，这不是真的！深度伪造已经彻底颠覆了人们几千年来坚信的那句话“我亲眼看到的还有假吗？”是的，你所看到的和听到的都可能是假的，是伪造的。

**深度伪造**是人工智能和大模型的应用之一，将图片或视频合并叠加到源图片或视频上，借助人工智能技术进行大样本学习，将个人的声音、面部表情及身体动作拼接合成为虚假内容。深度伪造最常见方式是 AI 换脸技术，此外还包括语音模拟、人脸合成、视频生成等。它的出现使得篡改或生成高度逼真且难以甄别的音视频内容成为可能，普通用户是无法通过肉眼明辨真伪的。所以，国家网信主管部门针对未履行安全评估程序的语音社交软件和深度伪造的应用多次依法约谈了多家相关企业。

笔者非常认同 Sectigo 的观点-深度伪造的扩散将破坏数字信任，这就急需快速普及应用 PKI 技术来实现所有数字记录的数字签名和时间戳。这也是零信技术的零信任五大原则之一的“不信任任何没有数字签名的文档”，当然包括各种类型的文件，如文字、音频和视频。只有实现了所有形式的数字记录都有可信的数字签名和时间戳才能确保所有数字记录都是可信的记录，才能实现让深度伪造再也无法以假乱真，也只有这样，才能重建人们对数字记录的信任。

零信技术不仅提出了“对没有数字签名文档零信任”的理念，而且已经付出了行动—零信浏览器全球独家率先支持实时验证 PDF 文档的数字签名和时间戳，让假冒文档立即现形-“此文档无数字签名，发布者身份未知。请谨慎！”，以此帮助用户识别可信文档和不可信文档。零信技术计划继续推动其他各种类型文件的数字签名和时间戳应用，包括音频文件和视频文件，普及 PKI 数字签名来保障所有数字记录的安全可信。

最后需要强调的是，依据《密码法》和《电子签名法》，只有采用商密算法实现的数字签名和时间戳才是具备法律效力的，所以，我国解决深度伪造的唯一解决方案是普及商用密码来保障数字记录的真实可信，人们无需过度担忧，可以通过普及应用商用密码技术来挽救和加强数字信任。

**<下面请读者朋友仔细阅读原文译文>**

人们可以相信自己的所见所闻的日子已经一去不复返了。鉴于我们对法律、安全和数字系统中数字记录的依赖，深度伪造的扩散将破坏数字信任。很快，所有形式的数字记录都将建立在唯一无懈可击的加密形式之上：PKI(公钥基础设施)。


数字记录的可靠性将在 2024 年面临崩溃。罪魁祸首是谁呢？深度伪造(Deepfake)，一种复杂的数字操纵形式，它将真实内容和捏造的内容无缝融合，侵蚀了我们对所见所闻的信任基础。这种令人震惊的趋势具有深远的影响，特别是在真实性至关重要的数字、安全和法律系统中。

**数字信任的侵蚀**

深度伪造的普遍性引发了一个紧迫的担忧：数字信任的侵蚀。随着事实与捏造之间的界限变得越来越模糊，接受数字记录的真实性的日子正在消失。这种现象有可能损害我们社会的结构，在社会中，对数字证据的信任是国家安全、法律程序和各种身份认证系统的基础。

在当前形势下，我们对数字记录的依赖从未如此明显。数字信息的完整性支撑着我们现代世界的关键方面以及日常生活的各个方面。但随着深度伪造变得更加复杂和易于获取，任何数字记录（无论是照片、视频还是录音）的真实性都将会受到质疑。

迫在眉睫的威胁之一在于基于数字记录验证身份的生物识别系统的脆弱性。 去年，欺诈攻击增加了 92%，随着深度伪造渗透到我们的数字系统，安全的基础崩溃了。想象一下这样一个世界：刷脸(面部识别)、语音认证和指纹认证不再保证个人身份的可信度，这对个人隐私、金融安全甚至国家安全的影响是深远的。

**保护真实性**

为了解决这一迫在眉睫的危机，一个潜在的解决方案是将加密时间戳集成为所有记录设备

的内置功能。 这些时间戳将充当数字水印，证明内容捕获时的真实性。 然而，这种对策的成功依赖于万无一失的加密方法的实施，在这里，公钥基础设施(PKI)成为数字领域信任的来源。

PKI 以非对称密码为基础，以其强大的安全功能而闻名。通过利用 PKI 创建加密水印，我们可以无可挑剔地确定录制内容的真实性。这种加密保护措施确保内容以无法被操纵或伪造的方式添加时间戳，从而提供了一种可靠的方法来区分真实记录和深度伪造记录。

**重建数字信任**

将基于 PKI 的加密时间戳集成到数字文档创建和分发中，通过增强数字记录的准确性来从根本上解决问题。当有一天，每张照片、视频或录音都带有不可磨灭的真实性印记时，信任的基础就可以重建。这项创新不仅可以保护生物识别系统，还可以增强法律诉讼中数字证据的可靠性。

这种解决方案的实施需要技术开发人员、立法者和广大公众的共同努力。任何解决方案都需要在隐私和安全之间取得适当的平衡。随着 2024 年的临近，社会对这种数字记录签名以及支持它所需的硬件、软件和生态系统的需求已经变得非常明显。

明年将是一个十字路口，一个数字记录的可靠性面临消亡的时刻，但也是一个可以依赖 PKI 强大加密技术的创新解决方案来挽救和加强数字信任的时刻。我们选择的道路将塑造数字世界的未来，决定我们是屈服于深度伪造的威胁，还是对数字世界的真实性重新产生信任感。

王高华

2023 年 12 月 22 日于深圳

---

请关注公司公众号，实时推送公司 CEO 精彩博文。