Akamai

白皮书

如今的 MFA - 是否只是一种安全假象？

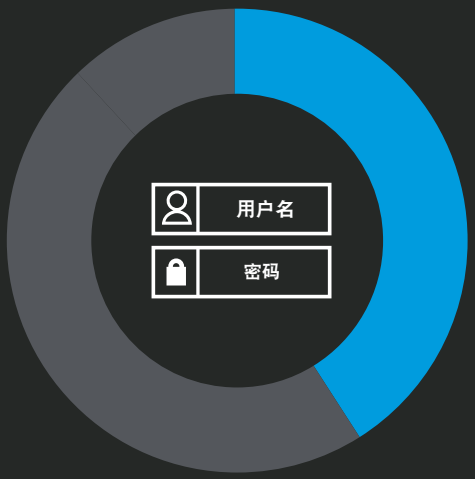
用户名和密码不足以保障安全

80% 的安全漏洞与泄露的凭据有关。[1] 密码使用习惯虽应对此承担部分责任，但即使是使用由算法开发的、无法破译的复杂密码，也会出现问题。[2] 最近的一项暗网调查表明，100,000 次数据泄露导致了 150 亿条登录信息被盗。[3]

数字化连接的必要性、对云服务的依赖以及混合环境的现状，再加上对密码的依赖，导致用户非常容易遭到各种身份验证攻击媒介的侵害：

- **撞库**
- **密码喷洒攻击和其他暴力破解机制**
- **本地查找和内部人员泄露**
- **网络钓鱼和社会工程**
- **按键记录**
- **恶意代理和回复活动**

全球疫情加剧了这一现状，这表明了人们进行与设备和位置无关的安全访问方面的需求。考虑到所有与凭据相关的泄露都发生在用户经过身份验证之后，仅凭密码显然无法对用户进行足够准确的身份验证。



尽管用户名和密码机制存在已知的弱点，41% 的企业仍然认为它是最有效的访问管理工具之一。[4]

500%

Akamai 发现，网络钓鱼、社会工程、撞库和暴力破解攻击的数量都在增加。2020 年 3 月至 5 月，我们看到恶意软件数量增加了近 500%。

多重身份验证的优势

因此，多重身份验证 (MFA) 技术的普及程度稳步增长，这并不会让人感到很意外。简而言之，MFA 在授予访问权之前，会使用一个以上的验证源来验证访问者的身份，从而保护您的企业。

MFA 要求访问者成功组合使用以下三种身份验证凭据中的至少两种：

您知道的信息

这是基于已知信息的身份验证。这种验证可以采用密码、PIN、安全问题答案甚至是图案的形式。

您所拥有的设备

这是基于令牌的身份验证硬件或软件）。这可能是智能卡或钥匙扣，或者一次性密码、推送通知或发送到移动设备上的短信验证码。

您自身的某个特征

这是基于情景或生物特征识别的身份验证。这可能是行为、位置信号或时间、指纹、面部识别、声音或语音模式或者签名。

实施 MFA 解决方案可显著降低未经授权的访问和系统漏洞的风险。事实上，相比不使用 MFA 的企业，使用 MFA 的企业遭到入侵的可能性要低 99.9%。[5] MFA 能够支持并优化对所有环境的安全访问，包括云环境、本地环境、基于 Web 的环境、SaaS 和 IaaS 应用程序。MFA 解决方案也是企业安全功能向 Zero Trust 和 SASE 等框架迁移时的重要一环。

MFA 技术与其他云原生安全工具集成，不仅要求访问者提供用户名和密码，还能确保统一的登录体验；而且，它还具备提高用户工作效率和可用性的潜力。此外，集中管理的身份验证解决了许多合规问题，也满足了许多要求。

可是传统的 MFA 并不像您想象的那样安全

建立在标准推送之上的 MFA 服务很容易被黑客操纵，以实现帐户接管。除非增加额外的安全措施，否则，如今的 MFA 技术仍会让您面临风险。

MFA 是防御层安全功能的一种形式，可是云环境 - 以及如今的工作方式 - 没有所谓的防御层。MFA 无法阻止与登录无关的攻击。它只是在防御层中保护登录，也就是说，在用户尝试获得系统访问权限时提供保护。网络犯罪分子为了规避这种保护，已经开发出了相对简单、却非常有效的社会工程和网络钓鱼机制。

设想以下场景：

1. 在某种形式的社会工程影响下，员工将自己的用户名和密码输入攻击者建立的虚假（网络钓鱼）网站。

2. 攻击者获得这些凭据后，便会将其输入到真实的登录门户中。

3. 此操作会造成系统向员工手机推送通知。

4. 员工把这当成理所当然的登录过程，也就接受了推送通知。

5. 攻击者现在已经完成了两种形式的验证，因此获得了访问权限。

这是标准推送通知存在的严重安全漏洞 - 拥有一组被盗凭据的任何攻击者都可以将推送通知发送到员工的手机上。企业只能寄希望于员工能辨别合法推送和诈骗，来避免发生安全违规，进而让企业正常运营。攻击者只需对数千名员工成功执行一次攻击，即可实现入侵。

可防范网络钓鱼的 MFA

真正安全的 MFA 解决方案采用 FIDO2 标准。在最基本的层面上，这意味着安全性是以技术为基础，而不是依赖于用户的决策。

这是如何实现的？FIDO2 标准使用了一些可防范网络钓鱼的技术。

首先，身份验证请求（MFA 质询）始终被发送到发起访问请求的工作站。该工作站上的浏览器会将身份验证请求定向到任何本地连接的安全密钥。套用到上述场景：现在，MFA 质询将返回到攻击者的工作站，而不是攻击者让 MFA 服务将推送通知发送到员工的手机上。由于攻击者没有员工的安全密钥，因此无法做出响应。这样就阻止了帐户接管。

定义：身份验证标准和规范

Fast IDentity Online (FIDO) 联盟

负责制定、使用和遵守身份验证标准的机构。

FIDO2

FIDO 联盟最新的一套身份验证规范的统称；收录的标准包括 CTAP1、CTAP2 和 WebAuthn。通过 FIDO2，用户能够利用常见设备在移动和桌面环境中轻松执行身份验证，以访问在线服务。

WebAuthn

由万维网联盟 (W3C) 发布的 Web 标准，是 FIDO2 的核心组成部分。该项目旨在为接口实现标准化，以使用公钥加密技术，针对基于 Web 的应用程序和服务验证用户身份。

客户端到身份验证器协议 (CTAP)

这是由 FIDO 联盟制定的规范，可在漫游身份验证器（例如智能手机）和内部身份验证器（客户端或平台）之间实现安全通信。

其次，浏览器在发送身份验证请求的同时，也会向安全密钥发送数据。这些数据包括浏览器看到的发送身份验证请求的源站域名。如果攻击者只是简单地将收到的身份验证请求转发到员工的工作站，这些数据将包含网络钓鱼网站的域名。安全密钥会识别出它最初注册的网站的域名和请求身份验证的域名之间存在的不匹配，并拒绝响应，从而再次阻止攻击。

如果更安全、可防范网络钓鱼的 MFA 是一种可能的解决方案，为什么此方案没有得到更广泛的应用？需要使用物理安全密钥 - 昂贵且麻烦。直到我们的解决方案出现，这一难题才得到解决。

在边缘部署的新一代 MFA

在评估和实施 MFA 技术时，IT 部门需要权衡各方因素。为了实现出色安全性，他们必须花费更多的资金来部署硬件，为每个员工购买物理安全密钥，并管理所有密钥的分配和操作。IT 部门还必须让每个用户都接受密钥所带来的、不太理想的使用体验 - 毕竟员工又多了一种需要使用和跟踪的硬件。

另一种方案是将便捷的推送通知发送到员工的智能手机上，这种方法的安全性略低于前一种，但不会增加成本。后者的便捷性是如今推送式 MFA 得到广泛采用的原因。也正是因此才会有如此多的公司面临着遭到入侵的风险。

现在，安全性、成本和采用便利性可以兼而有之。

Akamai MFA 服务引入了新的身份验证因素。它为 FIDO2 的安全功能实现了数字化，需要用到的只有一部智能手机和一个 Web 浏览器，而且还结合了简单易用、人们熟知的推送通知体验。它可作为漫游身份验证器在任何平台上使用。无需物理安全密钥。该解决方案以低廉的成本提供了 FIDO2 标准中高度安全的功能，安装和使用起来也很简单，并且可以与常见身份提供程序进行互操作。

使用 Akamai MFA 保护您的企业，抵御网络钓鱼、撞库和帐户接管。了解有关 Akamai 首创的 MFA 技术的更多信息，为真正无密码的安全未来做好准备。

要了解更多信息，请访问 akamai.com/mfa。

来源：

1. https://enterprise.verizon.com/resources/reports/dbir/
2. https://www.infosecurity-magazine.com/opinions/problem-password-everything-1/
3. https://www.forbes.com/sites/daveywinder/2020/07/08/new-dark-web-audit-reveals-15-billion-stolen-logins-from-100000-breaches-passwords-hackers-cybercrime/?sh=27fa6368180f
4. https://www.businesswire.com/news/home/20200616005047/en/Weakest-Link-Prevails-Overreliance-Passwords-Continues-Compromise
5. https://www.hipaajournal.com/multi-factor-authentication-blocks-99-9-of-automated-cyberattacks/