信息安全前沿课堂讨论

陆皓喆 2211044 网络空间安全学院

2023 年 12 月 19 日

2 口令为什么在可预见未来仍是不可替代的最主要身份认证方法，并从个人角度和企业角度谈谈如何保护口令？

首先我们先要了解**口令的定义**。

口令的英文是 password，词的组成很形象 pass（通过）+ word（词），就是“要通过此道关口，你要提供一个证据，证明‘你知道’这个词。”在非电子信息领域，早已存在“口令”。比如战争片中，经常看到岗哨看到可疑人物立刻提问：“口令”，若回答出来，表示是“好人”，否则就是“敌人”。

口令是一种验证鉴别（Authentication）手段，通过验证“我知”来证明“我”是自己声称的“身份”。身份不是必须的，例如前例中，只要知道就是好人，不区分你是师长还是连长。在当前大部分互联网应用中，会对不同的用户设置不同的身份和口令，用于下一步，对拥有此身份并通过身份验证（我知道此口令）进行访问控制。

口令有一个基本特征：

由可书写可读的字母、数字、符号、词组成，便于头脑记忆。

在“认证鉴别”技术中，一般有 3 类验证：

我知。通过提供一些只有此身份知晓的信息，证明自己拥有此身份。口令属于此类。此类验证，是对头脑中或书写中可记录、记忆的信息做验证，因此有上述特征，便于头脑或笔头记忆。

我有。通过一些为此身份颁发的“物件”，证明自己拥有此身份。例如，使用手机号码登录时，系统向此号码发送一个验证码，输入此验证码，证明 1）你有这部手机 2）你可以访问这部手机（不是捡来、偷来的）。再例如，银行颁发的 USB 卡，插入电脑可执行操作。

我是。通过一些与生俱来的特征，进行验证。例如，人脸识别，指纹识别等。我知、我有一般可以转移（告诉别人口令，或者把银行卡给别人用）。“我是”则很难转移。但“我是”的与生俱来的特征，也意味着一旦遭到复制、仿制，你可能是一辈子丢失了，无法修改。

在很多身份验证过程中，会使用上述 3 类验证中的多类，称为“多因子（multi-factor）”验证。例如，ATM 取钱，你需要提供“我有”（银行卡）和“我知”（取款口令）；再如，很多购物、支付、金融类操作，需要“口令 + 生物特征”的多因子识别。

我们都知道，在现代生活中，有许多口令，比如说密钥、密码等等。为什么口令在未来是不可替代的呢?

对于不可替代性，我们可以先从个人角度来看。

首先是便携性和易记性。口令相对于其他身份认证手段（如硬件令牌或生物识别）更易于记忆和传输。用户可以轻松地输入密码，而不需要携带额外的硬件设备。

然后是广泛应用。口令是一种通用的身份验证方法，几乎在所有在线服务和系统中都得到广泛应用。用户只需记住一个密码，就能够访问多个平台。

当然还有灵活性。用户可以相对容易地更改和管理他们的密码，以应对安全性威胁。这使得口令对于快速响应安全问题具有一定的灵活性。

当然，不仅仅是个人角度，在社会中，还有许多的企业，都在生产中使用了口令。我们继续从企业角度来看。

第一点是成本效益。实施口令作为主要身份认证手段通常比其他技术更经济实惠。不需要昂贵的硬件设备或生物识别技术，降低了系统的维护和运营成本。

第二点是用户管理。口令允许企业更好地管理用户凭证。企业可以实施密码策略，要求复杂性和定期更改，以提高安全性。

最后是兼容性。口令可以与现有的大多数身份管理系统和应用程序集成，而不需要大规模的改变或更新。

接着，我们来看看如何保护口令。

从企业角度来看，我们可以从以下六个方面来对口令进行保护。

1. 复杂性要求：实施密码策略，要求用户选择复杂的密码，包括数字、字母和特殊字符的组合。这可以增加密码的强度，防范简单的猜测攻击。

2. 定期更改：强制用户定期更改密码，以减少密码被滥用的风险。这有助于防范长期持有同一密码可能带来的潜在威胁。

3. 多因素认证：实施多因素认证，结合密码与其他认证方法，如短信验证码、硬件令牌或生物识别，提高身份验证的安全性。

4. 加密存储：在存储口令时使用强加密方法，防止数据库泄露导致的密码泄露。

5. 教育和培训：对用户进行安全教育，教导他们创建和保护强密码，以及注意避免社交工程和钓鱼攻击。

6. 监测与响应：实施实时监测和快速响应机制，以便检测异常活动并及时采取措施，例如锁定账户或发出警报。

作为个人，我们也可以采取一些方法来避免密码的泄露，从而对口令进行必要的保护。

1. 使用强密码：选择强密码，包括大小写字母、数字和特殊字符。避免使用容易被猜测或包含个人信息的密码。

2. 唯一性：针对不同的账户使用唯一的密码。这样，即使一个账户受到威胁，其他账户的安全性也不会受到影响。

3. 定期更改：定期更改密码，避免长期使用相同的密码。这有助于降低密码泄露导致的潜在风险。

4. 谨慎处理密码提示：避免使用容易猜测的密码提示，以及包含个人信息的提示。这样可以提高密码的安全性。

5. 不在公共设备上保存密码：避免在公共计算机或其他共享设备上保存密码。如果必须在其他设备上登录，确保在使用后注销账户。

6. 谨慎使用公共网络：在使用公共无线网络时，避免访问敏感账户或进行重要交易，以防止密码被监听或窃取。

7. 启用两步验证：对于支持两步验证的服务，尽量启用。这样即使密码泄露，仍需要额外的身份验证步骤。

8. 不分享密码：避免与他人分享密码，包括朋友、家人或同事。每个人应该有自己的独立账户和密码。

9. 及时更新软件：保持操作系统、浏览器和安全软件的更新。这有助于防范恶意软件和安全漏洞。

10. 定期检查账户活动：定期检查账户活动，查看是否有异常登录或未经授权的访问。及时发现问题，有助于迅速采取应对措施。

11. 教育自己：了解有关密码安全和网络安全的最佳实践，保持对潜在威胁的警觉。

通过采取这些措施，个人可以提高口令的安全性，减少被不法分子滥用的风险。