密码管理器学术报告

陈霖婕 2020102398 李婉晴 2020102390

摘要：本报告介绍了密码管理器的概念、功能和安全性，并探讨了密码管理器在密码管理和安全性方面的优势和挑战。通过综合分析现有的密码管理器，提出了改进和未来研究的建议。

## 1.引言

### 1.1背景介绍

密码管理器的发展可以追溯到上世纪90年代，当时人们开始意识到密码管理的重要性，并开始研究和开发相关的解决方案。最早的密码管理器是作为独立的桌面应用程序提供的，但随着移动设备的普及，密码管理器也逐渐发展成为跨平台的应用程序，支持多种设备和操作系统。

如今，密码管理器已成为个人和企业信息安全的重要工具。它们不仅能够安全地存储和管理密码，还提供了自动填充密码、生成强密码、同步和备份密码等功能，极大地提高了用户的密码安全性和使用便利性。

然而，密码管理器也面临一些挑战，如主密码的安全性、云同步和备份的隐私保护等问题。因此，密码管理器的研究和改进仍然是一个重要的课题，以提高其安全性和用户体验。

### 1.2研究问题和目的

在当今数字化时代，人们需要管理和使用大量的密码来保护个人和机密信息的安全。然而，由于密码的复杂性要求和数量的增加，人们往往难以记住所有的密码，导致使用弱密码、重复密码或将密码写在纸上的不安全做法。这为黑客攻击和身份盗窃提供了机会。

为了解决这个问题，密码管理器应运而生。现在市面上已经有各种各样的密码管理器，但我们还是会经常遇到类似这样的问题：

1. 那么多密码怎么记得住？
2. 如何在不安装密码管理器的情况下访问父母计算机上的密码？
3. 在没有安装任何应用程序的情况下，如何在手机上访问密码？

所以我们想寻找一个解决方案来解决这些问题，设计出了这款密码管理器，诀窍是计算密码而不是生成和存储随机密码

## 2.密码管理器概述

### 2.1定义和功能

密码管理器是一种软件工具，旨在帮助用户管理和保护他们的密码。它们提供了一个集中存储和组织密码的平台，用户可以将所有的密码保存在一个安全的数据库中，并通过一个主密码或生物识别身份验证来访问密码管理器。

密码管理器的主要功能有：

（1）密码存储和加密：密码管理器可以安全地存储用户的各种密码，如网站登录密码、银行账户密码、社交媒体密码等。这些密码通常会被加密，以确保只有授权的用户能够访问和使用它们。

（2）密码生成器：密码管理器通常还具有密码生成器功能，可以生成强密码，以增加用户账户的安全性。这些生成的密码通常包含随机的字母、数字和特殊字符，且具有一定的长度。

（3）多平台使用：密码管理器通常支持多设备同步，使用户能够在不同的设备上访问和使用他们的密码和敏感信息。这样用户可以在电脑、手机、平板等设备上同步更新和使用密码。

1. 密码更新：选项字段集中计数器字段的用途，增加它，将获得一个新密码。

### 2.2密码管理器的分类

如今的密码管理器大致可以分为两大类。第一类是由浏览器供应商提供的，作为浏览器的插件，在用户访问登入网页时自动记录用户的账户和密码并在用户下次登陆时自动填充。例如，最受欢迎的五种浏览器：Internet Explorer，Firefox，Google Chrome，Safari和Opera，均有其插件形式的密码管理器。从易用性来看，插件形式的密码管理器能自动记忆和填充账号和密码，省去了用户查找密码的麻烦，并且全程用户不需要复制密码，避免了被记录剪贴板的攻击获取密码。第二类是由第三方供应商提供，作为一个独立的应用程序，例如KeePass、Password Safe、LastPass、1Password等，其中又可细分为基于本地的和基于云的密码管理器。它们在用户的设备上独立运行，用户在需要使用密码时打开应用进行查询。应用程序形式的密码管理器则能记忆更多的密码，不受浏览器使用资源的限制，能调用更多的系统资源，执行更复杂的加密，并且功能更为强大。目前一些知名公司推出的密码管理器也陆续支持了多平台多形式，结合插件和应用程序，甚至提供网页版简化用户查找密码的程序。

### 2.3密码管理器的工作原理

密码管理器用户需要注册一个密码管理器账户，并设置一个主密码。主密码是访问密码管理器的唯一凭据，因此它应该是强密码且不易被猜测。

#### 2.3.1密码存储和加密

用户可以通过密码管理器添加和保存他们的密码和敏感信息。密码管理器会将这些数据进行加密，通常使用高级加密算法如AES（高级加密标准）来保护数据的安全性。加密后的数据会存储在本地设备或云服务器上，取决于密码管理器的类型。

#### 2.3.2密码生成器

密码管理器通常还提供密码生成器功能，用于生成强密码。用户可以根据自己的需求设置密码的长度和复杂度，密码生成器会随机生成一个符合要求的密码。这样可以帮助用户创建更安全的密码，避免使用弱密码或重复使用密码。

安全共享：密码管理器允许用户安全地共享密码和敏感信息给其他人，如家庭成员、同事或团队成员。共享的密码可以通过加密的方式传输，并设置权限以控制其他人的访问范围。

### 2.4密码生成过程

密码管理器的密码生成基于纯函数，经过100000次PBKDF2的迭代后，根据配置项信息处理生成的哈希值（即长度、小写字母、大写字母、数字、特殊字符）。如下图所示：

options

master password

username

site

哈希值

单个规则的字符集

所有规则的字符集

字符集

（里面含有每个规则的一个字符）

含有特定规则的密码

（但可能没有全部规则都满足）

密码

（符合所有规则）

## 3密码管理器的优势

### 3.1提高密码安全性

#### 3.1.1生成强密码

密码管理器通常具有密码生成器功能，可以生成随机、复杂且强壮的密码。这些密码通常包含大写字母、小写字母、数字和特殊字符，并具有一定的长度。相比于用户自行创建的密码，密码管理器生成的密码更难以被猜测或破解。

#### 3.1.2防止密码重复

密码管理器可以记录用户在不同网站和应用程序中使用的密码，并自动填充相应的登录信息。这样用户就不需要重复使用相同的密码，从而减少了密码泄露和风险。

#### 3.1.3加密存储

密码管理器通常会使用强大的加密算法，如AES（高级加密标准），对用户的密码和敏感信息进行加密存储。这样即使数据被盗或泄露，黑客也很难解密和获取用户的密码。

#### 3.1.4主密码保护

用户在使用密码管理器时需要设置一个主密码，用于访问和解锁密码管理器。这个主密码应该是强密码，并且只有用户自己知道。密码管理器会使用主密码对用户的密码数据库进行加密和解密，确保只有授权的用户可以访问密码数据。

### 3.2方便的密码管理

密码管理器可以让用户更轻松、更便捷地管理和使用他们的密码，减少了记忆负担，用户可以通过密码管理器更高效地管理和保护他们的密码和敏感信息。具体来说，主要包括以下几个方面：

* 单一登录：用户只需要记住一个主密码，即可访问和使用密码管理器中保存的所有密码和敏感信息。这样用户不再需要记住大量的密码，避免了因为密码遗忘而无法登录的尴尬和困扰。
* 密码生成器：密码管理器通常具有密码生成器功能，可以帮助用户生成强密码。用户可以根据自己的需求设置密码的长度和复杂度，密码生成器会随机生成一个符合要求的密码。这样用户无需费心思考和创建密码，轻松生成安全的密码。

### 3.3可靠性

* 源代码可审计：无法根据源代码破译出密钥
* 无需同步：在密码管理器输入相同的内容，就会生成同一个密码
* 多平台使用：密码管理器通常支持多设备同步，使用户可以在不同的设备上访问和使用他们的密码和敏感信息。用户可以在电脑、手机、平板等设备上同步更新和使用密码，提供了更大的灵活性和便利性。

## 4.密码管理器的挑战

互联网时代下，随着各种应用与服务的指数级增长，人们所持有的账户与密码也越来越多。为了安全高效地管理大量的账户与密码等隐私信息，密码管理器逐渐被广泛应用。一个安全的密码管理器可以在每个网站上为用户自动生成、填写并保存强（随机）密码，用户只需要记住一个主密码即可访问他们的隐私信息。然而，防御与攻击总是相伴相生，因此攻击者们也将目标从攻破单一的密码转向了密码管理器。一旦密码管理器的安全性无法保障，则用户的大量隐私信息将遭到泄露，其后果更加严重。而目前的密码管理器还不能为用户提供充分的保护。近年来，各种商业密码管理器中都经常发现漏洞。在这样的情况下，研究并提高密码管理器的安全性有着十分重要的意义。

### 4.1安全性考虑

在设计和使用密码管理器时，我们做了以下安全性考虑，如：

强密码生成：密码管理器应该具备一个强密码生成器，能够生成随机、复杂且不易猜测的密码。这样可以避免用户使用弱密码或常见密码。

数据加密：密码管理器应该使用强大的加密算法对保存的密码进行加密。这样即使密码管理器的数据库被盗，黑客也无法轻易获取到明文密码。

主密码安全性：密码管理器通常需要用户设置一个主密码，用于解锁和访问密码数据库。这个主密码应该是复杂且不易猜测的，同时用户应该避免使用与其他账户相同的密码。

用户教育和意识：密码管理器的用户应该接受相关的教育和培训，了解密码管理的最佳实践和安全风险。用户应该意识到他们的主密码的重要性，并采取措施保护其安全。

### 4.2主密码保护

密码管理器的安全性依赖于用户设置的主密码。如果用户选择了一个容易被猜测或破解的主密码，那么整个密码管理器的安全性就会受到威胁。因此，用户需要选择一个强大和独特的主密码，并定期更换以提高安全性。

### 4.3 数据泄露风险

密码管理器的数据库中的所有密码配置文件都是以明文方式存储的，如果数据库被非法分子入侵，将会导致数据库数据泄露。

## 5.密码管理器的安全性分析

### 5.1 密码加密和存储

密码管理器的密码加密和存储安全性是确保用户密码和敏感信息的保密性和完整性的关键方面，密码加密和存储的安全性主要体现在加密算法的选择、密钥管理、数据库加密等方面。

密码管理器应该使用强大的加密算法来对用户密码进行加密。常见的加密算法包括AES-256、Twofish和ChaCha20等。这些算法具有良好的安全性和广泛的应用，可以有效地保护用户密码的机密性。密钥管理方面密码管理器需要使用一个密钥来加密和解密用户密码。这个密钥应该是长且随机的，以增加破解的难度。密码管理器可以使用密码导出函数(PBKDF)来从用户提供的主密码生成密钥。PBKDF应该使用适当的迭代次数和盐值来增加攻击者破解的难度。数据库加密方面密码管理器的数据库应该进行加密，以防止未经授权的访问。数据库加密可以使用全盘加密或文件级加密来实现。全盘加密会对整个数据库进行加密，而文件级加密会对每个密码条目进行单独的加密。无论采用哪种方式，都需要确保数据库的加密密钥安全存储，并且只有在用户提供正确的主密码时才能解密。

### 5.2 访问控制和权限管理

密码管理器的访问控制和权限管理是确保只有授权用户能够访问和管理密码的关键。通过有效的用户身份验证、角色和权限管理等措施，可以提高密码管理器的访问控制和权限管理的安全性。

实施有效的用户身份验证机制，能确保只有授权用户能够访问密码和敏感信息。常见的身份验证方式包括主密码、指纹识别、面部识别、硬件密钥等。密码管理器应该对用户提供的身份验证信息进行验证，并且需要强制用户输入正确的身份验证信息才能访问密码。且密码管理器应该支持角色和权限管理，以控制用户对密码和敏感信息的访问权限。管理员可以分配不同的角色和权限给不同的用户，以限制他们的访问范围和操作权限。例如，管理员可以设置只读权限，让用户只能查看密码而不能修改或删除。

### 5.3 安全审计和监控

安全审计和监控也是确保密码管理器的运行和使用过程中的安全性的重要方面，通过安全审计和监控安全性分析，密码管理器系统能够及时发现和应对潜在的安全问题，保护用户密码和个人信息的安全。如对用户身份验证安全性审计，对密码管理器的用户身份验证机制进行审计，包括密码强度要求、多因素身份验证、密码重置过程等。登录和访问监控，监控用户登录和访问密码管理器的行为，及时发现异常登录或访问行为，如多次失败登录尝试、异常IP地址等。

## 6 结论和期待

密码管理器在我们的日常生活中发挥着重要的作用，省去了记忆大量密码的脑力劳动时间，又保证了用户使用时的方便快捷和充分的密码安全，给日常生活带来了很大的便利。密码管理器虽然改进了之前普通应用密码设置的不足，但也存在着很多不足。例如密码管理器主密码被破解的风险，密码算法的变换不够灵活，难解的算法储存将是之后提升的方向。未来研究方向还可以探索密码管理器与其他技术的结合，如人工智能、区块链等，以提高密码管理器的安全性、便利性和可信度。此外，随着密码管理器的普及和应用场景的不断扩展，还可以研究密码管理器在企业、物联网等领域的应用和安全性挑战。