**一． 传统身份验证方案的可能风险**

**1. SFA（单因素身份验证）**

* **主要风险：凭据泄露**
  + 传统的用户名+密码认证方式容易受到**暴力破解、字典攻击、凭据填充攻击**（攻击者利用已泄露的凭据尝试登录）等威胁。
  + 用户可能会**重复使用密码**，导致一个平台的数据泄露影响多个账户。
  + **钓鱼攻击**可能诱骗用户泄露密码。
  + 如果密码存储方式不安全（如明文存储、哈希方式不安全），黑客攻破数据库后可直接获取用户密码。

**2. MFA（多重身份验证，包括2FA等）**

* **主要风险：二要素劫持**
  + **短信验证码劫持**（SIM交换攻击、短信拦截）。
  + **OTP（一次性密码）钓鱼**：黑客创建伪造网站，骗取用户输入OTP。
  + **应用程序劫持**：如果二步验证码依赖于移动应用（如Authenticator），恶意软件可以窃取代码。
  + **中间人攻击（MITM）**：攻击者拦截用户登录请求，并同时登录真实网站，骗取验证码。

**3. 免密认证——生物识别技术**

* **主要风险：生物数据泄露**
  + **生物特征信息（如指纹、虹膜、人脸数据）一旦泄露，无法更改**，不同于密码的可重置性。
  + **假冒和欺骗攻击**：3D打印指纹、深度伪造（Deepfake）技术可骗过部分生物识别系统。
  + **存储安全风险**：如果生物数据未加密存储或存储在不安全的服务器上，被攻击者获取后可能被滥用。
  + **回放攻击**：黑客可利用截取的生物特征数据进行身份冒充。

**4. 自适应身份验证（基于风险的身份验证，RBA）**

* **主要风险：数据泄露与滥用**
  + 需要收集大量的**用户行为数据（如设备信息、IP地址、位置信息、行为模式）**，一旦泄露，可能被攻击者用于追踪用户身份或进行精准攻击。
  + **误报或误判风险**：如果RBA算法不够精确，可能会错误地降低安全性或阻止合法用户访问。
  + **数据传输拦截**：如果用户行为数据未加密传输，可能被黑客监听并利用。
  + **模型攻击**：如果攻击者可以分析和推测RBA的判定标准，可能会绕过系统检测（例如模仿正常用户行为以降低风险评分）。

|  |  |  |
| --- | --- | --- |
| 方案 | 主要风险 | 可能的措施 |
| SFA（单因素身份验证） | 密码泄露、钓鱼攻击、凭据填充 | 采用强密码策略、密码管理器、定期更换密码、启用MFA |
| MFA（多重身份验证） | 短信拦截、钓鱼、OTP劫持 | 避免使用短信验证码，推荐基于硬件的OTP（如U2F）、生物识别或App-based OTP |
| 免密认证（生物识别） | 生物数据泄露、伪造攻击、存储安全 | 采用加密存储、活体检测、基于设备本地存储（如Secure Enclave） |
| 自适应身份验证（RBA） | 用户行为数据泄露、算法绕过 | 强化数据加密，定期优化算法，结合MFA增强安全性 |

**二．金融机构身份验证和授权的漏洞总结**

**1. 关键信息保护措施不到位。**

金融机构用户信息注册将产生海量关键信息，属于敏感数据，比如照片、视频、身份信息、电话号码等。这些关键信息在存储、应用等环节中应最大限度保护隐私安全。网络黑客、恶意人员通过窃听、钓鱼等技术手段盗取、篡改关键信息进行非法行为。

1. **关键技术措施不完善。**

恶意人员利用自身账户信息合法地进入金融机构业务系统内，并在之后获得授权码。当合法用户通过授权请求资源访问时，恶意人员会向合法用户伪造一个成功的授权请求，并用他以前收到的授权代码替换授权代码，并将其发送给合法用户。合法用户的身份账户被绑定于恶意人员的访问指令上；同时，恶意人员的身份账户也将与合法用户绑定。可以使用CSRF攻击来控制合法用户金融机构业务系统的账户，而无需知道受害者真正的用户名和密码。

在金融机构的授权过程中，恶意人员通常会重放授权码。合法用户同意授权后，身份验证服务器将发送一个授权码进行响应。恶意人员将拦截此过程，然后手动向金融机构业务系统的重定向地址发出授权代码。这将触发客户端的授权码交换机制。金融机构业务系统错误地将恶意人员视为身份验证服务器端进行响应。

服务提供商经常忽略检查重定向地址是否被篡改，从而导致授权码泄漏。中间人攻击其具体方式通常为恶意篡改授权码的重定向地址。主要方式有三种：一是基于云服务或云存储的中间人攻击。通常情况下这些服务不会要求每次使用服务的时候都要重新登录，因为你验证后，它会在你的本地系统上保留会话令牌，如果恶意人员获取了你的会话令牌，就能访问你的账户，并盗取你的账户数据。二是基于浏览器的中间人攻击。恶意人员会诱导你下载木马（Trojan）。一旦你访问银行网站的时候，恶意软件就会向你访问的网页注入新的HTML代码，看起来和真正的网页一样。三是基于移动设备的中间人攻击。主要针对智能手机上进行的转账付款等操作。MiTMO专注攻击移动交易验证码以及其它各种类型的交易验证码，给身份验证系统带来了很大挑战。

1. **安全机制不健全。**

一是业务系统架构存在安全漏洞。在金融机构业务系统设计时，网络结构、硬件存在缺陷或冲突，业务流程存在漏洞，选择的信息技术不够成熟、完善，存在安全隐患和出错率，从而影响业务系统运行的稳定性和可靠性，给恶意人员带来可乘之机。

二是用户培训不到位。用户需要具备一定的操作技能，如果操作不熟练，就有可能产生误操作导致损失；用户的安全防范意识不强，泄露机密信息，或被犯罪分子利用短信、邮件、电话、钓鱼等方式骗取关键信息，导致损失。

**三．身份信息泄露的案例**

**SFA 相关案例**

* **领英数据泄露事件**：

2021年领英发生多起信息泄露事故。“近日，领英（LinkedIn）6亿用户个人信息再次出现在黑客论坛上被售卖。南都记者注意到，四个月内，领英用户个人信息已被兜售三次，数量分别为5亿条、7亿条以及6亿条。”

领英系微软旗下的拥有7亿多用户的职场社交平台，许多用户在此平台上公开自己的教育背景、从业经历等息。据网络安全类媒体CyberNews报道，当地时间7月10日，领英6亿条个人信息出现在某黑客论坛上，正在以不公开的价格出售。被出售的具体用户信息包括：领英用户id、姓名、电子邮件地址、电话号码、跳转到其他社交媒体的链接、个人资料URL、性别、出生日期、位置信息、从业经历等工作相关资料。对此，领英曾于当地时间6月26日回复媒体时强调，这并非领英的数据泄露事件，而是**公开数据的抓取**。网络钓鱼攻击者可以利用抓取到的联系方式，来实施自动呼叫、发送垃圾邮件、社会工程攻击，从而诱导用户透露更多的个人信息及财务信息。也正因为如此，许多网站应用程序才会使用相关工具防止机器人和黑帽黑客恶意收集数据。

* **雅虎数据泄露门**：

2016年12月14日，雅虎宣布该公司有10亿多用户账号于2013年被黑客窃取。此次被盗的资料中可能包括姓名、联系方式、密码以及安全问答等内容，事件导致该股跌幅超过6%。雅虎还披露该公司在2014年因为类似的攻击泄露了5亿账号资料。黑客通过攻击雅虎系统，窃取了用户的姓名、电子邮箱、电话号码、出生日期等信息，甚至可能包括加密后的密码。部分用户**仅依靠密码作为身份验证方式，没有额外的安全措施，导致信息安全面临极大风险**。

* **2013年Adobe数据泄露**

“本月初Adobe首次在官方博客承认约有290万Adobe用户数据被黑客窃取，包括用户密码、信用卡信息和邮件地址等重要隐私数据。

但近日Adobe公布的最新数据让所有人吃惊，约3800万活跃用户数据被黑客获取，范围从之前的Adobe Acrobat、Reader等产品线扩大到Photoshop等图形设计产品用户。

安全博客KrebsOnSecurity在浏览部分失窃用户数据后发现，除了信用卡记录外，Adobe各条产品线的数以千万计的用户账户都已被泄露。上周末AnoNews.org曾发布一个3.8G的超大文件（users.tar.gz），内含超过1.5亿个包括用户名和加密密码的用户账户信息”[[1]](#footnote-0)

攻击方式：攻击者**通过钓鱼邮件或漏洞利用**（具体未公开）获取了Adobe开发服务器的访问权限。攻击者从Adobe的备份服务器中**窃取了未加密的数据库副本。**除用户数据外，Adobe旗下Photoshop、ColdFusion等产品的部分源代码也被窃取，并在暗网传播。

存储方式漏洞：本平台用户密码采用3DES（Triple DES）算法加密，但**未添加“盐值”（Salt）进行随机化处理**。同时用户的密码提示问题及答案（如“宠物名字”“出生城市”）以明文形式存储，极大降低了攻击者破解密码的难度。

后续：大量用户遭遇撞库攻击，攻击者利用Adobe泄露的密码尝试登录其他平台账户

* **2015年OPM泄露事件**

“美国联邦人事管理局(OPM)公布，在上个月美国联邦政府机构被黑客攻击后，有超过2150万美国人的资料被盗取，这比当初公布的数字多了近6倍。据报道，美国人事管理局当天发表的报告称：“调查小组非常确定，在上个月联邦的背景调查资料库被黑客袭击后，有约2150万美国人的包括社会安全号在内的敏感信息遭到泄露。”报告称，受影响者包括1970万涉及背景调查的政府雇员，以及180万上述政府雇员的家庭成员。” 人事管理局还指出，黑客有可能盗取了几乎所有在2000年后所进行的背景调查的数据。

攻击方式：**承包商账号**被钓鱼攻击，黑客盗走了大量OPM人员填写的SF-86表格涉及个人过往和现在的大量隐私信息，包括社会安全码、出生年月、居住地址、教育经历、家庭成员和个人财务信息等。

存储方式漏洞：后台管理系统仅通过安全问题验证身份，这也导致黑客X2在后续冒充承包商进入系统进行二次盗窃

* **2019年canva数据泄露**

“自称 GnosticPlayers 的黑客声称窃取了澳大利亚网站 Canva 的 1.39 亿用户数据。Canva 是一个非常受欢迎的平面设计服务，Alexa 排名在 200 以内。黑客窃取的数据包括了用户名字、真名 、电邮地址、城市国家信息，其中 6100 万用户有哈希密码，其他用户的信息还有用于登陆的 Google 令牌。有 7800 万用户使用了 Gmail 地址。Canva 证实它的数据库遭到非法访问，表示尚未发现账号被入侵，出于谨慎考虑它已经鼓励用户更改密码。”

攻击方式：黑客利用第三方服务漏洞（MongoDB配置错误）入侵数据库，导致1.39亿用户电子邮件地址、用户名等详细信息被披露

存储方式漏洞：仅依赖密码认证，且部分用户**使用弱密码**（如“123456”），哈希被暴力破解

* **2020年推特比特币诈骗事件**

“2020年7月15日，多位美国名人政要的推特账户遭黑客入侵，发布诈骗话术和比特币地址，而有的针对区块链账号的则发布了钓鱼网站。

攻击方式：攻击者通过暗网购买或社工手段获取Twitter员工的个人身份信息，并将号码转移到攻击者控制的SIM卡，通过此新SIM卡接收Twitter后台系统的短信验证码

存储方式：Twitter员工后台系统仅依赖短信验证码进行登录，**未启用多因素认证（MFA）或硬件密钥**。短信验证码通过运营商网络传输，易被SIM交换或SS7漏洞拦截。员工账号未强制要求使用强密码，部分账号密码可能已在外泄密码库中流通（如通过撞库攻击）

**MFA 相关案例**

* **Twilio漏洞致Okta一次性MFA密码泄露**：

云端通讯平台Twilio在2022年8月7日坦承遭到黑客入侵，黑客通过钓鱼短信取得了Twilio员工的登陆凭证，并窃取了客户数据，而采用Twilio服务进行电话号码认证的Signal则表示，约有1900名用户受到Twilio黑客事件的波及。继Signal之后，另一个被Twilio黑客事件殃及的受害者，专门提供身份认证与存取管理服务的Okta指出，黑客盗走了Twilio员工的凭证，用以存取了Okta客户的电话号码，以及通过Twilio服务传送的一次性密码。

根据Okta的说法，该公司有各种认证机制供客户选择，包括以**短信来递送一次性密码**，并借由两家第三方服务来提供**短信身份验证服务**，Twilio即为其中一家。而在Twilio员工的凭证遭骇之后，调查发现黑客通过Twilio控制台存取了Okta的客户服务，有小部分Okta用户的电话号码，以及包含一次密码的短信遭到黑客存取。

Okta进一步分析了黑客的足迹与受影响的用户，显示黑客通过Twilio控制台搜索了38组电话，而它们几乎都隶属于同一个组织，意味着这是个极有针对性的攻击。 Okta推测，黑客应该事先就通过其它的钓鱼活动取得了这些用户的登陆凭证，并触发了基于短信的多因素认证，企图借由入侵Twilio系统找到相关的一次性密码。而该一次性密码的有效期间为5分钟。

* **微软MFA安全漏洞**

“IT之家 12 月 15 日消息，安全公司 Oasis 发现微软 MFA 多重验证系统中存在一项 AuthQuake 重大漏洞。允许黑客通过穷举暴力破解验证码绕过验证流程从而访问用户账户，安全公司称，这一漏洞如果遭黑客利用，可能带来广泛影响。

IT之家参考报告获悉，这一漏洞主要涉及微软多重认证的账号验证器动态码系统，在正常情况下，如果用户要在 PC 网页端登录微软账号，需要通过手机上绑定了微软账号的验证器 App 生成 6 位动态验证码（OTP），在时效内输入以完成认证。如果用户连续输入错误超过 10 次，系统将暂时禁止用户登录。

攻击方式：黑客如果使用大型计算机，直接在账号系统验证手机 App 上动态验证码的这一小段时间中通过快速生成新会话（Session），在短时间内**穷举尝试所有可能的验证密码排列组合（共计 100 万种），即可成功暴力破解认证机制**，接管用户账号

存储方式漏洞：该公司在设计验证手机 App 验证码时考虑到相关动态密码每 30 秒就会刷新一次，而认证系统与用户访问时间实际存在延迟，因此延长了验证码的有效时长，最长可达 3 分钟。这一设计给黑客提供了暴力破解机会。

* **2022年LastPass MFA绕过事件**

“据Bleeping Computer报道，LastPass当地时间12月22日透露，攻击者在今年早些时候使用2022年8月事件中窃取的信息侵入其云存储，窃取了客户的加密密码库数据。

此前，11月30日，该公司首席执行官曾公开承认遭黑客攻击致数据泄露，但他表示黑客仅获得了部分客户的关键信息，客户的密码仍被安全加密。这是一年内LastPass发生的两次因云存储漏洞而发生的安全事件。该公司透露，8月事件的攻击者在被驱逐之前，对其内部系统访问了四天。”

攻击方式：攻击者通过入侵员工家用电脑，窃取其云存储（如OneDrive）中保存的LastPass MFA恢复密钥。并利用恢复密钥和员工弱密码解密企业密码库，获取客户加密保险库的密钥

存储方式漏洞：LastPass允许员工将MFA恢复密钥存储在未加密的云盘中。员工主密码未强制使用复杂组合，易被暴力破解

* **Cisco Duo 第三方数据泄露暴露短信 MFA 日志**：

Cisco Duo 的一个处理短信和网络电话多因素认证 (MFA) 消息的供应商在 2024 年 4 月受到**钓鱼攻击**，威胁分子**获得员工证书后进入电话供应商系统**，下载了 2024 年 3 月期间特定多帐户相关的短信日志和网络电话管理局的消息日志，其中包含雇员的电话号码、载体、位置等可用于定向钓鱼攻击的数据。

**免密认证 —— 生物识别技术相关案例**

* **2019年Suprema数据泄露**

“据TheVerge网8月14日消息，网络公司vpnMentor研究人员在网络上发现了韩国Suprema公司Biostar 2安全系统的漏洞，超过100万人的指纹数据、面部识别信息和未加密的用户名及密码遭到泄露。泄露的数据共包含2780万条记录，总容量达23千兆字节，这些信息在一个可公开访问的数据库中被发现。Biostar 2是世界各地组织用于保护商业建筑的安全系统，其客户包括各地政府、银行及警察部门，漏洞可使黑客篡改用户安全凭证，从而进入被保护的建筑。目前，Suprema公司已完成漏洞修复，尚没有任何证据表明这些数据是否被恶意使用”

攻击方式：安全研究人员发现了一个名为BioStar 2的安全漏洞，这是一个由Suprema开发的基于网络的生物识别身份验证平台。研究人员能够无限制地访问数百万条记录，包括未加密的指纹和面部识别数据

存储漏洞：数据库中的生物识别信息以及用户名和密码**均以明文形式存储**，这极大地增加了数据泄露的风险

* **2019年美海关合作伙伴数据泄露**

“据 Buzzfeed 报道，近日，美国海关与边境保护局（CBP）发布公告，在未经联邦机构授权的情况下，其分包商私自转移了识别旅客及车牌图像的边境巡逻数据库。在此过程中，分包商的网络遭到黑客的“恶意网络攻击”，导致数据库内出入境旅客的照片泄露，具体涉及近一个半月以来通过入境口岸特定车道的车辆图像。

攻击方式：第三方承包商未能妥善保护CBP提供的用于旅客面部识别的照片，导致这些照片被黑客窃取

存储漏洞：**缺乏制度与标准上的规范**。原则上，此类数据无法流入外包公司内部，因为目前所有服务以私有云方式部署在使用方内网，训练算法也只能通过脱敏数据进行，无法追溯敏感信息。

1. 来自IT经理网《3800万Adobe用户数据和Photoshop源代码泄漏》 [↑](#footnote-ref-0)