登陆密码大规模泄露案例分析

付政烨[1)]

[1)](南开大学 网络空间安全学院, 天津市 中国 300071)

摘 要 本文详尽解析了2011年CSDN密码泄露事件的背景与成因，并提出了切实可行的预防措施。CSDN，作为中国最大的中文IT知识服务平台，在2011年12月遭遇黑客攻击，导致600万用户的登录名和密码被泄露，继而波及其他多家知名网站，影响范围达5000万用户。为杜绝此类事件再次发生，本文提出了几项关键措施。首先，实施零信任安全架构，确保所有访问请求都经过严格的身份验证和授权，从根本上颠覆传统的信任模型。其次，采用强加密算法如bcrypt和Argon2存储密码，以增强密码数据的安全性，避免因明文存储带来的巨大风险。最后，定期进行安全审计和渗透测试，通过全面评估系统安全状态、识别潜在漏洞并实施修补计划，提升整体防御能力。

关键词 密码泄露；系统漏洞；零信任安全架构；强加密算法；安全审计

Case Analysis of Large-Scale Password Leaks

Zhengye FU[1)]

[1)](College of Cyber Security, Nankai University, Tianjin 300071, China)

Abstract .

This article provides a comprehensive analysis of the background and causes of the 2011 CSDN password leakage incident and proposes practical preventive measures. CSDN, the largest Chinese IT knowledge service platform, was hacked in December 2011, leading to the leak of login names and passwords of 6 million users. This breach had a cascading effect, subsequently affecting multiple well-known websites and impacting a total of 50 million users. To prevent such incidents from recurring, this article outlines several key measures.Firstly, implementing a zero-trust security architecture is crucial. This model ensures that all access requests undergo strict identity verification and authorization, fundamentally overturning the traditional trust model that often assumes internal networks are secure. Zero-trust architecture treats every access attempt as a potential threat, requiring continuous verification.Secondly, the adoption of strong encryption algorithms for password storage is vital. Algorithms such as bcrypt and Argon2 significantly enhance the security of password data by making it computationally expensive for attackers to crack the passwords. This approach mitigates the significant risks posed by plaintext storage, where passwords can be easily compromised if accessed.Lastly, conducting regular security audits and penetration testing is essential for maintaining robust security. These practices involve a thorough assessment of the system's security status, identifying potential vulnerabilities, and implementing remediation plans. Security audits help organizations understand their current security posture, while penetration testing simulates real-world attacks to uncover weaknesses that might not be detected otherwise.By adopting these measures, organizations can significantly enhance their defense capabilities, protect sensitive user data, and reduce the likelihood of large-scale security breaches. This proactive approach to security management not only safeguards user information but also strengthens overall trust in the organization's commitment to data protection.

Keywords password leakage; system vulnerabilities; zero-trust security architecture; strong encryption algorithms; security audit

最终修改日期：2024年6月6日.付政烨，男，2003年生，主要研究领域为数据安全.E-mail:2113203@mai.nankai.edu.cn 第1作者手机号码:15719340667, E-mail:2113203@mai.nankai.edu.cn

1 引言

随着互联网的迅猛发展，信息安全问题日益凸显，严重威胁着用户的隐私和数据安全。2011年，CSDN密码外泄事件震惊了整个互联网行业，600万用户的登录名和密码被黑客公开，随后天涯社区、开心网等多家知名网站的用户信息也相继泄露，暴露了企业在信息安全管理和技术防护方面的巨大漏洞。本论文将对CSDN密码外泄事件进行详细的案情描述和原因分析，并提出相应的预防措施，以期为类似事件的防范提供参考和借鉴。

2 CSDN密码外泄门案情描述

CSDN是中国最大的中文IT知识服务集团。2011年12月21日，有消息指出该系统遭到黑客攻击，导致600万用户的登录名和密码被泄露。随后，天涯社区、开心网等十余家国内知名网站的近5000万用户信息也被黑客公开，引发了广泛的互联网用户恐慌。

根据国家互联网应急中心（CNCERT）的统计数据，公开的疑似泄露数据库多达26个，涉及账号和密码信息共计2.78亿条。警方调查显示，黑客于2010年4月通过利用CSDN网站漏洞非法侵入服务器，窃取了用户数据。北京警方对此事展开调查，发现CSDN未能落实国家信息安全等级保护制度，安全管理制度和技术保护措施存在严重不足。北京市公安局因此向CSDN运营公司提出整改要求，并对其进行了严厉的行政处罚。这也是国内首次因未落实信息安全等级保护制度而开出的罚单。

杭州安恒信息技术公司提供的审计报告显示，CSDN网站存在开源系统漏洞、已停用系统、应用程序漏洞及系统后台认证等四大安全风险。在后期CSDN对该事件的声明中称，其早期使用明文密码存储用户数据，这是为了与第三方聊天程序整合验证所带来的设计选择。然而，这一安全隐患在后续的开发过程中未得到及时处理，直至2009年4月才开始对密码进行加密处理。然而，部分旧的明文密码并未完全清理，直到2010年8月底才完成全部明文密码的清理工作。这些问题是导致大量用户信息泄露的主要原因。

3 密码泄露原因分析

3.1 系统漏洞维护失责

CSDN网站使用了存在漏洞的开源系统，这些漏洞可能没有及时得到修补。开源系统因其灵活性和低成本受到广泛使用，但同时也带来了安全隐患。如果没有及时更新和修补已知的安全漏洞，开源系统就容易成为黑客攻击的目标。在本案中，黑客正是通过这些未修补的漏洞绕过了系统的安全措施，直接访问了数据库，获取了大量敏感信息。开源系统的安全依赖于社区和开发者的持续维护，但企业在使用这些系统时，尤其应承担起及时跟踪和修补漏洞的责任，以确保系统的安全性。显然，CSDN在这一点上的做法是存在很大问题的。

此外，CSDN对停用的系统未进行彻底清理或隔离，这些系统仍然与现有系统存在连接。停用系统往往包含未修复的已知安全漏洞，并且由于其不再使用，通常缺乏定期的安全维护。这些老旧系统成为黑客利用的突破口，因其易被忽视的安全性，黑客能够通过它们入侵并获取系统的访问权限。未及时清理停用系统，使得这些漏洞长期存在，又进一步增加了安全风险。

3.2 明文密码存储

CSDN网站在其早期系统中采用明文密码存储用户数据，明文密码存储意味着用户的密码以未加密的形式存储在数据库中，这一做法极大地增加了安全风险。因为一旦黑客成功入侵服务器并获取数据库访问权限，他们能够直接读取用户的明文密码，无需任何额外的解密步骤。嫌疑人在2010年4月利用CSDN网站漏洞非法侵入服务器，获取了大量用户数据。这些数据中包含了大量未加密的明文密码，使得黑客能够轻松获取用户的真实密码，从而威胁到用户在CSDN平台上的账户安全。

用户在多个平台上使用相同密码是常见现象，主要是为了记忆方便。然而，这种习惯在CSDN数据泄露事件中暴露出极大的安全隐患。由于CSDN早期存储了大量明文密码，黑客在成功窃取这些密码后，可以利用“撞库”攻击方法，在其他平台尝试登录。如果用户在多个平台使用相同的登录凭证，黑客便可以通过这些泄露的明文密码，成功访问用户在其他平台的账户。此次CSDN泄露事件波及范围广泛，包括天涯社区、开心网等多个知名网站，总计约5000万用户的信息被公开，进一步凸显了明文密码存储的严重性。

明文密码存储不仅使得用户的密码信息处于危险之中，还可能导致其他敏感信息的泄露。黑客通过获取用户的密码，可以进一步访问用户在平台上的个人资料、通信记录、交易记录等敏感信息，造成更广泛的隐私泄露和安全风险。

3.3　安全管理制度缺失

CSDN在安全管理方面缺乏一套全面且严格的安全策略。这些策略应包括定期的安全评估、漏洞扫描、修补计划和应急响应预案等。缺乏这些策略会导致安全隐患无法及时发现和修复。此外，员工缺乏充分的安全意识培训，使他们难以识别和防范常见的网络攻击手段。培训的缺失使得员工在日常操作中容易忽视安全细节，从而增加了安全事件发生的风险。

4　预防措施

4.1　零信任安全架构

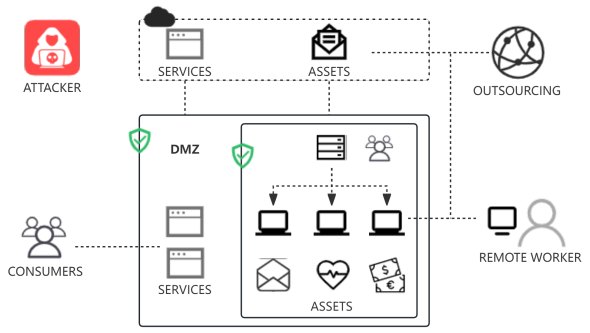

Fig. 1　零信任安全架构模型

零信任安全架构（ZTA）作为一种新兴的网络安全模型，其核心理念为“永不信任，始终验证”。传统的网络安全模型通常基于内部网络的信任假设，仅对外部威胁进行防范。而零信任架构则颠覆了这一传统假设，不再默认信任任何内部或外部网络，要求对所有访问请求进行严格的身份验证和授权。在实施零信任安全架构时，几项关键措施需要格外重视：

(1) **细粒度访问控制**：根据用户身份、设备、地理位置等信息，制定并执行严格的访问控制策略，确保每个用户只能访问其工作所需的最低权限资源。这种策略不仅有助于最小化安全风险，还能精确管理资源使用情况。

(2) **持续监控和分析**：利用先进的监控工具，对所有访问行为进行持续的监控和分析。通过及时发现异常活动和潜在威胁，能够更早地采取应对措施，防止安全事件的发生和扩散。

(3) **动态身份验证**：实施多因素认证（MFA）和动态身份验证机制，对每一个访问请求进行实时验证。这一措施确保只有经过合法身份验证的用户才能访问敏感数据和系统，从而大幅提升安全防护能力。

以零信任架构为基础，像CSDN这样的大型网站开发公司可以对所有访问行为进行严格控制，即便是内部员工也需要通过严格的身份验证才能访问数据库。这种方法不仅有效防止未授权访问，还能显著降低内部威胁，从而提升整体网络安全水平。

4.2　使用强加密算法存储密码

为了有效保护用户密码信息，采用强加密算法对密码进行存储是至关重要的。传统的明文密码存储方法存在严重的安全隐患，而现代加密算法则提供了更高的安全性。即使数据库遭到入侵，黑客也难以轻易获取到用户的密码。当前常用的强加密算法包括bcrypt和Argon2。

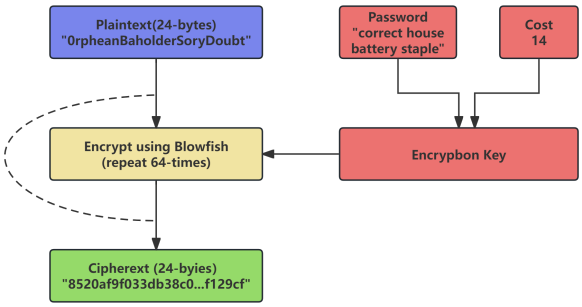

Fig. 2　bcrypt

bcrypt是一种专门用于密码加密的算法，它采用自适应哈希函数，可以根据硬件计算能力调整工作因子，从而增加破解难度。这一特性使bcrypt在应对不同计算环境时具有较高的灵活性和安全性。

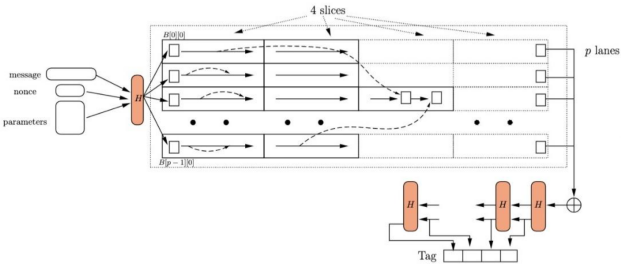

Fig. 3　Argon2

后者则被广泛认为是当今最安全的密码哈希算法之一。它具有较高的计算复杂性，并且具备防御并行攻击的能力，进一步增强了密码保护的有效性。不放设想一下，若CSDN早期系统采用了上述强加密算法来存储用户密码，即使数据库被黑客攻

破，黑客也难以直接获取用户的明文密码。这将显著降低密码泄露的风险，从而有效保护用户账户的安全。

4.3 定期安全审计和渗透测试

安全审计与渗透测试是保障信息系统安全的关键手段。通过安全审计，可以全面评估系统的安全状态，识别潜在的安全漏洞和风险；而渗透测试则模拟黑客攻击，主动寻找并利用系统中的安全漏洞，以验证系统的防御能力。主要步骤可以总结为：

(1) **识别和评估资产**：明确系统中的关键资产和敏感数据，评估其安全性和潜在风险。

(2) **漏洞扫描**：使用自动化工具对系统进行全面的漏洞扫描，发现已知的安全漏洞。

(3) **渗透测试**：模拟真实的黑客攻击，尝试利用发现的漏洞进行入侵，评估系统的防御能力，发现未被漏洞扫描工具检测到的潜在威胁。

(4) **修复和改进**：根据安全审计和渗透测试的结果，修复漏洞，优化安全策略，提升系统的整体安全性。

通过强制有关企业定期进行安全审计和渗透测试，可以及时发现和修补系统中的安全漏洞，从而大大降低黑客通过这些漏洞入侵系统的可能性。这不仅有助于有效防止类似密码泄露事件的发生，还能确保用户数据的安全。

5 总结与展望

CSDN密码外泄事件揭示了信息安全管理中的深刻漏洞，导致了大规模的用户信息泄露。通过对事件的剖析，我们深刻认识到，系统漏洞维护不力、明文密码存储以及缺乏有效的安全管理制度是导致安全事故的主要原因。展望未来，信息安全将成为保护用户权益的基石。全面而严格的信息安全管理不仅能有效防止类似密码泄露事件的发生，更能构筑起坚固的数字安全防线，为互联网用户营造一个安全、可信的网络环境。这一切将为信息时代的长久繁荣奠定坚实的基础。

参 考 文 献

[1] 糜苏赟. 从”CSDN密码库泄露事件”看计算机网络安全[J]. 电脑知识与技术, 2012(1X): 2. DOI: 10.3969/j.issn.1009-3044.2012.02.008.

[2] 刘欢, 杨帅, 刘皓. 零信任安全架构及应用研究[J]. 通信技术, 2020. DOI: 10.3969/j.issn.1002-0802.2020.07.028.

[3] Phiayura P, Teerakanok S. A comprehensive framework for migrating to zero trust architecture[J]. IEEE Access, 2023, 11: 19487-19511.

[4] Pereira T, Santos H. A security audit framework to manage Information system security[C]//Global Security, Safety, and Sustainability: 6th International Conference, ICGS3 2010, Braga, Portugal, September 1-3, 2010. Proceedings 6. Springer Berlin Heidelberg, 2010: 9-18.

[5] 徐红, 唐刚强. 数据安全与加密算法[J]. 企业技术开发, 2006, 25(9): 4. DOI: 10.3969/j.issn.1006-8937-B.2006.09.005.

[6] 常艳, 王冠. 网络安全渗透测试研究[J]. 信息网络安全, 2012(11): 2. DOI: 10.3969/j.issn.1671-1122.2012.11.001.

[7] Almeshekah MH, Gutierrez CN, Atallah MJ, 等. Ersatzpasswords: Terminating password cracking and detecting password leakage[C]//Proceedings of the 31st Annual Computer Security Applications Conference. 2015: 311-320.