Linnéuniversitetet
Kalmar Växjö

Report

FIDO-autentiseringens roll i lindring av identitetsstöld

Att flytta fokus från mänsklig sårbarhet till robust teknik

Author: Firas Moussa
Supervisor: Sergej Ivanov
Semester: HT23
Discipline: Technichal Information and Communication
Course code: 1DV510

Linnéuniversitetet
Kalmar Växjö

Abstract

This report assesses FIDO authentication's effectiveness in improving cybersecurity compared to traditional password-based systems. Amid rising data breaches and phishing threats, the demand for robust security solutions has surged. The analysis focuses on FIDO-UAF and U2F protocols, examining their ability to address security gaps and implementation challenges. Providing a comprehensive overview of FIDO authentication, the report discusses the balance between security and usability.

Keywords

Cybersecurity, FIDO-authentication, FIDO-UAF, FIDO-U2F, Biometric authentication, Two-factor authentication, Phishing-defence.

Sammandrag

Denna rapport bedömer FIDO-autentiseringens effektivitet för att förbättra cybersäkerheten jämfört med traditionella lösenordsbaserade system. I ljuset av ökande dataintrång och phishing-hot har efterfrågan på robusta säkerhetslösningar ökat. Analysen fokuserar på FIDO-UAF och U2F-protokollen, och undersöker deras förmåga att adressera säkerhetsbrister och implementeringsutmaningar. Genom att ge en övergripande översikt av FIDO-autentisering diskuterar rapporten balansen mellan säkerhet och användarvänlighet.

Nyckelord

Cybersäkerhet, FIDO-autentisering, FIDO-UAF, FIDO-U2F, Biometrisk autentisering, Tvåfaktorsautentisering, Phishing-motstånd.

Contents

1 Inledning

När det gäller cybersäkerhet är övergången från människocentrerade säkerhetsstrategier till teknikdrivna lösningar avgörande för att motverka dataintrång. Enligt Verizon involverar 74% av dataintrångsförsök den mänskliga faktorn. Majoriteten av dessa dataintrångsförsök blir lyckade genom identitesstöld [1]. Statistik från APWG (Anti-Phishing Working Group) visar att det tredje kvartalet av 2023 hade den tredje högsta kvartalsvisa totalen av dokumenterade phishing-attacker, med 1,286,208 rapporterade fall [2]. Dessa siffror understryker behovet av hållbara tekniska lösningar för att minska denna sårbarhet.

I en värld där teknologin ständigt utvecklas blir användarskapade lösenord alltmer osäkra som autentiseringsmetod. Användare tenderar ofta att skapa svaga lösenord som dessutom återanvänds över flera olika webbplatser och tjänster. Denna praxis är dock i förändring, då allt fler företag övergår från traditionell lösenordsbaserad autentisering till mer avancerade metoder [3].

I denna rapport undersöks vilken roll FIDO-autentisering (Fast Identity Online) spelar i denna övergång, med fokus på deras effektivitet när det gäller att minska antalet incidenter med stulna identitetshandlingar. FIDO-UAF (Universal Authentication Framework) och U2F (Universal 2nd Factor), som avancerade autentiseringsmetoder, erbjuder ett lovande alternativ till traditionella säkerhetsmetoder, som ofta är starkt beroende av mänsklig vaksamhet och är benägna att göra fel [3].

1.1 Syfte och frågeställningar

Syftet med denna rapport är att utvärdera varför FIDO-autentisering ska övervägas av företagsledningen jämfört med att bibehålla standard lösenordsautentisering. Genom att analysera FIDO-autentiseringens fördelar och utmaningar, syftar rapporten till att ge en djupare förståelse för dess roll i förbättringen av cybersäkerheten. Följande frågor besvaras för att ge en övergripande förståelse inom området:

- Varför är FIDO-autentisering en säkrare metod än lösenordsbaserad autentisering?
- Vilka faktorer hindrar företag från att implementera FIDO-autentisering

2 Resultat

I detta kapitel presenteras diverse säkerhetsfördelar med FIDO-autentisering jämfört med de traditionella lösenordsmetoder, dessutom de utmaningar som företag står inför vid dess implementering.

2.1 FIDO-autentiseringens säkerhetsfördelar

FIDO-UAF och U2F protokollen syftar på att eliminera problemen med den traditionella lösenordsautentiseringen genom fokus på användarvänlighet och ökad säkerhet. Protokollen skiljer sig signifikant från traditionell lösenordsautentisering genom en tre-stegs metod för att eliminera behovet av lösenord, vilket effektivt minskar sårbarheten för dataintrång. I denna process spelar servern, hårdvaran och användaren alla en kritisk roll. Serverinteraktion initierar inledningsvis en autentiseringsförfrågan. Detta steg säkerställer att begäran om inloggning är legitim och kommer från en betrodd källa. Hårdvaran, ofta i form av en säkerhetsnyckel eller ett mobilt enhet, verifierar användarens identitet. Detta görs genom en kombination av biometriska data, som fingeravtryck eller ansiktsigenkänning, och en PIN-kod. Denna tvåfaktorsautentisering förstärker säkerheten genom att kräva både något användaren har (hårdvaran) och något användaren känner till (PIN-koden). Slutligen fullbordas autentiseringsprocessen med användarens aktiva deltagande, vanligtvis genom att tillhandahålla biometrisk information eller ange en PIN-kod. Denna interaktion säkerställer att inloggningen är auktoriserad av den faktiska användaren [4, 5]. Nedan följer en figur som illustrerar inloggnings processen med FIDO-UAF:

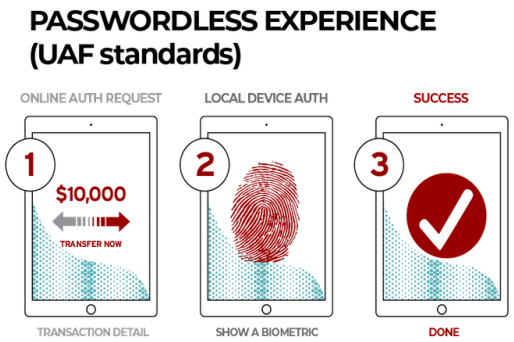

Fig. 1. FIDO UAF Standard[5]

Figur 1 illustrerar användarvänligheten med inloggningsprocessen genom FIDO-UAF. Genom att ha en registrerad enhet med biometriska uppgifter, kan användaren autentisera sig genom säkra mekanismer så som fingeravtryck, ansiktsigenkänning eller röstigenkänning [3]. Användaren behöver på detta sätt inte längre använda sig av traditionella användarnamn och lösenord [4].

FIDO-U2F erbjuder två-faktors verifiering för att förstärka säkerheten i system som använder användarnamn och lösenord. Vid inloggning skriver användaren in sitt användarnamn och lösenord som tidigare, därefter kräver systemet extra verifiering genom en sekundär enhet, till exempel en FIDO säkerhets nyckel. Den sekundära enheten är registrerad av användaren för att autentisera sig med till exempel en kort PIN-kod, eller biometriska uppgifter [5, 6]. Detta gör det möjligt för företag som fortfarande använder traditionella autentiseringsuppgifter att kunna smidigt integrera en säkerhetsförändring utan större problem. Nedan följer en figur som illustrerar inloggnings processen med FIDO-U2F:

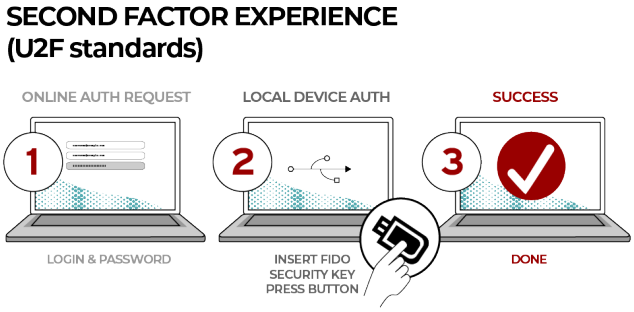

Fig. 2. FIDO U2F Standard[5]

Figur 2 illustrerar hur säkerheten av traditionella inloggningsmetoden med användarnamn och lösenord kan öka vid implementering av FIDO-U2F. Den mest signifikanta skillnaden mellan FIDO-autentisering och traditionella system är lagringen av autentiseringsuppgifter. Istället för att uppgifterna skall lagras på en central databas, lagras de lokalt på användarens enhet. Följden av detta blir positiv då en obehörig person inte kan få tillgång till autentiseringsuppgifterna. Dessutom använder FIDO biometriska metoder för autentisering, vilket lägger ytterliggare på ett lager av säkerhet. Biometriska uppgifter är svåra att stjäla eller duplicera vilket gör dem till

en stark autentiseringsfaktor. På grund av detta minskar risken betydligt för phising-attacker och dataintrång [4, 5, 7]. FIDO-alliansens arbete mot användarvänlighet visar sig även vara en väldigt stor fördel till ökad säkerhet. Inloggningsprocessen tar kortare tid och är mer användarvänlig, vilket medför att användare inte tar genvägar eller använder osäkra metoder. Exempel på genvägar är återanvändning av lösenord på flera webbtjänster, samt användning av väldigt korta och osäkra lösenord, vilket är vanligt i det traditionella lösenordssystemet [3].

2.2 Utmaningar vid implementering av FIDO-autentisering

Trots säkerhetsfördelarna med FIDO jämfört med traditionella autentiseringsmetoder, finns det flera utmaningar som företag kan stöta på vid implementeringen av denna teknik. Dessa utmaningar kan delas upp i tekniska, ekonomiska, och användarrelaterade utmaningar. En av de största utmaningarna är integrationen av FIDO i äldre IT-system. Då många företag redan har etablerade autentiseringsmetoder, orsakar det möjligtvis omfattande förändringar i deras infrastruktur. Dessutom kan det uppstå problem med kompatibiliteten mellan dessa äldre system och det moderna autentiseringensprotokollet. Detta kan vara en tidskrävande och kostsam process som kan få företag att fördröja övergången till FIDO [6]. Utöver detta kan det tillkomma kostnader för inköp av ny hårdvara såsom säkerhetsnycklar (FIDO-nycklar), om företaget väljer att till exempel implementera U2F. Inköpet kan vara en väldigt stor kostnad för vissa företag, som dessutom behöver ha en budget för underhåll och support av det nya systemet [3].

Användarupplevelse är en annan viktig faktor som ibland kan vara till utmaning. Även om FIDO erbjuder högre säkerhetsnivå och användarvänlighet, kan vissa användare vara ovilliga att ta till sig nya metoder, särskilt om man implementerar U2F som till exempel kräver en extra fysisk hårdvara. Utbildning och support om FIDO kan vara nödvändigt för att öka användaracceptansen [7]. För att illustrera dessa utmaningar kan vi titta på praktiska exempel på företag som anammat FIDO-autentisering i sin kultur. Enligt en studie publicerad av FIDO Alliance om Intuits implementering av lösenordsfri autentisering, framhävs vikten av balansen mellan användarvänlighet och säkerhet. Intuit upplevde initialt utmaningar med användaracceptans men kunde överkomma dessa genom att noggrant utforma användarupplevelsen [8]. Liknande erfarenheter rapporteras av eBay och Cloudflare i deras övergång till FIDO system [9, 10].

3 Diskussion

I denna del av rapporten diskuteras de viktigaste insikterna från resultaten och hur de relaterar till de initiala frågeställningarna. Diskussionen syftar till att ge en djupare förståelse för FIDO-autentiseringens roll i lindringen av identitesstöld, samt de utmaningar som kan uppstå vid dess implementering.

3.1 Säkerhetsfördelar kontra implementeringsutmaningar

Resultaten visar tydligt att FIDO-autentisering har betydande säkerhetsfördelar jämfört med traditionella lösenordsbaserade system. FIDO-autentisering åtgärdar effektivt flera säkerhetsbrister som ofta förekommer i traditionella system, genom att eliminera lösenord, och använda starka autentiseringsmetoder så som biometri och tvåfaktorsautentisering [3–6]. Dessa fördelar måste dock vägas mot de utmaningar som organisationer kan möta under implementeringen, vilket är tekniska begränsningar för äldre system, kostnad för ny hårdvara, och behov av användarutbildning.

En viktig aspekt är behovet av att hantera användaracceptans och kulturell förändring inom organisationer. Även om FIDO tekniskt sett är överlägsen, kan dess framgång i praktiken vara beroende av hur väl användarna är villiga att anpassa sig till den nya tekniken [7–10]. Detta kräver noggrann planering och genomförande av utbildningsprogram samt en förståelse för användarnas beteenden och behov.

Rapporten belyser även vikten av att hitta en balans mellan säkerhet och användarvänlighet. FIDO-autentiseringens framgång beror på dess förmåga att erbjuda en säker autentiseringsprocess utan att kompromissa användarupplevelsen [4, 6]. Det är avgörande att autentiseringssystemet är lättförståeligt och lättanvänt för att säkerställa bred användaracceptans.

3.2 Framtida perspektiv och teknologiska förändringar

Slutligen måste framtida tekniska förändringar och utvecklingar inom cybersäkerhet beaktas. Med tanke på den snabba utvecklingen av teknik och säkerhetshot är det viktigt att FIDO-autentisering fortsätter att utvecklas och anpassar sig till nya utmaningar. Detta innebär att organisationer måste vara flexibla och kunna uppdatera eller ändra sina autentiseringssystem i takt med att nya hot och teknologier uppstår.

4 Slutsats

Denna rapport har undersökt FIDO-autentiseringens roll i att lindra identitetsstöld, med fokus på dess säkerhetsfördelar jämfört med traditionella lösenordssystem, samt utmaningarna som kommer med implementeringen. Genom sina protokoll UAF och U2F, erbjuder FIDO en stark säkerhetslösning genom att eliminera lösenord och istället använda biometriska uppgifter samt tvåfaktorsautentisering. Dessa metoder minskar riskerna för lyckade phisingattacker och dataintrångsförsök, samtidigt som den erbjuder ett användarvänligt system.

Trots dessa fördelar har rapporten även belyst viktiga aspekter och utmaningar såsom tekniska begränsningar i äldre IT-system, användaracceptans, samt kostnader för ny hårdvara och användarutbildning. Rapporten har konstaterat att företag måste hantera och planera inför dessa utmaningar noggrant för att framgångsrikt implementera FIDO. Slutsatsen är att FIDO erbjuder ett lovande system för att förstärka cybersäkerheten och motarbeta phisingattacker. Men dess framgång beror på implemnteringsstrategier som tar hänsyn till de olika aspekterna från ett organisationsperspektiv. Det mest utmanande enligt denna rapport är de äldre IT-systemen som skall kunna uppdateras för att implementera FIDO system, därav borde forskning framöver undersöka och diskutera hur dessa tekniska system kan aktualiseras för att organisationer skall kunna adoptera denna nya teknik.

References

[1] Verizon. "2023 Data Breach Investigations Report,". 2023. Hämtad: Nov. 25, 2023. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/2023

[2] A. P. W. Group. "Phishing Attack Trends Report – 2 Q 2023,". Nov. 2023. Hämtad: Nov. 25, 2023. [Online]. Available: https://docs.apwg.org/reports/apwg_trends_report_q2_2023.pdf

[3] D. Engman and W. Hagman, "Säker nyckelhantering i webbläsaren," Bachelor's thesis, Mid Sweden Univ., 2023.

[4] K. Hu and Z. Zhang, "Security Analysis of an Attractive Online Authentication Standard: FIDO UAF Protocol," *China Communications*, vol. 13, no. 12, pp. 189–198, 2016.

[5] F. Alliance. "User Authentication Specifications Overview,". Hämtad: Dec. 1, 2023. [Online]. Available: https://fidoalliance.org/specifications/

[6] F. Alquibaisi, A. S. Wazan, L. Ahmad, and D. W. Chadwick, "Should We Rush to Implement Password-less Single Factor FIDO2 based Authentication?" in *2020 12th Annual Undergraduate Research Conference on Applied Computing (URC)*, Apr. 2020.

[7] C. I. S. Agency. "Fact Sheet: Implementing Phishing-Resistant MFA,". Oct. 2022. Hämtad: Dec. 3, 2023. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf

[8] F. Alliance. "Intuit's ROI from Passwordless Customer Authentication,". Jun. 29, 2023. Hämtad: Dec. 1, 2023. [Online]. Available: https://media.fidoalliance.org/wp-content/uploads/2023/06/Intuit-FINAL-June-28.pdf

[9] ——. "Cloudflare embraces FIDO to help improve its own security,". Mar. 2, 2023. Hämtad: Dec. 1, 2023. [Online]. Available: https://fidoalliance.org/wp-content/uploads/2023/03/Cloudflare-Case-Study.pdf

[10] ——. "eBay's Journey to Passwordless with FIDO,". Mar. 3, 2023. Hämtad: Dec. 1, 2023. [Online]. Available: https://fidoalliance.org/wp-content/uploads/2021/02/Fido-ebay.pdf