Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra Informačních Technologií

Bakalářská práce

Vícefaktorová autentizace a autorizace

Oleksandr Matvieiev

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Oleksandr Matvieiev

Informatika

Název práce

Vícefaktorová autentizace a autorizace

Název anglicky

Multi-factor authentication

Cíle práce

Bakalářská práce je tématicky zaměřena na problematiku vícefaktorové autentizace a autorizace. Hlavním cílem práce je analýza různých metod vícefaktorové autentizace a jejich bezpečnost včetně návrhu prototypu na základě zvolených hodnotících kritérií.
Dílčí cíle práce jsou:
- vypracování přehledu zpracovávané problematiky,
- vypracování přehledu různých metod vícefaktorové autentizace a jejich bezpečnosti,
- návrh vlastního prototypu na základě specifických kritérií.

Metodika

Metodika řešené problematiky bakalářské práce je založena na studiu a analýze odborných informačních zdrojů. Teoretická část bude věnována problematice jak jednofaktorové, tak vícefaktorové autentizace a autorizace a její bezpečnosti. Vlastní práce spočívá v analýze a porovnání několika systémů včetně návrhu vlastního prototypu dle konkrétních kritérií. Na základě syntézy teoretických poznatků a výsledků praktické části budou formulovány závěry bakalářské práce.

Doporučený rozsah práce

40 – 50 stran textu

Klíčová slova

autentizace, autorizace, biometrie, heslo, bezpečnost, OTP, TOTP, HOTP, hacking

---

Doporučené zdroje informací

BOONKRONG, S. Authentication and Access Control: Practical Cryptography Methods and Tools 1st Edition. New York City, NY: Apress, 2020 ISBN 978-1484265697

GRIMES, R. A. Hacking Multifactor Authentication 1st ed. New York City, NY: Wiley, 2020 ISBN 978-1119650799

OMETOV, A. – BEZZATEEV, S. Multi-factor Authentication: A Survey and Challenges in V2X Applications. Basel: MDPI, 2018

RAK, Roman; MATYÁŠ, Vašek; ŘÍHA, Zdeněk. *Biometrie a identita člověka ve forenzních a komerčních aplikacích.* Praha: Grada, 2008. ISBN 978-80-247-2365-5.

WILSON, Y. – HINGNIKAR, A. Solving Identity Management in Modern Applications: Demystifying OAuth 2.0, OpenID Connect, and SAML 2.0. New York City, NY: Apress, 2019. ISBN 978-1484250945

Předběžný termín obhajoby

2022/23 LS – PEF

Vedoucí práce

Věra Motyčková, MA

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 14. 7. 2022

doc. Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 27. 10. 2022

doc. Ing. Tomáš Šubrt, Ph.D.

Děkan

V Praze dne 07. 03. 2024

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci „Vícefaktorová autentizace a autorizace“ jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 15.03.2024 _____

Poděkování

Rád bych touto cestou poděkoval vedoucí své bakalářské práce Věře Motyčkové, MA, za odborné vedení a cenné rady, které mi pomohly tuto práci zpracovat.

Vícefaktorová autentizace a autorizace

Abstrakt

Stanovení identity je v naší společnosti stále důležitější. Scénáře mohou být velmi odlišné – počínaje vydáním řidičského průkazu a konče právem na vstup do jiné země. Rostoucí obavy o bezpečnost a rychlý rozvoj komunikace přispěly ke zvýšení potřeb spolehlivých autentizačních a autorizačních metod uživatelů. Práce se zabývá o diskuse o některých relevantních termínech, které jsou nezbytné pro pochopení technologií metody zjišťování totožnosti a důležitost jejich sjednocení.

Klíčová slova: autentizace, autorizace, biometrie, heslo, bezpečnost, OTP, TOTP, HOTP, hacking

Multi-factor authentication

Abstract

Establishing identity is becoming increasingly important in our society. Scenarios can be very different – starting with the issuance of a driver's license and ending with the right to enter another country. Growing concerns about security and the rapid development of communication have contributed to an increase in the need for reliable authentication and authorization methods of users. The thesis deals with a discussion of some of the relevant terms that are necessary for understanding the technologies of the method of identification and the importance of their unification.

Keywords: authentication, authorization, biometrics, password, security, OTP, TOTP, HOTP, hacking

Obsah

1 Úvod

V současné době je problematika identifikace a autentizace v internetové síti aktuálnější než kdy dříve. Na jedné straně existuje mnoho internetových služeb – od sociálních sítí až po bankovní služby a stránky státních organizací – které vedou evidenci uživatelů a rozlišují jejich přístupová práva k různým zdrojům. Tyto služby potřebují vědět, který konkrétní uživatel se snaží k nim získat přístup a zda je tento uživatel skutečně tím, za koho se vydává.

Na druhou stranu v poslední době výrazně vzrostly útoky hackerů na webové služby. Účely těchto útoků mohou být různé – od krádeže osobních údajů až po pokusy o vydírání a vymáhání peněz. Všude ale slabým místem systémů, které jsou napadány, je právě systém autentizace. Podle společnosti Verizon, která každoročně shromažďuje statistiky o únicích dat, se až 80 % úspěšných hackerských útoků (včetně útoků na největší služby s miliony uživatelů) podařilo právě kvůli slabosti systému ochrany heslem. (Verizon, 2022)

V současné době existuje mnoho systémů autentizace, z nichž každý má své přednosti i nedostatky. Vyvstává otázka výběru nejlepšího systému autentizace pro daný případ, k čemuž je potřeba definovat, podle jakých kritérií je nutné provádět srovnání a jak srovnávat mezi sebou systémy založené na zcela odlišných principech a faktorech.

V této práci jsou analyzovány metody používané pro autentizaci uživatelů v systémech. Je navržen rámec pro srovnání metod autentizace založených na různých principech a provedeno srovnání nejběžnějších metod podle několika kritérií. V praxi je implementována kombinace metod autentizace uživatelů.

2 Cíl práce a metodika

2.1 Cíl práce

Bakalářská práce je tématicky zaměřena na problematiku vícefaktorové autentizace a autorizace. Hlavním cílem práce je analýza různých metod vícefaktorové autentizace a jejich bezpečnost včetně návrhu prototypu na základě zvolených hodnotících kritérií.

Dílčí cíle práce jsou:

- vypracování přehledu zpracovávané problematiky;
- vypracování přehledu různých metod vícefaktorové autentizace a jejich bezpečnosti;
- návrh vlastního prototypu na základě specifických kritérií;

2.2 Metodika

Metodika řešené problematiky bakalářské práce je založena na studiu a analýze odborných informačních zdrojů. Teoretická část bude věnována problematice jak jednofaktorové, tak vícefaktorové autentizace a autorizace a její bezpečnosti. Vlastní práce spočívá v analýze a porovnání několika systémů včetně návrhu vlastního prototypu dle konkrétních kritérií. Analýza bude provedena mezi čtyřmi typy autorizace a to jsou jednofaktorové a dvoufaktorové metody, jejichž hodnotící kritéria budou rozdělena do tří hlavních skupin: bezpečnost, pohodlí a nasazení. Bude implementována vlastní kombinace autentizačních metod, která bude také analyzována. Pro implementaci vlastní vícefaktorové autorizace bude zakoupen badUSB, který bude použit jako autorizační faktor, a to jako fyzický klíč. Pro správnou funkci fyzického klíče bude provedeno programování zařízení v prostředí vývoje Arduino IDE. Jako druhý autorizační faktor bude napsán skript v prostředí vývoje Visual Studio, který implementuje metodu požadavku na heslo. V procesu testování bude rozhodnuto o některých výjimkách, které zajistí správnou funkci metody požadavku na heslo a sníží počet chyb při autorizaci. Pro pochopení vzájemné závislosti dvou metod bude napsán scénář autorizace pomocí vlastní implementace kombinace metod. Na základě syntézy teoretických poznatků a výsledků praktické části budou formulovány závěry bakalářské práce.

3 Teoretická východiska

3.1 Základní teorie

Identifikace

Identifikace je postup rozpoznávání uživatele v systému obvykle pomocí předem definovaného jménoa (identifikátoru) nebo jiné apriorní informace o něm, které systém vnímá. Tento termín obvykle znamená stanovení identity uživatele. (Ageev, 2020)

Identifikační postup je přímo spojen s ověřením: subjekt prochází ověřovacím procesem, a pokud ověřování probíhá úspěšně, informační systém identifikuje identitu subjektu na základě autentizačních faktorů. V tomto případě je spolehlivost identifikace zcela určena úrovní spolehlivosti prováděného autentizačního postupu. (Grimes, 2021)

Access control

Access control je důležitou součástí technologií informační bezpečnosti. Dalším termínem pro access control je autorizace. Ta označuje, zda je žádost o přístup k softwarovému prostředku schválena, nebo odmítnuta v závislosti na oprávnění uživatele a pravidlech řízení přístupu. Logika pro autorizaci je formalizována v modelech řízení přístupu. Komponenty modelu řízení přístupu zahrnují: sadu subjektů, sadu objektů, sadu operací, sadu oprávnění a sadu pravidel. Subjektem může být člověk, proces počítače, robot nebo zařízení. Objektem je softwarový prostředek. Operací se rozumí druh akce, pro kterou subjekt požádá o přístup k objektu. Oprávnění ukazuje, že subjekt může přistupovat k objektu prostřednictvím operace. Politika je pravidlo, které ukazuje, zda má být žádost o přístup schválena, nebo zamítnuta. (Penelova, 2021)

Každá akce procesoru, ve kterém se subjekt účastní počítačového systému nebo zařízení přístupového řadiče, vyžaduje, aby každý přístup byl spojen s určitým identifikátorem. Tím je digitální značka, která je jednoznačně vázána na subjekt. Identifikátor musí být jedinečný v rámci zúčastněného prostoru názvy, které používají autentizační systém. (Grimes, 2021)

Obecné identifikátory totožnosti:

- full name;
- logon name;
- email address;
- user principal name (UPN);
- LDAP;
- digitální certifikát;
- global unique identifier GUID nebo uneversally unique identifier UUID;
- media Access Control (MAC) address.

Autentizace

Autentizace je proces subjektu prokazujícího vlastnictví a / nebo kontrolu nad konkrétní identitou / identifikační štítek. To se provádí subjektem, který poskytuje „tajemství“, známá pouze subjektu, který se snaží autentizovat, a základní autentizační systém. Autentizační tajemství může zahrnovat mnoho věcí, jako jsou hesla, PINy, znalosti o tom, jak vyřešit konkrétní hádanku, digitální tajemství, zařízení nebo fyzický atribut. Některá tajemství mohou být uložena ve více formách. Například v systému Windows může uživatel zadat heslo jako tajemství, ale Windows převádí, ukládá a používá toto tajemství jako převedené na kryptografický hash. Autentizační tajemství nemusí být vždy globálně jedinečné, ačkoli někdy, jako v případě digitálních certifikátů a biometrických atributů, to může být požadavek. Autentizační tajemství musí být chráněna jak subjektem, který je používá, tak základním autentizačním systémem. Pokud se útočník dozví tajemství, může se vydávat za legitimní subjekt. (Grimes, 2021)

Je rozdíl mezi autentizací entity a autentizací zprávy. Tento rozdíl je vnímán z časové perspektivy. Autentizace zprávy (např. prostřednictvím elektronického podpisu) neposkytuje žádnou záruku ohledně toho, kdy byla zpráva vytvořena. Naopak autentizace entity zahrnuje jako pravidlo důkaz o identitě žadatele prostřednictvím aktuální komunikace s ověřovatelem. Příkladem autentizačního procesu je proces, při kterém se uživatel přihlašuje do aplikace pomocí uživatelského jména a hesla. Vedlejším efektem autentizačního procesu může být i skutečnost, že během autentizace entity je generován kryptografický materiál pro následnou komunikaci. (Dostálek, 2021)

Autentizační tajemství jsou obvykle uložena v autentizačním systému nebo na něj odkazuje, typicky v rámci jedné z následujících možností:

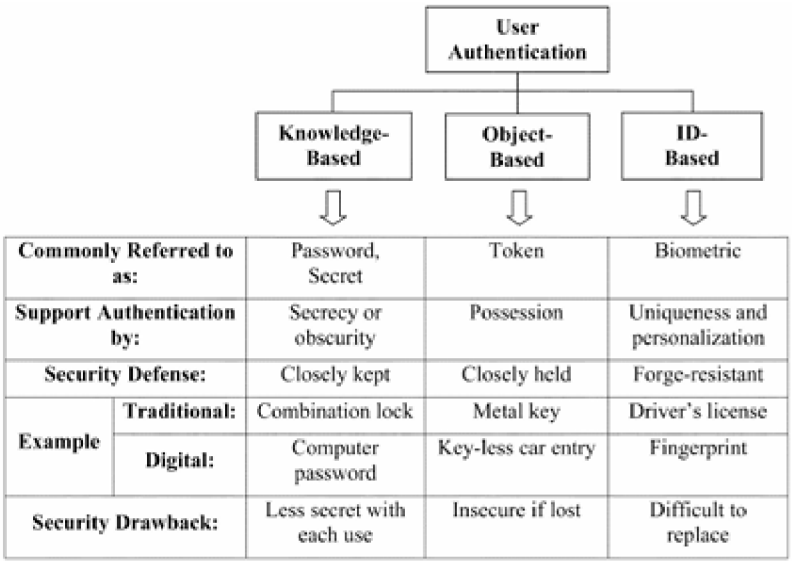
- lidská mysl;
- fyzický dokument;
- soubor;
- databaze;
- umístění registru;
- pamět';
- úložiště;
- kombinace jednoho nebo více z výše uvedených.

Všechna tato místa (s výjimkou lidské mysli) mohou být buď místní pro zařízení používaná pro ověřování, nebo vzdálená, v takovém případě se vyžaduje fyzický přístup nebo připojení k síti. Všude, kde jsou uchovávána autentizační tajemství, musí být ochrana. Každý úložný prostor se stává potenciálním bodem útoku (Grimes, 2021).

Autentizační faktory

Obecně existují tři skupiny faktorů autentizace: První skupina spočívá ve znalosti některých informací, které uživatelé musí poskytnout k autentizaci. Druhá skupina faktorů autentizace je založena na něčem, co uživatelé vlastní. Třetí skupina, dědičnost, spoléhá na vrozený, nezcizitelný a charakteristický prvek, který jedinečně identifikuje jednotlivé uživatele. (Marky et al, 2022)

Obrazek 1 - Autentizace uživatele je rozdělena do tří kategorií autentizátorů. Jsou uvedeny atributy každé z nich



Commonly Referred to as:		Password, Secret	Token	Biometric
Support Authentication by:		Secrecy or obscurity	Possession	Uniqueness and personalization
Security Defense:		Closely kept	Closely held	Forge-resistant
Example	**Traditional:**	Combination lock	Metal key	Driver's license
	Digital:	Computer password	Key-less car entry	Fingerprint
Security Drawback:		Less secret with each use	Insecure if lost	Difficult to replace

Autentizátory založené na znalostech – charakterizované tajemstvím nebo skrytostí. Tento typ zahrnuje zapamatované heslo. Může také zahrnovat informace, které nejsou tolik tajné, jako spíše „nejasné“, což lze volně definovat jako „tajné před většinou lidí“. Příklady v této kategorii zahrnují dívčí příjmení matky a vaši oblíbenou barvu. Bezpečnostní nevýhodou tajemství je, že pokaždé, když se sdílí pro autentizaci, stává se méně tajným.

Autentizátory založené na objektu – charakterizované fyzickým vlastnictvím. Fyzické klíče – které nazýváme kovovými klíči, abychom je odlišili od kryptografických klíčů – jsou tokeny, které obstály dobře časově. Bezpečnostní nevýhodou kovového klíče k domu je to, že pokud se ztratí, umožní svému nálezci vstoupit do domu. Proto mnoho digitálních tokenů kombinuje další faktor, přidružené heslo, k ochraně ztraceného nebo odcizeného tokenu. Existuje zjevná výhoda fyzického objektu používaného jako autentizátor; pokud se ztratí, vlastník vidí důkazy toho a může jednat odpovídajícím způsobem.

Autentizátory založené na identifikaci – charakterizované jedinečností pro jednu osobu. Řidičský průkaz, pas, kreditní karta, univerzitní diplom atd. – všechny patří do této kategorie. Sem spadá také biometrický prvek (sem se řadí otisk prstu, sken očí, hlasový otisk nebo podpis). Pro oba typy autentizačních prvků, ať už jsou to identifikační dokumenty, nebo biometrika, je dominantní bezpečnostní obranou obtížnost jejich kopírování nebo padělání. (O'Gorman, 2003)

Access control token

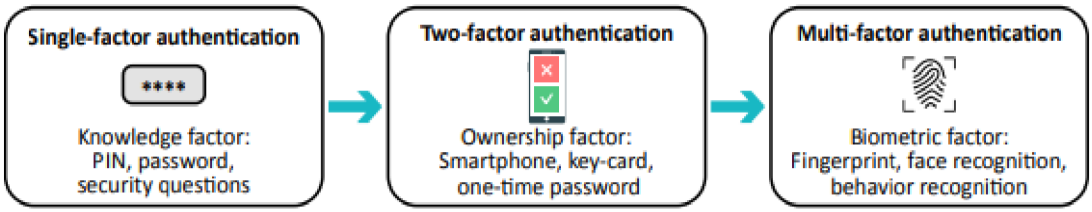
Po úspěšné autentizaci ve většině případů procesy řízení přístupu pak spojují objekt řízení přístupu (např. token, lístek) s již ověřenou, identifikační značkou. Co obsahuje tento token řízení přístupu, závisí na systému a protokolu. Téměř ve všech systémech bude obsahovat jedinečný identifikátor, jako je řada čísel nebo znaků, který konkrétně identifikuje identifikační značku, buď trvale, nebo pouze pro konkrétní přihlašovací relaci. V jiných systémech, například v systému Windows, je může také obsahovat seznam členství ve skupinách, oprávnění a další potřebné informace. (Grimes, 2021)

Token může mít předem stanovenou maximální životnost, která po vypršení platnosti způsobí, že subjekt musí znovu projít ověřením, aby zůstal v „aktivní" relaci. V systému Windows token řízení přístupu může přijít jako lístek Kerberos nebo správce LAN nové technologie (NTLM) nebo LAN token manažera (LM). Na webových stránkách a službách je většina tokenů pro kontrolu přístupu prezentována souborem cookie HTML, který je jednoduchý textový soubor. Většina webových souborů cookie obsahuje globální jedinečný identifikátor ověřeného uživatele a/nebo jeho relaci, po níž následuje datum vypršení platnosti. (Grimes, 2021)

3.2 Vícefaktorová autentizace

Řešení jednofaktorové autentizace (1FA) vyžaduje pouze jediný ověřovací důkaz pro subjekt úspěšně ověřeno. Dvoufaktorová autentizace (2FA) vyžaduje dva ověřovací důkazy, řešení multifaktorové autentizace (MFA) vyžaduje dva nebo více faktorů. Všechny ostatní věci jsou rovno, MFA je obvykle lepší než jednofaktorová autentizace pro lepší zabezpečení, ačkoli jediné řešení MFA je zřídka všeobecně povoleno ve všech scénářích použití subjektu, tak 1FA nebo bude obvykle zapotřebí více metod MFA. (Grimes, 2021)

Obrazek 2 - Vývoj autentizačních metod od SFA k MFA

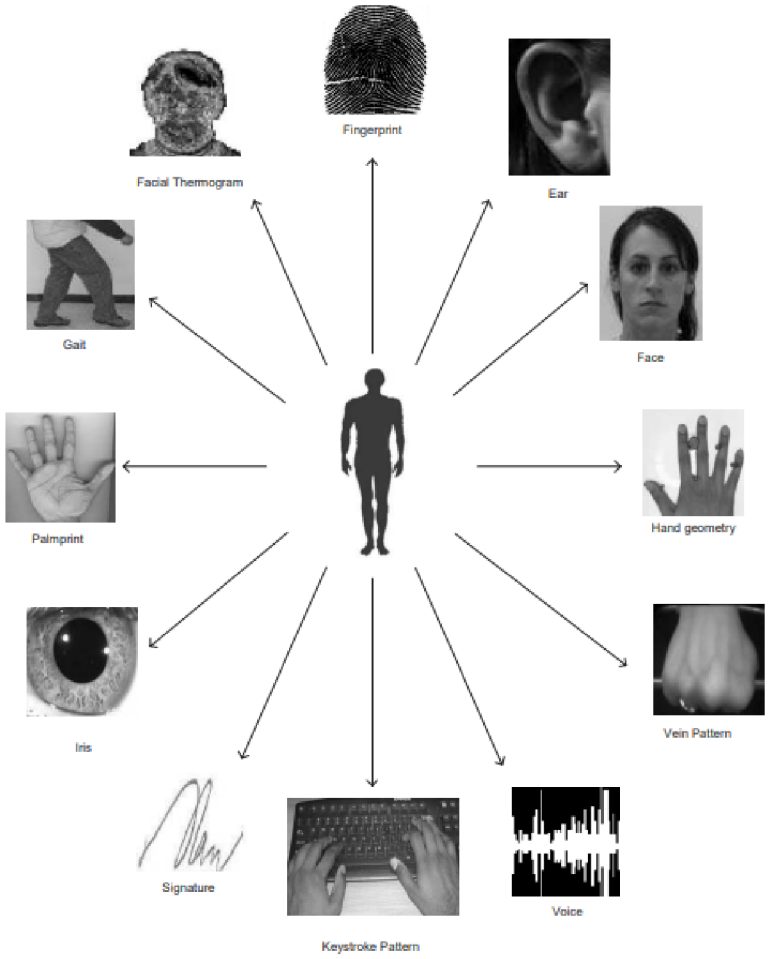


Aby ověřovací faktory poskytly nejlepší bezpečnostní ochranu v procesu vícenásobné autentizace, musí být faktory různých typů. Použití dvou nebo více stejných faktorů je stále lepší než použití jednoho faktoru při ověřování, ale ne tak spolehlivě při použití několika různých typů faktorů. (Ometov, 2018)

3.2.1 **Metody**

V současné době autentizační systémy již používají obrovské množství senzorů, které umožňují identifikovat uživatele. (Ross, 2007)

Obrazek 3 - Příklady biometrických charakteristik, které mohou být použity k ověření identity osoby



Ochrana heslem

Statické heslo je tajný řetězec znaků, který je uživatelem opakovaně používán k autentizaci k určitému chráněnému zdroji. Statická hesla jsou dnes běžně používána, ale mají několik nevýhod. Pokud jsou uživatelské jméno a heslo odcizeny, mohou být použity někým, kdo je vzdálený majiteli účtu, který si nemusí být vědom toho, že bylo heslo ohroženo, dokud není použito k něčemu neoprávněnému (Wilson a Hingnikar, 2019).

Hesla mohou být zadána uživateli, poskytována interakčními systémy nebo přenášena zprostředkující proxy programy. Jedny přihlášení a heslo mohou být zapojeny do několika procesů. (Grimes, 2021)

Token presence

Heslo pak může být doplněno fyzickým tokenem — například kartou, která se doporučuje jako druhá skupina faktorů-vlastníka. Z hlediska hardwaru si uživatel může představit čipovou kartu, telefon, nositelné zařízení atd., které je těžší delegovat. V takovém případě musí být systém vybaven rádiovým rozhraním, které zajišťuje obousměrnou komunikaci s tokenem. Na druhé straně nejrozšířenějším softwarovým tokenem je jednorázové heslo (OTP) generované softwarem. Hlavní nevýhodou výše uvedeného je problém nekontrolované duplikace. (Ometov, 2018)

OTP-zařízení automaticky generují jednoduché heslo, to lze zadat na přihlašovací obrazovce MFA, jež se synchronizuje s podobným procesem souvisejícím s ověřením pravosti. Uživatel zadá název pro přihlášení nebo identifikační kód, pak poskytuje kód generovaný OTP-zařízení jako druh hesla. V závislosti na rozhodnutí OTP spolu s měnícím se kódem může být také zapotřebí jiný, trvalejší kód pro vytvoření výsledného kódu větší velikosti. Bez ohledu na to, zda je kód generován, je dobrý pouze v daném časovém intervalu, pravděpodobně se nikdy nebude opakovat a často se během rozumného časového období neobnoví. OTP-zařízení mohou obsahovat funkci hash, a pokud ano, jsou známa jako zařízení HMAC-OTP nebo OTP založená na hashi (HOTP). Teorie zabezpečení, která je základem OTP-zařízení, je, že pokud se útočník dozví automaticky generovaný kód, tento kód lze použít pouze v daném časovém období a nikdy již nebude použit nebo generován. Časově omezuje výši škody, která může být způsobena v důsledku jednoho kompromisu. (Grimes, 2021)

Hlasová biometrie

Většina moderních inteligentních elektronických zařízení je vybavena mikrofonem, který umožňuje rozpoznávání hlasu jako faktoru pro MFA. Současně technologický pokrok zítřka může umožnit speciálním agenturám nejen rozpoznat řečníky, ale také napodobit jejich hlasy, včetně intonace, zabarvení atd., což je závažná nevýhoda použití hlasu jako hlavní metody autentizace. (Dai, 2019)

Rozpoznávání obličeje

Jako další krok by bylo možné zvážit rozpoznávání obličeje. Na začátku svého vývoje byla technologie založena na analýze obrazu orientačního bodu, který byl relativně jednoduchý k reprodukci tím, že systém poskytl fotografii. Dalším krokem bylo začlenění trojrozměrného rozpoznávání obličeje, tedy požadavek uživatele, aby během procesu ověřování určitým způsobem pohyboval hlavou. Nakonec vývoj tohoto systému dosáhl toho, že začal rozpoznávat skutečné výrazy obličeje uživatele. Rozpoznávání obličeje v neomezeném prostředí je stále běžnější v mnoha aplikacích, jako je ověřování identity, inteligentní vizuální dohled a automatizovaný systém kontroly imigrace. Chcete-li povolit rozpoznávání obličeje, musíte vybavit systém alespoň jedním výstupním zařízením a fotoaparátem. (Ometov, 2018)

Klasický kanál moderního systému rozpoznávání obličeje se obvykle skládá z rozpoznávání obličeje, zarovnání obličeje, reprezentace funkcí a klasifikace. Mezi nimi je nejzásadnějším krokem reprezentace objektů. Skvělá funkce může do určité míry zlepšit výkon. K dnešnímu dni bylo navrženo mnoho přístupů k zastupování jednotlivců. Funkce vytvořit ručně, jako je LBP, SIFT, byly dříve použity k extrahování funkcí vzhledu obrazu. Později byly vyvinuty funkce založené na kódování pro studium rozlišovacích znaků od dat. Například Fisher vector používá metody učení bez dozoru k naučení slovníku kódování z tréninkových dat. (Jiang-Jing, 2017)

Oční metodika

Metody rozpoznávání duhovky jsou na trhu již přes 20 let. Tento přístup nevyžaduje, aby uživatel byl v blízkosti zachycovacího zařízení při analýze barevného obrazu lidského oka. Analýza sítnice je další atraktivní metodou. Zde je zachycena a analyzována tenká tkáň složená z nervových buněk umístěných v zadní části oka. Vzhledem ke složité struktuře

kapilár, které dodávají sítnici krev, je sítnice každého člověka jedinečná. Nejpozoruhodnějšími problémy v těchto technikách jsou potřeba vysoce kvalitního zařízení pro zachycení a spolehlivé matematické techniky pro analýzu obrazu. (Ometov, 2018)

Mediální padělání a Spoofing jsou nejčastějším druhem útoků v autentizačním systému založeném na duhovce:

Spoofing: Spoofing je metoda útoku biometrické živosti proti identifikačnímu systému, kde je falešný umělý objekt uživatele prezentován vetřelcem do systému, aby napodobil identifikační prvek, který je proces navržen tak, aby zkontroloval, aby mohl umožnit autentizaci útočníkovi. Je to podobné jako použít klonovanou biometrickou část jakéhokoli ověřeného uživatele pro získání přístupu v systému. Spoofing je většinou používán většinou útočníků v biometrickém autentizačním útoku. Face spoofing lze udělat attack pomocí tištěného obrazu duhovky nebo jakékoli kosmetické kontaktní čočky. Tyto útoky mohou být zásadními a alarmujícími body pro autentizaci systému a způsobit vážné poškození systému. (Etienne, 2020)

Falešná Duhovka: systém rozpoznávání duhovky používá data uložená v systému, která jsou pouze kousky kódu v binární podobě. Reverzní inženýrství je možné získat skutečný obraz duhovky. Genetický algoritmus lze použít k provádění různých pokusů pomocí syntetické duhovky, aby byla rozpoznatelná pro detekci duhovky. Vytvoření podobného obrazu duhovky, který je uložen v systému rozpoznávání duhovky, trvá přibližně 100 až 200 iterací. (Etienne, 2020)

Prezentační útoky: prezentace biometrického spoofu se nazývá prezentační útok. Biometrický spoof může být nějaký obrázek, video místo živé osoby; nebo falešné křemíkové nebo želatinové otisky prstů nebo falešná syntetická duhovka místo skutečného oka. Systém rozpoznávání by měl být vybaven systémy detekce živosti. Zjistí, zda je prezentace živá nebo falešná. (Etienne, 2020)

Geometrie rukou

Některé systémy používají analýzu fyzické formy ruky k ověření uživatele. Zpočátku byly pro ověření subjektu použity vazby, ale použitelnost takových metod byla nízká. V budoucnu byl skener tablet použit k získání obrazu, aniž by bylo nutné opravit ruku uživatele v jedné konkrétní poloze. Některé systémy dnes používají běžné kamery, které nevyžadují těsný kontakt se zachycovacím povrchem. Tento přístup však není pro životní prostředí příliš spolehlivý. Někteří výrobci používají fotopletysmografii (PPG), aby

zjistili, zda je nositelné zařízení (například chytré hodinky) v současné době na zápěstí uživatele, nebo ne. Proces se podobá tomu, který se provádí při měření srdeční frekvence. (Ometov, 2018)

Rozpoznávání žil

Pokroky v oblasti skenerů otisků prstů umožňují také získat obraz žíly prstu. Složitější zařízení používají rozpoznávání otisků prstů pro získání a uložení tvaru/pohybu celé ruky. V současné fázi vývoje jsou biometrické údaje žil stále zranitelné vůči náhradním útokům. (Ometov, 2018)

Tato technologie má následující výhody:

1. jedinečnost žilní sítě - žilní síť každého člověka je jedinečná, což znamená, že žíly v prstech se u každého liší;
2. neměnnost žilní sítě - žilní síť v prstech je u každého člověka během života zcela neměnná;
3. snadná detekce - snímání žilní sítě je snadné a nenáročné;
4. bezpečnost modelu - model používaný v rozpoznávacím systému není originálním obrazem prstu, který lze získat pomocí funkce zobrazení. (Jasim Jasim, 2021)

Test žilní sítě na prstu se skládá ze čtyř kroků:

1. vyhodnocení vlastností předzpracování obrazu - tento krok zahrnuje analýzu vlastností obrazu před samotnou extrakcí informací o žilní síti;
2. extrakce znaků - extrakce znaků hraje v tomto kroku klíčovou roli. Mnoho vědců navrhlo alternativní metody extrakce žilní sítě z prstu s cílem zajistit jejich účinnost. Tyto metody extrakce lze rozdělit do dvou kategorií: frekvenční doménové metody - analýzu obrazu v jeho frekvenčním spektru; metody založené na lokálním binárním vzoru - analýzu lokálních oblastí obrazu pomocí binárního kódování;
3. Porovnání - v tomto kroku se získané informace o žilní síti porovnávají s uloženým vzorem pro účely identifikace;
4. Vyhodnocení - výsledkem je rozhodnutí, zda se jedná o shodu nebo neshodu. (Jasim Jasim, 2021)

Snímač otisků prstů

Použití skeneru otisků prstů jako hlavního autentizačního mechanismu je v současné době podporováno většinou výrobců smartphonů a osobních počítačů (Titcomb, 2017). Toto řešení je intuitivní, ale zůstává extrémně snadné – především proto, že naše otisky prstů mohou být získány prakticky ze všeho, čeho se dotýkáme. Integrační potenciál této metody je skutečně vysoký, i když se také nedoporučuje používat jako samostatný autentizační přístup. Většina výrobců smartphonů instaluje další fotoaparát, aby získal otisk prstu namísto bezpečnějšího rozpoznávání žil. (Ometov, 2018)

Rozpoznávání tepelných obrázků

Technologie rozpoznávání obličeje nemůže být v reálném životě široce využívána kvůli mnoha faktorům, jako je světlo, úhel, mimika a věk. Pro efektivnější řešení výše uvedených problémů se v posledních dvou desetiletích rychle rozvíjí také technologie termálního rozpoznávání obličeje. (Gao, 2022)

Termální zobrazování je metoda snímání infračerveného záření cíle bez ohledu na osvětlení viditelným světlem. Termální infračervené obrazy jsou typicky pořizovány termokamerou, která detekuje záření v infračervené oblasti elektromagnetického spektra a vytváří obraz odpovídajícího záření. Podle zákona o vyzařování černého tělesa všechny objekty s teplotami nad absolutní nulou vyzařují infračervené světlo. Termokamera dokáže pozorovat prostředí s viditelným světlem i bez něj a není omezena špatným osvětlením. Množství záření emitovaného objektem se zvyšuje s rostoucí teplotou. Technologie termálního zobrazování tedy dokáže snímat změny teploty objektu. (Gao, 2022)

Mezitím různé objekty vyzařují infračervené záření s různými vlnovými délkami v závislosti na teplotě. Rozsah teploty obličeje a těla je téměř stejný a poměrně uniformní, pohybuje se od 35,5 °C do 37,5 °C, a poskytuje tak konzistentní signál infračerveného záření. Tepelné charakteristiky lidské tváře jsou odvozeny především od mělkého cévního systému pod kůží obličeje. Protože žíly a tkáňová struktura obličeje jsou u každého člověka relativně jedinečné, jsou také jedinečné i termálně infračervené obrazy obličeje každého člověka. Proto mohou být použity jako základ pro termální infračervené rozpoznávání obličeje.

Mnoho problémů s touto metodou autentizace může vyplynout z uživatelských podmínek: onemocnění nebo emoce mohou významně ovlivnit vnímaná čísla. (Gao, 2022) (Ometov, 2018).

Zeměpisná poloha

Použití geografického umístění zařízení a uživatele k ověření, zda lze mít přístup k zařízení/službě, je zvláštním případem autentizace založené na umístění. Je důležité si uvědomit, že signál GPS může být snadno potlačen nebo rozpoznán jako vadný kvůli distribučním vlastnostem; proto se doporučuje použít alespoň dva zdroje určování polohy, jako jsou GPS a ID bezdrátové sítě. Smartphone může být použit k podpoře MFA z hlediska lokalizace. (Ometov, 2018)

V současnostije většina online autentizačních služeb založena na znalostech, to znamená, že závisí na kombinaci uživatelského jména a hesla. Složitější systémy vyžadují, aby uživatel komunikoval s dalšími žetony (jednorázová hesla, generátory kódů, telefony atd.). Doplněním tradičních autentizačních strategií není MFA možné bez biometrie. (Ometov, 2018)

Následně tabulka 1 uvádí srovnání hlavních ukazatelů pro již rozvinuté faktory. Faktory/senzory jsou hodnoceny na základě následujících parametrů:

- univerzálnost znamená přítomnost faktoru v každé osobě;
- jedinečnost ukazuje, jak dobře tento faktor odlišuje jednu osobu od druhé;
- sběr měří, jak snadné je získat data pro zpracování;
- výkon naznačuje dosažitelnou přesnost, rychlost a spolehlivost;
- přijatelnost znamená míru přijetí technologie lidmi v jejich každodenním životě;

Výměna označuje úroveň složitosti zachycení a padělání vzorku.

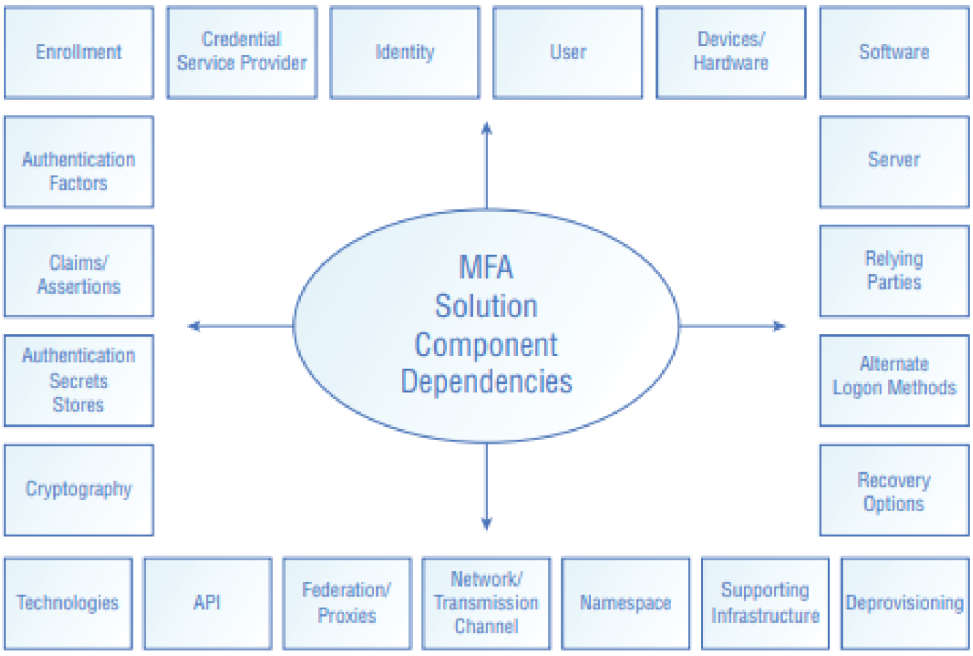
Tabulka 1 - Srovnání vhodných faktorů pro MFA: H—high; M—medium; L—low; n/a—unavailable.

Factor	Universality	Uniqueness	Collectability	Performance	Acceptability	Spoofing
Password	n/a	L	H	H	H	H
Token	n/a	M	H	H	H	H
Voice	M	L	M	L	H	H
Facial	H	L	M	L	H	M
Ocular-based	H	H	M	M	L	H
Fingerprint	M	H	M	H	M	H
Hand geometry	M	M	M	M	M	M
Location	n/a	L	M	H	M	H
Vein	M	M	M	M	M	M
Thermal image	H	H	L	M	H	H

3.3 Bezpečnost systém MFA

Jakákoli struktura MFA je digitální systém složený z kritických komponent, jako jsou senzory, zařízení pro ukládání dat, zpracování a komunikační kanály. Všechny jsou obecně zranitelné různými útoky na zcela odlišných úrovních, od pokusů o přehrávání až po útoky nepřítele. Bezpečnost je tedy nezbytným nástrojem pro zajištění a udržení soukromí. Každé řešení MFA je jen jednou částí mnoha komponent, vztahů a závislostí a každá z těchto komponent představuje další oblast, kde může dojít ke zranitelnosti, kterou lze použít. (Grimes, 2021)

Obrazek 4 - Komponenty závislé na MFA

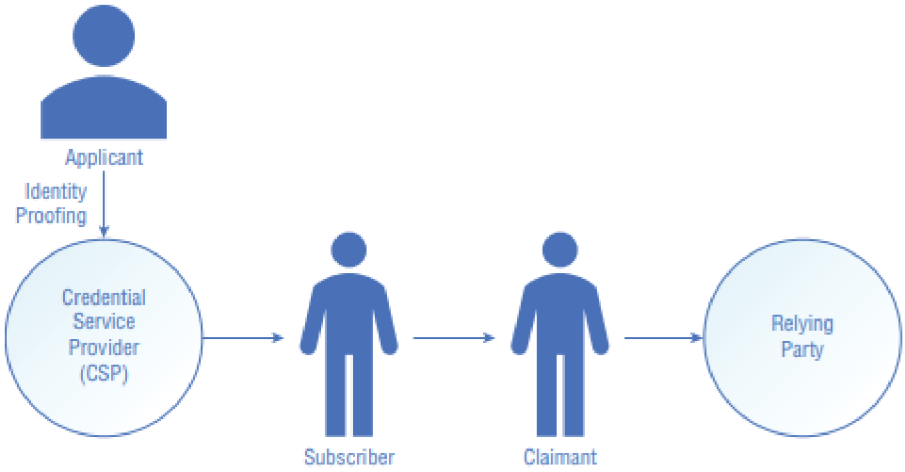


Enrollment

Registrace (také známá jako příprava) je proces registrace a ověření subjektu pro získání ověřeného průkazu totožnosti (označení). Neověřený a neregistrovaný subjekt je znám jako žadatel. Žádají o průkaz totožnosti, který byl ověřen. Poskytovatel pověření (CSP) požaduje a získá jeden nebo více (jedinečných) atributů subjektu, které lze použít k jasné identifikaci subjektu. Tento proces je znám jako ověřování. Subjekt se může zaregistrovat sám, nebo požádat jiného registračního agenta, který je důvěryhodný, jak žadatel, tak CSP, tak činí jeho jménem. Důležitou součástí procesu je, že CSP kontroluje atributy předložené žadatelem. Bez důkladného ověření CSP předložených atributů žadatele a zajistit, že žadatel

je tím, za koho se vydává, a které předložené atributy žadatele skutečně patří žadateli, autentizace je prakticky zbytečná. Jak pečlivě CSP kontroluje identitu a atributy žadatele, určuje úroveň důvěry. (Grimes, 2021)

Obrazek 5 - Generalized common enrollment process



Hardware

Jakékoli zařízení, které se účastní ověřování, může být ohroženo. Zařízení zahrnují vlastní počítače, telefony, autentizační zařízení, úložiště, paměť RAM, síťové rozhraní, antény a všechna ostatní fyzická zařízení zapojená do procesu ověřování. Mohou být ohroženy krádeží ověřovacího tajemství, krádeží výsledného tokenu řízení přístupu, odposloucháváním, krádeží dat a přesměrováním uživatele nebo procesu ověřování na podvodné webové stránky či služby. Pokud je hardwarové zařízení ohroženo, je těžké (i když ne nemožné) důvěřovat procesu autentizace. To neznamená, že některé hardwary nejsou odolnější proti hackingu než jiné. (Grassi, 2017)

Schémata důvěryhodného hardwaru obvykle zahrnují "základní zdroj důvěry", který ověřuje, zda zařízení nebylo škodlivě upraveno. Často si jednotlivé hardwarové komponenty jednoho zařízení ověřují samy sebe a/nebo je ověřuje nadřazená komponenta v řetězci kontrol důvěry. Například v moderním počítači se systémem Windows hardware začíná dříve důvěryhodnou základní hardwarovou komponentou nazvanou Univerzální rozhraní pro rozšiřitelný firmware (UEFI). Nahradilo méně důvěryhodné čipy systému BIOS (Basic Input/Output System) nalezené na starších systémech. Firmware spouštěcího čipu UEFI obsahuje kód, který je digitálně podepsán dodavatelem jako autentický. Každá hardwarová komponenta na vyšší úrovni se spoléhá na komponentu předchozí úrovně, aby ověřila její digitální podpis. Tento systém řetězených kontrol důvěry pokračuje, dokud není dokončen celý proces bootování operačního systému Windows, pomocí procesů nazývaných Secure

Boot (bezpečné spuštění), Trusted Boot (důvěryhodné spuštění) a Measured Boot (měřené spuštění). (Intel)

Software

Tak jako veškerý hardware musí být spolehlivý a nekompromisní, stejný by měl být i celý software. Software obsahuje kód firmwaru, zaváděcí kód, operační systém a aplikace. Nejdůvěryhodnější software nejen kontroluje sami pro neoprávněné změny, ale také používá jiné procesy na vyšší úrovni a/nebo software ověřený důvěrou. Stejně jako rizika pro hardware, jakákoli škodlivá změna softwaru zapojeného kdekoli v procesu ověřování ohrožuje spolehlivost. Nejlepší autentizace bere v úvahu softwarové hrozby a snaží se zachovat si co největší spolehlivost. (Grimes, 2021)

API

Mnoho řešení MFA přichází se soukromým nebo otevřeným (tj. sdíleným) rozhraním pro programování aplikací (API). Tato rozhraní API mohou obsahovat chyby zabezpečení nebo mohou být škodlivým způsobem zneužita útočníkem. (Grimes, 2021)

Faktory autentizace

Samotné autentizační faktory mohou být ohroženy. Například jakýkoli biometrický atribut (otisk prstu, otisk sítnice atd.) může být zachycen a opětovně použit škodlivým způsobem. Malware může odcizit hesla a PIN-kódy nebo podvodně nutí uživatele, aby je vydali. Tajemství autentizace může být ukradeno z autentizačních zařízení. Je také možné škodlivě manipulovat s příslušným tvrzením. Mnozí hackeři jsou zaměřeni proti faktoru autentizace nebo schválení. (Grimes, 2021)

Authentication secrests store

Velice často směřují hackerské útoky proti databázím/úložištím, kde jsou uloženy autentizační tajemství. Neoprávněný přístup k úložišti autentizačních tajemství patří mezi nejničivější útoky, protože útočník může získat přístup ke všem tajemstvím uloženým v úložišti a znovu je použít.

Cryptography

Většina autentizačních řešení (i když ne všechna) používá kryptografii k ochraně sebe a svých vlastních tajemství. Většina autentizačních systémů používá kryptografické algoritmy a velikosti klíčů „industry-accepted“. Mnoho hackerů se snaží ohrozit buď samotnou kryptografii (detekují její vlastní slabost), nebo zjistit chyby v implementaci. To bývá mnohonásobně jednodušší a častější (Grassi, 2017).

Všechny standardy kryptografie přijaté v průmyslu postupem času slábnou. Kryptografické útoky se v průběhu času stávají jen lepšími, a to buď kvůli zvýšeným výpočetním zdrojům, nebo proto, že útoky najdou stále dokonalejší způsoby, jak využít vrozené kryptografické chyby v šifře. Povaha použití kryptografie je taková, že dodavatelé by měli vždy vědět, že stávající kryptografie se časem neustále oslabuje a že řešení MFA založené na této kryptografii by mělo být připraveno k přechodu na nové, silnější kryptografické standardy. Řada řešení MFA je implementována, pokud jde o kryptografické algoritmy a velikosti klíčů, jež mohou použít, tak, že je často nelze aktualizovat bez úplné výměny hardwaru a/nebo softwaru. (Grassi, 2017)

Technologie

Stejně jako kryptografie může být ohrožena jakákoli technologie používaná řešením MFA. Například mnoho řešení fyzických zařízení MFA je založeno na standardu univerzální sériové sběrnice (USB). USB je specifikace softwaru, rozhraní API a hardwaru a každá z těchto komponent může být vystavena útoku kdykoliv. (Grimes, 2021)

Transmission / Network Channel

Většina autentizačních řešení vyžaduje a používá přenos nebo síťový kanál, zvláště když se jedná o ověřování sítě nebo přístupu. Kanál se skládá ze softwaru a hardwaru přičemž tento software může být ohrožen, stejně jako jakýkoli jiný software a hardware. (Grassi, 2017)

Supporting infrastructure

Mnoho, ne-li většina řešení MFA závisí na řadě podpůrných infrastruktur, jako jsou DHCP, TCP/IP a IP adresy. Routery, které se podílejí na pomoci řešení MFA, pracují v síti pomocí směrovacích protokolů, jako jsou Router Internet Protocol (RIP), Interior Gateway Routing Protocol (IGRP), Enhanced Interior Gateway Routing Protocol (EIGRP), Open

Shortest Path First (OSPF), Intermediat, System to Intermediate System (IS-IS) a Border Gateway Protocol (BGP). Téměř všechna řešení MFA nakonec vycházejí z mnoha standardů, protokolů a technologií, které sami nevymysleli a neovládali. Každá z těchto technologií a podpůrné infrastruktury může být napadena, aby ohrozily řešení MFA. Například, škodlivý port USB může přepsat instrukce vestavěného USB zařízení nebo poslouchat a zaznamenávat data zařízení. (Grimes, 2021)

Adresy v síti jsou převáděny na fyzické adresy Media Access Control (MAC) pomocí protokolu Address Resolution Protocol (ARP). Většina počítačů získává své IP adresy z dynamických služeb konfigurace hostitele (DHCP). Síťové počítače s Windows používají pro připojení služby Active Directory. Počítače Linux často využívají LDAP. Počítače Apple zase pro automatickou konfiguraci síťových služeb sázejí na Bonjour. Nová zařízení USB jsou často automaticky registrována a rozpoznána díky standardu Universal Plug-n-Play (UPnP). Eéměř všechna řešení MFA nakonec závisí na více standardech, protokolech a technologiích, které si samy nevymyslela ani neovládá. A každá z těchto technologií a podpůrných infrastruktur může být napadena a hacknuta s cílem narušit řešení MFA. Například je možné, aby škodlivý port USB přepsal instrukce firmwaru zařízení USB nebo odposlouchával a zaznamenával data zařízení. (Grimes, 2021)

Relying party

Strana, která požaduje vaši autentizaci nebo se na ni spoléhá, může být ohrožena. Útočník může obcházet požadavky na autentizaci ověřovací strany, nebo dokonce hackovat jejich ověřovací stranu. Každá složka, která se podílí na autentizaci, je potenciálním vektorem útoku a zahrnuje v sobě poslední ověřovací stranu. (Grimes, 2021)

Federation / Proxies

Mnoho stránek a služeb se při rozhodování spoléhá na proces ověřování jiných stránek nebo služby umožnit subjektu, aby se na nich ověřoval. Ověřovatel webu nebo služby říká: „Důvěřuji vaší autentizační službě natolik, abych si byl jistý, že jste ověřili subjekt správně, a budu se spoléhat na tuto autentizaci.“ To lze provést pomocí sdílených rozhraní API, ověřování proxy, společného jediného přihlášení (SSO), služby a federace. Federace se stává nejčastějším řešením. Jedná se o propojení nebo použití ověřených identifikačních údajů ve více systémech správy identit, webových stránek a služeb. Kombinované služby mohou být jednoduše mezi vnitřními jednotkami stejné organizace,

mezi několika organizacemi nebo globálně mezi všemi zúčastněnými stranami. Existuje zde riziko, že je mnoho technologií zapojeno do ověřování, například federace, jedná se o řešení jednotného vstupu. Pokud dojde k ohrožení autentizace nebo jednotného vstupního tokenu, bude snazší kompromitovat vše, co toto řešení umožňuje nebo na co spoléhá. (Grimes, 2021)

Alternativní metody autentizace / Obnovení

Většina hlavních řešení MFA, dodavatelů a kontrolních stran má alternativní prostředky ověřování účastníků. Řešení MFA je vždy více, jsou složitější než řešení 1FA, a proto jsou náchylné k poruchám všech typů. Dodavatelé vytvářejí jednoduché automatizované metody, aby se uživatel mohl přihlásit, pokud nemůže použít své řešení MFA podle původního záměru. Útočníci často zneužívají tyto alternativní metody. (Grimes, 2021)

Migrace

Migrace je méně obvyklá metoda hackingu. Vzácně organizace užívají nebo získávají jednu metodu autentizace, kterou používají po zbytek své existence v síti. Obvykle se ověřovací systém nebo jeho databáze identit aktualizují nebo přecházejí na nové, dokonalejší metody. Organizace se v důsledku fúzí a akvizic často mění. Tyto změny nezřídka vyžadují přenos starých a stávajících autentizačních systémů i uživatelů na novější nebo jiný systém. Existují určité hackery, které mohou při těchto migracích vzniknout (Grimes, 2020).

Příkladem hacku na eskalaci privilegií (EOP) je tzv. útok SID History (*Mitre att&ck*), ke kterému může dojít během migrací sítí Active Directory. Všechny účty principálů zabezpečení AD (uživatelé, počítače, skupiny atd.) mají pole atributu s názvem Historie SID. Toto pole bylo zamýšleno tak, aby administrátoři mohli předem naplnit aktuální a/nebo budoucí členství principála zabezpečení v bezpečnostních skupinách, když je existující principál zabezpečení migrován do nového lesa nebo domény AD. Migrace AD se dějí neustále v důsledku konsolidace sítí a fúzí. Pole Historie SID nebylo široce známé, chráněné ani monitorované až do příchodu Windows Server 2003. Předtím mohl škodlivý administrátor přidat do účtu principála zabezpečení členství ve vysoce privilegovaných skupinách (např. Administrátoři schématu, Administrátoři domény, Administrátoři) a po migraci se tato учетная запись stala členem privilegované bezpečnostní skupiny, někdy bez úmyslu administrátorů cílového lesa nebo domény a aniž by si byli vědomi, že se to stalo.

Po mnoho let to byl málo používaný, ale kritický útok na eskalaci privilegií. Od Windows Server 2003 AD standardně "filtruje" hodnoty historie SID, aby se zabránilo nechtěnému zvýšení zabezpečení. I dnes vyžaduje zapnutí nebo vypnutí filtrování historie SID pouze změnu jediné binární hodnoty v AD. Vše, co musí škodlivý administrátor udělat, je změnit hodnotu z 1 na 0 na jednom místě, aby útok s využitím historie SID znovu fungoval. (Grimes, 2021).

Migrace bývají vesměs neobvyklé, nepravidelné činy. Mnoho procesů nekontroluje potenciální zranitelnosti a řada administrátorů nekontroluje takové útoky a neobtěžuje se o ně. Proto, bez ohledu na to, jak neobvyklé migrace bývají, stále představují významné riziko pro každou organizaci. (Grimes, 2021)

Deprovize

Chcete-li dokončit procesy životního cyklu autentizace, zrušení autorizace je proces odstranění, nebo deaktivace průkazů. To se obvykle provádí registračním CSP, ale může být provedeno nebo požadováno spoléhající stranou. Deprovize bývá často špatně řízena. Mnohdy se stává, že neaktivní a nepoužívané účty jsou mnohem více než aktivní, používané účty v ověřovací systému. Každý neaktivní, nepoužívaný účet, s nímž není zrušeno oprávnění, představuje potenciální hrozbu pro všechny ostatní v systému, zejména pokud jde o nepoužívané účty, které mají přístup administrátora k použitému autentizačnímu systému. Všechny autentizační systémy by se měly snažit přísně měřit a kontrolovat to, které účty jsou aktivní a používané, a které se stávají neaktivními a nepoužívanými, a zrušit povolení k použití druhé.

3.4 Detekce zranitelnosti MFA

Zranitelnosti mohou být objeveny pomocí mnoha různých metod, včetně oficiálních, jako jsou modelování hrozeb, analýza kódu, fuzzy testování, penetrační testování, skenování zranitelností, testování na lidech a náhodou – buď dobře míněnými lidmi, nebo vetřelci.

Modelování hrozeb

Nejlepší způsob, jak zabránit zranitelnosti a najít ji, je provést simulaci hrozeb. Modelování hrozeb je, když vývojáři nebo následní recenzenti přezkoumají komponentu nebo ještě lépe celý systém jako celek a snaží se předpovědět všechny různé způsoby, jak

může být ohrožena, nebo dokonce náhodně zlomena. Když je vše provedeno správně, modelování hrozeb pomáhá ve výchozím nastavení zajistit vyšší bezpečnost. Proces modelování hrozeb začíná zobecněním navrhovaného řešení, členěním jednotlivé fáze komponentu a brainstorming všech možných způsobů, jak každý z nich může být opraven s chybami. To zahrnuje úvahy o různých hranicích bezpečnosti a důvěry a objasnění, jak je možné zneužít cokoliv z nich. Vývojáři modelů hrozeb mohou vytvářet „stromy útoků“, které ukazují, jak může útočník přejít z jednoho nebo více exploitů na dosažení konečného cíle (obcházení ochranných prostředků, prohlížení chráněných informací atd.). Existují modely, nástroje a strukturovaná měření rizika, jež pomáhají při modelování hrozeb. V případě úspěchu tým pro modelování hrozeb může analyzovat všechny známé hrozby i rizika a minimalizovat je pomocí vestavěných kontrol a zmírňování následků. Jakékoli řešení MFA, které využívá dobře navržené modelování hrozeb, bude pravděpodobně mít méně chyb a zranitelností než něco, co to neudělalo. (Grimes, 2021)

Code review

Všechna řešení MFA zahrnují programovací kód. Výsledkem kódu může být software, instrukce firmwaru nebo obojí. Celý kód obsahuje chyby. Kontrola kódu, provedená buď lidmi, nebo automatizovaným softwarem skenuje, může najít předdefinované chyby zabezpečení. Nejlepší recenze kódu zahrnují oba, jako každý často najde to, co druhému chybí. (Grimes, 2021)

Fuzz testing

Software pro testování Fuzz najde potenciální využití různými vstupy desítky až stovky různých způsobů. Předpokládejme například, že část softwaru požádá uživatele, aby zadali své přihlašovací jméno, kde se očekává přihlašovací jméno, které by se skládalo z dvaceti nebo méně znaků. Fuzzer by spustil program a případně zadejte přihlašovací jména složená ze stovek různých kombinací. Mohlo by to dát příliš dlouhá přihlašovací jména, přihlašovací jména složená pouze z čísel, řídicí znaky tiskárny nebo spustitelný soubor například kód. Fuzzer by proaktivně vyzkoušel nejrůznější kombinace, očekávané a neočekávané. Podíváme-li se, zda přijímající program vyvolá chybu, a pokud je chyba vyhozena, zda se jedná o chybu, která by mohla být zneužita. (OWASP)

Penetration testing

Penetrační testování zahrnuje softwarové nebo kvalifikované lidské protivníky, kteří chtějí využít cíl. Mohou používat fuzzingové techniky, ale obvykle jdou daleko nad rámec jen různých reakcí na vstupy. Zaměří se na všechny zúčastněné komponenty, které hledají nové a staré zranitelnosti. Stejně jako u kódu recenze, nejlepší penetrační testování používá kombinaci automatizovaných a lidských útočníků. (Grimes, 2021)

Existují dva odlišné typy virtuálního penetračního testování. Prvním typem je penetrační testování s bílou skříňkou (white-box). Tato strategie spočívá v prozkoumání celého systému s maximálním množstvím předchozích znalostí pro přístup k informacím v systému. Ať už na fyzické nebo virtuální straně, jde spíše o zjevný přístup než o nenápadný. Díky této strategii může tester penetrace najít nejvíce informací, protože má povolený největší přístup. Jednou z nevýhod tohoto přístupu je, že neodráží zcela přesně, jak by se do systému dostal skutečný hacker. (Sweigert,2022)

Druhá používaná metoda se nazývá penetrační testování s černou skříňkou (black-box). Je opakem testování s bílou skříňkou. Penetrační testování s černou skříňkou je realističtějším způsobem testování systému nebo sítě organizace. Tuto metodu lze považovat za realističtější přístup, protože tester dostává stejné informace jako skutečný hacker, což znamená málo nebo žádné informace. To vše by záviselo na tom, kolik informací byl hacker schopen najít předem nebo získat z předchozího průzkumu. Tato strategie je považována za diskrétnější než ostatní přístup, protože společnost nebo klient, který má být hodnocen, nemusí nutně vědět, kdy tester tento test provádí. To je realističtější způsob, jakým by hacker provedl svůj útok. Po provedení útoku se ukáže, jak zranitelný může být systém skutečnému útoku. (Sweigert,2022)

Při provádění fyzického penetračního testu, který zahrnuje skutečné vniknutí do zařízení nebo pokus o získání přístupu k citlivým informacím například pomocí páčení zámků nebo šplhání po plotech, tester penetrace nejprve před provedením těchto taktik vypracuje plán, jak fyzický test provede, a to předchozím průzkumem místa. Ať už se jedná o fyzický nebo virtuální penetrační test, oba mají stejný účel - pokusit se získat přístup k citlivým informacím. (Sweigert,2022)

Vulnerability scanning

Skenování zranitelností je téměř vždy prováděno automatizovaným softwarem, který hledá známé zranitelnosti, jež lze použít. Skenování zranitelností je podmnožinou

penetračního testování, ale je zaměřeno pouze na vyhledávání zranitelností aplikací způsobených chybami a slabými místy. Obvykle se hledají známé chyby zabezpečení, které byly opraveny dodavatelem, ale které zůstávají nepoužitelné zkoumaný cíl. Ale to může také zahrnovat nalezení běžných chyb v kódování, nesprávných nastavení, výchozí hesla a problémy, které snižují výkon. Nejlepší skenery zranitelnosti mají vzestupný z více než 50 000 testů. Skenery zranitelnosti jsou skvělé nástroje, ale pokud je to jediná věc, která se používá defender pro vyhledávání a prevenci zranitelnosti, mohou se ukázat jako neefektivní. Je třeba použít i jiné metody. (Grimes, 2021)

Human testing

Mnoho zranitelností bylo objeveno jen člověkem, který se podíval na konkrétní řešení a snažil se odhadnout různé možné zneužití. Každý profesionální penetrační tester používá kombinaci svých oblíbených nástrojů pro automatizaci a vlastní mysl pro hledání chyb a zranitelností. Být dobrým člověkem, který hledá chyby, vyžaduje kombinaci zkušeností, vynalézavosti a vytrvalosti. Většina testerů chyb má tendenci se specializovat na typ chyb, které zjistí. Zaměřují se na jeden typ operačního systému, jeden jazyk, jeden typ funkčnosti serveru a tak dále. (Grimes, 2021)

3.5 Metody hackingu MFA

Technická metoda

Technické útoky jsou útoky na technické prvky digitálního řešení. Jsou to útoky na samotné řešení, na to, jak je navrženo a jak funguje. Představují přímý útok na digitální komponenty řešení. Například technický útok může být metodou zveřejňování uložených tajemství autentizace. (Grimes, 2021)

Dokonce i místní správce nebo členové domény Administrátoři skupiny zabezpečení nemohou přímo přistupovat k tajemstvím uloženým v systému Windows nebo k aktivnímu Databáze ověřování adresářů. Chcete-li zobrazit uložená autentizační tajemství, předmět nebo proces, je potřeba mít ještě vyšší systémová (tj. lokální systémová) oprávnění nebo ekvivalent. Kromě toho, procesy operačního systému, které chrání tato tajemství, se snaží zabránit známým útokům a prostředky útoku z přístupu k těmto tajemstvím, i když útočník má potřebná oprávnění. (Grimes, 2021)

Dalšími příklady technických útoků jsou porušení šifrování, které chrání tajemství, hledání předvídatelných šablon v tom, co by mělo být skutečně náhodná informace, detekce náhodných textových kopií toho, co by mělo být zašifrovanou informací, ohrožení použitých koncových bodů a ostatní účastníci, zachycení jmenných prostorů, odposlech komunikačních kanálů a další podobné útoky. Technický útok spočívá ve zjištění nedostačující digitální technologie, která je základem spolehlivosti řešení. (Grimes, 2021)

Lidská metoda

Sociální inženýrství může být definováno jako proces škodlivého maskování jako důvěrník za účelem získání neoprávněných informací nebo vytvoření požadovaného opatření v rozporu s osobními zájmy oběti nebo jejich organizace. Jednoduše řečeno, sociální inženýrství je „podvod“ s kriminálními nebo neetickými úmysly zaměřenými na manipulaci se zákonným chováním lidí. To lze provést několika způsoby, včetně osobního, taktéž prostřednictvím e-mailu či služby Instant Messaging, Short Messaging Service (SMS), sociálních sítí a hlasový telefon v zákulisí. V závislosti na formě a záměru sociálního inženýrství může být také nazýván phishingem, phishingem s kopím (tj. cíleným), rozesíláním spamu nebo visingem (tj. pomocí hlasů v zákulisí). Systémy sociálního inženýrství mohou zahrnovat autoritativní subjekty, které tvrdí, že jsou orgány činné v trestním řízení, vládní úředníci, přátelé, kolegové, populární sociální stránky, banky, aukční stránky nebo správci IT. Jakýkoli vztah, který může povzbudit někoho, aby se řídil navrhovaným, se obvykle používá k nalákání nic netušící oběti. (Newman, 2019)

Lze argumentovat, že jakékoli selhání autentizace způsobené lidskou chybou nebo špatným rozhodnutím o riziku lze oprávněněji přičítat technickému selhání. Můžete si myslet, že kdyby bylo řešení lépe navrženo, nebyl by člověk požádán o učinění riskantního rozhodnutí, které by mohlo vést k sebepoškození. A kdyby bylo možné navrhnout systém, který by nezahrnoval člověka, byla by to pravda. Všechny systémy pro ověřování uživatelů však inherentně zahrnují uživatele. Minimálně se člověk obvykle (ale ne vždy) podílí na spuštění systému ověřování, aby získal přístup k chráněnému zdroji, ke kterému se snaží dostat. (Newman, 2019)

Fyzická metoda

Mnohé hackerské útoky vyžadují fyzický přístup k hackerskému objektu. Nejjednodušší typ fyzického útoku je krádež zařízení, které chránilo řešení MFA (například ukradený notebook nebo telefon), případně krádež samotné řešení MFA (například někdo ukradne samotný autentizační token). Krádež je útok typu odmítnutí služby (DoS). Fyzické útoky jsou spíše způsoby, kterými tajemství řešení MFA mohou být ohrožena nebo obcházena útočníkem, který má fyzický přístup k zařízení MFA. Fyzické držení je klíčem k metodě potřebné k provedení tohoto typu útoku. Pro tuto kategorii útok nelze provést na dálku nebo virtuálně anebo alespoň téměř tak snadno. Některé z fyzických, a tak vyžadují spoustu zkušeností a/nebo drahé vybavení. Jiné vyžadují velmi málo zkušeností a prakticky žádné vybavení (Grimes, 2020).

4 Vlastní práce

Cílem praktické části mé práce je navrhnout vlastní systém dvoufaktorové autorizace a provedení srovnávací analýzy různých metod. Pro implementaci mé verze dvoufaktorové autorizace byla zvolena metoda s využitím fyzického klíče jako prvního faktoru a zadávání hesla jako druhého faktoru autorizace. Volba této kombinace byla založena na dostupnosti metod.

4.1 Fyzický klíč

Jako fyzický klíč bude použito zařízení badUSB, obvykle určené pro nelegální nebo škodlivé účely. Ve vlastní implementaci, využívající jeho mechanismus emulace klávesnice, lze toto zařízení použít jako fyzický klíč.

Obrazek 6 - badUSB

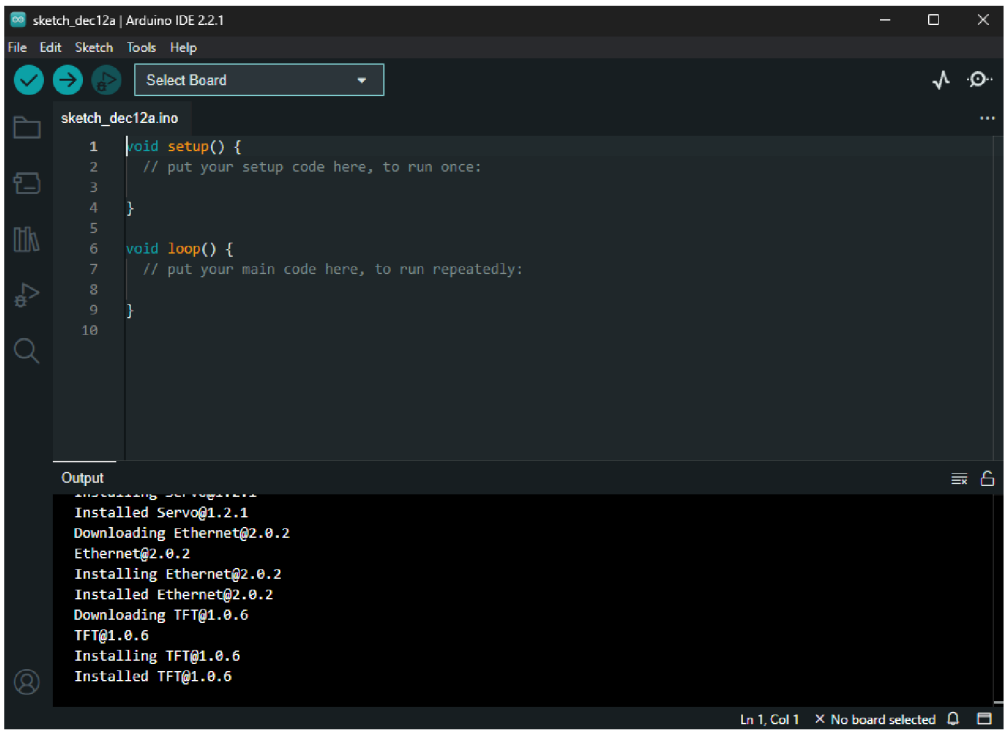
Přístroj byl zakoupen v internetovém obchodě s následujícími parametry:

- ATmega32u4;
- PWM Channels : 4;
- clock speed : 16MHz;
- digital I/O Pins : 10;
- analog Input Channels : 5;
- I2C : 1;
- UART : 1;
- SRAM : 2.5KB;
- micro USB : 1;
- size : 41.93x16.27x8.12mm (15g).

Programování

Pro programování modulů Arduino Leonardo a také badUSB bude nutné prostředí Arduino IDE.

Obrazek 7 - Vývojové prostředí Arduino IDE



Před začátkem programování badUSB bylo nejprve připraveno vývojové prostředí. K tomu byla připojena knihovna HID-Project, která umožňuje z badUSB udělat emulátor klávesnice. Zakoupený badUSB je založen na Arduinu Leonardu, takže byla následně v nastavení vybrána tato deska a port COM7, na kterém toto zařízení funguje.

Pro správné fungování skriptu byl nejprve povoleno záhlaví HID-Project, bylo definováno makro s názvem PWD s hodnotou „password“. Následně byly deklarovány dvě globální celočíselné proměnné: change_lang a main_delay. Poté byla přidána funkce pro emulaci stisknutí a uvolnění klávesy, funkce pro emulaci kombinace kláves Ctrl+Alt+Del a funkce pro stisknutí klávesy Enter.

Obrazek 8 - Přidání funkce kláves

```
#include "HID-Project.h"
#define PWD "password"

int change_lang = 0;
int main_delay = 0;

void PressKey(unit8_t key) {
  Keyboard.press(key);
  delay(50);
  Keyboard.release(key);
}

void AltCtrlDel() {
  Keyboard.press(KEY_LEFT_ALT);
  Keyboard.press(KEY_LEFT_CTRL);
  Keyboard.press(KEY_DELETE);
  delay(40);
  Keyboard.releaseAll();
}

void Enter() {
  Keyboard.press(KEY_RETURN);
  delay(40)
  Keyboard.release(KEY_RETURN);
}
```

Pro větší pohodlí byly do kódu implementovány tři mechanismy, a to konkrétně:

1. změna rozložení klávesnice;
2. volání správce úkolů;
3. umělá prodleva.

Pomocí prodlevy lze přizpůsobit skript konkrétní výkonnosti počítače. Pokud nejsou dostatečné výpočetní kapacity, je třeba prodlevu zvětšit. Aby se zabránilo náhodnému spuštění kódu, když je klíč vložen do odemčeného počítače, je volán správce úkolů, heslo není nikam zadáváno.

Nastavení systému se může lišit, a proto byla implementována část se změnou rozložení klávesnice. To je zapotřebí k tomu, aby byl po zapnutí počítače změněn jazyk, pokud výchozí jazyk není vhodný pro zadání hesla.

Obrazek 9 - Změna jazyka rozložení

```
void setup(){
  Keyboard.begin();
  delay(1000);
  AltCtrlDel();

  if(main_delay != 0){
    delay(main_delay*1000);
  }

  if(change_lang !== 0){
    delay(1000);

    if(change_lang == 1) {
      keyboard_press(KEY_LEFT_ALT);
      keyboard_press(KEY_LEFT_SHIFT);
      delay(500);
      Keyboard.releaseAll();
  }

    else
      if(change_lang == 2) {
        keyboard_press(KEY_LEFT_CTRL);
        keyboard_press(KEY_LEFT_SHIFT);
        delay(500);
        Keyboard.releaseAll();
    }
}
delay(500);

Keyboard.print(PWD);
Enter();
}
```

Po všech kontrolách podle scénáře skriptu je zadáno heslo, které odemkne systém Windows.

4.2 Dotaz na heslo

Po přihlášení do systému Windows je jako druhý faktor, konkrétně faktor znalosti, spuštěn skript vyžadující heslo, které uživatel zná. Skript je implementován v prostředí Visual Studio ve Windows Forms.

Hlavními úkoly tohoto skriptu jsou ověření znalosti hesla, provedení autorizace a správná práce s výjimkami.

Programování

Před sestavením formy byly přidány důležité části rozhraní. Na formě se nachází textové pole (TextBox) pro zadávání hesla a tlačítko (Button) „Odemknout“ pro odemčení. Textové pole je nakonfigurováno tak, aby zobrazovalo hvězdičky místo zadaných znaků pro zvýšení bezpečnosti.

Byly také přidány potřebné konstanty pro zprávy Windows, virtuální kódy kláves, delegát pro zpětné volání procedury hooku a samotný hook i procedura zpětného volání pro sledování událostí klávesnice.

Obrazek 10 - Rozhraní formuláře

```
private TextBox passwordTextBox;
private Button unlockButton;
private const string CorrectPassword = "password";
private bool isPasswordRight = false;


private const int WH_KEYBOARD_LL = 13;
private const int WM_KEYDOWN = 0x0100;
private const int WM_SYSKEYDOWN = 0x0104;


private const int VK_TAB = 0x09;
private const int VK_LWIN = 0x5B;
private const int VK_RWIN = 0x5C;


private delegate IntPtr LowLevelKeyboardProc(int nCode, IntPtr wParam, IntPtr lParam);


private static IntPtr _hookID = IntPtr.Zero;
private static LowLevelKeyboardProc _proc = HookCallback;
```

Při vytváření instance formuláře je volána metoda InitializeComponent(), která nastavuje parametry komponent formuláře. Poté je volána metoda InitializeUI(), jež nastavuje rozhraní formuláře.

Pro správný chod je skript automaticky spuštěn na celou obrazovku, skrývá ovládací panel a odstraní okenní rámečky. Pro zajištění spolehlivosti má okno skriptu také prioritu před ostatními okny.

Další bezpečnostní metody zpracování událostí:

- UnlockButton_Click(). Volá se po stisku tlačítka „Odemknout“. Zkontroluje zadané heslo. Pokud je správné, nastaví příznak odemknutí (isPasswordRight) na true a ukončí aplikaci. V opačném případě zobrazí chybové hlášení.

- Form3_Resize(). Volá se po změně velikosti formuláře. Zabraňuje minimalizaci okna.
- OnFormClosing(). Volá se při zavírání formuláře. Zabraňuje zavření, pokud heslo nebylo zadáno.

Hook klávesnice:

- SetHook(). Nastavuje hook na klávesnici pomocí funkce SetWindowsHookEx z předem připojené knihovny user32.dll. Hook zachytává události kláves před jejich zpracováním operačním systémem.
- HookCallback(). Procedura zpětného volání hooku. Volá se při každé události klávesnice. Pokud je stisknuta klávesa Alt+Tab nebo klávesa Win, vrátí se (IntPtr)1, což zabrání dalšímu zpracování této klávesy.

Uživatel proto nemůže minimalizovat okno, vytvořit další pracovní plochu, zavolat správce úkolů nebo násilně ukončit běh skriptu pomocí klávesových zkratek.

Importované funkce:

Importované funkce z user32.dll se používají k řízení hooku klávesnice: SetWindowsHookEx k nastavení hooku, UnhookWindowsHookEx k odstranění hooku (používá se, když hook již není potřebný a měl by být uvolněn tímto způsobem, aby se zabránilo úniku paměti), CallNextHookEx k předání řízení dalšímu handleru (je to důležité, aby jiné programy nebo systém mohly zpracovat klávesu poté, co ji váš hook zpracoval), GetModuleHandle k získání handle modulu.

Obrazek 11 - Řízení hooku klávesnice

```
[DllImport("user32.dll", CharSet = CharSet.Auto, SetLastError = true)]
Ссылок: 1
private static extern IntPtr SetWindowsHookEx(int idHook, LowLevelKeyboardProc lpfn, IntPtr hMod, uint dwThreadId);

[DllImport("user32.dll", CharSet = CharSet.Auto, SetLastError = true)]
[return: MarshalAs(UnmanagedType.Bool)]
Ссылок: 0
private static extern bool UnhookWindowsHookEx(IntPtr hhk);

[DllImport("user32.dll", CharSet = CharSet.Auto, SetLastError = true)]
Ссылок: 1
private static extern IntPtr CallNextHookEx(IntPtr hhk, int nCode, IntPtr wParam, IntPtr lParam);

[DllImport("kernel32.dll", CharSet = CharSet.Auto, SetLastError = true)]
Ссылок: 1
private static extern IntPtr GetModuleHandle(string lpModuleName);
```

Tyto funkce zajistí správné nastavení i odstranění globálního hooku na klávesnici a také předání řízení dalšímu závěsu v řetězci zpracování událostí, což zajišťuje správnou funkčnost mechanismu zachytávání kláves.

Scénář dvoufaktorové autentizace

1. Zadání fyzického klíče.
    - Zaměstnanec vloží USB klíč (fyzický klíč) do počítačového portu.
    - Klíč automaticky provede skript, který zadává jedinečné heslo pro primární autentizaci do systému Windows.
2. Potvrzení vlastnictví klíče.
    - Automaticky zadané heslo slouží jako první faktor autentizace a potvrzuje vlastnictví fyzického klíče.
3. Spuštění uživatelské aplikace.
    - Po úspěšné autentizaci se otevře pracovní plocha Windows.
    - Automaticky se spustí uživatelská aplikace vyvinutá zaměstnavatelem nebo distributorem.
4. Zadání druhého faktoru (hesla).
    - Uživatelská aplikace vyžaduje druhý faktor autentizace ve formě hesla.
    - Zaměstnanec zadá předem známé heslo, které slouží jako druhý faktor.
5. Potvrzení identity
    - Zadání hesla zaměstnancem potvrzuje jeho identitu a slouží jako druhý faktor autentizace.
6. Přístup k prostředkům

Při úspěšné kontrole obou faktorů je zaměstnanci poskytnut přístup k zabezpečeným prostředkům.

4.3 Úvod do analýzy a kritéria srovnání metod autentizace

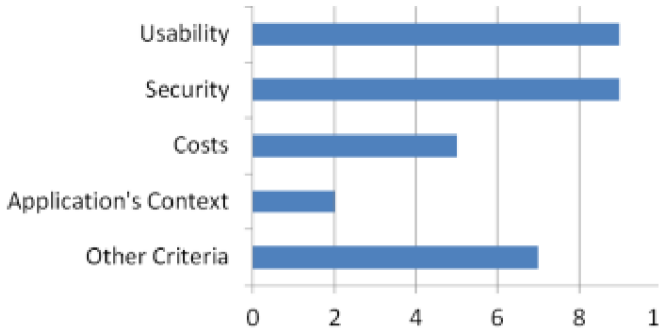
Jak bylo uvedeno v předchozích částech této práce, v současné době existuje mnoho různých metod autentizace založených na různých principech. Kromě toho použití páru „uživatelské jméno – heslo“, které bylo dlouhou dobu považováno za hlavní mechanismus autentizace ve většině případů, postupně ztrácí na aktuálnosti. Tyto faktory zdůrazňují potřebu provádět srovnávací analýzu existujících metod autentizace s cílem identifikovat nejperspektivnější metody, které lze použít v různých situacích spojených s ověřováním identity uživatele.

Pro srovnání různých metod autentizace lze identifikovat celou řadu kritérií srovnání, včetně kvantitativních (například procenta falešných přijetí a odmítnutí), stejně jako kvalitativních (bezpečnost, spolehlivost, pohodlí používání atd.). Důležité je určit, jak mezi mnoha kritérii vybrat nejvýznamnější a jak provádět srovnání, pokud jsou kritéria samotná složitá a mnohostranná a jejich přesné určení bývá často nejednoznačné.

Výzkumníci z chilské univerzity Bío-Bío Ignacio Velasquez, Angelika Karo a Alfonso Rodriguez realizovali studie, během nichž zjistili, která kritéria jsou nejčastěji považována za nejdůležitější při výběru konkrétní metody autentizace. (Velásquez, 2017)

Na obrázku 12 je zobrazeno srovnání kritérií podle počtu vědeckých článků na téma autentizace, jež zohledňují dané kritérium.

Obrazek 12 - Počet článků, které zohledňují dané kritérium



V tabulce 2 jsou uvedena kritéria, která byla častěji než ostatní označena jako důležitá respondenty z výzkumných institucí a firemními zástupci, kteří se ocitli před volbou nové metody autentizace. (Velásquez, 2019)

Tabulka 2 - Seznam kritérií podle počtu dotázaných, kteří je zohledňují

Criterion	Interviewees that consider the criterion
Client's requirements	11
Application context	11
Usability-related criteria	9
Security-related criteria	11
Cost-related criteria	8
Other criteria	2

Tímto způsobem, z množiny kritérií, podle kterých lze porovnávat metody autentizace, je vhodné vyzdvihnout následující jako nejdůležitější:

- bezpečnost;
- pohodlí používání;
- škálovatelnost;
- kontext aplikace a požadavky klienta.

4.3.1 **Framework srovnání mechanismů autentizace**

Za účelem srovnání podle jakéhokoli z těchto kritérií, kde každé z nich je dostatečně obecné a sama o sobě zahrnují celou řadu faktorů, a pro určení v etapě rozhodování o volbě metody, nikoli až po jejím nasazení a získání empirických dat o jejím využití, byla pozornost zaměřena na jednu z metodik srovnání různých mechanismů autentizace, který byl navržen v článku „The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes“, napsaném výzkumníky z univerzity v Cambridge Josephem Bonnem a Frankem Stajanem ve spolupráci s Paulem van Orschotem z kanadské univerzity Carlton a zaměstnancem společnosti Microsoft Cormacem Herleyem. Ti navrhují framework pro hodnocení metod pomocí tří kritérií, který je v článku označen jako „UDS“ (usability-deployability-security). (Bonneau, 2012)

V rámci tohoto frameworku se každé z kritérií skládá z určitého počtu výhod, jež daný mechanismus autentizace může uživateli poskytnout. Na základě počtu výhod v každé ze tří kategorií, přičemž každá kategorie může mít svou váhu v závislosti na její důležitosti, lze provést kvantitativní srovnání několika mechanismů autentizace a vybrat nejvhodnější.

Dále jsou zkoumána výše uvedená kritéria v rámci tohoto rámce, uvedeny jsou klíčové výhody pro každé kritérium. Poté je ukázáno, jak na jejich základě můžeme posoudit

konkrétní metodu. Nakonec jsou prozkoumány některé metody, které byly zmíněny v předchozích částech práce, z pohledu rámce UDS.

Bezpečnost

Pro jakýkoli systém autentizace je bezpečnost jedním z nejdůležitějších požadavků. Výhody, ze kterých se skládá kritérium bezpečnosti v rámci rámce UDS, jsou především spojeny s odolností vůči různým útokům na mechanismus autentizace.

Pro toto kritérium lze identifikovat následující výhody:

1. Odolnost vůči fyzickému pozorování. Tato kategorie útoku zahrnuje sledování obrazovky nebo získání výsledků zadávání z klávesnice.

2. Odolnost vůči impersonaci. Osoba, která dobře zná uživatele, nemůže získat přístup k systému, znalostí jeho osobních údajů (např. jako odpověď na „tajnou otázku“).

3. Odolnost vůči brute-force útokům. Částečnou shodou se rozumí odolnost vůči útokům, jejichž počet je v určeném časovém úseku omezen.

4. Odolnost vůči internímu pozorování. Útočník nemůže získat přístup k systému odposlechem zpráv, které procházejí komunikačním kanálem.

5. Odolnost vůči únikům z jiné služby. Údaje, které by útočník mohl získat při prolomení serveru potvrzující strany nebo jejich únikem jiným způsobem, nemohou být použity k autentizaci pod stejným uživatelem v jiné službě.

6. Odolnost vůči phishingovým útokům. Útočník nemůže získat uživatelské údaje potřebné k autentizaci simulací reálné služby.

7. Odolnost vůči fyzické krádeži klíče. Pokud útočník získá fyzické zařízení, nemůže ho použít k přihlášení do systému pod záminkou uživatele. Částečně odpovídá slabé ochraně, např. PIN-kódu.

8. Absence důvěryhodné třetí strany. Metoda nespoléhá na třetí stranu, která by také mohla být napadena a stát se zdrojem úniku dat.

9. Nutnost explicitního souhlasu. Proces autentizace nemůže začít bez explicitního souhlasu uživatele.

10. Nemožnost spojit různé autentizátory stejného uživatele. Toto výhoda poskytuje ochranu identity uživatele. Zde nejsou brány v úvahu faktory, jako je například stejná IP-adresa.

Pohodlnost používání

Pohodlí používání může ovlivnit i bezpečnost mechanismu autentizace. Klasickým příkladem jsou dlouhá, složitá hesla, která mnoho uživatelů raději zaznamenává na papírová média, což samo o sobě není bezpečné. Potřeba si pamatovat velké množství hesel vede k jejich opakovanému používání, což zvyšuje úroveň rizika při krádeži jednoho z nich.

Mezi výhody, které systémy autentizace mohou poskytovat v oblasti pohodlí používání, patří následující:

1. Absence potřeby pamatovat si informace. Uživatel si nemusí pamatovat žádná tajemství (hesla, kódy). Částečnou shodou může být situace, kdy si uživatel musí pamatovat pouze jedno heslo bez ohledu na počet účtů.

2. Škálovatelnost z pohledu uživatele. Používání metody k vytváření velkého množství účtů nemá vliv na zkušenost konkrétního uživatele.

3. Absence potřeby nošení fyzického objektu. Částečnou shodou může být použití mobilního telefonu (protože většina lidí ho nosí stále u sebe).

4. Fyzická lehkost autentizace. Není nutné například zadávat dlouhá hesla nebo fráze.

5. Snadnost ovládání. Lze snadno pochopit a zapamatovat si, jak metodu používat.

6. Rychlost používání. Zohledňuje jak dobu nutnou k přihlášení, tak i dobu nutnou k vytvoření nového účtu.

7. Malý počet chyb při přihlašování. Úroveň falešných odmítnutí (FRR) by měla být dostatečně nízká.

8. Jednoduchost obnovení. Pokud uživatel z nějakého důvodu ztratí možnost přihlásit se do systému, měla by existovat možnost snadného a rychlého znovuzískání přístupu.

Rozvinutelnost

Rozvinutelnost (z anglického *deployability* – schopnost nasazení) je poměrně široké kritérium, které obecně určuje, jak snadné a pohodlné je implementovat daný mechanismus do reálného distribuovaného systému.

V rámci frameworku UDS zahrnuje kritérium rozvinutelnosti následující možné výhody:

1. Nízká cena za jednoho uživatele. Náklady na připojení uživatele k systému (jak ze strany uživatele, tak ze strany majitele systému) by měly být relativně nízké.

2. Kompatibilita se serverem. Metoda je kompatibilní s použitím textových hesel.

3. Kompatibilita s prohlížeči. Uživatelé mohou používat libovolný moderní prohlížeč bez nutnosti instalace dalšího softwaru.
4. Historie použití. Tato metoda je již používána v rozsáhlém systému autentizace. Také mohou být brány v úvahu projekty, které tuto metodu používají, dostupnost dokumentace, absolvování testů, atd.
5. Otevřený přístup. Zdrojový kód projektu je volně dostupný, není nutné platit za používání metody.
6. Dostupnost. Metoda autentizace může být používána uživateli s omezenými schopnostmi (alespoň těmi, kteří mohou používat přihlášení na základě uživatelského jména a hesla).

4.3.2 Metodika numerického srovnání mechanismů autentizace

Nyní můžeme přidělit hodnocení odpovídajícího mechanismu autentizace požadavkům každého kritéria na základě přítomnosti, nebo nepřítomnosti každé výhody. Výhody kritérií nemusí být nutně binární („poskytováno /poskytováno částečně“). Nejméně v některých případech může být částečné poskytování určité výhody možné. Takže ve svém nejjednodušším případě lze číselné hodnocení výhodě přiřadit hodnotu 0 (není poskytována), 0,5 (poskytována částečně), nebo 1 (poskytována).

Dále může být význam každé z výhod v rámci jednoho kritéria různý. Například kompatibilita s prohlížečem může být málo důležitá, pokud použití prohlížeče v daném kontextu není předpokládáno. Proto pro přesnější číselné hodnocení lze každé z výhod přiřadit určitou váhu, která závisí na její důležitosti v tomto nebo onom kontextu.
Takže shodu mechanismu autentizace s jakýmkoli kritériem lze ocenit podle následujícího vzorce:

$$S_i = \sum_j W_j \cdot b_j$$

kde S_i je kvantitativní hodnota kritéria i

W_j je váha přiřazená určité výhodě tohoto kritéria

b_j je přítomnost (částečná nebo plná), nebo nepřítomnost této výhody ve zkoumaném mechanismu autentizace

Jelikož jsou v rámci rámce UDS zkoumána tři kritéria, platí $i \in [1; 2; 3]$.

Hodnoty vah závisí na konkrétním scénáři, který vyžaduje autentizaci, ale „ve výchozím nastavení “lze považovat $W_j = 1$ pro všechna j. Nakonec, ve svém nejjednodušším případě, jak bylo řečeno výše, $b_j \in [0; 0,5; 1]$.

4.3.3 **Srovnání běžných metod autentizace**

Jako ilustraci tohoto přístupu jsme provedli číselné srovnání dříve diskutovaných metod autentizace s použitím popsaného rámce.

Před zahájením srovnání je nutné zmínit několik provedených předpokladů. Každá výhoda tedy může nabývat hodnoty [0; 0,5; 1], jak bylo ukázáno dříve. Kromě toho jsme zjednodušili věci tím, že jsme všechny váhy předpokládali jako rovny 1. Ve skutečnosti by v hodnocení v konkrétním kontextu hodnoty vah byly různé. Výsledky, které budou následovat, proto nelze považovat za kompletní a univerzální srovnání metod.

Shoda metod s kritérii je znázorněna v tabulkách 3-5.

Tabulka 3 - Odpovídání zkoumaných metod kritériu bezpečnosti

Metoda/Kritérium	Fyzické pozorování	Impersonace	Bruteforce-útoky	Interní pozorování	Úniky z jiných služeb	Phishingové útoky	Krádež kliče	Třetí strana	Výslovný souhlas	Vazby autentikátorů
	1	2	3	4	5	6	7	8	9	10
Přihlašovací jméno a heslo	0	0,5	0	0	0	0	1	1	1	1
Biometrie	1	0	1	0	0	0	0	1	1	0
Fyzický klíč	1	1	1	1	1	1	1	0	1	1

Tabulka 4 - Splnění kritérií použitelnosti

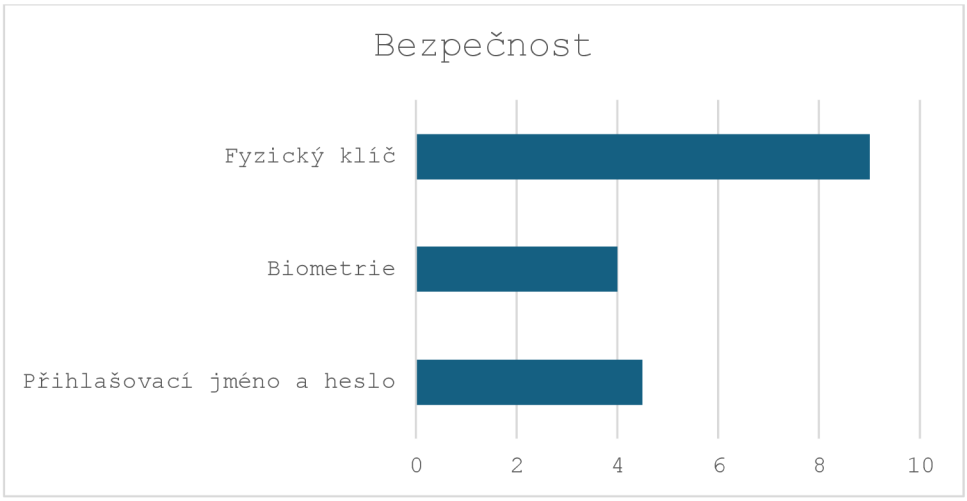
Metoda/Kritérium	Zapamatování	Škálovatelnost	Nošení fyz. klíče	Fyzická lehkost	Snadnost ovládání	Rychlost použití	Chyby při vstupu	Obnovování
	1	2	3	4	5	6	7	8
Přihlašovací jméno a heslo	0	0	1	0	1	1	0,5	1
Biometrie	1	1	1	0,5	1	0,5	0	0
Fyzický klíč	0	0	0	0	1	0,5	0,5	0

Tabulka 5 - Odpovídající kritéria rozvinutelnosti

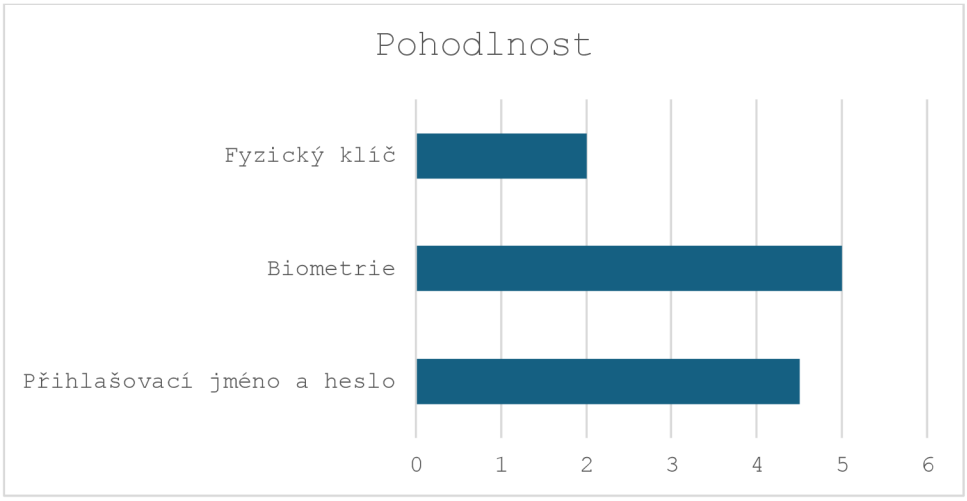
Metoda/Kritérium	Nízká cena	Server	Prohlížeč	Historie	Otevřený přístup	Dostupnost
	1	2	3	4	5	6
Přihlašovací jméno a heslo	1	1	1	1	1	1
Biometrie	0	0	0	0,5	0	0,5
Fyzický klíč	0	0	1	1	0	0

Takže můžeme provést numerické srovnání na základě uvedených vzorců. Výsledky srovnání podle kritérií jsou zobrazeny na grafech 1-3.

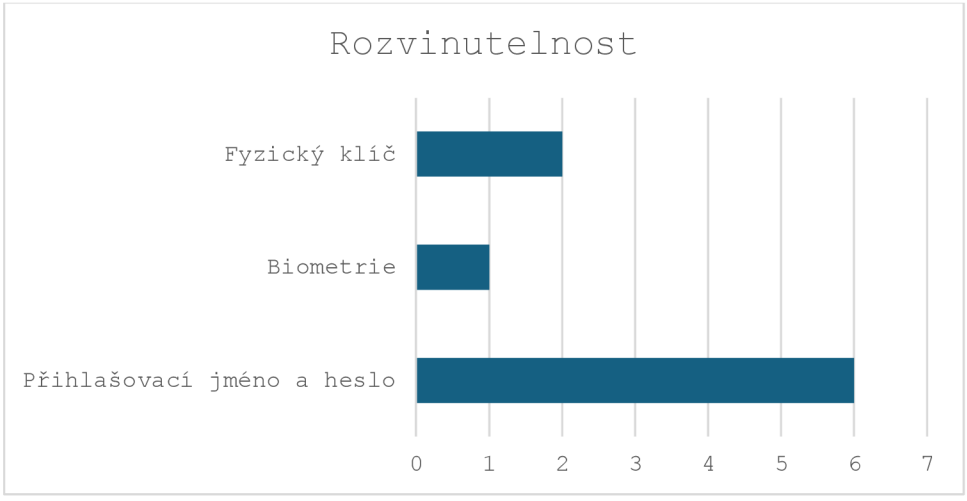
Graf 1 - Porovnání metod podle bezpečnostního kritéria



Graf 2 - Porovnání metod podle kritéria pohodlnosti

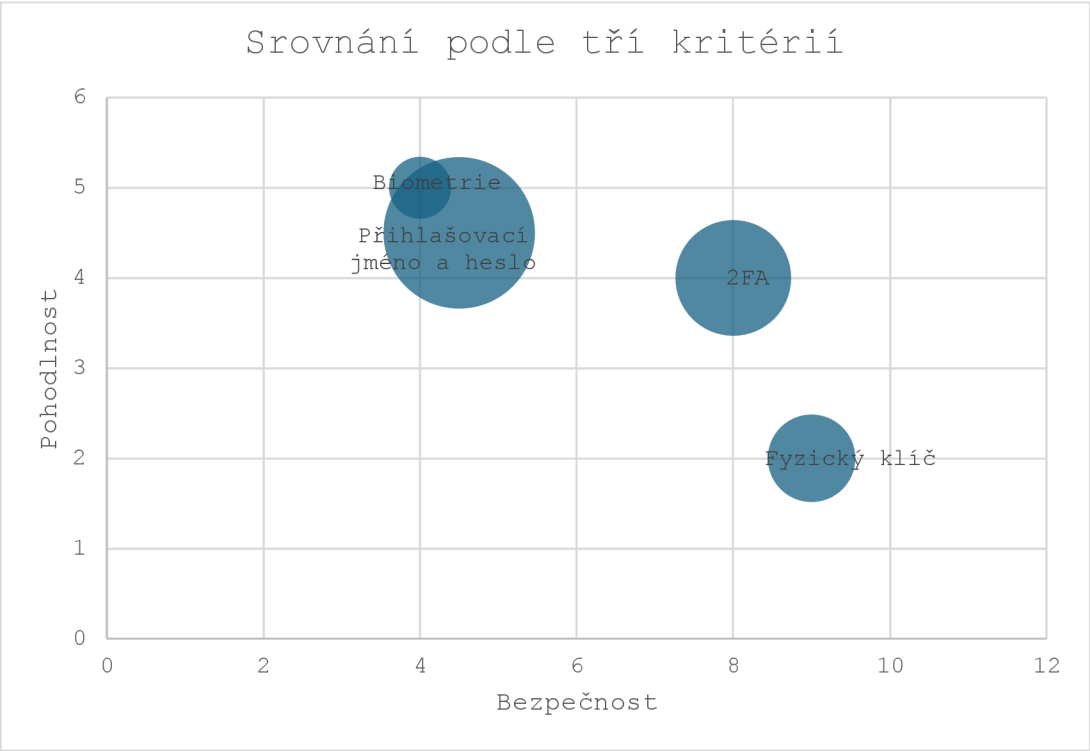


Graf 3 - Porovnání metod podle kritéria Rozvinutelnosti



Na grafu 4 je znázorněno srovnání metod autentizace podle tří kritérií. Na ose x je vynesena bezpečnost, na ose y pohodlnost a velikost kruhu znázorňuje rozvinutelnost.

Graf 4 - Srovnání podle tří kritérií



Závisle na konkrétním úkolu před námi můžeme přiřazovat různou váhu různým výhodám, což se odráží ve výsledcích srovnání.

5 Výsledky a diskuse

Pro získání výsledků s vybranou metodou autorizace s použitím badUSB a dotazu na heslo (dále 2FA) byla dosazena jeho váhová hodnocení ve třech kritériích – bezpečnosti, pohodlí a flexibilitě.

Systém vykazuje částečnou odolnost vůči fyzickému pozorování a odolá impersonaci. Brute-force útokům a vnitřnímu pozorování je chráněn pouze částečně. Je také odolný vůči únikům z jiných služeb. Phishing nemá ani potenciální zranitelnost. Krádež fyzického klíče je částečně nebezpečná vzhledem k tomu, že pro úplnou autorizaci je kromě fyzického klíče nutné znát heslo. Metoda se spoléhá na třetí stranu, která by také mohla být napadena a stát se zdrojem úniku dat. Nakonec systém požádá o výslovný souhlas ze strany uživatele.

Systém neplní podmínku absence potřeby pamatovat si informace. Nutnost nosit fyzický klíč zde je. Systém je jednoduše zvládnutelný, ale rychlost použití negativně ovlivňuje doplnující faktor autentizace. Počet chyb při přihlášení by měl být malý – stačí si zapamatovat a zadat pouze jedno heslo. Fyzický klíč funguje automaticky. Není splněna podmínka snadné obnovy – uživatel musí žádat o nový fyzický klíč.

Není splněna podmínka nízké ceny za jednoho uživatele, protože je vyžadováno použití fyzických zařízení. Byly splněny podmínky kompatibility se serverem a kompatibility s prohlížeči. Je splněna podmínka existence historie. Částečně splněny podmínky otevřeného přístupu, ale existuje přístupnost (použitelný pro uživatele se zdravotním postižením).

Výsledky srovnání jsou uvedeny v tabulkách.

Tabulka 6 - Odpovídání zkoumaných metod kritériu bezpečnosti

Metoda/Kritérium	Fyzické pozorování	Impersonace	Bruteforce útoky	Interní pozorování	Úniky z jiných služeb	Phishing útoky	Krádež klíče	Třetí strana	Výslovný souhlas	Vazby autentikátorů
	1	2	3	4	5	6	7	8	9	10
Přihlašovací jméno a heslo	0	0,5	0	0	0	0	1	1	1	1
Biometrie	1	0	1	0	0	0	0	1	1	0
Fyzický klíč	1	1	1	1	1	1	1	0	1	1
2FA	0,5	1	0,5	0,5	1	1	0,5	0,5	1	0,5

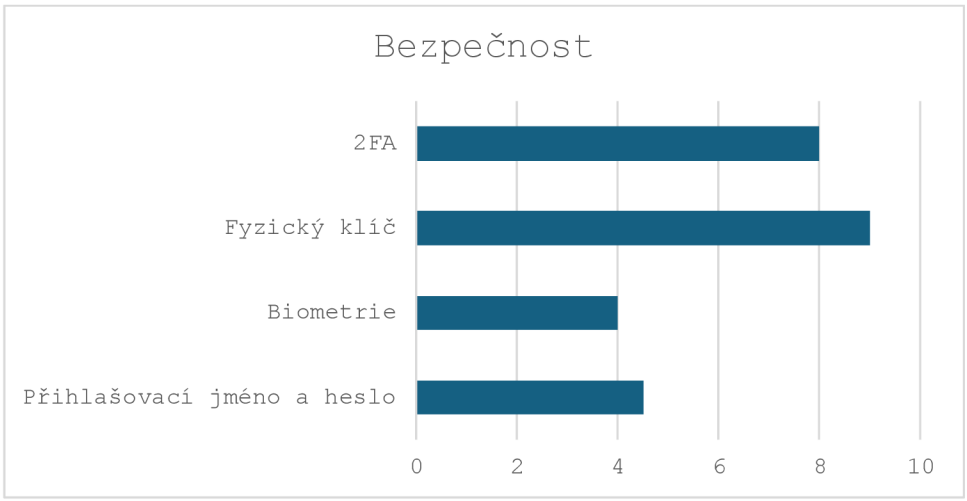
Tabulka 7 - Splnění kritérií použitelnosti

Metoda/Kritérium	Zapamatování	Škálovatelnost	Nošení fyz. klíče	Fyzická lehkost	Snadnost ovládání	Rychlost použití	Chyby při vstupu	Obnovování
	1	2	3	4	5	6	7	8
Přihlašovací jméno a heslo	0	0	1	0	1	1	0,5	1
Biometrie	1	1	1	0,5	1	0,5	0	0
Fyzický klíč	0	0	0	0	1	0,5	0,5	0
2FA	0	1	0	1	1	0,5	0,5	0

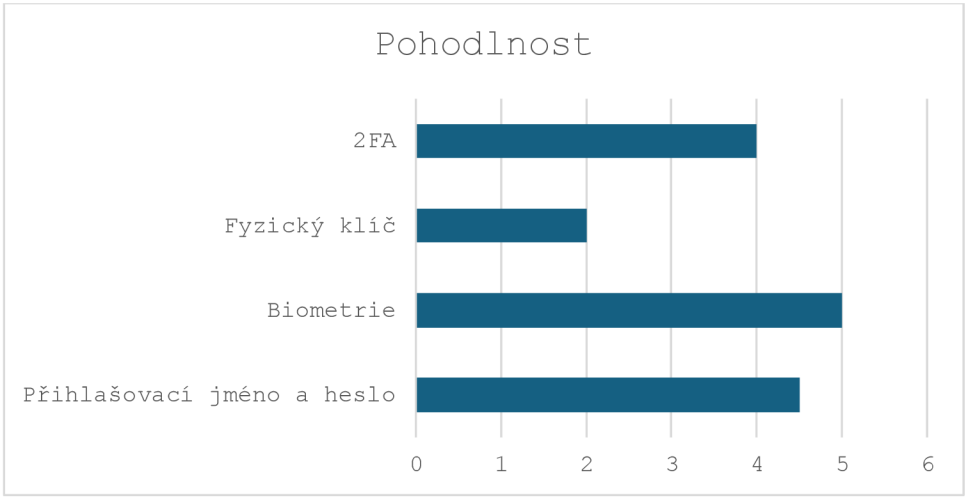
Tabulka 8 - Odpovídající kritéria rozvinutelnosti

Metoda/Kritérium	Nízká cena	Server	Prohlížeč	Historie	Otevřený přístup	Dostupnost
	1	2	3	4	5	6
Přihlašovací jméno a heslo	1	1	1	1	1	1
Biometrie	0	0	0	0,5	0	0,5
Fyzický klíč	0	0	1	1	0	0
2FA	0	1	1	1	0,5	0

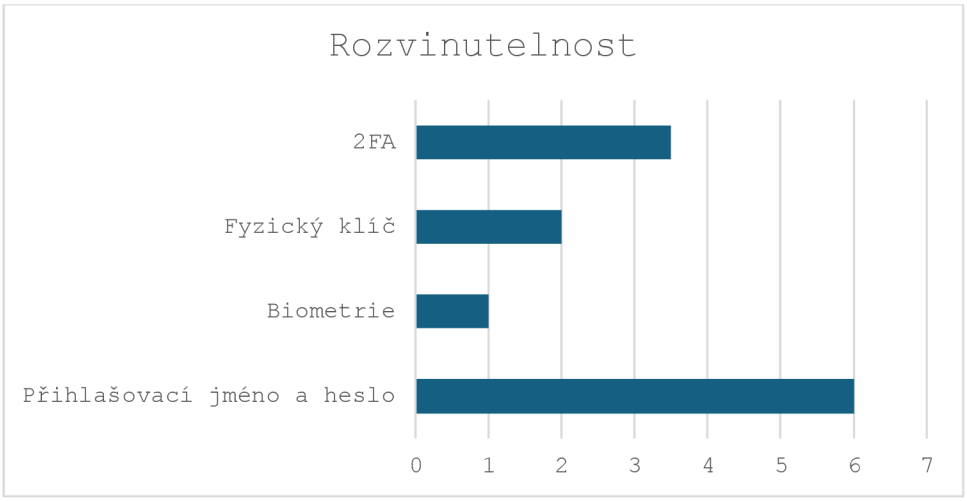
Graf 5 - Porovnání metod podle bezpečnostního kritéria



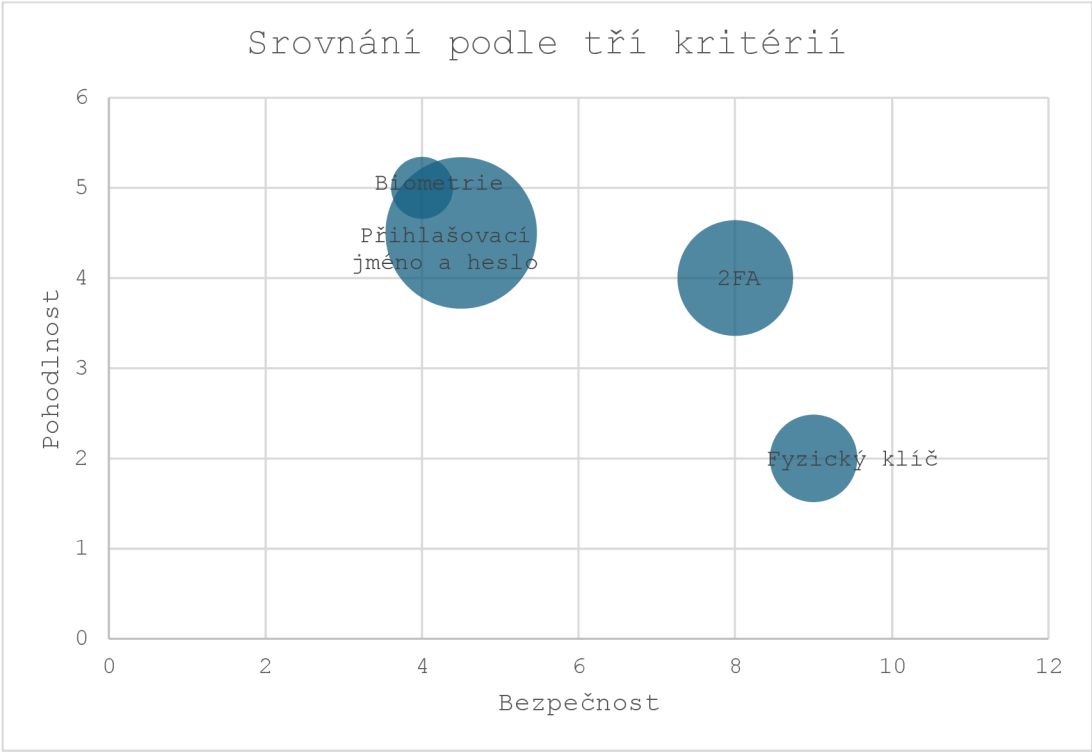
Graf 6 - Porovnání metod podle kritéria pohodlnosti



Graf 7 - Porovnání metod podle kritéria Rozvinutelnosti



Graf 8 - Srovnání podle tří kritérií



Jak je vidět, implementovaná metoda ukazuje vysoká data v bezpečnostní oblasti a dostatečně vysoká v oblasti použitelnosti. Požadavek na heslo jako druhý faktor autentizace mírně snižuje bezpečnostní skóre oproti samotné metodě s použitím fyzického klíče. Přítomnost fyzického klíče jako faktoru autentizace snižuje skóre rozvinutelnosti, na rozdíl od jednofaktorové metody s požadavkem na heslo. Z analýzy vyplývá, že metoda má poměrně dobré výsledky ve všech kritériích.

6 Závěr

Byla provedena studie problematiky autentizace uživatelů v distribuovaných výpočetních systémech. Byly zhodnoceny hlavní metody používané v současné době, principy jejich fungování, klady a zápory.

Bylo provedeno srovnání metod používaných pro autentizaci uživatelů. Byly definovány hlavní kritéria srovnání, byl použit rámec, který zohledňuje nejdůležitější kritéria.

Pro implementaci vlastní vícefaktorové autorizace byl zakoupen badUSB, který byl použit jako autorizační faktor, a to jako fyzický klíč. Pro správnou funkci fyzického klíče bylo provedeno programování zařízení v prostředí vývoje Arduino IDE. Jako druhý autorizační faktor byl napsán skript v prostředí vývoje Visual Studio, který implementuje metodu požadavku na heslo. Byly identifikovány hodnoticí kritéria, každý faktor byl hodnocen podle každého kritéria. Na základě výsledků byly vyvozeny závěry. Vlastní varianta vícefaktorové autorizace byla hodnocena výše průměru ve všech třech hodnotících kritériích.

Všechny úkoly formulované před zahájením práce byly splněny v plném rozsahu. Cíle stanovené v průběhu práce byly dosaženy.

7 Seznam použitých zdrojů

Mitre att&ck. Access token manipulation: Sid-history injection. *Access Token Manipulation: SID-History Injection, Sub-technique T1134.005 - Enterprise | MITRE ATT&CK®* [online] [vid. 15. březen 2024 a]. Dostupné z: https://attack.mitre.org/techniques/T1134/005/

OWASP. Fuzzing. *Fuzzing | OWASP Foundation* [online] [vid. 15. březen 2024 b]. Dostupné z: https://owasp.org/www-community/Fuzzing

Intel. *Trusted-execution-technology-security-paper.pdf* [online] [vid. 15. březen 2024 c]. Dostupné z:https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/trusted-execution-technology-security-paper.pdf

Dostálek, Libor, 2022. Více Faktorová autentizace V mobilních sítích. *Handle Proxy* [online] [vid. 10. březen 2024]. Dostupné z: http://hdl.handle.net/11025/50465

Etienne, Laeticia a Hossain SHAHRIAR, 2020. Attacks and mitigation techniques for Iris-based Authentication Systems. *2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC)* [online]. 7. Dostupné z: doi:10.1109/compsac48688.2020.0-120

Gao, Chi, Xinming ZHANG, Hui WANG, Liyao SONG, Bingliang HU a Quan WANG, 2022. Two-directional two-dimensional PCA: An efficient face recognition method for thermal infrared images. *2022 5th International Conference on Information Communication and Signal Processing (ICICSP)* [online]. 26.11. Dostupné z: doi:10.1109/icicsp55539.2022.10050541

Grassi, Paul A, James L FENTON, Elaine M NEWTON, Ray A PERLNER, Andrew R REGENSCHEID, William E BURR, Justin P RICHER, Naomi B LEFKOVITZ, Jamie M DANKER, Yee-Yin CHOONG, Kristen K GREENE a Mary F THEOFANOS, 2017. *Digital Identity Guidelines: Authentication and lifecycle management* [online]. 22.6. Dostupné z: doi:10.6028/nist.sp.800-63b

Grimes, Roger A., 2021. *Hacking multifactor authentication*. Indianapolis, IN: John Wiley & Sons, Inc. ISBN 978-1119650799

Jasim Jasim, Zinah Khalid, Alaa HAMID MOHAMMED, Lina ELWIYA, Baraa Dhafer AL-JABBARI a Haitham ALHAJI, 2021. Human identification with finger Vien image using Deep Learning. *2021 5th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)* [online]. 21.10. Dostupné z: doi:10.1109/ismsit52890.2021.9604672

Lv, Jiang-Jing, Xiao-Hu SHAO, Jia-Shui HUANG, Xiang-Dong ZHOU a Xi ZHOU, 2017. Data Augmentation for face recognition. *Neurocomputing* [online]. 3., roč. 230, s. 184–196. Dostupné z: doi:10.1016/j.neucom.2016.12.025

MARKY, Karola, Kirill RAGOZIN, George CHERNYSHOV, Andrii MATVIIENKO, Martin SCHMITZ, Max MÜHLHÄUSER, Chloe EGHTEBAS a Kai KUNZE, 2022. "nah, it's just annoying!" A deep dive into user perceptions of two-factor authentication. *ACM Transactions on Computer-Human Interaction* [online]. 20.10., roč. 29, č. 5, s. 1–32. Dostupné z: doi:10.1145/3503514

NEWMAN, George E., 2019. The psychology of Authenticity. *Review of General Psychology* [online]. 3., roč. 23, č. 1, s. 8–18. Dostupné z: doi:10.1037/gpr0000158

O'GORMAN, Lawrence, 2003. Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE* [online]. 12., roč. 91, č. 12, s. 2021–2040. Dostupné z: doi:10.1109/jproc.2003.819611

PENELOVA, Maria, 2021. Access control models. *Cybernetics and Information Technologies* [online]. 1.12., roč. 21, č. 4, s. 77–104. Dostupné z:: doi:10.2478/cait-2021-0044

REESE, Ken a Trevor SMITH, 2019. A usability study of five two-factor authentication methods. *USENIX* [online] [vid. 10. březen 2024]. Dostupné z: https://www.usenix.org/system/files/soups2019-reese.pdf

SWEIGERT, Devin, Md Minhaz CHOWDHURY a Nafiz RIFAT, 2022. Exploit security vulnerabilities by penetration testing. *2022 IEEE International Conference on Electro*

Information Technology (eIT) [online]. 19.5. Dostupné z: doi:10.1109/eit53891.2022.9813929

TITCOMB, James, 2017. Why your smartphone's fingerprint scanner isn't as secure as you might think. *The Telegraph* [online] [vid. 12. březen 2024]. Dostupné z: http://www.telegraph.co.uk/technology/2017/04/11/smartphone-fingerprint-scanners-could-easily-fooled-fake-prints/

WILSON, Yvonne a Abhishek HINGNIKAR, 2019. *Solving identity management in modern applications* [online]. Dostupné z:: doi:10.1007/978-1-4842-5095-2

GORELIK, Vladimir, PISKUNOV, Georgiy, 2020. Перспективные системы и технологии как парадигма технического прорыва. Сборник статей по итогам международной научно-практической конференции. ISBN 978-5-907235-85-4

Velásquez, I., Caro, A., & Rodríguez, A. (2017). *Identifying Comparison and Selection Criteria for Authentication Schemes and Methods*. https://www.semanticscholar.org/paper/Identifying-Comparison-and-Selection-Criteria-for-Vel%C3%A1squez-Caro/ef84889bee078f02289bb6e126cf5dbcab962435

Velásquez, Ignacio, Caro Angélica, a Rodríguez, Alfonso. 'Multifactor Authentication Methods: A Framework for Their Comparison and Selection', Computer and Network Security. IntechOpen, Jun. 10, 2020. Dostupné z: doi: 10.5772/intechopen.89876

J. Bonneau, C. Herley, P. C. v. Oorschot and F. Stajano, "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes," 2012 IEEE Symposium on Security and Privacy, San Francisco, CA, USA, 2012, pp. 553-567, Dostupné z: doi: 10.1109/SP.2012.44.

Verizon. DBIR report 2022 - master's guide. Verizon Business [online] [vid. 15. březen 2024]. Dostupné z: https://www.verizon.com/business/resources/reports/dbir/2022/master-guide/

8 Seznam obrázků, tabulek, grafů a zkratek

8.1 Seznam obrázků

8.2 Seznam tabulek

8.3 Seznam grafů