

**UNIVERZITA KONŠTANTÍNA FILOZOFA V NITRE
FAKULTA PRÍRODNÝCH VIED A INFORMATIKY**

**BEZPEČNOSTNÉ ASPEKTY DIGITÁLNEJ
IDENTITY**

BAKALÁRSKA PRÁCA

2022

MAREK HRABČÁK

**UNIVERZITA KONŠTANTÍNA FILOZOFA
V NITRE**

FAKULTA PRÍRODNÝCH VIED A INFORMATIKY

BEZPEČNOSTNÉ ASPEKTY DIGITÁLNEJ IDENTITY

BAKALÁRSKA PRÁCA

Študijný odbor: 18. Informatika
Študijný program: Aplikovaná informatika
Školiace pracovisko: Katedra informatiky
Školiteľ: doc. Ing. Zoltán Balogh, PhD.

Nitra 2022

Marek Hrabčák



224184

Univerzita Konštantína Filozofa v Nitre
Fakulta prírodných vied

ZADANIE ZÁVEREČNEJ PRÁCE

Meno a priezvisko študenta: Marek Hrabčák

Študijný program: aplikovaná informatika (Jednoodborové štúdium, bakalársky I. st., externá forma)

Študijný odbor: informatika

Typ záverečnej práce: Bakalárska práca

Jazyk záverečnej práce: slovenský

Sekundárny jazyk: anglický

Názov: Bezpečnostné aspekty digitálnej identity

Anotácia: Bezpečnosť informácií sa zaobera ochranou informácií vo všetkých ich formách a po celý ich životný cyklus - teda počas ich vzniku, spracovania, ukladania, prenosu a likvidácie. Pre našu budúcnosť sú dôležité rôzne spôsoby využitia digitálneho priestoru: vzdialená práca, vzdelávanie, spolupráca vo virtuálnych tínoch a podobné aktivity, ktoré vytvárajú hodnoty a sú kľúčové pre rozvoj znalostnej ekonomiky. Všetky tieto aktivity však spája spoločný koncept: digitálna identita. Digitálna identita je elektronický spôsob na identifikáciu používateľa.

Cieľom bakalárskej práce popis a definovanie digitálnej identity vo virtuálnom priestore, návrh autentizácie a modelovanie výberu správneho autentifikačného mechanizmu. Bakalár vytvorí ukážku funkčnej aplikácie, ktorá na základe vstupov používateľa navrhne model pre optimálnu formu autentizácie. Požadované vstupné údaje sú: typ spracovávaných dát (osobné údaje, iné klasifikované dátá, neklasifikované dátá); typ aplikačnej architektúry (klient-server, server-server); typ autentizačného protokolu (LDAP, Radius, oauth/SAML/OIDC); umiestnenie konzumera a providera služby (verejný cloud, privátny cloud, vlastné datacentrum); požiadavka na multifaktorovú autentizáciu; požiadavka na adaptívnu autentizáciu.

Charakter práce: aplikačný

Požiadavky na obsah podľa charakteru práce: popis riešeného problému, návrh systému/hardvérového riešenia a pod. (modely, ..), metodika vývoja/tvorby, implementácia, popis vytvoreného riešenia, testovanie;

Požiadavky na vedomosti a zručnosti študenta: dobrá znalosť anglického jazyka, šifrovanie, modelovanie bezpečnosti, znalosť problému digitálnej identity

Školiteľ: doc. Ing. Zoltán Balogh, PhD.

Oponent: Mgr. Michal Kohútek

Katedra: KI - Katedra informatiky

Dátum zadania: 29.10.2020

Dátum schválenia: 05.04.2021

RNDr. Ján Skalka, PhD., v. r.
vedúci/a katedry

POĎAKOVANIE

Chcel by som sa podakovať školiteľovi za pripomienky a odbornú pomoc pri vypracovaní práce a rodine za podporu počas jej prípravy.

ABSTRAKT

Hrabčák, Marek: Bezpečnostné aspekty digitálnej identity. [Bakalárska práca]. Univerzita Konštantína Filozofa v Nitre. Fakulta prírodných vied. Školiteľ: doc. Ing. Zoltán Balogh, PhD. Stupeň odbornej kvalifikácie: Bakalár odboru Aplikovaná informatika. Nitra: FPVaI, 2022. 74 strán.

Ochrana informácií je neoddeliteľnou súčasťou komunikácie v modernej spoločnosti. Zdieľanie citlivých dát na sociálnych sieťach, ľahká dostupnosť služieb, čoraz sofistikovanejšie hrozby a zraniteľnosti, prudký nárast digitálnych identít spôsobený rozvojom e-commerce a digitálneho bankovníctva a neplánovaná celosvetová digitalizácia počas pandémie vyžadujú aktívny prístup k ochrane dát a hľadanie nových možností na minimalizáciu dopadov pri bezpečnostných incidentoch. Práca poukazuje na bezpečnostné aspekty, ktoré vstupujú do komunikácie medzi konzumerom a poskytovateľom služby počas autentizácie a navrhuje postupy, ktoré dokážu tieto faktory pomenovať, kategorizovať, merať a vyhodnocovať ich dopad na bezpečnosť autentizácie. Výstupom práce je aplikácia, ktorá na základe vstupov používateľa navrhne optimálnu formu autentizácie. Požadované vstupné údaje sú: typ klasifikovaných dát (verejné údaje, interné údaje, chránené dátá, prísne chránené dátá, neklasifikované dátá); typ aplikačnej architektúry (1-vrstvová, 2-vrstvová, atď.); typ autentizačného protokolu (mTSL, LDAP, NTLM, Radius,...) alebo autentizačného frameworku (Kerberos/OAuth/SAML/OIDC); umiestnenie konzumera a providera služby (lokálna siet, clouдовé úložisko); požiadavka na silu autentizácie (1FA, 2FA, 3FA, MFA), požiadavka na funkcie použité pri digitálnom podpisovaní alebo kontrole integrity (RSA, HMAC, OTP, HASH), požiadavka na šifrovanie (RSA, ECC, AES, DEC, 3DES) a požiadavka na oprávnenia autentifikovaného používateľa (anonymný používateľ, štandardný používateľ, administrátor,...).

Kľúčové slová: Informatika. Digitálna identita. Kybernetická bezpečnosť. Autentizácia. Autentizačný protokol. Aspekty bezpečnosti.

ABSTRACT

Hrabcak, Marek: Security aspects of digital identity. [Bachelor thesis]. Constantine the Philosopher University in Nitra. Faculty of Natural Sciences. Supervisor: Doc. Ing. Zoltán Balogh, PhD. Degree of professional qualifications: Bachelor Department Applied Informatics. Nitra: FPVai, 2022. 74 pages.

Information protection is an integral part of the communication in a modern society. Sharing sensitive data on social networks, easy to use services, increasingly sophisticated threats and vulnerabilities, increasing number of digital identities in e-commerce and digital banking and unmanaged global digitization during pandemics require active approach to data protection and research new options to minimize the impact of security incidents. The thesis describes security aspects in communication between the consumer and service provider during authentication and proposes procedures that can describe these factors, categorize, measure and evaluate their impact on authentication.

The output of work is an application that suggests an optimal form of authentication based on the user's inputs. Required input data are: Type of classified data (public data, internal data, data protected, strictly protected data, non-classified data); Application architecture (1-layer, 2-layer, etc.); Type of authentication protocol (MTSL, LDAP, NTLM, RADIUS, ...) or authentication framework (Kerberos / OAuth / SAML / OIDC); Location of consumer and provider (local network, cloud storage); Requested authentication factors (1FA, 2FA, 3FA, MFA), Requirement for digital signing or integrity control (RSA, HMAC, OTP, HASH), Requested encryption (RSA, ECC, AES, DEC, 3DES) and Requested application role (an anonymous user, standard user, administrator, ...).

Keywords: Informatics. Digital identity. CyberSecurity. Authentication. Authentication protocol. Security aspects.

OBSAH

Úvod	14
1 Analýza súčasného stavu	15
1.1 Definícia digitálnej identity	15
1.2 Trendy v oblasti ochrany digitálnej identity	16
1.3 Digitálna identita vo finančnom sektore	18
1.4 Digitálna identita a NFT	19
1.5 Technológia blockchain v KYC procesoch	21
1.6 Autentifikácia	23
1.7 Zhrnutie poznatkov z analýzy	24
1.8 Analýza autentizačných protokolov	26
1.8.1 Basic access authentication	26
1.8.2 SAML	27
1.8.3 OAuth2	28
1.8.4 Mutual TLS	30
1.8.5 LDAP	31
1.8.6 Kerberos	32
1.8.7 Radius	33
2 Ciele záverečnej práce	35
3 Metodika práce	36
3.1 Dekompozícia aplikácie	36
3.2 Modelovanie hrozieb a analýza rizík	36
3.3 Návrh mitigačných opatrení	38
4 Návrh algoritmu na výpočet optimálneho protokolu	38
4.1 Faktorizácia aspektov	39
4.2 Zápis hodnoty aspektov pomocou DREAD faktorov	40
4.3 Worst-case scenario	41
4.4 Vyjadrenie závislosti autentizačného protokolu na aspektoch	42
4.5 Popis algoritmu na výber optimálneho autentifikačného protokolu	44
4.6 Prípravy vstupných dát pre aplikáciu	45
5 Aplikácia na modelovanie autentizačných protokolov	47
5.1 Použité technológie	47
5.1.1 Bootstrap	47
5.1.2 Javascript	47
5.1.3 PHP	48

5.1.4	Apache.....	48
5.1.5	MySQL.....	48
5.1.6	XAMPP	48
5.2	Prípady použitia	48
5.3	Popis a štruktúra aplikácie	50
5.4	Databáza.....	51
5.5	Testovanie aplikácie.....	52
5.6	Výhody a nevýhody implementácie.....	52
Záver	54
Zoznam bibliografických odkazov	55
Zoznam príloh	58

ZOZNAM ILUSTRÁCIÍ A TABULIEK

Obrázok 1 Popis procesu farbenia dát	17
Obrázok 2 Scénár autentizácie s FORT protokolom	20
Obrázok 3 Popis štandardného KYC procesu	21
Obrázok 4 Obrázok: KYC proces založený na technológii blockchain	23
Obrázok 5 Popis MITM útoku na https protokol.....	23
Obrázok 6 UML sekvenčný diagram pre http basic authentication	27
Obrázok 7 Sekvenčný diagram pre SAML autentizáciu	28
Obrázok 8 Sekvenčný diagram pre OAuth Implicit Grant Flow	30
Obrázok 9 Sekvenčný diagram mutual TLS s použitím certifikátov.....	31
Obrázok 10 Sekvenčný diagram pre LDAP autentizáciu.....	32
Obrázok 11 Sekvenčný diagram Kerberos autentizácie	33
Obrázok 12 Sekvenčný diagram pre autentizáciu RADIUS protokolom	34
Obrázok 13 Popis procesu výpočtu optimálnej autentizácie	44
Obrázok 14 Algoritmus výpočtu optimálneho autentizačného protokolu.....	45
Obrázok 15 Obrázok s prípadmi použitia	49
Obrázok 16 Zoznam súborov s funkciami pre CRUD operácie	50
Obrázok 17 Doménové objekty a ich vzťahy.....	51
Obrázok 18 Obrazovka s aspektami	69
Obrázok 19 Obrazovka s hrozbami	70
Obrázok 20 Obrazovka so správou používateľov	71
Obrázok 21 Obrazovka s ukážkou navrhovaných protokolov	72
Obrázok 22 Zoznam tabuliek v databáze	73
Tabuľka 1 Určenie hodnoty L a I.....	37
Tabuľka 2 Určenie miery rizika.....	37
Tabuľka 3 Príklady rozloženia hodnôt pri faktorizácii	40
Tabuľka 4 Matica závislostí aspektov a DREAD faktorov.....	40
Tabuľka 5 Príklad formy zápisu výstupu analýzy autentizačného protokolu	42
Tabuľka 6 Porovnanie rizík pred a po implementácii aspektu	43
Tabuľka 7 Zoznam a popis jednotlivých tabuliek databázy	51
Tabuľka 8 Klasifikácia faktorov pre pravdepodobnosť.....	59
Tabuľka 9 Klasifikácia faktorov pre dopad	60
Tabuľka 10 Popis hrozieb a mitigácií pomocou techniky STRIDE	61
Tabuľka 11 Vzor protokolu pre modelovanie hrozieb.....	62
Tabuľka 12 Zoznam aspektov a pridelených faktorov.....	63
Tabuľka 13 Namerané hodnoty DREAD faktorov pre všetky hodnoty aspektov...64	64
Tabuľka 14 Zoznam autentizačných protokolov podľa pozorovaných aspektov ..66	66
Tabuľka 15 Hodnoty TMPO pre autentizačné protokoly použité pri výpočtoch ...67	67

ZOZNAM SKRATIEK A ZNAČIEK

OWASP	Open Web Application Security Project (OWASP) je online komunita vedená neziskovou organizáciou s názvom The OWASP Foundation, ktorá produkuje voľne dostupné články, metodiky, dokumentáciu, nástroje a technológie v oblasti bezpečnosti webových aplikácií.
GDPR	General Data Protection Regulation, všeobecné nariadenie o ochrane údajov (GDPR) je najprísnejším zákonom o ochrane súkromia a bezpečnosti na svete.
CCPA	California Consumer Privacy Act (CCPA), zákon zabezpečuje spotrebiteľom v Kalifornii nové práva na súkromie.
LGPD	Brazilian General Data Protection Law
POPI	Protection of Personal Information Act v Južnej Afrike
IoT	Internet of Things
PKI	Pricate Key Infrastructure

SLOVNÍK POJMOV

Entita	Človek, skupina ľudí alebo zariadenie (SIM karta), ktorá je jasne odlišiteľná od ostatných entít.
Agent (User Agent)	Sprostredkovateľ informácií medzi človekom a poskytovateľom identity a je naj slabším článkom v bezpečnosti autentizácie. Agent je vždy technicky komponent, napr. aplikačný komponent pri webovej komunikácii, komunikačný kanál pri hlasovej autentizácii alebo skener pri overovaní pomocou biometrie tváre.
Zriadenie digitálnej identity	Proces, pri ktorom je potrebné overiť entitu priamo fyzicky alebo pomocou inej, už existujúcej digitálnej identity. Entitu je možné overiť pomocou samotnej existencie entity (napr. počas návštevy klienta na pobočke banky), ale v digitálnom priestore je fyzická prítomnosť nahradená sadou atribútou, ktoré môžu byť zastúpené identifikátorom identity .
Autonómna (lokálna) digitálna identita	Digitálna identita, ktorá je platná len v systéme jednej spoločnosti.
Identifikácia	Proces, pri ktorom je neznámej entite pridelená známa identita. Vo fyzickom svete prebieha identifikácia tak, že overovanej entite položíme otázku „Ako sa voláte?“ a v odpovedi dostaneme informáciu o identite: „Volám sa Marek.“. V digitálnom svete prebieha identifikácia rovnako: po zostavení komunikačného kanála je agenta požiadany o sprostredkovanie identity alebo identifikačného čísla (UserID). Agent ho získa od entity alebo ho má v konfigurácii a odošle ho v odpovedi.
Autentizačný protokol	Typ počítačového komunikačného protokolu alebo kryptografického protokolu špeciálne navrhnutého na prenos autentifikačných údajov medzi dvoma entitami.[6] . V tejto práci sú popisované len komplexné protokoly

	určené pre služby, ktoré vyžadujú Autentizáciu, Autorizáciu, prípadne aj Accounting. V praktickej časti práce je možné používať akýkoľvek typ autentizačného protokolu, aj napr. proprietárny.
Autentizácia	Proces, pri ktorom sú bezpečnou formou overené známe atribúty digitálnej entity.
Dôvernosť (Confidentiality)	Proces alebo funkcia potrebná na zachovanie autorizovaných obmedzení prístupu k informáciám a ich zverejňovania, vrátane prostriedkov na ochranu osobného súkromia a vlastníckych informácií.
Integrita (Integrity)	Ochrana pred nevhodnou modifikáciou alebo zničením informácií a zabezpečenie nepopierateľnosti a autentickosti informácií.
Dostupnosť (Availability)	Zabezpečenie včasného a spoľahlivého prístupu k informáciám a ich využívania.
Neodmietnutie (Non-Repudiation)	Ubezpečenie, že odosielateľovi informácie je poskytnutý doklad o doručení a príjemcovi doklad totožnosti odosielateľa, takže ani jeden z nich nemôže neskôr popriť spracovanie informácie.
Prístup (Access)	Sada obmedzení na fyzickej alebo logickej úrovni. Pre fyzickú osobu je možné obmedzenie prístupu pomocou fyzickej zábrany (napr. dvere s čítačkou odtlačkov prstov). Pre digitálnu identitu je možné obmedzenie prístupu pomocou obmedzení na siet'ovej vrstve (filter zdrojových IP adries) alebo použitím proprietárneho protokolu (napr. TLS/SSL v IBM MQ).
Kategorizácia dát	Proces pri ktorom sú dátá rozdelené do kategórií a prístup k nim je riadený na základe aplikačných rolí. Klasifikácia dát je závislá od regiónu. V komerčných firmách sú dátá kategorizované podľa ISO 27001 do 4 kategórií na Dôverné (prístup má iba vyšší manažment), Obmedzené

	(väčšina zamestnancov má prístup), Interné (prístup majú všetci zamestnanci), Verejné informácie (každý má prístup). Kedže by mal pri klasifikácii platiť „zero trust approach“, tak by mal byť pri klasifikácii použitý postup, že neklasifikované dátá sú automaticky označené najvyšším stupňom utajenia. Pri návrhu autentizácie platí závislosť: čím sú spracovávané dátá citlivejšie, tým silnejšia autentizácia musí byť použitá.
Security architektúra	Procesy, ktoré tvoria celkovú vyspelosť informačného systému a jeho bezpečnosti.
Zraniteľnosť, hrozba, riziko	V prípade výskytu technickej slabiny (zraniteľnosti) v aplikácii, komunikačnom kanáli alebo na aplikačnom serveri nastane stav, kedy overenie identity nie je jednoznačné. Tento stav nazývame hrozba. Ak vznikne pravdepodobnosť zneužitia slabiny s dopadom pri verifikácii identity (napr. nejednoznačnosť), tak hovoríme o riziku. Miera (výška) rizika závisí od pravdepodobnosti zneužitia a od dopadu tohto zneužitia na celkový proces autentizácie. Napr. ukradnutie identity používateľa verejného portálu má odlišný dopad na vlastníka identity (reputačné riziko) ako ukradnutie bankovej identity (majetková ujma až existenčné problémy).
Fintech	Finančná technológia, ktorá sa snaží zlepšiť prípadne automatizovať poskytovanie finančných služieb.

ÚVOD

Téma digitálnej identity je v súčasnosti často mediálne diskutovaná v dôsledku meniacich sa podmienok pre elektronickú komunikáciu ako dôsledok pandémie COVID-19, ktorá zaviedla online vyučovanie v školách a nútenu prácu z domu pre väčšinu zamestnancov nevýrobných firiem. Táto téma však dlhodobo rezonovala v rôznych odvetviach spoločnosti aj pred pandémiou. Vo finančnom sektore sa banky a fintechy dlhodobo snažia zjednodušovať (a zlacniť) komunikáciu s klientom, v štátom sektore sa neustále vylepšuje elektronická identita občana (eID) a zmeny prichádzajú aj so zavádzaním digitálnej identity na úrovni Európskej únie vo forme tzv. "European Digital Identity". Oblast' digitálnej identity je celosvetovo riešený problém a riešenia sú závislé na spoločenstvách, ktoré sa rozhodnú pre digitalizáciu. Niektoré štáty sveta plne podporujú digitálnu identitu (napr. Estónsko, Austrália), krajinu s veľmi vysokým počtom obyvateľov sa snažia digitalizovaním identity zlepšiť celkový stav identifikácie obyvateľstva. Niektoré, hlavne ekonomicky vyspelejšie krajinu o tejto téme len dlhodobo diskutujú a nemajú jednotný prístup (napr. EU). Dôvody môžu byť ekonomické (nákladovosť), právne (ochrana identifikačných údajov) alebo technologická komplexnosť (zložitosť) nasadenia a prevádzkovania takéhoto riešenia. Toto všetko sú aspekty (pohľady), ktoré vstupujú do procesov overenia identity.

V tejto práci je popísaný analytický pohľad na bezpečnostné aspekty digitálnej identity. Z odborných článkov je pripravený zoznam aspektov, ktorý je rozdelený do kategórií. Aspekty sú klasifikované a usporiadane podľa miery rizika posudzované metodikou pre kvalitatívnu risk analýzu (OWASP Risk assessment framework).

Cieľom práce je vyjadriť vzťah (závislosť) miery rizika autentizačného protokolu na meraných aspektoch a pripraviť praktický nástroj (aplikáciu), ktorá používateľovi zjednoduší výber autentizačného protokolu podľa zvoleného aspektu.

V práci boli použité primárne zdroje informácií z Centa vedecko-technických informácií, ScienceDirect, SpringerLink a IEEE.

Kapitoly bakalárskej práce sú rozdelené na analýzu súčasného stavu, popis použitej metodiky a postupov na dosiahnutie cieľa, funkčná a technická špecifikácia aplikácie a prílohy s výsledkami meraní.

1 ANALÝZA SÚČASNÉHO STAVU

Digitálna identita je kľúčovou informáciou o reprezentácii používateľa v každom informačnom systéme. Miera dôvery v túto informáciu je závislá od komplexnosti identifikácie, sily autentizácie, prítomnosti zraniteľnosti komunikačného a aplikačného rozhrania, vplyvu nežiadúcich autorizovaných aj neautorizovaných procesov na autentizáciu, zjednodušovanie autentizačného mechanizmu atď. Neustále navyšovanie funkčných požiadaviek na aplikácie a zvyšovanie komfortu používateľa s cieľom optimalizácie a znižovania nákladov na poskytovanie služieb v elektronickom priestore vyvoláva prirodzený tlak na znižovanie zložitosti bezpečnostných procedúr. Protiváhou je tlak na zvyšovanie odolnosti aplikácií voči kybernetickým útokom.

Téma bezpečnosti digitálnej identity nadobúda význam vďaka dlhodobým trendom v navyšovaní a personalizácii komunikačných technológií (mobilné telefóny, smart zariadenia, IoT). Tieto zariadenia sú súčasťou identity vlastníka a často obsahujú všetky jeho osobné a transakčné údaje. Sprísňovaniu legislatívy zameranej na ochranu osobných údajov (GDPR v EU, CCPA v Kalifornii, LGPD v Brazílii, POPI v Južnej Afrike) nútí spoločnosti, ktoré osobné údaje zbierajú k aktívnej ochrane počas celého životného cyklu dát. Cielový marketing zameraný na vytvorenie profilu správania koncového používateľa a neočakávané zmeny v oblasti mobility obyvateľstva sú výzvy, ktoré musia jednotlivé krajiny prijať a riešiť ich.

Problémom dôvery v digitálnej identity je správne vyhodnotenie rizík spojených s preukázaním dôvery a výber efektívneho mechanizmu na overenie identity. Nesprávne vyhodnotenie rizík a neefektívny príp. neúčinný autentizačný mechanizmus má za následok hrozbu odcudzenia digitálnej identity a nepríjemný dopad na skutočnú identitu, teda človeka.

1.1 DEFINÍCIA DIGITÁLNEJ IDENTITY

Medzinárodný uznávaný štandard (ISO/IEC 24760-1, 2019) popisuje framework pre Identity Management. Entita je v ňom definovaná ako „Osoba, organizácia, zariadenie, skupina takýchto položiek, predplatiteľ telekomunikačnej služby, SIM karta, pas, karta sietového rozhrania, softvérová aplikácia, služba alebo webová lokalita“. Entita vlastní identitu a identita je sadou atribútov ako je napr. rodné číslo, adresa bydliska a pod., teda ako „súbor atribútov súvisiacich s entitou“. Pre účel tejto práce je zaujímavé

rozdelenie implementačných aspektov na Centralized, Distributed, User-centric a Federated a je zakomponované do vyhodnocovania pozorovaných aspektov.

Filozofickým pohľadom na digitálnu identitu vo svete sociálnych sietí a hodnôť sa zaoberá vo svojej práci Ernesta Molotokiené (2020). Keďže každá identita žije univerzálny život, podľa autorky neexistuje univerzálny spôsob života a preto nemôžu existovať ani dve rovnaké identity. Vo virtuálnom svete ale nastáva zásadná zmena. Ten istý jednotlivec má v rôznych sociálnych sieťach rôzne pseudo-identity.

1.2 TRENDY V OBLASTI OCHRANY DIGITÁLNEJ IDENTITY

Na Slovensku sa venuje kybernetickej bezpečnosti a ochrane osobných údajov niekoľko právnych predpisov. Medzi najdôležitejšie patrí niekoľko zákonov o ochrane utajovaných skutočnosti¹, ochrane informácií² a kybernetickej bezpečnosti³. Veľmi dôležitým dokumentom je aj Národná stratégia kybernetickej bezpečnosti na roky 2021 až 2025.⁴ Dokument popisuje základné ľudské pravá a slobody v kybernetickom priestore, riadenie rizík pre národnú kybernetickú bezpečnosť, prístup ku kybernetickým hrozbám a strategické ciele pre najbližšie roky. Národný bezpečnostný úrad na svojich stránkach⁵ zverejňuje aj nariadenia a smernice Európskej únie, ktoré súvisia s touto problematikou.

Digitálna identita vo svete je výstižne opísaná v článku CyberSecurity z pohľadu digitálnej identity a ochrany údajov píšu autori (SULE et al, 2021) o súčasných trendoch v oblasti ochrany dát a digitálnej identity v Nigérii, Kanade, Austrálii a UK. Autori uvádzajú, že podľa článku Svetovej banky z roku 2020 by niektoré krajinu počas pandémie s využitím systému digitálneho identifikačného systému mohli spoľahlivejšie identifikovať zraniteľné skupiny, ktoré by napríklad potrebovali núdzové dávky finančnej pomoci. Vláda Thajska by napr. mohla filtrovať tých obyvateľov, ktorí sú oprávnení získať pomoc z ďalších (napr. neštátnych) dostupných systémov pomoci a indické orgány by mohli urobiť rýchle platby na viac ako 200 miliónov žien navyše oproti súčasnemu

¹<https://www.nbu.gov.sk/urad/pravne-predpisy/pravne-predpisy/ochrana-utajovanych-skutocnosti/index.html>

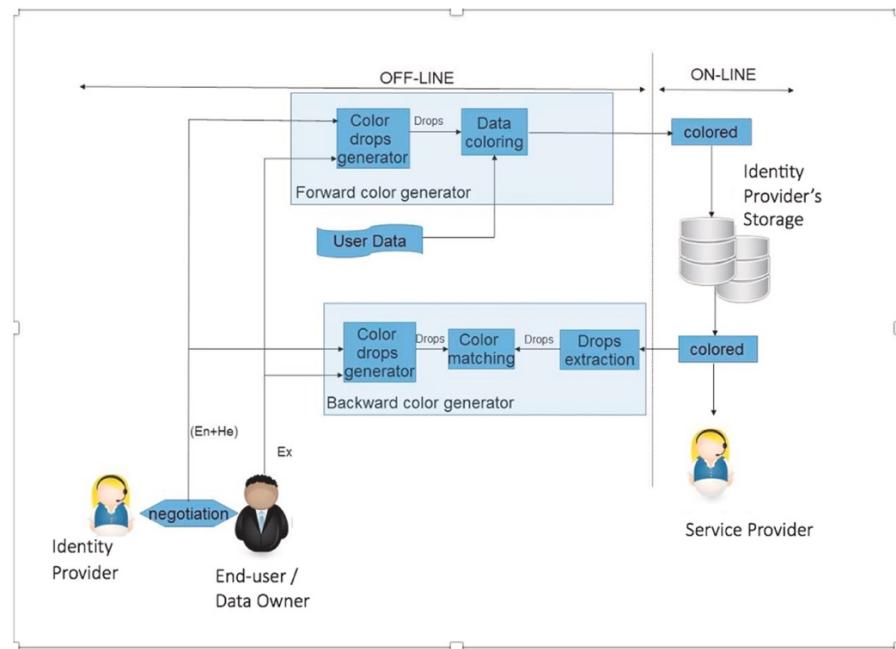
² <https://www.nbu.gov.sk/urad/pravne-predpisy/pravne-predpisy/sifrova-ochrana-informacii/index.html>

³ <https://www.nbu.gov.sk/urad/pravne-predpisy/pravne-predpisy/kyberneticka-bezpecnost/index.html>

⁴ <https://www.nbu.gov.sk/wp-content/uploads/kyberneticka-bezpecnost/Narodna-strategia-kybernetickej-bezpecnosti.pdf>

⁵ <https://www.nbu.gov.sk/index.html>

stavu, pretože by došlo k zlepšeniu procesu, ktorý spája fyzickú identitu s jeho digitálnou identitou. Ďalšími nespornými benefitmi je podľa autorov redukcia kybernetických podvodov lepšou identifikáciou falósných identít, zníženie nákladov súvisiacich s administratívou a prevádzkovými nákladmi súvisiacimi s Identity managementom a systémami na zlepšenie ochrany súkromia. Autori vo svojej práci navrhujú techniky na zvýšenie ochrany dát identity, ktoré sú implementovateľné tak vo verejnkom cloudom ako aj v privátnych datacentrách. Technika digitálnych odtlačkov (fingerprinting) zabezpečuje, že digitálne vodoznaky sú súčasťou každej kópie distribuovaného datasetu v digitálnych súboroch a je tak možné odsledovať bod úniku (krádeže) dát alebo zmienu integrity údajov. Technika farbenie dát (tzv. Data Colouring) je špeciálna forma digitálneho vodoznaku, v ktorom sú fragmenty digitálneho odtlačku známe ako farebné kvapky a sú distribuované v datasete. Farebné kvapky na obrázku 1. vznikajú kombináciou „očakávanej“ hodnoty (artefakty + súhlás), ktorú pozná iba vlastník údajov (koncový používateľ), hodnota „entropie“ je známa iba poskytovateľovi identity a hodnota „hyperentropie“ známa poskytovateľovi služby. Tieto hodnoty sa kombinujú a vytvárajú kolekciu farebných „kvapiek“, ktoré tvoria jedinečnú farbu. Farba dokáže jednoznačne identifikovať jednotlivé transakcie identity.



Obrázok 1 Popis procesu farbenia dát⁶

⁶ https://ars.els-cdn.com/content/image/1-s2.0-S0160791X21002098-gr2_lrg.jpg

Potreba digitálneho podpisovania bola v tejto práci zahrnutá aj do aspektov, ktoré vplývajú na digitálnu identitu a digitálne podpisovanie je jedným z pozorovaných a vyhodnocovaných aspektov.

V článku Digital Identity (LAURENT, DENOUEL, LEVALLOIS-BARTH,WAELBROECK, 2015) autori štatisticky vyhodnotili, že podľa ACSEL, čo je skratka pre francúzsku asociáciu digitálnej ekonomiky, francúzski používatelia v roku 2013 používali v priemere 16,4 digitálnych identít v porovnaní s 12.2 v roku 2009. Za digitálnu identitu autori považovali prihlásovacie meno a heslo potrebné na aktiváciu účtu, ale aj všetky stopy, ktoré zostali po jednotlivcovi počas ich aktivity (IP adresa, fotografie, typy nákupu atď.). Medzi ďalšie zaujímavé štatistiky patria údaje podľa ktorých 90% používateľov používa digitálnu identitu na prístup do e-komerčných služieb, 8% do online bankingu a 77% do sociálnych sietí. V tej istej štúdii je vyhodnotené aj povedomie o rizikách: 42% respondentov si je vedomých chýb v údajoch svojej digitálnej identity a 40% sa obáva zneužitia svojich osobných údajov.

1.3 DIGITÁLNA IDENTITA VO FINANČNOM SEKTORE

V prípade fyzickej osoby a jej identifikácie je totožnosť entity vždy overovaná na základe štátom vydaných dokladov. Digitálny svet sa snaží tento proces napodobňovať, ale samozrejme musia existovať rozdiely. Napríklad v prípade transakcií v bankovom sektore nemusí byť účasť digitálnej identity nutná. Článok Digitálne občianstvo a právo na digitálnu identitu podľa medzinárodného práva (SULLIVAN, 2016) opisuje pohľad na digitálnu identitu z právnych aspektov. Digitálna identita je podľa autora dokonca len aktérom transakcie, transakčné systémy ďalej používajú len atribúty (teda fragmenty) digitálnej identity a všetky činnosti spojené s transakciou už prebiehajú v pozadí bez priamej účasti identity. Inak povedané, účasť digitálnej identity je potrebná len počas inicializácie a autorizácie platby, transakčným systémom pri ďalšom spracovávaní transakcie postačuje len zhoda atribútov a vyhodnotia identitu ako overenú. Transakčná identita priamo implikuje fyzickú osobu, ktorá je naviazaná na digitálnu identitu bez ohľadu na to, či táto osoba transakciu skutočne vykonala. To má za následok, že finančné inštitúcie v súkromnom sektore vykonávajú transakcie v mene skutočných identít a následne vznikajú spory súvisiace s dokazovaním relevantnosti transakcie. Autor sa v článku venuje aj právnym aspektom digitálneho občianstva, právu na sebaurčenie a ľudskému právu ako základnou súčasťou digitálneho občianstva.

V ďalšom článku Digitálna identita – Od vznikajúceho právneho konceptu k novej realite (SULLIVAN, 2018) sa autor zaobera procesmi, ktoré sa dotýkajú denného života entity v modernej spoločnosti: zakladaniu a overeniu identity. Pri registrácii identity (napr. v banke) je zvyčajne vyžadovaný štátom vydaný doklad ako napríklad rodný list, občiansky preukaz, vodičský preukaz alebo pas a v prípade zmeny atribútov je požadovaný iný štátom vydaný dokument, napríklad sobášny list alebo univerzitný diplom. Primárnym dokumentom totožnosti je vždy rodný list od ktorého sa odvíjajú všetky ostatné dokumenty (napríklad občiansky preukaz), ktoré sú ale tiež považované za primárne. Pri overovaní identity sú použité rôzne techniky na overenie atribútov. Často sa používa elektronická validácia kópie štátom vydaného dokladu. Dáta z kópie sú overované v štátom prevádzkovaných registroch. Overujú sa elektronicke vytvorené dátá napr. z odskenovaného fyzického dokladu. Dôležitým aspektom je aj čas. V čase registrácie identity sa zhromažďujú atribúty identity požadované aktuálnou schémou (datasetom) atribútov. Pri overovaní sa atribúty ale vytvázia z aktuálnych identifikátorov identity ako je napríklad fotografia, video (tzv. liveness check) alebo odskenovaný ručný podpis. Technológie nedokážu dostatočne silno ani spoľahlivo túto väzbu spojiť a jednoznačne identifikovať digitálnu identitu a preto je overovanie digitálnej identity určované s určitým stupňom pravdepodobnosti.

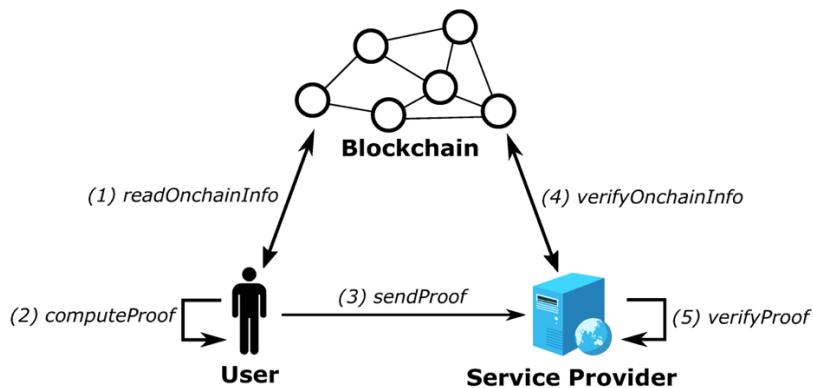
Prístup k ochrane atribútov digitálnej identity je vždy závislý od identifikovaných rizík. V inštitúciach, ktoré sú regulované, je hrozba vysokej pokuty účinným urýchľovačom implementácie systémov na ochranu dát. Keďže sú tieto systémy náročné na investície a prevádzkové náklady, tak je naj efektívnejšie riešenie ochrana dát na základe ich klasifikácie. Napríklad na ochranu *Interných* dát s nízkou životnosťou finančné inštitúcie vynakladajú nižšie prostriedky ako na dátá klasifikované ako *Chránené* alebo *Prísne chránené*. Všetky typy atribútov finančné inštitúcie zbierajú, spravujú len so súhlasm klienta alebo prospektu (fyzická osoba, ktorej banka spracuváva osobné údaje pred podpisom zmluvy) a pod dozorom regulačných orgánov. Benefitom je zvýšená kvalita zbieraných dát, ktorá je často rozhodujúcim faktorom pri úspešnosti nových finančných produktov. Klasifikácia dát je preto jedným z aspektov, ktoré sú merané a vyhodnocované v praktickej časti tejto práce.

1.4 DIGITÁLNA IDENTITA A NFT

Často používame online služby, ktoré namiesto štandardného prihlásenia menom a heslom používajú jednorazové tokeny. Tokeny sú používateľom vydané po

zaregistrovaní na platforme, ktorá tieto služby poskytuje. Tieto platformy sú len digitálnou verziou procesov, ktoré už dávno fungujú v reálnom svete. Veľmi podobne to už funguje aj v štandardných službách. Napríklad vstupenky na koncerty alebo múzeá si používateľ si zakúpi vo forme papierového lístka, ktorý ho oprávňuje navštíviť dané podujatie. Tieto systémy sú vo fyzickom aj digitálnom svete väčšinou centralizované a často si navzájom nedôverujú.

Autori (SALLERAS et al, 2022) navrhli decentralizovaný systém fungujúci na technológii blockchain, ktorý používateľom na spomínaný účel generuje jednorazové NFT (non-fungible) tokeny. Návrh je výnimcočný v tom, že tokeny je možné použiť v zariadeniach s nízkym výpočtovým výkonom, napr. smartfóny. Navrhovaný autentizačný protokol pod názvom FORT je kombinovaný s blockchainovými technológiami. Používateľovi umožňuje posielat atribúty (časti svojich osobných informácií) vo forme NFT tokenu a v rozsahu, ktorý si sám určí. NFT tokeny sú overované mimo blockchainu, u Service providera (poskytovateľa služby), čím je dosiahnuté jednak ušetrenie poplatkov za blockchainové transakcie a zároveň nie je možné spárovanie NFT tokenu s identitou používateľa v blockchaine.



Obrázok 2 Scenár autentizácie s FORT protokolom⁷

Postup celého procesu je nasledovný:

- Používateľ získa niektoré atribúty 3-tich strán, napr. poskytovateľa služby, u ktorého chce zakúpiť lístok, získať certifikát solventnosti z banky a pod.. Tieto atribúty sú uložené v blockchaine vo forme NFT.

⁷ <https://www.mdpi.com/2227-7390/10/4/617/htm>

2. Service provider vydá NFT, ktorý reprezentuje používateľove atribúty a pošle ho používateľovi.
3. Používateľ vystupuje ako overovateľ a vypočíta ZKP z informácií získaných z NFT a nainštaluje si certifikát na smartfón.
4. Používateľ chce použiť zakúpenú službu a preukáže sa certifikátom.
5. Service provider si načíta dátá z blockchainu a overí reťazosť certifikátu používateľa (NFT).

1.5 TECHNOLÓGIA BLOCKCHAIN V KYC PROCESOCH

Navrhovanie frameworku pre digitálne procesy KYC (Known Your Customer) založené na technológií blockchain popisuje štvorica autorov (SCHLATT et al, 2021). KYC procesy sú vyžadované regulátormi, ale sú nákladné, neefektívne a nepohodlné hlavne pre zákazníkov. Niektoré banky používajú KYC procesy len ako prostriedok ako sa vyhnúť pokutám od regulátorov spôsobených nedostatočnou ochranou pred praním špinavých peňazí (Anti Money Laundering), ku ktorému sa hlási 130 štátov sveta. Niektoré banky však vnímajú KYC aj ako príležitosť lepšie porozumieť potrebám zákazníkov a prispôsobiť im svoje produkty. Štandardný KYC proces začína zberom údajov o zákazníkovi zo štátom vydaných alebo iných fyzicky overiteľných dokumenov, napr. občiansky preukaz, faktúra za telefón. Po overení týchto údajov banka posúdi riziká vlastnou internou metodikou a následne vyhodnotí rizikové skóre na základe zoznamov známych teroristov, zločincov a politicky exponovaných osôb. Niektoré z týchto procesov prebiehajú v cykloch.



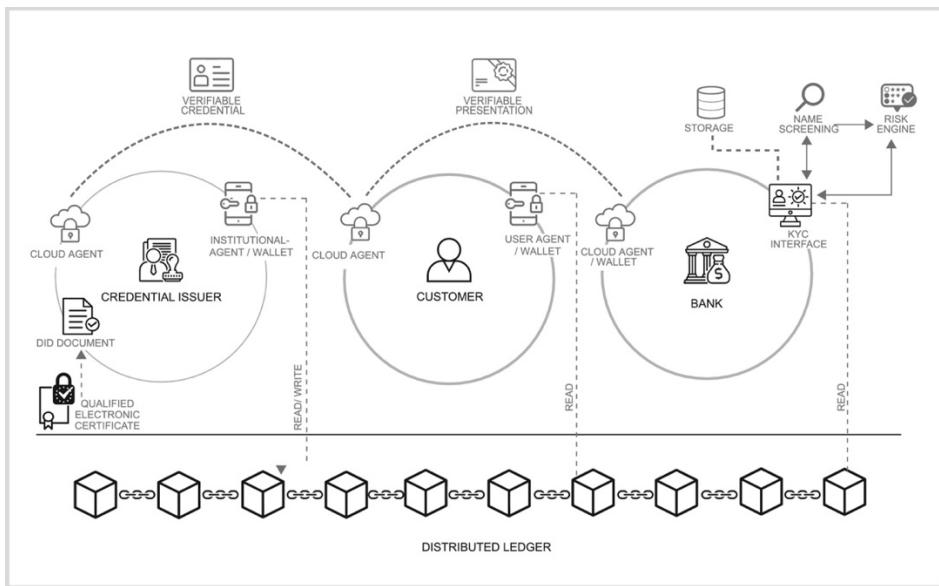
Obrázok 3 Popis štandardného KYC procesu⁸

V snahe vylepšiť používateľský komfort používateľa bol vyvinutý koncept tzv. federovaného modelu identity. Jeho princíp spočíva v tom, že organizácie akceptujú digitálnu identitu zriadenú u verejne známeho a Identity providera, napr. Google alebo Facebook a tvrdenie tohto Providera o úspešnej autentifikácii považujú za dostatočne pri autentifikácii do vlastného systému. Toto tvrdenie je často digitálne podpísané

⁸ <https://www.sciencedirect.com/science/article/pii/S0378720621001270>

a overiteľné pomocou PKI (Private Key Infrastructure). V tomto koncepte sa používajú digitálne identity aj za hranicami organizácie, štátu alebo kontinentu. Poskytovateľ identity spravuje atribúty používateľa a sprístupňuje ich bezpečným spôsobom tretím stranám, pričom klient udeľuje súhlas so spracovaním atribútov. Predpokladom tohto modelu je vytvorenie vzťahu dôvery medzi poskytovateľom identity (Identity providerom) a poskytovateľom služby (Service providerom).

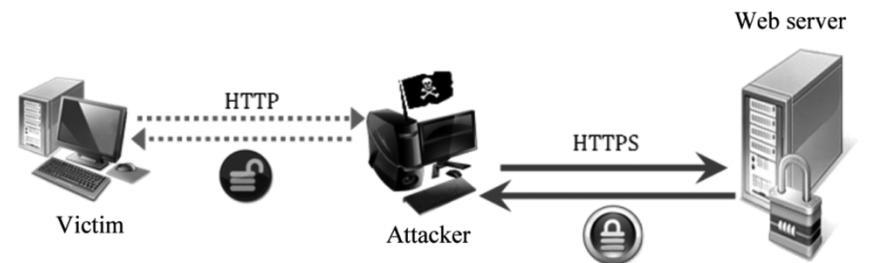
Federovaný model identity však nemôže byť použitý v KYC procesoch, lebo entita musí udeliť súhlas so spracovaním svojich osobných údajov treťou stranou, čo je v praxi dosť nepravdepodobné. Preto autori v článku navrhujú použiť pre KYC proces technológiu blockchain, ktorá má výhody, ale aj nevýhody. Medzi výhody patrí integrita dát zaručená asymetrickou kryptografiou, čiže dáta sú uložené do blokov a každý blok dát obsahuje hash predchádzajúceho bloku. Bloky teda tvoria reťazec a vytvárajú záznam historicky odolný voči manipulácii. Ide o decentralizovanú architektúru dát a každá kópia databázy s názvom distribuovaná účtovná kniha (DLT) je hodnoverným zdrojom pravdy. Medzi nevýhody patrí rozpor z pohľadu regulácie GDPR, lebo právo na zabudnutie v prípade DLT nemôže byť uplatnené, lebo dáta v DLT sa nedajú pozmeniť alebo anonymizovať. Preto sa v DLT ukladajú len informácie o ukončených KYC procesoch, ktoré neobsahujú osobné údaje fyzických osôb. Identita zákazníkov je uložená u centrálneho poskytovateľa KYC a banka si s ním môže tieto informácie vymeniť iným kanálom.



Obrázok 4 Obrázok: KYC proces založený na technológii blockchain⁹

1.6 AUTENTIFIKÁCIA

Vo svojej publikácii Authentication Systems autor (KIENNERT et al, 2015) detailne opisuje koncept autentizácie. Na autentifikáciu sa pozera ako na široký rozsah protokolov, systémov a architektúr ktoré sa podieľajú na identifikácii a autentifikácii digitálnej identity. Keďže každý protokol má zraniteľnosti, je potrebné poznať aj základné scenáre útoku na protokol, napríklad Man-In-The-Middle (MITM), útok hrubou silou, replay attack atď.. Slabiny autentizačných protokolov sú veľmi dôležité pri rizikovej analýze autentizácie, lebo aj na dobre navrhnutý protokol s nezlomiteľným šifrovaným je možné použitím vhodnej technicky útoku získať dátá používateľa. Príkladom je MITM útok na https protokol zobrazený na nasledujúcom obrázku.



Obrázok 5 Popis MITM útoku na https protokol¹⁰

⁹ <https://www.sciencedirect.com/science/article/pii/S0378720621001270>

¹⁰ <https://www.sciencedirect.com/science/article/pii/B9781785480041500031>

Autor (KIENNERT et al, 2015) opisuje kryptografické princípy, hašovanie a hašovacie funkcie a ich použitie v autentizačných mechanizmoch a tzv. challenge-response funkciách. Tieto informácie boli inšpiráciou v návrhu kategórie šifrovanie ako jeden z aspektov, ktorá majú zásadný vplyv na digitálnu identitu. Medzi protokoly používajúce streamovú (prenosovú) šifru patrí napríklad TLS protokol, ktorý bol zaradený do zoznamu autentizačných protokolov v tejto práci pre svoju univerzállosť a možnosť použitia zdieľaného tajomstva so symetrickou (heslo) alebo asymetrickou (certifikát) kryptografiou.

Miesto v zozname autentizačných protokolov bolo priradené aj OTP (One time password) autentizácii, ktorú autor (KIENNERT et al, 2015) považuje za 2-faktorovú a rozdeľuje ju na hardvérovú a tabuľkovú (u nás známe GRID karty).

3-tí faktor (biometriu) rozdeľuje na typ verifikačný (porovnávanie v databáze s očakávanou zhodou 1:1) a identifikačný (hľadanie identity podľa vzoriek s porovnávaním 1:N). V tejto práci bola biometria zaradená k aspektom autentizačné faktory.

Samostatná kapitola tejto publikácie je venovaná Identity management (IDM) systémom. Autor (KIENNERT et al, 2015) popisuje procesy registrácie, pridelenie oprávnení, integráciu s klientom, autentizačné frameworky a úlohy identifikácie, autentizácie a autorizácie v komunikácii s IDM. Pre účely tejto práce boli použité často používané autentizačné frameworky SAML, OpenID a OAuth.

1.7 ZHRNUTIE POZNATKOV Z ANALÝZY

V tejto kapitole je zhrnutie získaných poznatkov z predchádzajúcej analytickej časti práce a výber kategórií aspektov, ktoré majú vplyv na proces autentifikácie a boli použité ako kategórie aspektov. Do kategórií boli pridané aspekty opísané v tejto kapitole. **Klasifikácia dát** je rozhodujúcim faktorom pri výbere autentizácie. Má najväčší vplyv na dopad rizika a je klíčovým faktorom pri ochote investovať do zlepšenia kvality autentizácie.

Architektúra aplikácie a aplikačného servera rozhoduje o pravdepodobnosti výskytu zraniteľnosti alebo hrozby. Čím je architektúra jednoduchšia a transparentnejšia, tým je jednoduchšie identifikovať útočníka, aktualizovať systém alebo pridať ďalšie komponenty.

Sieťová lokácia (alebo aj komunikácia) je aspekt, ktorý má vplyv na pravdepodobnosť útoku na autentizačný protokol. Čím je viac sietí a serverov, cez ktoré prebieha komunikácia klienta a servera, tým je vyššia pravdepodobnosť nežiaducej inšpekcie komunikácie.

Autentizačné faktory sú klúčovým aspektom pri identifikácii, autentizácii a autorizácii. Dôvera medzi klientom a serverom je závislá od sily autentizácie. Počas autentizácie používateľa sú bezpečnou formou overené známe atribúty digitálnej entity. Často to býva len tajomstvo (napr. heslo, vlastníctvo klúčov a pod.) zdieľané medzi digitálnou identitou a poskytovateľom identity. Autentizovať je možné aj na základe biometrických atribútov (tvár, hlas, šošovka, odtlačok prsta) porovnávaním biometrických vzoriek pomocou vopred daného algoritmu s akceptovateľnou pravdepodobnosťou. Overované tajomstvo môže byť spravované priamo entitou (napr. používateľom zapamätané heslo), uložené v aplikácii (napr. session ID v session cookie) alebo uložené v neexportovateľnej a nečitateľnej forme v HSM module. Často je autentizácia kombinovaná z niekoľkých faktorov, vtedy hovoríme o tzv. multifaktorovej autentizácii. Dôvodom je mitigácia známych rizík identifikovaných počas prvého (niečo vedieť, napr. heslo), druhého (niečo vlastniť, napr. hardvérový token) alebo tretieho (niekým byť) faktoru autentizácie. Silnejšia forma autentizácie môže byť dosiahnutá aj viac-krokovou autentizáciou. Je to autentizácia rozdelená do viacerých krokov, počas ktorých sa verifikuje vlastníctvo ďalších autentizačných prostriedkov (napr. heslo + OTP token z Google autentifikátora). Je možná aj kombinácia v rámci jedného faktora, napr. druhý faktor môže byť ešte chránený PIN-om alebo tretí faktor (biometria tváre) je podmienený vlastníctvom mobilného telefónu, v ktorom je možné uskutočniť biometriu. Aplikácie nainštalované v mobilnom telefóne je spárovaného s identitou jedinečnými klúčmi pridelenými poskytovateľom identít. Adaptívna autentizácia je proces, pri ktorom je možné vynechať niektoré kroky viac-krokovej alebo multi-faktorovej autentizácie na základe dynamického vyhodnocovania rizikového faktoru.

Digitálne podpisovanie je aspekt, ktorý zabezpečuje integritu dát prenášaných počas autentizácie ale aj po nej. Podpisovanie, resp. nepopierateľnosť v challenge-response procesoch v autentizácii je klúčovým prvkom pri pridelení oprávnení k dátam používateľa.

Šifrovanie priamo nezlepšuje autentizačný proces, ale je najvýraznejším mitigačným opatrením pre zníženie rizika a preto bolo zaradené v tejto práci k aspektom. Bezpečná

forma výmeny dát je dosiahnutá na úrovni komunikačného kanála (šifrovanie prenosu) alebo aj na úrovni prenášaného tajomstva (šifrovanie alebo hašovanie hesla).

Privilégia používateľa sú dôležitým faktorom pri komunikácii klienta a servera, lebo majú najvýraznejší vplyv na zamedzenie neoprávneného prístupu k dátam na serveri. Počas procesu autoritácie je digitálnej identite poskytnutý prístup k definovaným zdrojom. Je podmienená úspešnou autentizáciou a nie je potrebná interakcia používateľa. Oprávnenia sú pridelené na strane servera a sú definované v matici oprávnení. Poznáme niekoľko modelov pre riadenie autorizačných rolí, najpoužívanejšie sú RBAC (role based access control) a ABAC (attribute based access control).

1.8 ANALÝZA AUTENTIZAČNÝCH PROTOKOLOV

Spomínané aspekty nemajú rovnaký vplyv na autentizačné protokoly, preto je v ďalších odsekoch vyhodnotený vplyv aspektov na vybrané autentizačné protokoly samostatne.

1.8.1 Basic access authentication

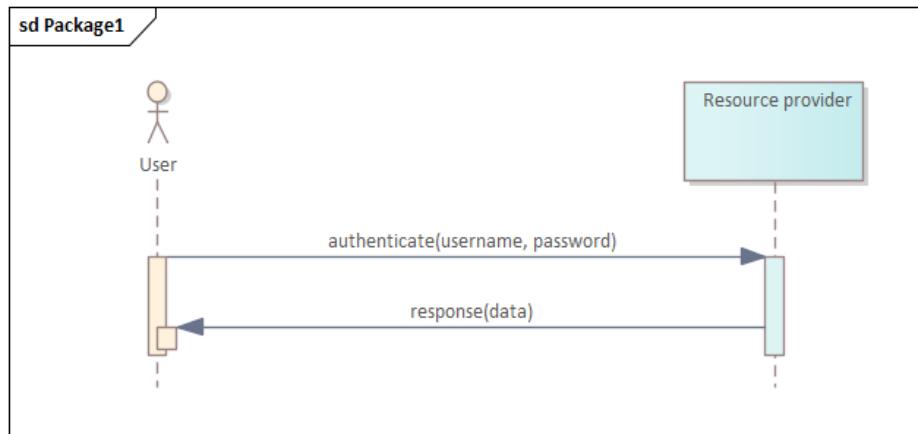
Medzi najpoužívanejšie autentizačné protokoly v internetovej komunikácii patrí Basic access authentication (RFC2617). User Agent posiela meno a heslo v HTTP protokole v hlavičke enkódované v BASE64 tvare a nešifrované. Autentizačné údaje môžu byť šifrované len prenosovou šifrou (napr. TLS) v prípade použitia HTTPS protokolu. Príklad autentizačnej hlavičky v HTTP protokole:

```
Authorization: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==
```

Určitým vylepšením ochrany prihlásovacích údajov je použitie Digest access authentication (RFC2617). V tejto forme autentizácie je namiesto enkódovania použitá hashovacia funkcia. Ak útočník počas MITM útoku odchytí hash mena a hesla, tak za predpokladu, že používateľ použije aktuálne odporúčané hashovacie algoritmy a nounce (inicializačný vektor), je meno aj heslo v podstate nezlomiteľné.

Najzraniteľnejším miestom HTTP Basic autentizácie je možnosť nešifrovať komunikáciu, čo na jednej strane urýchľuje a zjednodušuje implementáciu, ale zároveň umožňuje útočníkovi odchytíť alebo pozmeniť prihlásovacie údaje. Protokol je možné použiť aj komunikáciu cez proxy servery load balancery, čo ale zvyšuje riziko odchytenia

autentifikačných údajov. Protokol nedokáže podpisovať komunikáciu, ani poskytnúť informáciu o aplikačnej role používateľa.



Obrázok 6 UML sekvenčný diagram pre http basic authentication

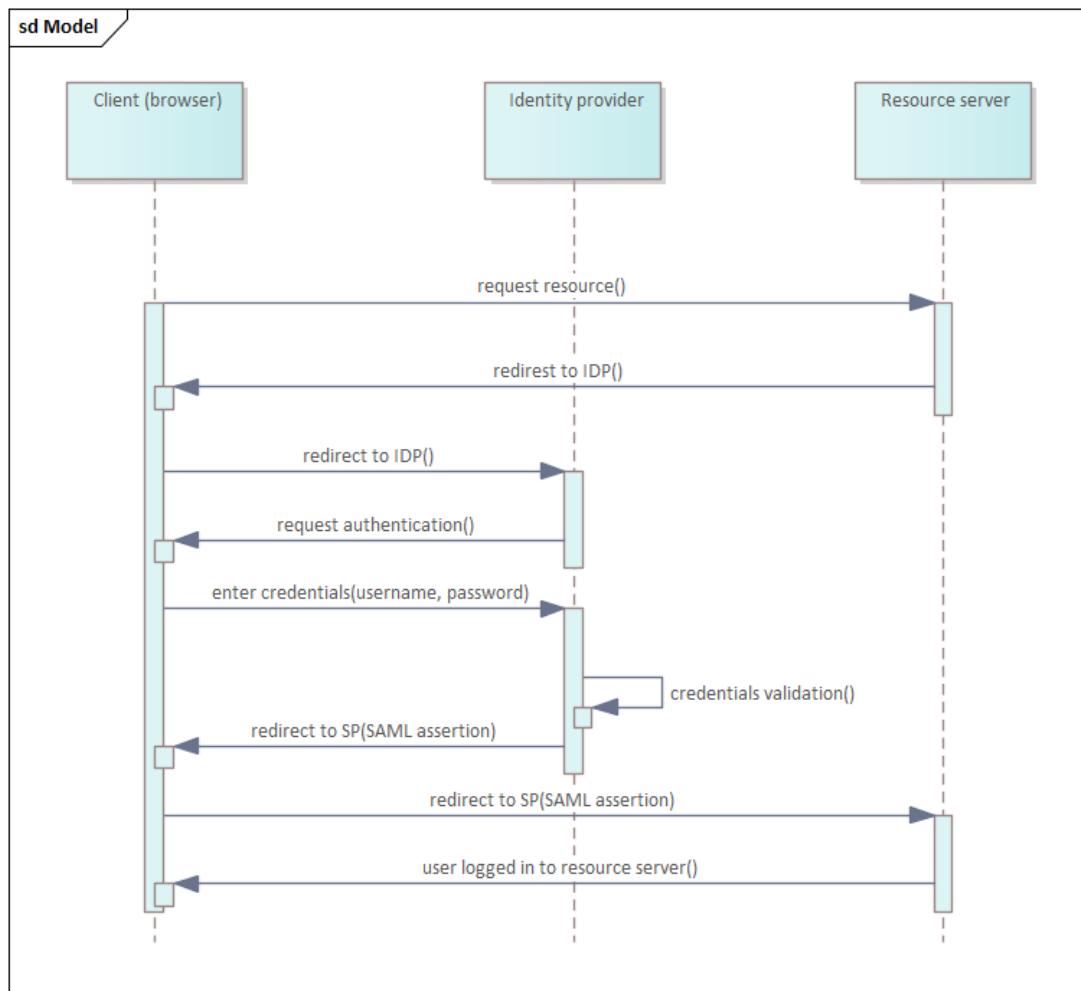
1.8.2 SAML

SAML protokol je otvorený štandard pre autentizáciu do webových aplikácií založený na XML (KEMP, 2005). Digitálne podpísané tvrdenie, tzv. Security assertion je vymieňané medzi Identity providerom a Service providerom. SAML je vhodné použiť na autentifikáciu pri nezávislých webových aplikáciách napriek domény. Vyriešil tak limitácie cookies, ktoré je možné použiť len v rámci jednej domény. Pri používaní SAML protokolu si Servis provider overuje digitálne podpísaný XML súbor. V XML súbore sú všetky informácie, ktoré potrebuje poskytovateľ služby na autentifikáciu používateľa. V procese vystupujú 3 roly: Identity provider, Service provider a používateľ. Pri kombinácii s inými mechanizmami (session cookies, Kerberos ticket) je možné pri SAML autentifikácii použiť Single-Sign-On alebo pre tzv. federatívny login.

Komunikácia medzi klientom a Service providerom, pri ktorej je overený SAML assertion, je najbezpečnejšou časťou frameworku. Pri overení SAML assertion nie je potrebná online komunikácia medzi Identity providerom a Servis providerom, digitálny podpis je overovaný na základe certifikátov, ktorý si obe strany vymenia počas integrácie (podpisuje sa nielen SAML assertion, ale aj žiadosť o vydanie SAML assertion).

Menej bezpečnou je komunikácia s Identity providerom, pri ktorej sa klient môže autentifikovať pomocou iného autentizačného mechanizmu, napr. HTTP Basic authentication, Kerberos ticket alebo pomocou session cookies. Táto komunikácia je najzraniteľnejšou a v prípade MITM útoku dokáže útočník odchytiať prihlásovacie údaje používateľa. Pri celkovom návrhu autentizácie je potrebne SAML protokol nadizajnovať

end-to-end, čím vznikne kombinácia napr. HTTP Basic authentication + SAML + Cookies Session management. Ked'že integritu SAML assertion zabezpečuje digitálny podpis pomocou RSA, SAML nie je závisý na šifrovaní transportnou šifrou. Šifrovanie je ale potrebné na ochranu prenosu klasifikovaných dát. SAML je rezistentný aj voči inšpekcii pri komplexnejšej architektúre, bezpečnosť komunikácie nie je závislá od lokality používateľa a v XML štruktúre SAML assertion môžu byť umiestnené a podpísané aj informácie o role používateľa.



Obrázok 7 Sekvenčný diagram pre SAML autentizáciu

1.8.3 OAuth2

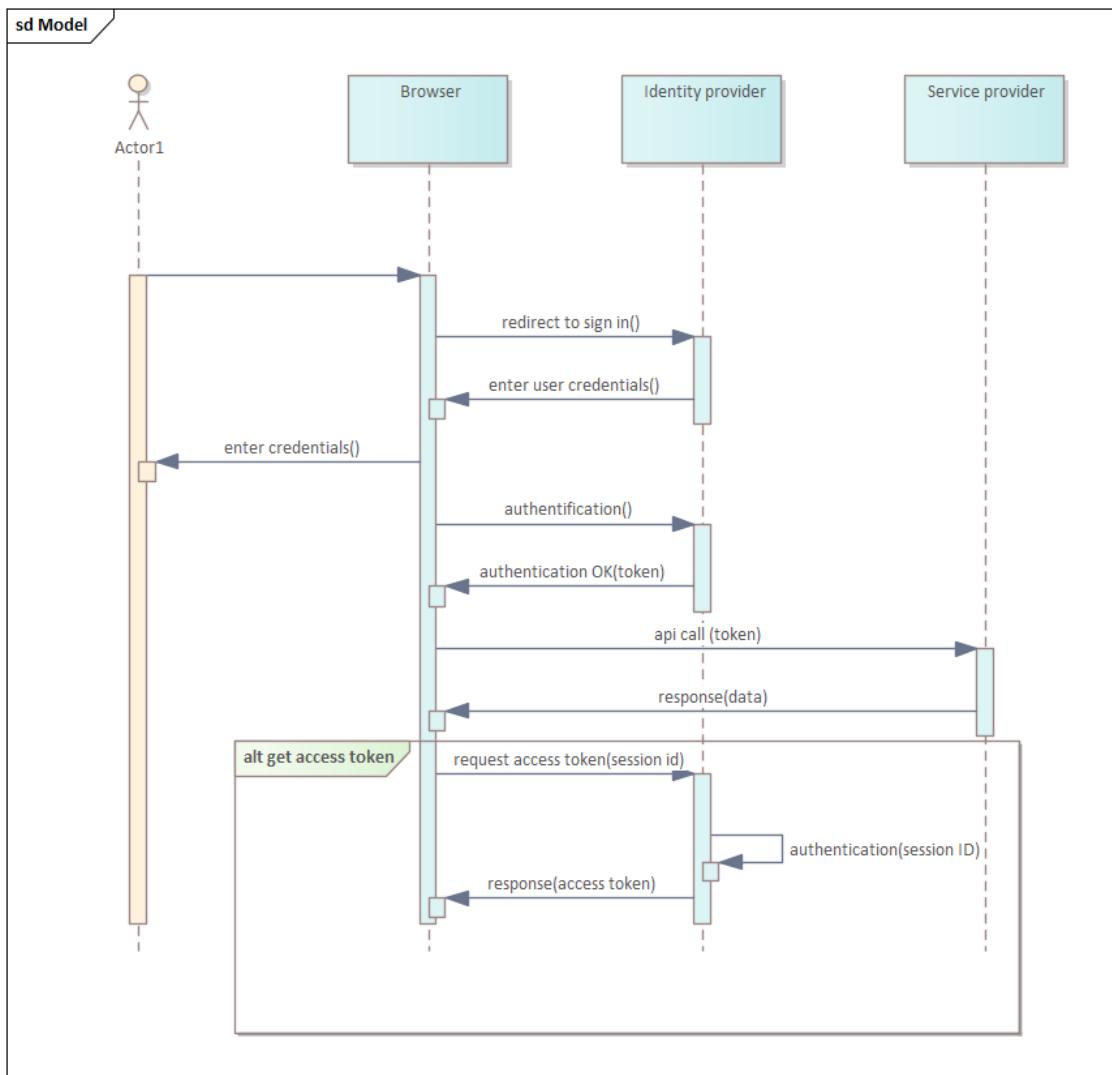
OAuth je otvorený štandard pre bezpečný delegovaný prístup v tzv. pseudoautentizácii v HTTP aplikáciách (HARDT, 6749). Používateľ (resource owner) deleguje oprávnenie (authorization grant) na autorizačnom serveri pre front-endovú klientskú aplikáciu (oauth klient), autorizačný server pridelí aplikácii sadu tokenov (access a refresh token) a oauth klient používa na prihlásovanie na aplikačný server

(resource server) už len len tokeny. Medzi najjednoduchšie scenáre v OAuth frameworku patrí Implicit Grant Flow, ktorý je používaný napr. Microsoft technológiách pre SinglePage aplikácie. Vo frameworku sú použité 3 role: browser s používateľom, identity provider (napr. Microsoft ADFS služba) a resource provider (webová API).

Kľúčovým komponentom je JSON Web token (JWT). JWT je kompaktná reprezentácia tvrdení (claims), ktoré si navzájom vymieňajú 2 strany (JONES, 2015). JWT môže byť pre posielaný vo forme JWS (JSON WEB Signature) alebo vo forme JWE (JSON WEB Encryption). JWS je digitálne podpísany ale v nešifrovanej forme, JWE je nielen podpísaný ale aj šifrovaný.

Podobne ako v prípade SAML, aj OAuth framework je z pohľadu autentizácie odolný voči MITM útokom, lebo je podpísaný. Je odolný aj voči inšpekcii komunikácie a môže obsahovať informácie o aplikačnej role v tzv. Custom claims.

Medzi slabé miesta patrí komunikácia s Identity providerom. Používateľ sa musí voči Identity providerovi najprv overiť napr. pomocou mena a hesla a následne mu je vydaná sada access a refresh tokenov, ktorá sa ukladá bud' v aplikácii alebo na aplikačnom serveri, v závislosti od implementácie. Ak útočník získa sadu tokenov, získa na Resource providerovi rovnaké oprávnenia ako používateľ.

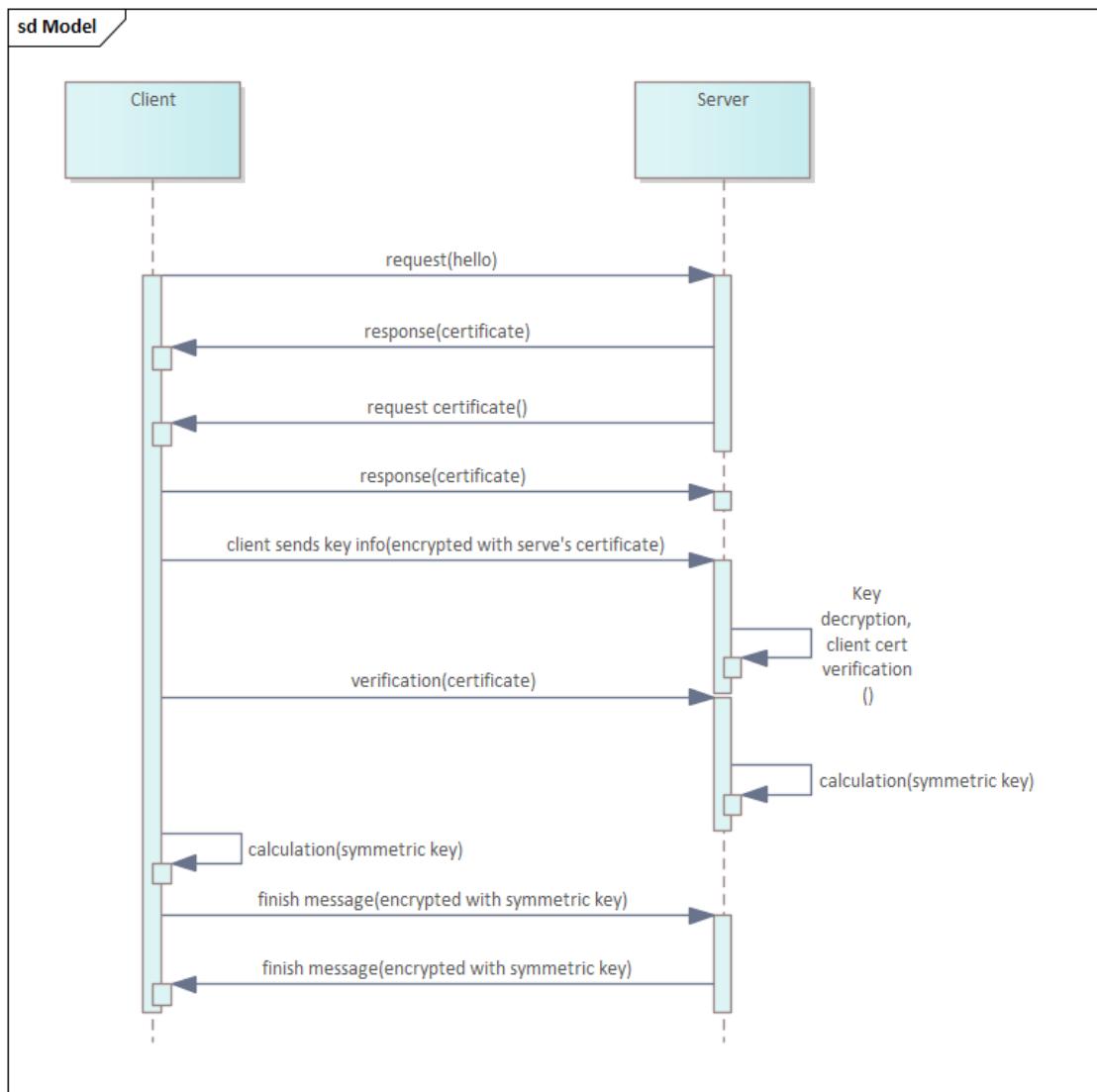


Obrázok 8 Sekvenčný diagram pre OAuth Implicit Grant Flow

1.8.4 Mutual TLS

Často používanou je takzvaná mutuálna (obojstranná) autentifikácia (ORACLE CORPORATION, 2010), pri ktorej sa overuje identita klientskej aj serverovskej časti aplikácie na základe mena a hesla alebo asymetrickej kryptografie (pár privátneho a verejného RSA kľúča). Táto forma autentifikácie je implementovaná napríklad v IKE protokole (IPSec VPN) alebo vo webovej komunikácii medzi dvoma servermi s použitím TLS (transport layer security). Mutual TLS používa na prihlásование konzumera pomocou symetrickej kryptografie (heslo) alebo asymetrickej kryptografie, pri ktorej sú dátia šifrované verejným kľúčom a dešifrované privátnym kľúčom protistrany. V prípade použitia PKI (Public Key Infrastructure) si protistrany navzájom overia aj verejné kľúče certifikačných autorít alebo celého stromu certifikačných autorít.

Medzi slabé miesta tejto formy autentizácie patrí manažement kľúčov. V prípade RSA kľúčov je nutné kľúče uložiť do chránených úložísk (napr. JavaKeyStore, systémové úložisko kľúčov a pod.). V prípade MTLS s použitím hesla je potrebné také uloženie hesla, aby k nemu nemal prístup ani administrátor aplikácie. Mutual TLS používa niekoľko vrstiev OSI modelu a preto nie je vhodná pre komunikáciu cez proxy servery a load balancery. Je odolná voči SSL/TLS inšpekcii na sietovej infraštruktúre a natívne šifruje celú komunikáciu, vrátane autentizácie.



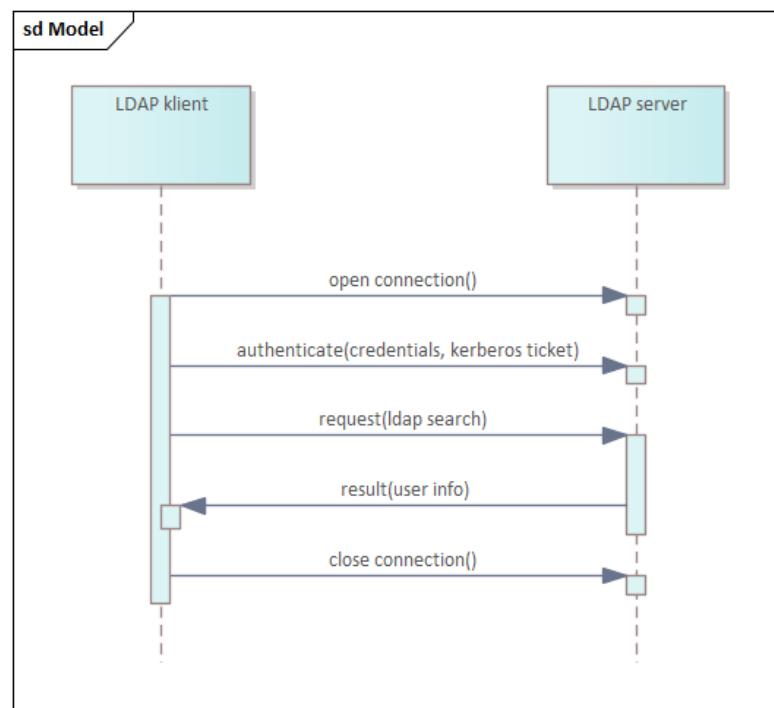
Obrázok 9 Sekvenčný diagram mutual TLS s použitím certifikátov

1.8.5 LDAP

Pri prístupe k súborom alebo zariadeniam v sieti sa často používa Lightweight Directory Access Protocol LDAP (SERMERSHEIM, 2006). Je to systém adresárových služieb. Používateľ, ktorým môže byť človek alebo iný subjekt (server, IoT a pod.),

pristupuje do adresára prostredníctvom LDAP klienta. Klient v mene adresára interaguje s jedným alebo viacerými servermi. Na tomto protokole Microsoft vybudoval Active Directory, ktorá je veľmi často používaná v korporátnych prostrediach. Pomocou LDAP sa vymieňajú správy medzi servermi a klientskymi aplikáciami. Správy môžu obsahovať akékoľvek informácie uložené v databáze servera.

Medzi nevýhody protokolu patrí náročná integrácia, preto je používaný hlavne v korporátnych prostrediach. Protokol je natívne šifrovaný a odolný voči infraštruktúrnym problémom v segmentovaných sieťach. LDAP protokol umožňuje validáciu „členstva“ v adresári, preto je používaný aj pre validáciu aplikačnej role.



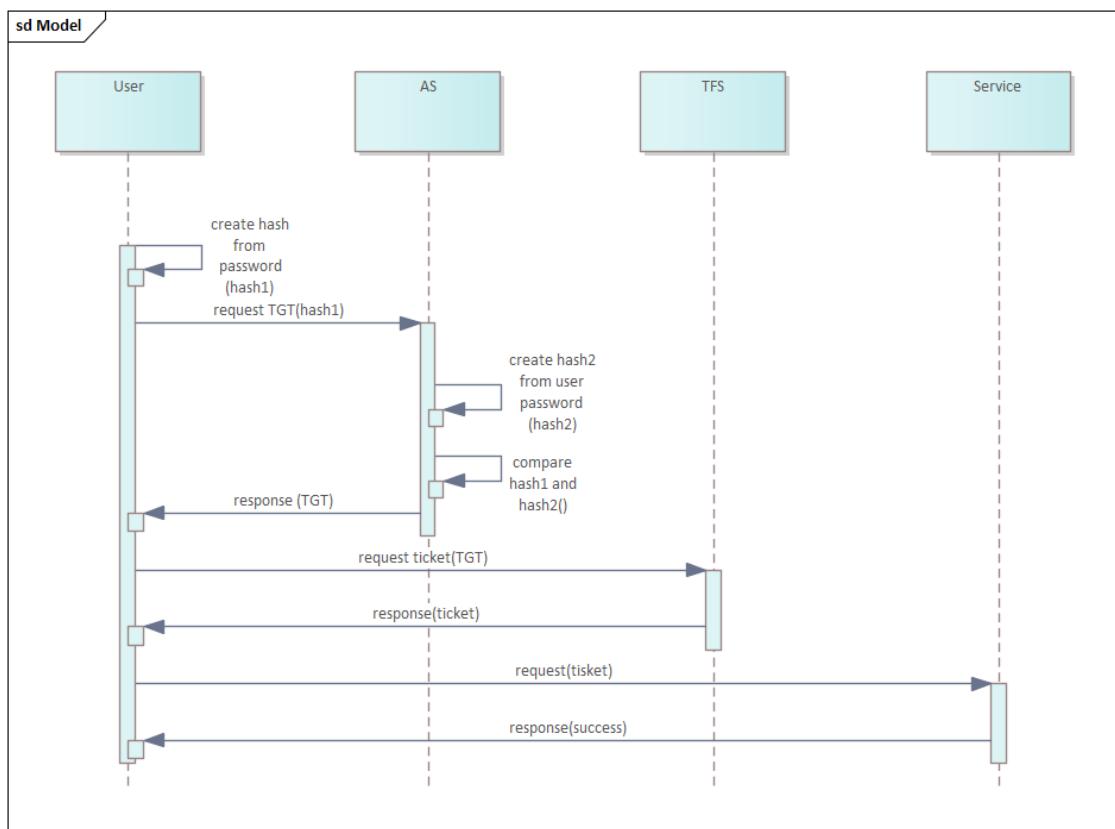
Obrázok 10 Sekvenčný diagram pre LDAP autentizáciu

1.8.6 Kerberos

Ďalším často používaným siet'ovým autentizačným protokolom je Kerberos Network Authentication Service (V5) (NEUMAN, 2005). Je navrhnutý tak, aby poskytoval silnú autentifikáciu pomocou kryptografie s tajným klúčom. Bezzplatná implementácia tohto protokolu je k dispozícii na Massachusetts Institute of Technology. Kerberos je dostupný aj v mnohých komerčných produktoch, napr. Active Directory od spoločnosti Microsoft. Pri Kerberos autentifikácii musia byť dostupné 3 služby: Autentizačného servera (AS), Servisného strediska (SS) a Ticket-granting servera (TGS). Používateľ má autentizačné údaje (napr. meno a heslo) a na prístup do aplikácie potrebuje získať Ticket granting

ticket (TGT). Autentizácia pomocou Kerberos v prostredí HTTP protokolov má názov SPNEGO a je často používaná v komerčných prostrediach. Kerberos spolu s SPNEGO tvoria veľmi používanú implementáciu Single-Sign-On, pri ktorej používateľ získa Kerberos ticket pri prihlásení do operačného systému a následne ho použije na prihlasovanie do služieb na aplikačných serveroch na rôznych protokolov (napr. HTTP, CIFS, SMB a pod.) .

Medzi nevýhody Kerberos autentizácie patrí náročnosť implementácie a management služieb, preto je v komerčných prostrediach postupne nahradzovaný SAML alebo JWT tokenmi.

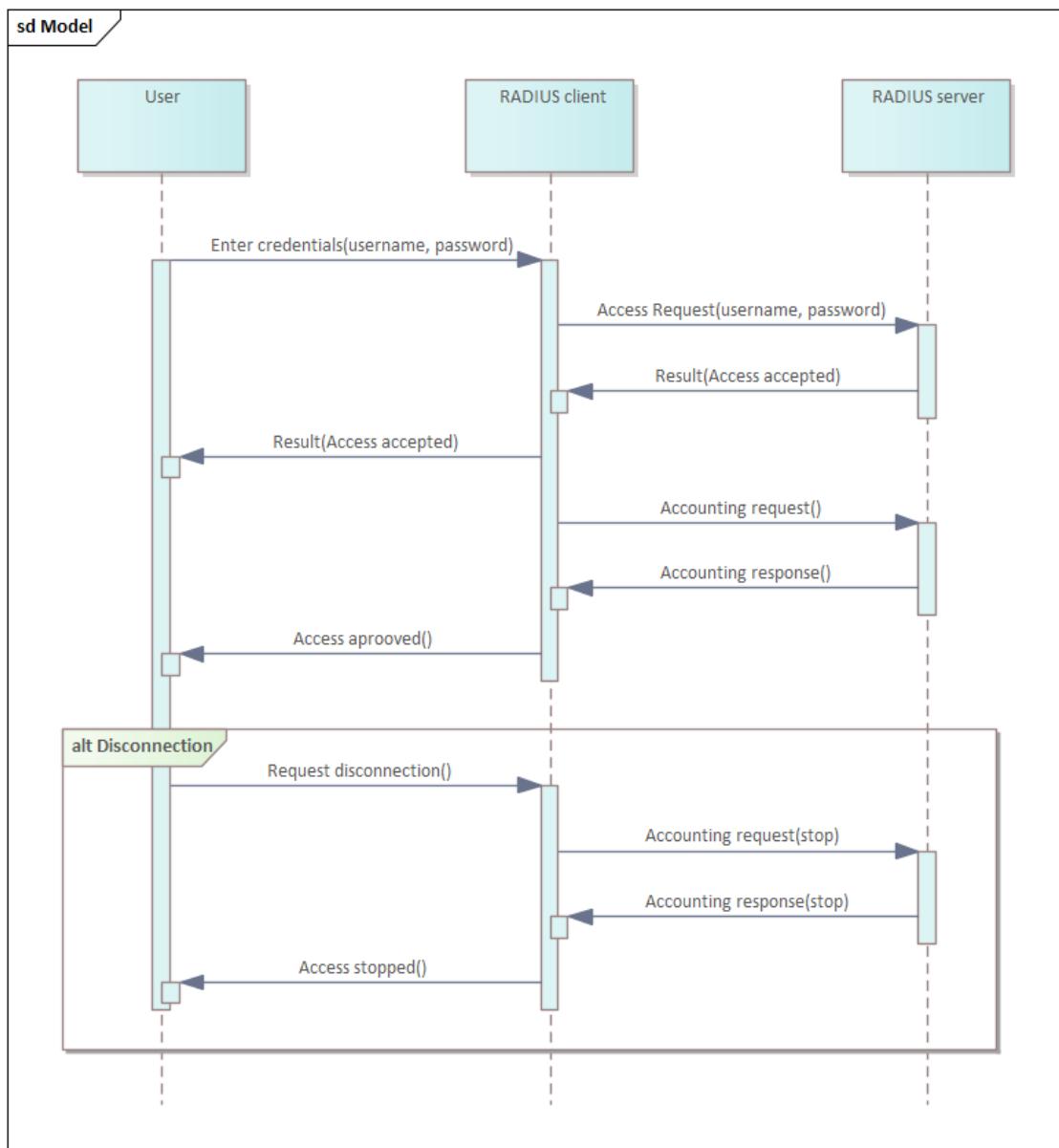


Obrázok 11 Sekvenčný diagram Kerberos autentizácie

1.8.7 Radius

Často používaným hlavne vo svete IoT zariadení je Remote Authentication Dial In User Service: RADIUS (RIGNEY, et al., 2000). Pri tejto forme autentizácie používateľ zadá svoje prihlasovacie údaje cez šifrovaný kanál do RADIUS klienta, ktorý ich prepošle na RADIUS server. RADIUS protokol dokáže zabezpečiť nielen autentifikáciu, ale aj autorizáciu (rolu používateľa) a accounting, čiže zbieranie štatistických informácií na základe ktorých je možné klientovi napr. účtovať poplatky za používanie služby.

Medzi nevýhody patrí náročná implementácia a prevádzka serverovskej časti služby.



Obrázok 12 Sekvenčný diagram pre autentizáciu RADIUS protokolom

2 CIELE ZÁVEREČNEJ PRÁCE

Hlavným cieľom záverečnej práce je analyzovať a identifikovať aspekty, ktoré majú vplyv na autentizačné protokoly. Tieto aspekty je potrebné pomenovať, zoradiť do kategórií a určiť váhu jednotlivých aspektov, aby možné merať ich vplyv na celkové riziká autentizačného mechanizmu. Na meranie rizikovosti je potrebné použiť objektívnu metodiku, ktorá vyhodnotí nielen rizikovosť aspektov a protokolov, ale dokáže merať mieru rizika aj po zmene modelu, napr. po aplikovaní vybraného aspektu. Zoznam aspektov by mal byť otvorený, editovateľný a mal by obsahovať predpripravené dátá, ktoré je možné ihneď použiť na modelovanie autentifikácie.

Ďalším cieľom je pripraviť aplikáciu, ktorá používateľovi umožní vybrať optimálny autentizačný protokol na základe vybraných aspektov so zvolenou hodnotou. Aplikácia by mala okrem štandardných funkčností (webové rozhranie, správa používateľov, bezpečnosť, aplikačné roly) poskytnúť predpripravené dátá, ktoré môže používateľ použiť na modelovanie autentizácie. Predpripravené dátá by mali zohľadňovať rizikovosť použitých autentifikačných protokolov a zohľadniť ich rizikovosť pri návrhu optimálnej formy autentifikácie. Zoznam štandardných autentizačných protokolov je potrebné pripraviť z analytickej časti tejto práce a klasifikovať ich rizikovosť podľa rovnakej metodiky ako sú klasifikované aspekty. Vzniknutý zoznam protokolov musí byť otvorený, t.j. používateľ alebo organizácia, ktorá bude s aplikáciou pracovať má mať možnosť pridania vlastného autentizačného protokolu, prípadne upraviť predpripravený protokol podľa vlastných potrieb. Namodelovaný protokol by si mal používateľ vedieť uložiť a mal by mať možnosť s ním v prípade potreby pracovať aj neskôr.

Ďalšie podciele alebo čiastkové ciele:

- navrhnuť efektívnu metodiku pre analýzu rizík, ktorá nevyžaduje príliš detailné informácie a poskytnúť používateľovi základné informácie o rizikovosti nameraného výsledku,
- chrániť citlivé dátá (analýzy rizík, katalóg hrozieb) riadením prístupu do aplikácie pomocou autentizácie a aplikačných rolí,
- použiť všeobecne známu a ľahko použiteľnú metodiku na modelovanie hrozieb a analýzu rizík.

3 METODIKA PRÁCE

V tejto práci je použitá metodika OWASP Threat Modeling Process (CONKLIN, 2022), v ktorej autor odporúča postupy na identifikáciu, kvantifikáciu a riešenie bezpečnostných hrozieb a rizík. Metodika umožňuje modelovanie a hodnotenie hrozieb pomocou DREAD faktorov a výpočet kvalitatívnej miery rizika pomocou pravdepodobnosti a dopadu. Metodika je nie je licencovaná a je verejne uznávaná hlavne pri klasifikácii rizík pri penetračných testoch.

Odporúčaný postup je rozdelený do 3 krokov: dekompozícia aplikácie, modelovanie hrozieb a návrh mitigačných opatrení. Pre účely tejto práce boli kroky prispôsobené a ich popis je detailnejšie rozpísaný nasledujúcich odsekok.

3.1 DEKOMPOZÍCIA APLIKÁCIE

Počas dekompozície je pripravený stručný popis aplikácie: *Názov protokolu, Popis prípadu použitia; administratívny zoznam vlastníkov: Vlastník dokumentu, Zúčastnení, Kontroloval; zoznam meraných aspektov Klasifikácia dát, Architektúra, Sieťová lokalita, Autentizačné faktory, Podpisovanie, Šifrovanie, Privilégia aplikačného účtu*. Na uloženie týchto administratívnych informácií je pripravená šablóna protokolu dostupná v prílohe C tohto dokumentu.

3.2 MODELOVANIE HROZIEB A ANALÝZA RIZÍK

Hodnotenie hrozieb je klasifikované pomocou subjektívneho modelovania DREAD (CONKLIN, 2022), ktoré je vhodné do firemného prostredia aj internetových aplikácií, lebo zohľadňuje odlišnú implementáciu štandardov pre autentifikačné protokoly. Autentifikačné protokoly často nie sú aplikované poľa štandardu a subjektívnosť posudovania umožňuje risk analytikovi presnejšie posúdenie faktoru modelu. DREAD faktory je možné vo firemnom prostredí upraviť, doplniť alebo zduplikovať podľa aktuálnych potrieb. Hodnoty kategórii faktorov (*Threat Agent Factors, Vulnerability Factors, Technical Impact Factors, Business Impact Factors*) sú v tejto práci ponechané podľa odporúčaní OWASP a sú uvedené v prílohe A.

Forma zápisu napr. pre faktor *Skills required* s hodnotou *No technical skills (1)* je zapísaný v tvare DREAD(SL) = 1 . Zápis maximálnych hodnôt všetkých DREAD faktorov je zapísaný v tvare:

$$DREAD(max) = [9, 9, 9, 9, 9, 9, 9, 9, 9, 9, 9, 9, 9, 9]$$

Pravdepodobnosť L (Likelihood) vypočítame ako aritmetický priemer faktorov pravdepodobnosti:

$$L = (TAF(SL + M + O + S + ED)/4 + VF(ED + EE + A + ID) / 4) / 2$$

Autor (CONKLIN, 2022) odporúča vypočítať technický dopad a biznis dopad samostatne z dôvodu objektívnejšieho posúdenia rizika. Keďže pre účel tejto práce postačuje práca s modelmi, vypočítame len celkový dopad I (*Impact*) ako aritmetický priemer:

$$I = (TIF(LC + LI + LAV + LAC)/4 + BIF(FD + RD + NC + PV) / 4) / 2$$

Mieru (hodnotu) pravdepodobnosti a dopadu určíme podľa nasledujúcej tabuľky č.1.

Tabuľka 1 Určenie hodnoty L a I ¹¹

Likelihood and Impact Levels	
0 to <3	LOW
3 to <6	MEDIUM
6 to 9	HIGH

Na definovanie celkovej miery rizika OWASP používa jednoduchú formulu na kvalitatívne hodnotenie miery rizika:

$$\text{Riziko} = (\text{pravdepodobnosť výskytu hrozby}) \times (\text{dopad na organizáciu})$$

Výsledné riziko je možné určiť pomocou nasledujúcej tabuľky č.2 :

Tabuľka 2 Určenie miery rizika¹²

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH

¹¹ https://owasp.org/www-community/OWASP_Risk_Rating_Methodology

¹² https://owasp.org/www-community/OWASP_Risk_Rating_Methodology

	Likelihood
--	-------------------

Priradené faktory, vypočítanú pravdepodobnosť, dopad a riziko zapíšeme do protokolu podľa vzoru v prílohe C do riadku *DREAD vektor, Pravdepodobnosť, Dopad, Rizikové skóre.*

Ďalším odporúčaným krokom po podľa OWASP metodológie modelovanie hrozieb. Modelovanie hrozieb je proces pri ktorom risk analytic vyhodnocuje a následne aj klasifikuje hrozby súvisiace s posudzovanou aplikáciou. Pre modelovanie hrozieb je v tejto práci použitá technika STRIDE Threat Modeling Process (CONKLIN, 2022). V STRIDE sú hrozby rozdelené do kategórií s názvom Falšovanie, Manipulácia, Odmietanie, Zverejnenie informácií, Odmietnutie služby a Navýšenie oprávnenia. STRIDE popisuje hrozby a ich dopad z pohľadu útočníka. Typ hrozby, popis a dopad sú uvedené v tabuľke v prílohe B. Výsledok modelovania hrozieb je zapísaný do protokolu podľa vzoru v prílohe C.

3.3 NÁVRH MITIGAČNÝCH OPATRENÍ

Na stanovenie protiopatrení na identifikované hrozby a riziká je podľa odporúčaní OWASP použitý zoznam mitigačných opatrení a je uvedený v prílohe B tejto práce. Navrhované mitigácie pre jednotlivé aspekty a autentizačné mechanizmy sú vložené do tabuľky podľa vzoru v prílohe C.

Poznámka: aplikácia navrhuje optimálny autentizačný mechanizmus a nepracuje s mitigačnými opatreniami ani s reziduálnymi rizikami (miera zmeneného rizika po uplatnení mitigačného opatrenia). Mitigačné opatrenia by mali byť súčasťou každej analýzy rizík a preto sú súčasťou protokolu z analýzy rizík uvedeného v prílohe C.

4 NÁVRH ALGORITMU NA VÝPOČET OPTIMÁLNEHO PROTOKOLU

Na splnenie zadania bolo potrebné pripraviť niekoľko vlastných postupov. Najprv bolo nájsť postup na hodnotenie aspektov. Tento postup musí aplikovať používateľ pri každom pridávaní nového aspektu, preto je rozpisany detailnejšie v kapitola 4.1.

Ďalej bolo potrebné nájsť postup na vyjadrenie aspektu pomocou DREAD modelu (kapitola 4.2), aby bolo možné merať dopad aspektu na autentizačný protokol (kapitola 4.5).

Poslednou chýbajúcou časťou bolo pripraviť algoritmus na výpočet optimálnej formy autentizácie (kapitola 4.5), k čomu bolo potrebné nájsť postup merania zmeny rizika po aplikovaní aspektu a na to bol použitý koncept používaný v oblasti riadenia rizík nazvaný ako „Worst-case scenario“ (kapitola 4.3).

4.1 FAKTORIZÁCIA ASPEKTOV

Postup faktorizácie aspektov začína prípravou zoznamu aspektov, ktoré majú vplyv na autentizáciu. Základný zoznam pozorovaných aspektov bol získaný zo zadania bakalárskej práce a bol doplnený o aspekty identifikované počas prípravy v analytickej časti tejto práce. Pozorovaním bolo zistené, že čím je zoznam pozorovaných aspektov bohatší, tým je modelovanie hrozieb presnejšie. Zoznam aspektov vytvorených počas prípravy tejto práce je nasledovný:

- Klasifikácia dát (dataclass)
- Aplikačná architektúra (architect)
- Sietová lokácia (netloc)
- Faktory autentifikácie (authfact)
- Podpisovanie (sign)
- Šifrovanie (enc)
- Používateľské oprávnenia (userpriv)

Pozn.: v zátvorke sú uvedené skratky, ktoré sú použité v tejto práci aj v aplikácii.

Po príprave zoznamu boli aspekty rozdelené do kategórií a každému z aspektov bola pridelená hodnota v rozmedzí 0 až 9 (podobne ako pri hodnotení DREAD faktorov). Aspekty boli zoradené od najmenej rizikových, ktorým bola pridelená najnižšia hodnota až po najrizikovejšie s najvyššou hodnotou.

Návod: Ak pri klasifikácii dát uvažujeme o kategóriach Public, Internal, Confidential a Strictly confidential, tak môžeme kategóriam pridelit' hodnoty 1,4,6,9, čiže hodnoty rovnomerne rozdeliť od 0 po 9. Kategóriu Internal môžeme zapísat' v tvare dataclass(4), Confidential v tvare dataclass(6) a dokumenty typu Strictly confidential v tvare dataclass(9).

Faktorizácia každej kategórie pozorovaných aspektov nám umožňuje presnejšie odhadnúť hodnotu meraného aspektu a pridelit' mu váhu. Zmenou váhy môžeme ovplyvniť celkovú hodnotu rizika, lebo pri výpočte miery rizika má aspekt s vyššou hodnotou väčší vplyv (zvyšuje priemer DREAD faktorov). Pri faktorizácii aspektov v tejto práci je použité rovnomerné rozloženie hodnôt medzi 0 (bez vplyvu) a 9 (maximálny

vplyv). V praxi je toto rozloženie vhodné pre organizáciu, ktorá má kvalitne klasifikované a tagované dátá. Nerovnomerne rozmiestnenie hodnôt je vhodné pre organizáciu, ktorá sice používa 4 kategórie klasifikácie dát, ale rozdiel medzi napr. Internal-Public a Confidential-Strictly confidential nie je jednoznačný. V nasledujúcej tabuľke č.3 je uvedený príklad na rovnomerne a nerovnomerné rozloženie faktorov pre aspeky.

Tabuľka 3 Prieklady rozloženia hodnôt pri faktorizácii

Faktor Klasifikácia dát (dataclass)	Rovnomerne rozložené faktory	Nerovnomerne rozložené faktory
Public	1	1
Internal	4	3
Confidential	6	7
Strictly confidential	9	9

Zoznam všetkých aspektov a pridelených faktorov je uvedený v prílohe D.

4.2 ZÁPIS HODNOTY ASPEKTOV POMOCOU DREAD FAKTOROV

Zápis hodnoty aspektu pomocou DREAD faktorov je vlastný postup a je dôležitý pre pochopenie algoritmu na výpočet optimálnej formy autentifikácie. Je preto rozpísaný tejto kapitole detailnejšie.

Porovnávaním rôznych hodnôt aspektov a vyhodnocovaním rizík bolo zistené, že merané aspekty nemajú vplyv na všetky DREAD faktory. Napríklad faktor dataclass má vplyv len na DREAD faktory M (Motive), LC (Loss of confidentiality), FD (Financial Damage), RD (Reputation Damage), NC (Non-compliance), PV (Privacy Violation). Závislosť všetkých pozorovaných aspektov a DREAD faktorov je uvedená v nasledujúcej tabuľke č.4 .

Tabuľka 4 Matica závislostí aspektov a DREAD faktorov

Aspekty	Likelihood factors								Impact factors							
	Threat Agent Factors (TAF)				Vulnerability Factors (VF)				Technical Impact Factors (TIF)				Business Impact Factors (BIF)			
	S L	M	O	S	E D	E	A	ID E	L C	L I	LA V	LA C	F D	R D	N C	P V
DataClass		Y							Y	Y			Y	Y	Y	Y
Architectur e	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

NetLocation	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Signing	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y			Y	Y	Y	Y	Y
Encryption	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y			Y	Y	Y	Y	Y
UserPriv	Y	Y	Y	Y	Y	Y	Y		Y				Y	Y	Y	Y	Y
AuthFact	Y	Y	Y	Y		Y	Y	Y			Y	Y	Y	Y	Y	Y	Y

Z tabuľky vyplýva, že hodnoty DREAD faktorov sa pri posudzovaní hrozby menia v závislosti od pozorovaného aspektu. Napríklad klasifikácia dát (dataclass) vplýva len na 7 faktorov, ale architektúra (arch) vplýva na všetkých 16 DREAD faktorov.

V ďalšom kroku bol meraný vplyv hodnoty aspektu na celkové riziko. Napríklad pri spracovaní dát typu Confidential je dopad na celkové riziko vyšší ako pri spracovaní dát typu Internal. Vyhodnocovaním DREAD faktorov pre rôzne hodnoty rovnakého aspektu vzniklo vyjadrenie aspektu pomocou DREAD faktorov vo forme vektora.

Príklad: Aspekt dataclass s hodnotou Public(1), Internal(4), Confidential(6) a Strictly confidential(9) boli zapísané pomocou DREAD faktorov nasledovne:

$$\begin{aligned} \text{dataclass}(1) &= [0,1,0,0,0,0,0,2,0,0,0,1,1,2,3] \\ \text{dataclass}(4) &= [0,4,0,0,0,0,0,6,0,0,0,7,4,5,5] \\ \text{dataclass}(6) &= [0,9,0,0,0,0,0,6,0,0,0,7,9,7,7] \\ \text{dataclass}(9) &= [0,9,0,0,0,0,0,9,0,0,0,9,9,7,9], \end{aligned}$$

DREAD = 0 znamená, že aspect dataclass nemá vplyv na DREAD factor (viď tabuľka č.4).

Pre modelovanie hrozieb počas autentizácie bolo ešte potrebné vytvoriť zoznam autentifikačných protokolov. Zoznam bol získaný v analytickej časti tejto práce. Zoznam je možné priebežne dopĺňať, prípadne modifikovať existujúce protokoly v závislosti od implementácie v konkrétnej spoločnosti. V praktickej časti tejto práce sú použité protokoly: Mutual TLS, SAML, OAuth2, OIDC, Kerberos/SPNEGO, NTLM, Digest access authentication, LDAP, RADIUS, OTP, CAPTCHA, APIKEY, Basic access authentication, ClearText authentication, Cookies authentication.

4.3 WORST-CASE SCENARIO

Pre vybrané autentizačné protokoly boli v analytickej časti tejto práce pripravené risk analýzy, ktorých cieľom je vyjadriť mieru rizika protokolu pri najhoršom rizikovom scenári. Bol na to použitý koncept riadenia rizík, pri ktorom plánovač odhaduje najhoršiu

možnú pravdepodobnosť a dopad a tým aj najvyššiu možnú mieru rizika tzv. Worst-case scenario (YOE, 2011). Aplikovaním tejto metodiky bol získaný model autentizačného protokolu, ktorý neobsahuje žiadne voliteľné funkcionality ale je zachovaná jeho funkčnosť. Tento postup je potrebné urobiť pri každom pridaní nového autentizačného protokolu a preto je detailnejšie rozpisany na nasledujúcim príklade.

Príklad: HTTP basic autentizáciu (overovanie používateľa menom a heslom) je možné technicky prevádzkovať aj vo veľmi rizikovej implementácii, v ktorej sa spracovávajú dátá klasifikované ako Strictly confidential (dataclass(9)), architektúra aplikácie umožňuje proxy mód s inšpekciami protokolu (arch(7)), aplikačný server je voľne dostupný z internetu (netloc(9)), komunikácia nie je šifrovaná (enc(9)), používateľ má právo administrátora (userpriv(9)) a podobne. Tento scenár je v praxi málo pravdepodobný, ale aplikovanie tohto Worst-case scenario umožnilo zmerať rozdiel v mieri rizika po pridaní aspektu. Príklad „zoštíhleného“ modelu autentizácie je možné zapísat aj vo forme tabuľky č.5. Je v nej vyjadrená hodnota aspektov pre HTTP basic autentizáciu, hodnota DREAD faktorov v uvažovanom modeli hrozieb a vypočítaná pravdepodobnosť, dopad a celkové riziko. Označenie TMP0 je skratkou Threat modeling process 0, čiže modelovanie hrozieb pre najrizikovejší scenár. Hodnoty TMP0 pre všetky autentizačné protokoly sú uvedené v prílohe G a boli použité aj v praktickej časti práce.

Tabuľka 5 Priklad formy zápisu výstupu analýzy autentizačného protokolu

TMP0 pre Basic access authentication	
Merané aspekty	[9,7,9,5,9,8,9]
Namerané DREAD faktory	[9, 9, 7, 9, 9, 9, 9, 8, 9, 7, 7, 7, 7, 9, 7, 7]
Namerané výsledky risk analýzy:	
Pravdepodobnosť	HIGH 8,625
Dopad	HIGH 7,500
Miera rizika	CRITICAL

4.4 VYJADRENIE ZÁVISLOSTI AUTENTIZAČNÉHO PROTOKOLU NA ASPEKTOCH

Ked'že pomocou DREAD faktorov je možné vyjadriť rizikovosť aspektov aj autentizačných protokolov vo Worst-case scenári (TMP0), je možné vyjadriť aj závislosť autentizačných protokolov na aspektoch. Túto závislosť môžeme zapísat všeobecne v nasledujúcim tvare:

$$\text{Authprot}(\text{dataclass}, \text{arch}, \text{netloc}, \text{authfact}, \text{sign}, \text{enc}, \text{userpriv})$$

=

$$[SL, M, O, S, ED, EE, A, IDE, LC, LI, LAV, LAC, FD, RD, NC, PV]$$

Zo vzťahu vyplýva, že ten istý autentizačný protokol bude mať pri zmenenej hodnote aspektu zmenenú hodnotu DREAD vektora, čím sa zmení aj celkové riziko.

Tento zápis je pochopiteľnejší na príklade pre HTTP Basic autentizáciu.

Príklad: $\text{HTTPBasic}(9,7,5,5,9,8,9) = [5, 9, 7, 5, 7, 5, 6, 8, 7, 7, 5, 7, 7, 5, 5, 5]$,

čo je vlastne skrátený zápis pre dataclass(9)= Strictly confidential, architect(7)= 2-tier architecture, netloc(5)= 3 inspection nodes, authfact(5)= 1-factor authentication, ... atď.

Zmenou formy autentizácie z 1-faktorovej na 3-faktorovú (hodnota authfact(5) sa zmení na authfact(2),) získame nový DREAD vektor:

$\text{HTTPBasic}(9,7,5,2,9,8,9) = [3, 4, 4, 2, 7, 3, 4, 3, 6, 5, 5, 7, 3, 4, 2, 3]$,

ktorý bude obsahovať minimálne hodnoty DREAD vektorov pre authfact(3) a authfact(5).

Ďalším pozorovaním a vyhodnocovaním miery rizika bolo zistené, že zmenou hodnoty niekoľkých aspektov súčasne je hodnota výsledného DREAD vektora daná minimom hodnôt z počítaných DREAD faktorov. Hodnota DREAD faktorov autentizačného protokolu sa teda rovná minimu hodnôt vektorov všetkých aplikovaných aspektov a tento vzťah bol doplnený do postupu výpočtu rizikovosti pri modelovaní hrozieb.

Príklad: Výpočet rozdielu miery rizika HTTP protokolu po aplikovaní šifrovania.

V postupe najprv vypočítame TMP0 pre nešifrovaný HTTP protokol a DREAD vektry pre TLS šifrovanie (enc(4)). Potom vypočítame minimum hodnôt oboch vektorov.

$\text{BasicAuth}(9,7,9,5,9,8,9) = \{[5, 9, 7, 5, 7, 5, 6, 8, 7, 7, 5, 7, 7, 5, 5, 5]\}$

$\text{enc}(4) = [5, 4, 4, 4, 7, 5, 4, 8, 6, 5, 0, 0, 7, 4, 5, 5]$.

$\text{MIN}\{\text{BasicAuth}(9,7,9,5,9,8,9), \text{enc}(4)\} = [5, 4, 4, 4, 7, 5, 4, 8, 6, 5, 5, 7, 7, 4, 5, 5]$.

Výsledkom je vektor, ktorý vyjadruje basic autentizáciu pomocou šifrovaného HTTPS protokolu s hodnotou $[5, 4, 4, 4, 7, 5, 4, 8, 6, 5, 5, 7, 7, 4, 5, 5]$.

Vypočítaním a porovnaním miery rizika pred a po aplikovaní aspektu a doplnením do tabuľky č. 6 bolo zistené, že po implementácii šifrovania do HTTP protokolu sa riziko autentizačného protokolu znížilo z HIGH na MEDIUM, pričom pravdepodobnosť sa znížila o -1,334 a dopad sa znížil o -0,500.

Tabuľka 6 Porovnanie rizík pred a po implementácii aspektu

	BasicAuth(TMP0)	ENC(TLS)	HTTPS
--	-----------------	----------	-------

Probability	HIGH 6,556	MEDIUM 5,222	MEDIUM 5,222
Impact	HIGH 6,000	MEDIUM 5,500	MEDIUM 5,500
Risk level	CRITICAL	MEDIUM	MEDIUM

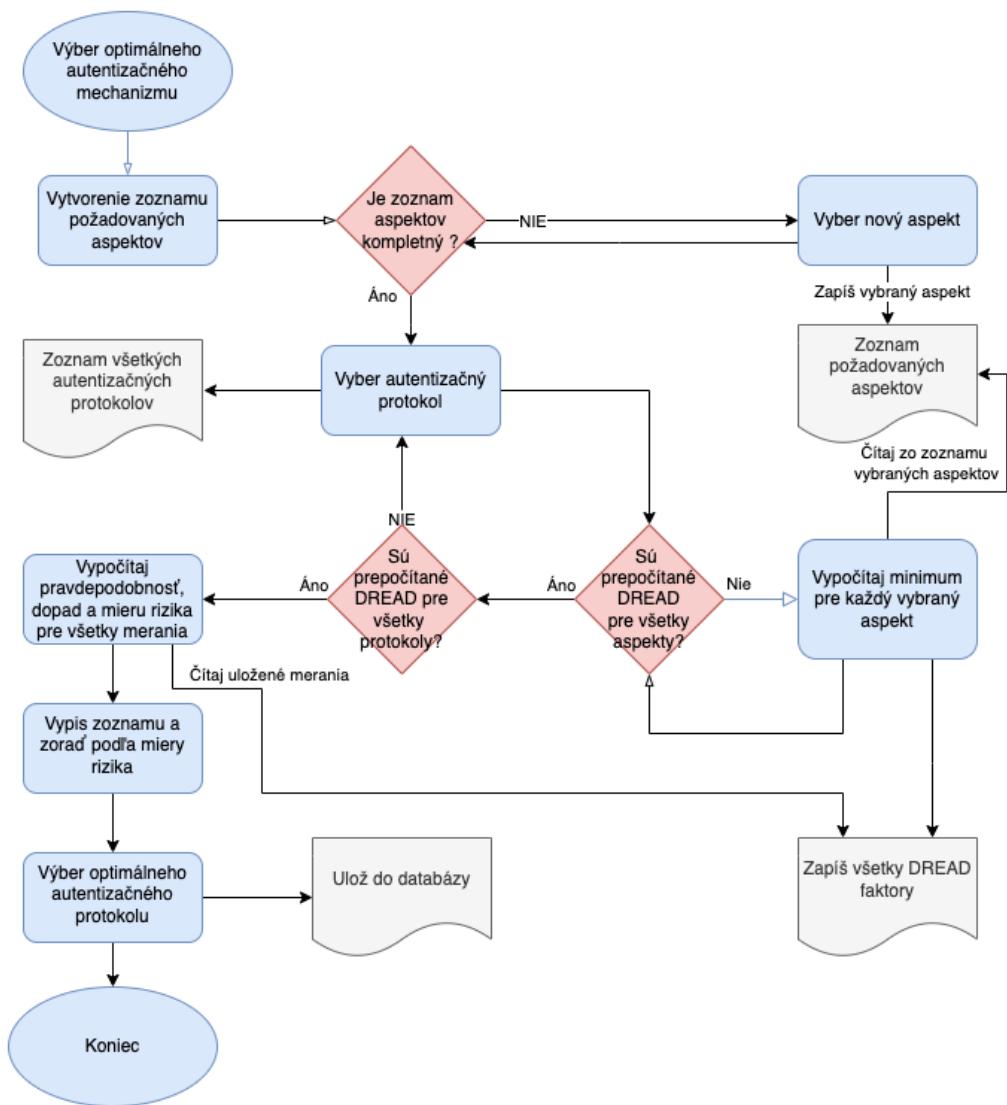
4.5 POPIS ALGORITMU NA VÝBER OPTIMÁLNEHO AUTENTIFIKAČNÉHO PROTOKOLU

Tento algoritmus vznikol počas písania práce na základe zadania. Vychádza z postupu v kapitole 4.4 . Algoritmus počíta minimum z hodnotených vektorov a jeho súčasťou je aj výpočet miery rizika. Po príprave TMP0 pre všetky autentifikačné protokoly a DREAD faktorov pre aspekty je výpočet optimálneho protokolu nasledovný: Používateľ aplikácie si zvolí aspekt s určitou hodnotou. Aplikácia v cykloch vypočítava minimum z vektora zvoleného aspektu (kapitola 3.2) a z TMP0 všetkých autentizačných protokolov (kapitola 3.4). Pre všetky výsledné vektory vypočíta mieru rizika a protokoly zoradí podľa miery rizika. Odporúčaný autentizačný protokol je ten, ktorý má najnižšiu mieru rizika. Proces výpočtu je zobrazený na obrázku č. 13.



Obrázok 13 Popis procesu výpočtu optimálnej autentizácie

Na obrázku č. 14 je zobrazený celý algoritmus výpočtu vo väčšom detaile. Zoznam aspektov, protokolov a ich hodnoty DREAD faktorov si algoritmus načíta z pripravených dát uložených v databáze. Funkcia minimum je v algoritme súčasťou oboch vnorených cyklov. Algoritmus je elementárny (obsahuje jednoduché kroky), konečný (končí pri splnení aj nesplnení podmienok) a má jasne definovaný výstup (odporúčaný protokol), ktorý si používateľ uloží do databázy.



Obrázok 14 Algoritmus výpočtu optimálneho autentizačného protokolu

V prílohe F sa nachádza zoznam autentizačných protokолов podľa pozorovaných aspektov, ktorý je použitý aj v aplikácii a používa sa na modelovanie optimálnej formy autentizácie. Keďže používame subjektívny hodnotenie rizikových faktorov, hodnoty jednotlivých faktorov v prílohe F si môže používateľ upraviť podľa aktuálnych podmienok alebo potrieb tak, aby čo lepšie popisovali skutočný stav implementovaného protokolu alebo hodnoty aspektu v jeho podmienkach.

4.6 PRÍPRAVY VSTUPNÝCH DÁT PRE APLIKÁCIU

Na záver tejto kapitoly je zhrnutý postup prípravy dát, ktoré potrebuje aplikácia pre svoje fungovanie. Od kvality týchto dát závisí aj kvalita výstupov, preto je potrebné tieto dátá pripraviť veľmi dôsledne a mali by opisovať reálny stav implementácie autentizačných protokolov. Postup je nasledovný:

1. Pripraviť zoznam autentizačných protokolov
2. Pripraviť TMP(0) pre všetky autentizačné protokoly
3. Pripraviť zoznam aspektov
4. Pripraviť DREAD faktory pre všetky aspekty
5. TMP0 a DREAD faktory pre aspekty vložiť do databázy
6. Aplikácia je pripravená na modelovanie

5 APLIKÁCIA NA MODELOVANIE AUTENTIZAČNÝCH PROTOKOLOV

Jedným z cieľov tejto práce bolo pripraviť aplikáciu, ktorá umožňuje modelovanie autentizačných mechanizmov a návrh optimálnej autentizácie.

5.1 POUŽITÉ TECHNOLÓGIE

5.1.1 Bootstrap

Pre realizáciu na strane používateľa je použitý framework Bootstrap 5 Framework obsahuje hotové knižnice CSS, ktoré výrazne uľahčujú vytváranie webových stránok a iných informácií zobraziteľných vo webovom prehliadači vo vyladenom štýle. Bootstrap bol zvolený pre jednoduchosť, prehľadnosť zdrojového kódu, minimálne rozdiely pri zobrazení v rôznych prehliadačoch a hlavne pre jeho rozšírenosť.

Pre účel tejto práce bola vybraná voľne dostupná šablóna distribuovaná pod MIT licenciou s názvom SB Admin¹³. Medzi základné prednosti tejto šablóny patrí:

- Rozloženie stránky v mriežkovou systéme bootstrap-u založenom na FLEXBOX
- Prepínateľné bočné menu
- Interaktívne tabuľky zobrazované pluginom dataTables
- Predpripravené stránky Login, Registration, Forgot Password, 404, Blank starter.

5.1.2 Javascript

Javascript umožňuje meniť obsah webovej stránky priamo v prehliadači používateľa, preto bola táto technológia vybraná na tvorbu dynamického menu, kontajnerov a vizualizáciu. Javascript je v práci použitý na dynamické zobrazovanie výsledkov risk analýzy a počítanie miery rizika, čo umožňuje používateľovi operatívne meniť DREAD parametre v procese modelovania hrozieb s možnosťou zobrazovania grafu v reálnom čase. V práci bol prepoužitý voľne šíriteľný kód aplikácie OWASP-Calculator (OLMEDO, 2022) a bol upravený do dizajnu aplikácie pomocou spoločných CSS štýlov.

¹³ <https://startbootstrap.com/template/sb-admin>

5.1.3 PHP

Pre prácu s dátami na backende bol zvolený jazyk PHP. Je voľne dostupný, ľahko prevádzkovateľný na väčšine webových serverov vo webhostingových centrách a umožňuje rýchle riešenie pre vývoj backendu webových aplikácií. Dodržuje jednoduchosť a čitateľnosť kódu a prácu s databázou. Pre použitie aplikácie v tejto práci nebolo potrebné používať žiadny PHP framework a je použité PHP vo verzii 7.2.34. Pre prácu v PHP bolo zvolené IDE PHPStorm vo verzii 2021.3 .

5.1.4 Apache

Pre účely tejto aplikácie je vhodný akýkoľvek webový server, aplikácia nemá špeciálne požiadavky na webserver. Preto bol zvolený Apache, webový server s otvoreným kódom. V práci je použitá verzia Apache/2.4.46 (Unix), OpenSSL/1.1.1i, PHP/7.2.34, mod_perl/2.0.11, Perl/v5.32.0.

5.1.5 MySQL

MySQL je voľne použiteľný a najpoužívanejší SQL relačný databázový server. Je podporovaný na viacerých platformách a implementovateľný vo viacerých programovacích jazykoch. V tejto práci je použitý MySQL server vo verzii 10.4.17-MariaDB a je manažovaný pomocou webovej konzoly phpMyAdmin verzia 5.0.4 . MySQL databáza bola použitá z inštalácie aplikácie XAMPP verzie 7.2.34 pre Mac OS Monterey 12.2.1 .

5.1.6 XAMPP

Aplikácia bola vyvíjaná a testovaná v prostredí XAMPP vo verzii 7.2.34 pre Mac OS Monterey 12.2.1. XAMPP je open-source platforma s Apache web serverom, s MariaDB databázou a podporou pre PHP a je použiteľná na väčšine podporovaných operačných systémoch.

5.2 PRÍPADY POUŽITIA

Diagram prípadov použitia popisuje hlavné funkcie aplikácie. V aplikácii sú vytvorené 4 aplikačné role, medzi ktorými je nastavené dedenie oprávnení.

Neprihlásený používateľ má k dispozícii len prihlásovací formulár a nemá oprávnenia na používanie aplikácie.

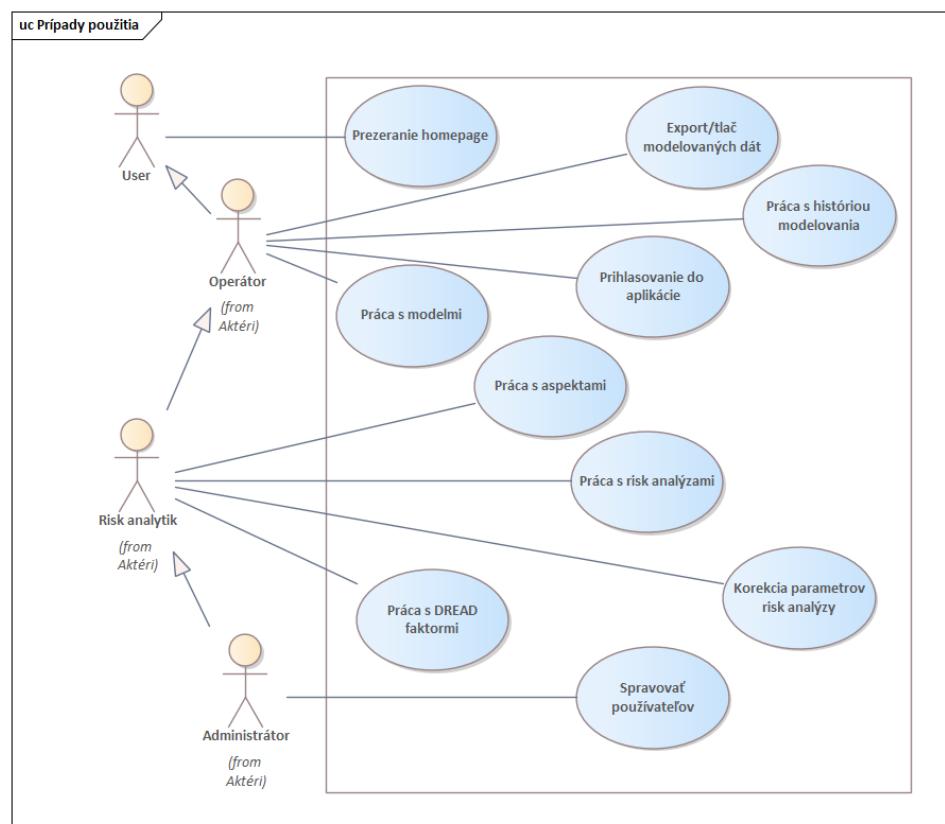
Používateľ s rolou user má po úspešnom prihlásení možnosť vidieť domovskú stránku (homepage), na ktorej sú zobrazené len všeobecné informácie s popisom aplikácie. User

nemá dostupné navigačné menu aplikácie, ani iné stránky na modelovanie alebo editovanie. Na homepage sú zobrazené štatistiky o počte uložených aspektov, modelov a hrozieb, ale nie je možné získať detail štatistik.

Používateľ s rolou operátor má po prihlásení k dispozícii domovskú stránku a záložku modely. V modeloch si operátor môže namodelovať autentifikačný mechanizmus podľa vybraných aspektov a hrozieb. Aplikáciou navrhnutý model si používateľ môže uložiť do databázy a v prípade potreby ho editovať. V rámci svojej role si operátor nemôže meniť hodnoty pripravených hrozieb, upravovať výsledky risk analýz ani editovať aspekty.

Používateľ s rolou risk analytik má k dispozícii záložky homepage, modely, aspekty a hrozby. V záložke aspekty môže pridať, editovať a mazať aspekty. V záložke hrozby môže pridať, editovať a mazať hrozby a upravovať DREAD faktory. Modelovaním DREAD faktorov môže ovplyvňovať celkovú mieru rizika podľa aktuálnych potrieb spoločnosti.

Používateľ s rolou administrátor má k dispozícii prístup k všetkým spomínaným záložkám. Oproti ostatným rolám má navyše prístup aj k záložke Users, v ktorej môže pridať a mazať používateľov, pridelovať aplikačné role a resetovať používateľom heslá.

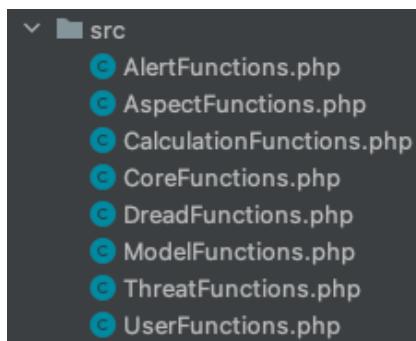


Obrázok 15 Obrázok s prípadmi použitia

5.3 POPIS A ŠTRUKTÚRA APLIKÁCIE

Základom aplikácie je kontroler umiestnený v súbore `index.php`, ktorý obsahuje podmienky, ktoré umožňujú načítať stránku s formulárom podľa informácie v URL v tvare napríklad `index.php?page=models`.

Po načítaní stránky s formulárom, sa používateľovi pomocou cyklu s podmienkou zobrazí výpis z databázy vložený do tabuľky v HTML. Každú z položiek výpisu v tabuľke môže používateľ editovať alebo zmazat. Všetky CRUD operácie (create, read, update, delete) sú dostupné vo forme PHP funkcií, ktoré si volá každá stránka (aspekty, hrozby, modely) pomocou HTTP POST metódy kliknutím na tlačidlo formulára. Každá CRUD operácia je volaná ako samostatná funkcia umiestnená v súbore `NazovModeluFunction.php`, ktoré sú uložené v adresári `src/`.



Obrázok 16 Zoznam súborov s funkciami pre CRUD operácie

Každý z modulov aplikácie má vlastný adresár, ktorý obsahuje súbory s formulármami na pridanie záznamu (napr. `addModel.php`), editáciu záznamu (napr. `editModel.php`), zmazanie záznamu (napr. `deleteModel.php`).

Pre volanie databázy je vytvorená trieda uložená v súbore `core.php`, ktorá obsahuje definíciu pripojenia do databázy pomocou funkcie nainštalovanéj pomocou mysqli drivera¹⁴.

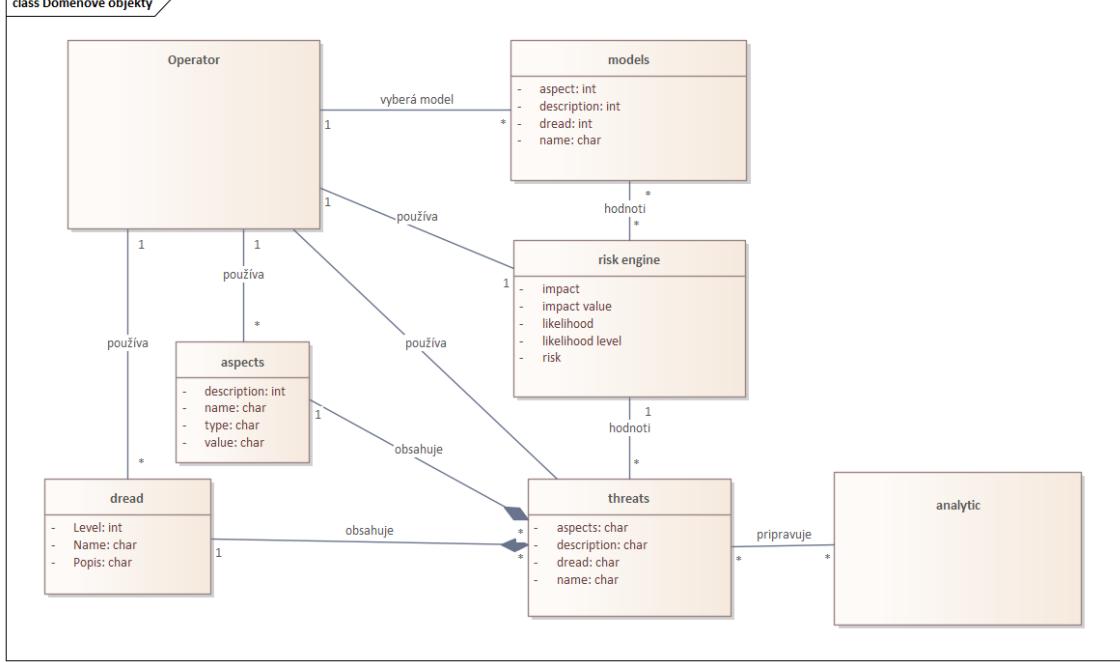
Funkcie na výpočet pravdepodobnosti, dopadu a rizika sú umiestnené v súbore `CalculationFuncions.php`. Hodnoty pre mieru rizika (LOW, MEDIUM, HIGH, CRITICAL) sú definované pomocou konštánt.

Funkcie pre prácu s používateľmi sú uložené v `UserFunctions.php`. Je tam niekoľko funkcií:

¹⁴ <https://www.php.net/manual/en/mysqli.construct.php>

`findUserAnd GetUser($email)` je funkcia na identifikáciu, či používateľ existuje,
`login($email, $password)` je funkcia na validáciu hesla používateľa pri autentifikácii s použitím hašovacej funkcie bcrypt,
`displayUserRoleInfo()` je funkcia na identifikáciu aplikačnej role používateľa.
Hesla používateľov sú uložené v databáze zahešované, nie je možné ich zobrazíť v čitateľnej forme a pri autentizácii je porovnávaná len hash hesla používateľa.
Session management je riadený serverom. Používateľ získa session ID pri prvom načítaní `index.php` a po odhlásení je session na serveri zmazaná.

Vzťahy medzi modulmi a používateľmi sú zobrazené na obrázku č. 17.



Obrázok 17 Doménové objekty a ich vzťahy

5.4 DATABÁZA

Databáza slúži na ukladanie dát pre modelovanie a zároveň slúži aj na zobrazovanie obsahu pre jednotlivé stránky aplikácie. Aplikácia nepotrebuje špecifický typ databázy, lebo nie je určená pre špecifický typ OS, preto používa MySQL databázu. Detailný zoznam tabuľiek databázy sa nachádza v prílohe H.

Tabuľka 7 Zoznam a popis jednotlivých tabuľiek databázy

Názov tabuľky	Popis
Aspects	Zoznam a popis aspektov
Dread	Zoznam a popis DREAD faktorov

Dshb_menu	Tabuľka položiek pre navigačné menu
Models	Zoznam, parametre a popis modelov
Threats	Zoznam, parametre a popis hrozieb
Users	Zoznam používateľov, emaily a heslá
User_roles	Zoznam aplikáčných rolí

5.5 TESTOVANIE APLIKÁCIE

Testovanie aplikácie prebiehalo priamo počas implementácie a v tomto čase bolo odhalených aj najviac chýb. Keďže aplikácia pracovala s dátami, ktoré boli predpripravené v aplikácii MS Excel, výsledky výpočtov mohli byť validované počas každej operácie. Pri identifikovaní chýb s výpočtom bola väčšina chýb spojených s počítaním minima v algoritme na backende, po zavedení podmienok na vstup sa chyby neprejavili. Chyby spojené so zobrazovaním, vkladaním, mazaním a úpravou dát vo formulároch boli diagnostikované sa odstránené priamo v developerskom IDE.

5.6 VÝHODY A NEVÝHODY IMPLEMENTÁCIE

Medzi výhody zvolených technológií patrí jednoduchosť riešenia postaveného na klient-server architektúre, ktorá je výhodná pre dizajnovovo nenáročné formulárové aplikácie. Jednoduchá implementácia v XAMPP prostredí alebo na zdieľaných webhostingových serveroch je oproti iným technológiám (Java, Python) nákladovo aj prevádzkovo veľmi nenáročné riešenie. Široká podpora použitých technológií na strane developerov aj na strane komunit, ktoré technológie podporujú, umožňuje jednoduchší prechod na novšie verzie. Responzívny dizajn front-end aplikácie je široko podporovaný od desktopových prehliadačov po tablety.

Medzi nevýhody navrhovaného riešenia patrí nutnosť manuálnej prípravy vstupných dát (modelov hrozieb) a manuálne určenie DREAD faktorov odborne zdaným personálom (risk analytikom).

Ďalším možným rozvojom aplikácie je v prvom rade integrácia na verejné databázy existujúci hrozieb a zraniteľnosti, ktorá by umožnila pracovať so Zero-day zraniteľnosťami. Zároveň by používateľa upozornila na nepodporované alebo zastaralé protokoly a pomohla by presnejšie identifikovať verejne známe hrozby a odhadnúť mieru rizika. Z pohľadu použitého risk frameworku by aplikáciu pomohlo pridanie ďalších risk frameworkov (NIST, ENISA a pod.), čo by pravdepodobne uvítali väčšie spoločnosti, prípadne pobočky zahraničných spoločností po ktorých legislatíva vyžaduje spomínané

risk frameworky. Z prevádzkových funkcií by aplikácia mohla podporovať integráciu na interných identity providerov pomocou Single-Sign-On, integráciu na interné auditné systémy pre účely logovania prístupov a možnosť šifrovania dát v databáze kvôli citlivosti spracovávaných dát.

ZÁVER

Cieľom práce bolo identifikovať, analyzovať a klasifikovať bezpečnostné aspekty, ktoré vplývajú na digitálnu identitu. Klasifikáciu bolo potrebné navrhnúť tak, aby ju bolo možné použiť pri hodnotení bezpečnosti a tým zlepšiť návrh na ochranu digitálnej identity. Výstupom z práce mala byť aplikácia, pomocou ktorej si používateľ vytvorí model autentifikácie na základe zvolených aspektov.

V práci sa podarilo opísť stav digitálnej identity na Slovensku aj v zahraničí, nájsť nové výzvy a technológie pre ďalší rozvoj v oblasti ochrany identity a nájsť ich využitie pre rozvoj služieb pre zriaďovateľov akými sú štát alebo súkromné sektory, ktoré sú pod dohľadom regulátorov.

Práca pomohla nájsť postupy na identifikáciu aspektov pomocou bezpečnostných analýz, ich kategorizáciu a klasifikáciu určením hodnoty a váhy aspektu, čo dáva spoločnostiam možnosť prispôsobiť význam aspektov svojim potrebám alebo sektoru pôsobenia. Vďaka analytickej časti práce vznikli postupy na prípravu editovateľných dát vo forme rizikových analýz pre najpoužívanejšie autentizačné protokoly a preto je aplikácia okamžiteľne použiteľná v akejkoľvek spoločnosti, ktorej záleží na bezpečnosti a dizajne autentifikácie.

V praktickej časti sa podarilo navrhnúť, pripraviť a implementovať funkčnú webovú aplikáciu, ktorá umožní používateľovi vybrať požadované aspekty a navrhnuť optimálny autentifikačný protokol. Aplikácia je určená hlavne pre risk analytikov alebo IT architektov, ktorí potrebujú navrhnúť optimálnu autentifikáciu rýchlo a efektívne z predpripravených dát. Je to komplexné databázové riešenie s vizualizáciou rizika, čo umožňuje rýchlejšie rozhodovanie pri výbere riešenia pre autentizáciu a umožňuje uloženie výsledku pre neskoršiu editáciu. Aplikáciu je možné použiť aj na prípravu podkladov na akceptáciu rizika pre rizikové komisie alebo na vyhodnocovanie bezpečnosti integrácie systémov v informačných technológiách.

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

- CONKLIN, L., DRAKE, V. OWASP THREAT MODELING PROCESS. [online] 2022. [cit. 2022-04-01]. Dostupné na internete: < https://owasp.org/www-community/Threat_Modeling_Process >.
- INTERNET ENGINEERING TASK FORCE (IETF). RFC 2617: Intellectual Property Rights in IETF Technology [online]. Edited by J. Franks. June 1999 [cit. 2022-04-01]. Dostupné na internete: < <https://datatracker.ietf.org/doc/html/rfc2617> >.
- INTERNET ENGINEERING TASK FORCE (IETF). RFC 2865: Intellectual Property Rights in IETF Technology [online]. Edited Rigney, et al. June 2000 [cit. 2022-04-01]. Dostupné na internete: < <https://datatracker.ietf.org/doc/html/rfc2865> >.
- INTERNET ENGINEERING TASK FORCE (IETF). RFC 4120: Intellectual Property Rights in IETF Technology [online]. Edited Neuman, et al. July 2005 [cit. 2022-04-01]. Dostupné na internete: < <https://datatracker.ietf.org/doc/html/rfc4120> >.
- INTERNET ENGINEERING TASK FORCE (IETF). RFC 4511: Intellectual Property Rights in IETF Technology [online]. Edited by J. Sermersheim, Ed. June 2006 [cit. 2022-04-01]. Dostupné na internete: < <https://datatracker.ietf.org/doc/html/rfc4511> >.
- INTERNET ENGINEERING TASK FORCE (IETF). RFC 6749: Intellectual Property Rights in IETF Technology [online]. Edited by D. Hardt, Ed.. October 2012 [cit. 2022-04-01]. Dostupné na internete: < <https://datatracker.ietf.org/doc/html/rfc6749#section-4.2> >.
- INTERNET ENGINEERING TASK FORCE (IETF). RFC 7519: Intellectual Property Rights in IETF Technology [online]. Edited by JONES, M.. Máj 2015 [cit. 2022-04-01]. Dostupné na internete: < <https://datatracker.ietf.org/doc/html/rfc7519> >.
- ISO/IEC 24760-1:2019(E). A framework for identity management - Part 1: Terminology and concepts. ISO. 2019-05.
- KEMP, J. et al. Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS SSTC. [online]. March 2005. [cit. 2022-04-01]. Dostupné na internete: < <http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf> >.

KIENNERT, CH. BOUZEFRANE, S. THONIEL, P. WAELBROECK, P. 2015. 3 – Authentication Systems. [online] Digital Identity Management. [cit. 2022-04-13]. Dostupné na internete <<https://www.sciencedirect.com/science/article/pii/B9781785480041500031>>.

LAURENT,M. DENOUEL, J. LEVALLOIS-BARTH,C. WAELBROECK, P. 2015. Digital Identity. [online] Digital Identity Management. [cit. 2022-04-12]. Dostupné na internete <https://www.sciencedirect.com/science/article/pii/B9781785480041500018?dgcid=raven_sd_recommender_email>.

MOLOTOKIENÉ, E. 2020. The transformation of narrative identity into digital identity: challenges and perspectives. Colloquium 2(38)/2020. 124-125 s. ISSN 2081-3813, e-ISSN 2658-0365.

OLMEDO, J., OWASP-Calculator. [online] 2022. [cit. 2022-04-10]. Dostupné na internete: <<https://github.com/JavierOlmedo/OWASP-Calculator>>.

ORACLE CORPORATION, Mutual authentication. [online]. 2010. [cit. 2011-02-14]. Dostupné na internete:<<https://docs.oracle.com/cd/E19798-01/821-1841/bncbt/index.html>>.

SALLERAS,X., ROVIRA,S., DAZA,V. 2022. FORT: Right-Proving and Attribute-Blinding Self-Sovereign Authentication. [online] Mathematics. [cit. 2022-04-03]. ISSN 2227-7390. Dostupné na internete <<https://www.mdpi.com/2227-7390/10/4/617>>.

SULE, M. et al. 2021. Cybersecurity through the lens of Digital Identity and Data Protection: Issues and Trends. [online] Technology in Society 67 (2021) 101734. [cit. 2022-04-03]. Dostupné na internete <<https://www.sciencedirect.com/science/article/pii/S0160791X21002098>>.

SULLIVAN, C. 2016. Digital citizenship and the right to digital identity under international law. [online] Computer Law & Security Review. Volume 32, Issue 3, s. 474-481 (2016). [cit. 2022-04-03]. Dostupné na internete <<https://www.sciencedirect.com/science/article/pii/S0267364916300292>>.

SULLIVAN, C. 2018. Digital identity – From emergent legal concept to new reality. [online] Computer Law & Security Review. Volume 34, Issue 4, s. 723-731

- (2016). [cit. 2022-04-03]. Dostupné na internete <<https://www.sciencedirect.com/science/article/pii/S0267364918302024>>.
- SCHLATT, V., SEDLMEIR, J., FEULNER,S., URBACH,N.. 2021. Designing a Framework for Digital KYC Processes Built on Blockchain-Based Self-Sovereign Identity. [online] Information & Management. [cit. 2022-04-03]. Dostupné na internete <<https://www.sciencedirect.com/science/article/pii/S0378720621001270>>.
- WILLIAMS, J., OWASP Risk Rating Methodology. [online] 2022. [cit. 2022-04-01]. Dostupné na internete: <https://owasp.org/www-community/OWASP_Risk_Rating_Methodology>.
- YOE, CH. 2011. Principles of Risk Analysis: Decision Making Under Uncertainty. CRC Press LLC, 2017. 429-430 s. ISBN 0429108117, 9780429108112.

ZOZNAM PRÍLOH

Príloha A – Klasifikácia faktorov pre pravdepodobnosť a dopad

Príloha B – Popis hrozieb a mitigácií pomocou techniky STRIDE

Príloha C – Vzor protokolu pre modelovanie hrozieb

Príloha D – Zoznam všetkých aspektov a hodnôt faktorov

Príloha E – Namerané hodnoty DREAD faktorov pre všetky hodnoty aspektov

Príloha F – Zoznam autentizačných protokolov podľa pozorovaných aspektov

Príloha G – Hodnoty DREAD faktorov pre TMP0

Príloha H – Ukážky obrazoviek aplikácie

Príloha I – Zoznam tabuliek v databáze

Príloha J – Zdrojové kódy aplikácie

PRÍLOHA A

Tabuľka 8 Klasifikácia faktorov pre pravdepodobnosť¹⁵

Likelihood factors							
Threat Agent Factors (TAF)				Vulnerability Factors (VF)			
Skills required (SL)	Motive (M)	Opportunity (O)	Population Size (S)	Easy of Discovery (ED)	Ease of Exploit (EE)	Awareness (A)	Intrusion Detection (IDE)
Not Applicable [0]	Not Applicable [0]	Full access or expensive resources required [0]	Not Applicable [0]	Not Applicable [0]	Not Applicable [0]	Not Applicable [0]	Not Applicable [0]
No technical skills [1]	Low or no reward [1]	Special access or resources required [4]	System Administrators [2]	Practically impossible [1]	Theoretical [1]	Unknown [1]	Active detection in application [1]
Some technical skills [3]	Possible reward [4]	Some access or resources required [7]	Intranet Users [4]	Difficult [3]	Difficult [3]	Hidden [4]	Logged and reviewed [3]
Advanced computer user [5]	High reward [9]	No access or resources required [9]	Partners [5]	Easy [7]	Easy [5]	Obvious [6]	Logged without review [8]
Network and programming skills [6]			Authenticated users [6]	Automated tools available [9]	Automated tools available [9]	Public knowledge [9]	Not logged [9]
Security penetration skills [9]			Anonymous Internet users [9]				

¹⁵ https://owasp.org/www-community/OWASP_Risk_Rating_Methodology

Tabuľka 9 Klasifikácia faktorov pre dopad¹⁶

Impact factors							
Technical Impact Factors (TIF)				Business Impact Factors (BIF)			
Loss of confidentiality (LC)	Loss of Integrity (LI)	Loss of Availability (LAV)	Loss of Accountability (LAC)	Financial damage (FD)	Reputation damage (RD)	Non-Compliance (NC)	Privacy violation (PV)
Not Applicable [0]	Not Applicable [0]	Not Applicable [0]	Not Applicable [0]	Not Applicable [0]	Not Applicable [0]	Not Applicable [0]	Not Applicable [0]
Minimal non-sensitive data disclosed [2]	Minimal slightly corrupt data [1]	Minimal secondary services interrupted [1]	Attack fully traceable to individual [1]	Damage costs less than to fix the issue [1]	Minimal damage [1]	Minor violation [2]	One individual [3]
Extensive non-sensitive data disclosed [6]	Minimal seriously corrupt data [3]	Minimal primary services interrupted [5]	Attack possibly traceable to individual [7]	Minor effect on annual profit [3]	Loss of major accounts [4]	Clear violation [5]	Hundreds of people [5]
Extensive critical data disclosed [7]	Extensive slightly corrupt data [5]	Extensive primary services interrupted [7]	Attack completely anonymous [9]	Significant effect on annual profit [7]	Loss of goodwill [5]	High profile violation [7]	Thousands of people [7]
All data disclosed [9]	Extensive seriously corrupt data [7]	All services completely lost [9]		Bankruptcy [9]	Brand damage [9]		Millions of people [9]

¹⁶ https://owasp.org/www-community/OWASP_Risk_Rating_Methodology

PRÍLOHA B

Tabuľka 10 Popis hrozieb a mitigácií pomocou techniky STRIDE¹⁷

Type	Description	Security Control
Spoofing	Threat action aimed at accessing and use of another user's credentials, such as username and password.	Authentication
Tampering	Threat action intending to maliciously change or modify persistent data, such as records in a database, and the alteration of data in transit between two computers over an open network, such as the Internet.	Integrity
Repudiation	Threat action aimed at performing prohibited operations in a system that lacks the ability to trace the operations.	Non-Repudiation
Information disclosure	Threat action intending to read a file that one was not granted access to, or to read data in transit.	Confidentiality
Denial of service	Threat action attempting to deny access to valid users, such as by making a web server temporarily unavailable or unusable.	Availability
Elevation of privilege	Threat action intending to gain privileged access to resources in order to gain unauthorized access to information or to compromise a system.	Authorization

¹⁷ https://owasp.org/www-community/Threat_Modeling_Process#stride

PRÍLOHA C

Tabuľka 11 Vzor protokolu pre modelovanie hrozieb

Dekompozícia aplikácie	Názov protokolu	
	Popis prípadu použitia	
	Vlastník dokumentu	
	Zúčastnení	
	Kontroloval	
	Klasifikácia dát	
	Architektúra	
	Sieťová lokalita	
	Autentizačné faktory	
	Podpisovanie	
Analýza hrozieb a rizík	Šifrovanie	
	Privilégia apl. účtu	
	STRIDE THREATS	Spoofing
		Tampering
		Repudiation
		Information disclosure
		Denial of service
		Elevation of privilege
	DREAD vektor	
	Pravdepodobnosť	
	Dopad	
	Rizikové skóre	
Mitigácie	Mitigačné techniky STRIDE	Spoofing
		Tampering
		Repudiation
		Information disclosure
		Denial of service
		Elevation of privilege

PRÍLOHA D

Tabuľka 12 Zoznam aspektov a pridelených faktorov

Aspects							
Dataclass (DC)	Architectur e (ARCH)	Network location (NL)	Authenticatio n factors (AF)	Signing (SIG)	Encryptio n (ENC)	User Privileges (UP)	Authenticatio n protocols (AP)
Not Applicable [0]	Not Applicable [0]	Not Applicable [0]	Not Applicable [0]	Not Applicable [0]	Not Applicable [0]	Anonymous web User [0]	RSA Key based (certificate) [2]
Public [1]	More than 3-tier [4]	No inspection [1]	Multi factor authentication [1]	RSA Asymmetric Signature [1]	RSA, ECC, GPG, PGP, Hybrid [2]	User with valid credentials [2]	SAML, OAuth2, OIDC [3]
Internal [4]	3-tier [5]	1 inspection node [3]	3 factor authentication [2]	HMAC symmetric signature [2]	AES, TLS [4]	DB server Administrator [4]	Kerberos ticket [4]
Confidential 1 [6]	2-tier [7]	2 inspection nodes [4]	2 factor authentication [3]	Event based token [5]	3DES [6]	Service provider Administrator [5]	NTLM [5]
Strictly confidential, unknown data classification [9]	1-tier, Unknown architecture [9]	3 inspection nodes [5]	1 factor authentication [5]	Time based token [6]	DES [7]	Service provider user process [7]	LDAP, RADIUS [6]
		4 inspection nodes [7]	User identification only [7]	Timestamp [7]	ENCODE [8]	Service provider root/administrator or process [9]	OTP, CAPTCHA [7]
		More than 4, Unknown Location [9]	No authentication [9]	HASH [8]	None, Unknown encryption [9]		APIKEY, BASE64, ClearText, Cookies [8]
				None, Unknown signing [9]			None, Unknown authentication mechanism [9]

PRÍLOHA E

Tabuľka 13 Namerané hodnoty DREAD faktorov pre všetky hodnoty aspektov

Aspects / Threats	Aspect Value	Likelihood factors								Impact factors							
		Threat Agent Factors (TAF)				Vulnerability Factors (VF)				Technical Impact Factors (TIF)				Business Impact Factors (BIF)			
		SL	M	O	S	ED	EE	A	IDE	LC	LI	LAV	LAC	FD	RD	NC	PV
		1,3,5,6,9	1,4,9	4,7,9	2,4,5,6,9	1,3,7,9	1,3,5,9	1,4,6,9	1,3,8,9	2,6,7,9	1,3,5,7	1,5,7,9	1,7,9,	1,3,7,9	1,4,5,9	2,5,7	3,5,7,9
dataclass (0,1,5,6,9)	1		1							2				1	1	2	3
dataclass (0,1,5,6,9)	4		4							6				7	4	5	5
dataclass (0,1,5,6,9)	6		9							6				7	9	7	7
dataclass (0,1,5,6,9)	9		9							9				9	9	7	9
architect(0,1,4,7,9)	1	1	1	4	2	1	1	1	1	2	1	1	1	1	1	2	3
architect(0,1,4,7,9)	4	5	4	4	4	7	5	4	8	6	5	5	7	7	4	5	5
architect(0,1,4,7,9)	7	9	9	7	9	7	9	9	8	7	7	7	7	9	7	7	
architect(0,1,4,7,9)	9	9	9	9	9	9	9	9	9	9	7	9	9	9	9	7	9
netloc(0,1,3,4,5,7,9,)	1	1	1	4	2	1	1	1	1	2	1	1	1	1	1	2	3
netloc(0,1,3,4,5,7,9,)	3	3	4	4	4	3	3	4	3	6	3	5	7	3	4	5	3
netloc(0,1,3,4,5,7,9,)	4	5	4	4	4	7	5	4	8	6	5	5	7	7	4	5	5
netloc(0,1,3,4,5,7,9,)	5	5	9	7	5	7	5	6	8	6	5	5	7	7	5	5	5
netloc(0,1,3,4,5,7,9,)	7	9	9	7	9	7	9	9	8	7	7	7	7	9	7	7	
netloc(0,1,3,4,5,7,9,)	9	9	9	9	9	9	9	9	9	9	7	9	9	9	9	7	9
sign(1,2,5,6,7,8,9)	1	1	1	4	2	1	1	1	1	2	1		1	1	1	2	3
sign(1,2,5,6,7,8,9)	2	3	4	4	2	3	3	4	3	2	3		7	3	4	2	3
sign(1,2,5,6,7,8,9)	5	5	9	7	5	7	5	6	8	6	5		7	7	5	5	5

sign(1,2,5,6,7,8,9)	6	6	9	7	6	7	9	6	8	6	7		7	7	9	7	7
sign(1,2,5,6,7,8,9)	7	9	9	7	9	7	9	9	8	7	7		7	7	9	7	7
sign(1,2,5,6,7,8,9)	8	9	9	9	9	9	9	9	8	9	7		9	9	9	7	9
sign(1,2,5,6,7,8,9)	9	9	9	9	9	9	9	9	9	9	7		9	9	9	7	9
enc(2,4,6,7,8,9)	2	3	4	4	2	3	3	4	3	2	3			3	4	2	3
enc(2,4,6,7,8,9)	4	5	4	4	4	7	5	4	8	6	5			7	4	5	5
enc(2,4,6,7,8,9)	6	6	9	7	6	7	9	6	8	6	7			7	9	7	7
enc(2,4,6,7,8,9)	7	9	9	7	9	7	9	9	8	7	7			7	9	7	7
enc(2,4,6,7,8,9)	8	9	9	9	9	9	9	9	8	9	7			9	9	7	9
enc(2,4,6,7,8,9)	9	9	9	9	9	9	9	9	9	9	7			9	9	7	9
up(2,4,5,7,9)	2	3	4	4	2	3	3	4		2				3	4	2	3
up(2,4,5,7,9)	4	5	4	4	4	7	5	4		6				7	4	5	5
up(2,4,5,7,9)	5	5	9	7	5	7	5	6		6				7	5	5	5
up(2,4,5,7,9)	7	9	9	7	9	7	9	9		7				7	9	7	7
up(2,4,5,7,9)	9	9	9	9	9	9	9	9		9				9	9	7	9

PRÍLOHA F

Tabuľka 14 Zoznam autentizačných protokолов podľa pozorovaných aspektov

Autentizačné protokoly	Aspekty	Likelihood factors								Impact factors							
		Threat Agent Factors (TAF)				Vulnerability Factors (VF)				Technical Impact Factors (TIF)				Business Impact Factors (BIF)			
		SL	M	O	S	ED	EE	A	IDE	LC	LI	LAV	LAC	FD	RD	NC	PV
	dc, arch, nl, af, sig, enc, up	1,3,5,6,9	1,4,9	4,7,9	2,4,5,6,9	1,3,7,9	1,3,5,9	1,4,6,9	1,3,8,9	2,6,7,9	1,3,5,7	1,5,7,9	1,7,9,	1,3,7,9	1,4,5,9	2,5,7	3,5,7,9
mTLS	9,7,3,3,9,2,2	3	4	4	2	3	3	4	3	2	3	5	7	3	4	2	3
SAML	9,5,4,5,1,9,2	1	1	4	2	1	1	1	1	2	1	5	1	1	1	2	3
OAuth2	9,5,4,5,1,9,2	1	1	4	2	1	1	1	1	2	1	5	1	1	1	2	3
OIDC	9,4,5,5,1,9,2	1	1	4	2	1	1	1	1	2	1	5	1	1	1	2	3
Kerberos/SPNEGO	9,4,4,5,6,4,5	5	4	4	4	7	5	4	8	6	5	5	7	7	4	5	5
NTLM	9,4,3,5,8,9,5	3	4	4	4	3	3	4	3	6	3	5	7	3	4	5	3
Digest access authentication	9,4,3,5,8,9,5	3	4	4	4	3	3	4	3	6	3	5	7	3	4	5	3
LDAP	9,7,3,5,8,9,7	3	4	4	4	3	3	4	3	6	3	5	7	3	4	5	3
RADIUS	9,7,3,5,7,9,7	3	4	4	4	3	3	4	3	6	3	5	7	3	4	5	3
OTP	9,5,4,7,9,9,9	5	4	4	4	7	5	4	8	6	5	5	7	7	4	5	5
CAPTCHA	9,7,4,7,5,9,9	5	4	4	4	7	5	4	8	6	5	5	7	7	4	5	5
APIKEY	9,7,9,7,9,9,9	9	9	7	9	7	9	9	8	7	7	7	7	7	9	7	7
HTTP Basic	9,7,9,5,9,8,9	5	9	7	5	7	5	6	8	6	5	7	7	7	5	5	5
ClearText	9,9,9,7,9,9,9	9	9	7	9	9	9	9	8	9	7	7	7	7	9	7	7
Cookies	9,4,3,5,9,9,9	3	4	4	4	3	3	4	3	6	3	5	7	3	4	5	3
Unknown	9,9,9,9,9,9,9	9	9	9	9	9	9	9	9	9	7	9	9	9	9	7	9
None	9,9,9,9,9,9,9	9	9	9	9	9	9	9	9	9	9	9	9	9	9	7	9

PRÍLOHA G

Tabuľka 15 Hodnoty TMP0 pre autentizačné protokoly použité pri výpočtoch

	dc, arch, nl, af, sig, enc, up	Likelihood factors					Impact factors								risklevel	liklevel	likvalu e	implevel	impvalu e			
		Threat Agent Factors (TAF)		Vulnerability Factors (VF)			Technical Impact Factors (TIF)				Business Impact Factors (BIF)											
		S L	M	O	S	E D	E E	A	ID E	LC	LI	LAV	LAC	FD	RD	NC	PV					
Certificate	9,7,3,3,9,2, 2	3	4	4	2	3	3	4	3	2	3	5	7	3	4	2	3	MEDIUM	MEDIUM	3,250	MEDIUM	3,625
SAML	9,5,4,5,1,9, 2	1	1	4	2	1	1	1	1	2	1	5	1	1	1	2	3	INFO	LOW	1,500	LOW	2,000
OAuth2	9,5,4,5,1,9, 2	1	1	4	2	1	1	1	1	2	1	5	1	1	1	2	3	INFO	LOW	1,500	LOW	2,000
OIDC	9,4,5,5,1,9, 2	1	1	4	2	1	1	1	1	2	1	5	1	1	1	2	3	INFO	LOW	1,500	LOW	2,000
Kerberos/SPNEGO	9,4,4,5,6,4, 5	5	4	4	4	7	5	4	8	6	5	5	7	7	4	5	5	MEDIUM	MEDIUM	5,125	MEDIUM	5,500
NTLM	9,4,3,5,8,9, 5	3	4	4	4	3	3	4	3	6	3	5	7	3	4	5	3	MEDIUM	MEDIUM	3,500	MEDIUM	4,500
Password based mTLS	9,4,3,5,8,9, 5	3	4	4	2	3	3	4	8	2	5	5	7	3	4	2	3	MEDIUM	MEDIUM	3,875	MEDIUM	3,875
Digest access authentication	9,4,3,5,8,9, 5	3	4	4	4	3	3	4	3	6	3	5	7	3	4	5	3	MEDIUM	MEDIUM	3,500	MEDIUM	4,500
LDAP	9,7,3,5,8,9, 7	3	4	4	4	3	3	4	3	6	3	5	7	3	4	5	3	MEDIUM	MEDIUM	3,500	MEDIUM	4,500
RADIUS	9,7,3,5,7,9, 7	3	4	4	4	3	3	4	3	6	3	5	7	3	4	5	3	MEDIUM	MEDIUM	3,500	MEDIUM	4,500

OTP	9,5,4,7,9,9, 9	5	4	4	4	7	5	4	8	6	5	5	7	7	4	5	5	MEDIUM	MEDIUM	5,125	MEDIUM	5,500
CAPTCHA	9,7,4,7,5,9, 9	5	4	4	4	7	5	4	8	6	5	5	7	7	4	5	5	MEDIUM	MEDIUM	5,125	MEDIUM	5,500
APIKEY	9,7,4,7,9,9, 9	5	4	4	4	7	5	4	8	6	5	5	7	7	4	5	5	MEDIUM	MEDIUM	5,125	MEDIUM	5,500
BASE64	9,7,9,5,9,8, 9	5	9	7	5	7	5	6	8	7	7	5	7	7	5	5	5	CRITICAL	HIGH	6,500	HIGH	6,000
ClearText	9,9,9,7,9,9, 9	9	9	7	9	9	9	9	8	9	7	7	7	7	9	7	7	CRITICAL	HIGH	8,625	HIGH	7,500
Cookies	9,4,3,5,9,9, 9	3	4	4	4	3	3	4	3	6	3	5	7	3	4	5	3	MEDIUM	MEDIUM	3,500	MEDIUM	4,500
Unknown	9,9,9,9,9,9, 9	9	9	9	9	9	9	9	9	9	7	9	9	9	9	7	9	CRITICAL	HIGH	9,000	HIGH	8,500
None	9,9,9,9,9,9, 9	9	9	9	9	9	9	9	9	9	7	9	9	9	9	7	9	CRITICAL	HIGH	9,000	HIGH	8,500

PRÍLOHA H

BADI

- Models
- Aspects
- Threats
- Users

Aspects

Data classification level

#	Name	Value	Description	New
1	Not Applicable [0]	0	Not Applicable [0]	
2	Public [1]	1	Public [1]	
3	Internal [4]	4	Internal [4]	
4	Confidential [6]	6	Confidential [6]	
5	Strictly confidential, unknown data classification [9]	9	Strictly confidential, unknown data classification [9]	

Architecture

#	Name	Value	Description	New
6	Not Applicable [0]	0	Not Applicable [0]	
7	More than 3-tier [4]	4	More than 3-tier [4]	
8	3-tier [5]	5	3-tier [5]	
9	2-tier [7]	7	2-tier [7]	
10	1-tier, Unknown architecture [9]	9	1-tier, Unknown architecture [9]	

Authentication protocol

#	Name	Value	Description	New
46	Certificate		Certificate	
47	SAML		SAML	
48	OAuth2		OAuth2	
49	OIDC		OIDC	
50	Kerberos/SPNEGO		Kerberos/SPNEGO	
51	NTLM		NTLM	
52	Digest access authentication		Digest access authentication	
53	LDAP		LDAP	
54	RADIUS		RADIUS	
55	OTP		OTP	
56	CAPTCHA		CAPTCHA	
57	APIKEY		APIKEY	
58	RASFRA		RASFRA	

Obrázok 18 Obrazovka s aspektami

BADI

Threats

Threat list

New

#	Name	Desc.	Auth	DataClass	Arch.	Location	Auth fact.	Sign	Enc	Priv.	Risk	Lik.	Lik. value	Imp.	Imp. value	Timestamp
50	tmp0	Worst case scenario	APIKEY	Strictly confidential, unknown data classification [9]	2-tier [7]	More than 4, Unknown Location [9]	User identification only [7]	None, Unknown signing [9]	None, Unknown encryption [9]	Service provider root/administrator process [9]	CRITICAL	HIGH	8.375	HIGH	7.25	2022-03-31 16:29:13
51	tmp0	Worst case scenario	BASE64	Strictly confidential, unknown data classification [9]	2-tier [7]	More than 4, Unknown Location [9]	1 factor authentication [5]	None, Unknown signing [9]	ENCODE [8]	Service provider root/administrator process [9]	CRITICAL	HIGH	6.5	HIGH	6	2022-03-31 16:27:54
3	dc(6)	Data classification (6)		Confidential [6]							LOW	LOW	1.125	MEDIUM	4.5	2022-03-31 16:06:16
2	dc(4)	Data classification (4)		Internal [4]							LOW	LOW	0.5	MEDIUM	3.375	2022-03-31 16:05:10
4	dc(9)	Data classification (9)		Strictly confidential, unknown data classification [9]							LOW	LOW	1.125	MEDIUM	5.375	2022-03-31 16:04:41
1	dc(1)	Data classification 0 (1)		Public [1]	0	0	0	0	0	0	INFO	LOW	0.125	LOW	1.125	2022-03-31 15:57:42
31	enc(7)	Encryption type (7)							DES [7]		HIGH	HIGH	8.375	MEDIUM	5.5	2022-03-24 17:18:04
30	enc(6)	Encryption type (6)							3DES [6]		HIGH	HIGH	7.25	MEDIUM	5.375	2022-03-23 17:18:04
29	enc(4)	Encryption type (4)							AES [4]		MEDIUM	MEDIUM	5.125	MEDIUM	4	2022-03-22 17:18:04
28	enc(2)	Encryption type (2)								RSA, ECC, GPG, PGP, Hybrid [2]	LOW	MEDIUM	3.25	LOW	2.125	2022-03-21 17:18:04
27	sign(9)	Signature (9)								None, Unknown signing [9]	CRITICAL	HIGH	9	HIGH	7.375	2022-03-20 17:18:04
26	sign(8)	Signature (8)							HASH [8]		CRITICAL	HIGH	8.875	HIGH	7.375	2022-03-19 17:18:04
25	sign(7)	Signature (7)							Timestamp [7]		CRITICAL	HIGH	8.375	HIGH	6.375	2022-03-18 17:18:04
24	sign(6)	Signature (6)							Time based token [6]		CRITICAL	HIGH	7.25	HIGH	6.25	2022-03-17 17:18:04
54	tmp0	Worst case scenario	Unknown	Strictly confidential, unknown data classification [9]	1-tier, Unknown architecture [9]	More than 4, Unknown Location [9]	No authentication [9]	None, Unknown signing [9]	None, Unknown encryption [9]	Service provider root/administrator process [9]	CRITICAL	HIGH	9	HIGH	8.5	2022-03-17 17:18:04

Obrázok 19 Obrazovka s hrozbami

BADI

Models Aspects Threats Users

Users

User list

#	Email	Status	Role	
1	user	Active	Standard user	
4	operator	Active	Operátor modelov	
21	ra	Active	Risk analytic	
3	admin	Active	Administrátor aplikácie	

Application role list

#	Role name	Role description	
1	Standard user	USER	
2	Operátor modelov	OPERATOR	
3	Risk analytic	RISK_ANALYST	
4	Administrátor aplikácie	ADMIN	

Copyright © 2022

admin ▾

Obrázok 20 Obrazovka so správou používateľov

submit
Cancel

DREAD faktorizácia

model_name	Authprot	SL	M	O	S	ED	EE	A	IDE	LC	LI	LAV	LAC	FD	RD	NC	PV	Risklevel	Likvalue	Liklevel	Impvalue	Implevel	Action	
0																		INFO	0	LOW	0	LOW	save	
APIKEY		5	4	4	4	7	5	4	8	5	5	5	5	7	7	4	5	5	MEDIUM	5.125	MEDIUM	5.375	MEDIUM	save
BASE64		5	9	7	5	7	5	6	8	7	7	5	5	7	7	5	5	5	CRITICAL	6.5	HIGH	6	HIGH	save
CAPTCHA		5	4	4	4	7	5	4	8	6	5	5	5	7	7	4	5	5	MEDIUM	5.125	MEDIUM	5.5	MEDIUM	save
Certificate		3	4	4	2	3	3	4	3	2	3	5	5	7	3	4	2	3	MEDIUM	3.25	MEDIUM	3.625	MEDIUM	save
ClearText		9	9	7	9	9	9	9	8	9	7	7	7	7	7	9	7	7	CRITICAL	8.625	HIGH	7.5	HIGH	save
Cookies		3	4	4	4	3	3	4	3	6	3	5	5	7	3	4	5	3	MEDIUM	3.5	MEDIUM	4.5	MEDIUM	save
Digest access authentication		3	4	4	4	3	3	4	3	6	3	5	5	7	3	4	5	3	MEDIUM	3.5	MEDIUM	4.5	MEDIUM	save
Kerberos/SPNEGO		5	4	4	4	7	5	4	8	6	5	5	5	7	7	4	5	5	MEDIUM	5.125	MEDIUM	5.5	MEDIUM	save
LDAP		3	4	4	4	3	3	4	3	6	3	5	5	7	3	4	5	3	MEDIUM	3.5	MEDIUM	4.5	MEDIUM	save
None		9	9	9	9	9	9	9	9	9	7	9	9	9	9	9	7	9	CRITICAL	9	HIGH	8.5	HIGH	save
NTLM		3	4	4	4	3	3	4	3	6	3	5	5	7	3	4	5	3	MEDIUM	3.5	MEDIUM	4.5	MEDIUM	save
OAuth2		1	1	4	2	1	1	1	1	2	1	5	5	1	1	1	2	3	INFO	1.5	LOW	2	LOW	save
OIDC		1	1	4	2	1	1	1	1	2	1	5	5	1	1	1	2	3	INFO	1.5	LOW	2	LOW	save
OTP		5	4	4	4	7	5	4	8	6	5	5	5	7	7	4	5	5	MEDIUM	5.125	MEDIUM	5.5	MEDIUM	save
RADIUS		3	4	4	4	3	3	4	3	6	3	5	5	7	3	4	5	3	MEDIUM	3.5	MEDIUM	4.5	MEDIUM	save
SAML		1	1	4	2	1	1	1	1	2	1	5	5	1	1	1	2	3	INFO	1.5	LOW	2	LOW	save
Unknown		9	9	9	9	9	9	9	9	9	7	9	9	9	9	9	7	9	CRITICAL	9	HIGH	8.5	HIGH	save

Copyright © 2022

Obrázok 21 Obrazovka s ukážkou navrhovaných protokolov

PRÍLOHA I

The screenshot displays ten tables from a database:

- badi threats**: Columns include id (int(255)), sl (int(10)), m (int(10)), o (int(10)), s (int(10)), ed (int(10)), ee (int(10)), a (int(10)), ide (int(10)), lc (int(10)), li (int(10)), lav (int(10)), lac (int(10)), fd (int(10)), rd (int(10)), nc (int(10)), pv (int(10)), threat_name (varchar(150)), threat_description (varchar(250)), dataclass (varchar(150)), architect (varchar(150)), authprot (varchar(150)), netloc (varchar(150)), authfact (varchar(150)), sign (varchar(150)), enc (varchar(150)), userpriv (varchar(150)), risklevel (varchar(150)), liklevel (varchar(150)), likvalue (varchar(150)), implevel (varchar(150)), impvalue (varchar(150)), and timestamp (timestamp).
- badi aspects**: Columns include id (int(25)), aspect_type (varchar(250)), aspect_name (varchar(250)), aspect_value (varchar(250)), and aspect_description (varchar(250)).
- badi dread**: Columns include id (int(11)), dread_name (varchar(45)), dread_level (int(11)), and dread_description (varchar(255)).
- badi user_roles**: Columns include id (int(11)), code (varchar(25)), and name (varchar(250)).
- badi users**: Columns include id (int(11)), email (varchar(256)), password (varchar(256)), status (tinyint(1)), and role (int(11)).
- badi models**: Columns include id (int(255)), sl (int(10)), m (int(10)), o (int(10)), s (int(10)), ed (int(10)), ee (int(10)), a (int(10)), ide (int(10)), lc (int(10)), li (int(10)), lav (int(10)), lac (int(10)), fd (int(10)), rd (int(10)), nc (int(10)), pv (int(10)), model_name (varchar(150)), model_description (varchar(250)), dataclass (varchar(150)), architect (varchar(150)), authprot (varchar(150)), netloc (varchar(150)), authfact (varchar(150)), sign (varchar(150)), enc (varchar(150)), userpriv (varchar(150)), risklevel (varchar(150)), liklevel (varchar(150)), likvalue (varchar(150)), implevel (varchar(150)), impvalue (varchar(150)), and timestamp (timestamp).
- badi dshb_menu**: Columns include id (int(11)), icon (varchar(45)), name (varchar(45)), href (varchar(25)), and min_user_role (int(11)).

Obrázok 22 Zoznam tabuľiek v databáze

PRÍLOHA J

Zdrojové kódy sú umiestnené na GITHUB: <https://github.com/MarekHrabcak/badi>