Kreiranje sigurnih sistema primjenom koncepata nultog povjerenja

Studentski rad

Aleksandar Vidaković
Student drugog ciklusa studija
Univerzitet u Istočnom Sarajevu, Elektrotehnički fakultet
Istočno Sarajevo, Bosna i Hercegovina
aleksandar.vidakovic.m192@student.etf.ues.rs.ba

Sažetak — **Primjena informacionih sistema se praktikuje radi efikasne digitalizacije poslovanja čime se optimizuju poslovni procesi i omogućava veća kontrola nad resursima. Imajući u vidu značaj njihovog uvođenja u brojne privredne djelatnosti, neophodno je obratiti pažnju na aspekt informacione bezbjednosti u savremenom, veoma dinamičnom i nepredvidljivom, virtuelnom okruženju gdje se kao imperativ nameće zaštita podataka od potencijalnih prijetnji. Nakon uvodne analize rizika i statističkih podataka, rad nudi razumijevanje bezbjednosnih koncepata: autentifikacija, autorizacija i kontrola pristupa, segmentacija i šifrovanje koje prate praktične realizacije na primjeru veb aplikacije i lokalne računarske mreže uz posebno isticanje mogućnosti integracije navedenih elemenata na naprednom nivou čime se dostiže arhitektura nultog povjerenja kao sveobuhvatno rješenje.**

Ključne riječi – informaciona bezbjednost; autentifikacija; autorizacija; segmentacija; šifrovanje; arhitektura nultog povjerenja;

I. UVOD

Savremene aplikacije i sistemi, ali i računarska mreža kao njihova infrastrukturna podloga, moraju pored zadovoljenja funkcionalnih zahtjeva krajnjih korisnika pružiti i svu prateću podršku radu sistema, što na prvom mjestu uključuje informacionu bezbjednost. Sajber bezbjednost (engl. *cybersecurity*), prema jednoj od definicija NIST-a (engl. *National Institute of Standards and Technology*), predstavlja skup tehnika i metoda kojima se preveniraju oštećenja informacionih, komunikacionih i elektronskih sistema i usluga uključujući i informacije sadržane u njima kako bi se osigurao njihov integritet, dostupnost, povjerljivost i nepobitnost.

Agencija Evropske unije za sajber bezbjednost (engl. *European Union Agency for Network and Information Security - ENISA*) svojim godišnjim izvještajem *ENISA Threat Landscape – ETL* sumira neprestano praćenje stanja sajber bezbjednosti usmjeravajući se ka obavještajnoj analizi prijetnji i podizanju situacione svijesti, nerijetko u geopolitičkom kontekstu, a sve na osnovu javno prijavljenih događaja i incidenata. ETL za period od jula 2023. do juna 2024. godine naglašava porast sajber napada zbog eskalacije regionalnih konflikata. Izdvajaju se sljedeće prijetnje: ransomver (uvodi blokadu pristupa čiji je prekid uslovljen otkupom velike vrijednosti koja u posljednje vrijeme skače i do 500%, sa prosječnim vremenom obustave rada sistema od 136 sati u 2023. godini), malver, drušveni inženjering (oslanja se na ljudske greške sa 74%, a ne na tehničke manjkavosti - primjer je *phishing* gdje od 75% do 91% ciljanih napada počinje slanjem zlonamjernog mejla), povrede i curenje podataka, otkazivanje dostupnosti resursa (DDoS napad) i nezakonita manipulacija informacijama [1]-[2]. Izvještaj o globalnim rizicima Svjetskog ekonomskog foruma za 2024. godinu upozorava da je nova tehnologija put za sve sofisticiranije sajber napade. Među ključnim događajima navodi se razbijanje mreže od 19 miliona računara zaraženih malverom od strane FBI, međunarodna operacija „Kronos", 140 prijavljenih napada tokom Olimpijskih igara u Parizu, brojni prekidi u IT uslugama koji mogu dovesti do globalnih poremećaja i razne tehnike sticanja povjerenja žrtava prije nanošenja velikih gubitaka [3]. MMF-ov izvještaj o globalnoj finansijskoj sigurnosti objavljuje podatak o procijenjenih 2.5 milijardi štete od 2020. godine zbog sajber napada [3]. Interesantni podaci stižu i iz izvještaja kompanije *CrowdStrike* za 2024. godinu kojim se iznosi: najbrže zabilježeno vrijeme proboja u sistem žrtve od 2 minuta i 7 sekundi, povećanje od 75% napada u oblaku, učestala kompromitacija kupoprodajnih odnosa i primjena generativne vještačke inteligencije za vješto zaobilaženje metoda autentifikacije [4].

Uvidom u statističke podatke predočene iz literature otvaraju se pitanja identiteta i autentičnosti korisnika, formata i načina prenosa podataka te organizacije mrežne infrastrukture. Od implementacije navedenih važnih elemenata u velikoj mjeri zavisi nivo zaštite sistema.

U modernim korporativnim sistemima zahtjeva se napredna realizacija ovih koncepata sa akcentom na kontinuiranu verifikaciju identiteta i korisničkih privilegija, kontekstualizaciju i granulaciju pri kontrolisanju pristupa u mikrosegmentisanom okruženju uz obaveznu tzv. formalizaciju krajeva komunikacije za šifrovanje podataka koji se prenose između tih krajeva. Upravo se arhitektura nultog povjerenja (*engl. Zero Trust Architecture – ZTA*) pojavila kao reakcija na brz tehnološki razvoj i predstavila kao objedinjeno rješenje koje ispunjava sve pomenute potrebe.

II. PREGLED OSNOVNIH BEZBJEDNOSNIH ZAHTJEVA

A. Autentifikacija

Esencijalni zahtjev za uspješno korišćenje sistema sa stanovišta krajnjih korisnika je omogućavanje bezbjednog pristupa istom, ali i adekvatna zaštita korisničkih podataka koji, u skladu sa namjenom sistema, mogu biti veoma osjetljivi. Korisnikom se smatra svaki entitet koji koristi resurse sistema za obradu podataka i ne podrazumijeva samo osobe već i pametne IoT uređaje, automatizovane procese ili druge aplikacije i sisteme posredstvom veb servisa i API-ja.

Autentifikacija predstavlja verifikaciju identiteta korisnika i ukoliko se uspješno sprovede otvara put upotrebi resursa sistema u skladu sa dodijeljenim privilegijama. Podatak ili faktor koji se koristi za prepoznavanje korisnika se naziva autentifikator i kao takav se u bazi podataka mora čuvati u zaštićenoj formi. U autentifikatore spadaju faktori koje korisnik zna (tajni podaci kao što su lozinke, PIN kodovi, fraze, tajna pitanja i odgovori), faktori koje korisnik posjeduje (pametne kartice, USB ključevi, beskontaktni tokeni i hardverski ili softverski generatori kodova) i biometrijski faktori (fizičke ili bihevioralne karakteristike čovjeka). Najzastupljeniji je klasični metod prijave na sistem pomoću korisničkog imena i lozinke. S obzirom da se u tom slučaju koristi jedan faktor riječ je o jednofaktorskoj autentifikaciji (engl. *Single-Factor Authentication – SFA*), dok je radi veće sigurnosti preporučljivo koristiti veći broj faktora čime se postiže višefaktorska autentifikacija (engl. *Multi-Factor Authentication – MFA*) koja je jedan od postulata ZTA [5].

B. Autorizacija i kontrola pristupa

Nakon prepoznavanja korisnika postavlja se pitanje njegovih ovlašćenja za izvođenje pojedinih sistemskih funkcionalnosti što se reguliše procesom autorizacije gdje je neophodno da korisnik može izvršavati samo one operacije za koje je autorizovan. Ovo je ujedno povezano i sa kontrolom pristupa resursima sistema. Čest način je dodjeljivanje korisničkih uloga korisničkim nalozima (engl. *Role-Based Access Control*) koje sadrže podatke o svim dozvoljenim aktivnostima za datog korisnika i provjeravaju se prije izvršenja određene akcije. Vrlo je važno odrediti nivo privilegija, u skladu sa potrebama korisnika za obavljanje njegovih zadataka, kako bi se spriječile zlonamjerne aktivnosti i kompromitovanje zaštićenih podataka.

U kontekstu ZTA, potrebno je voditi se principom minimalnih privilegija za svakog korisnika gdje mu se pridružuje samo najmanji, neophodni obim pristupa na osnovu relevantnosti njegove uloge u sistemu. Ovim se sprječava zloupotreba podataka na osnovu neovlašćenog pristupa u veoma kompleksnom virtuelnom okruženju gdje su danas u najvećem broju slučajeva klasične monolitne aplikacije sa čvrsto spregnutim komponentama zamijenjene onima zasnovanim na mikroservisnoj arhitekturi, računarstvu u oblaku i multitenant sistemima [5].

C. Šifrovanje

Format i način čuvanja podataka (bilo u mirovanju, tokom razmjene podataka između klijenta i servera ili pri obradi) je sljedeći važan korak koji treba uraditi nakon dodjele privilegija validnom korisniku.

Šifrovanje je mehanizam za osiguravanje povjerljivosti, integriteta, autentičnosti i proslijeđene tajnosti podataka i komunikacionih protokola kojim se podaci transformišu iz čitljivog u nečitljiv oblik kako bi se onemogućilo otkrivanje sadržaja. Proces šifrovanja i dešifrovanja obezbjeđuje niz znakova nazvan kriptografskim ključem koji treba da bude što duži, nasumičan i nepredvidljiv. Na osnovu vrste ključa razlikuju se tipovi šifrovanja: asimetrično (koristi jedan javno dostupni ključ za šifrovanje i jedan privatni ključ koji posjeduje primalac poruke, primjer upotrebe je u HTTPS, SSH i TLS protokolima) i simetrično (koristi jedan ključ koji se dijeli među učesnicima komunikacije, poznat primjer je primjena AES algoritma). Oba tipa imaju svoje prednosti i nedostatke, a izbor se vrši shodno potrebama konkretne primjene [5].

Moderni pravci u razvoju kriptografije su: šifrovanje podataka u blokovima, tehnologije uspostavljanja ključeva, kriptografski heš algoritmi sa primjenom u digitalnim potpisima kojima se potvrđuje autentičnost izvora podataka, metode postkvantne kriptografije i kriptografije za male elektronske uređaje u IoT sistemima kao i tehnike generisanja slučajnih bitova. Sa druge strane, ZTA zahtjeva šifrovanje s kraja na kraj (engl. *End-to-End Encryption, E2EE*) sa eksplicitnim poznavanjem krajnjih tačaka komunikacije.

D. Segmentacija mrežnog okruženja

Dijeljenjem mrežne platforme na kako fizičke tako i logičke segmente koji funkcionišu kao odvojene cjeline postiže se lakše održavanje jer se upravlja manjim dijelovima pa se i resursi efikasnije dodjeljuju, poboljšavaju se performanse regulacijom saobraćaja te povećava sigurnost zbog lakše detekcije problema u izolovanim segmentima čime se izbjegava automatska propagacija na kompletnu mrežu. Na lokalnom nivou uređaji se povezuju svičevima i pristupnim tačkama dok se rutiranjem bira optimalan put podataka u spoljašnju mrežu koja može biti proizvoljno komplikovana u smislu različitih medijuma za prenos i brojnih posredničkih uređaja na etapama puta s obzirom da se danas podaci čuvaju u velikim centrima za podatke ili platformama u oblaku koje pružaju mnoge usluge i servise. Prednost segmentacije je da svaki čvor ima pristup kompletnom propusnom opsegu prenosnog medijuma, a mana je usložnjavanje fizičke topologije novim elementima aktivne i pasivne opreme i logičke topologije korišćenjem softvera za orkestraciju [5].

Segmentacija se može izvršiti pomoću svičeva kreiranjem virtuelnih lokalnih mreža, rutera koji povezuju udaljene segmente, zaštitnih zidova koji kontrolišu saobraćaj na osnovu sigurnosnih pravila, softverski definisanih mreža (engl. *Software-Defined Network – SDN*) za dinamičku segmentaciju, MPLS (engl. *Multiprotocol Label Switching*) za WAN mreže i tehnologija za segmentaciju u oblaku i IoT uređaja.

Osnovna prednost mikrosegmentacije koja je zapravo zahtjev ZTA je u tome što se klasičnim segmentiranjem kontroliše vertikalna komunikacija između klijenta i servera dok se mikrosegmentacijom kontroliše i horizontalna komunikacija između ravnopravnih uređaja čime se smanjuje prostor za napad i lateralno kretanje napadača u mreži [5].

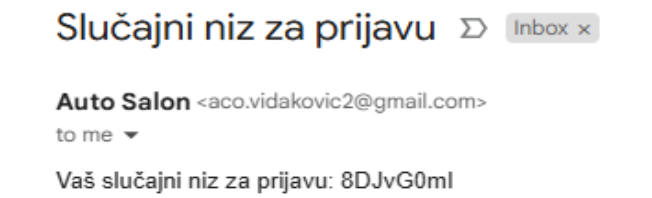
III. PRIMJERI REALIZACIJE

A. 2FA

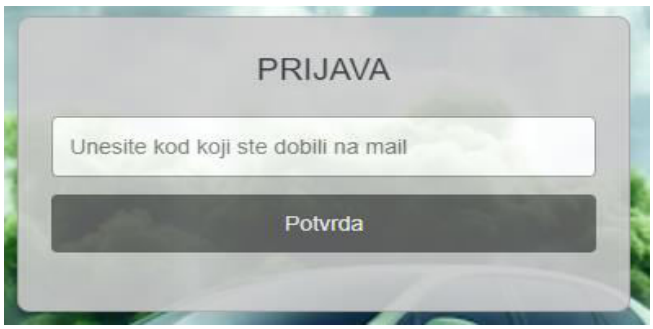
Skoro sve aplikacije podržavaju funkcionalnost prijave na sistem gdje je dvofaktorska autentifikacija (engl. *Two-Factor Authentication- 2FA*) jedan od čestih načina povećanja sigurnosti. U konkretnoj aplikaciji 2FA je implementirana pomoću verifikacionog koda poslatog sa serverske strane na adresu elektronske pošte koja je povezana sa korisničkim nalogom. Ova funkcionalnost je kreirana za administratore aplikacije koji moraju da se prijave kako bi dobili pristup administratorskim opcijama, a gosti imaju samo mogućnost pregleda podataka i ne prijavljuju se.

Nakon što korisnik unese korisničko ime i lozinku na formi za prijavu, u pozadini se šalje HTTP zahtjev serveru gdje se uneseni podaci provjeravaju i ukoliko su validni generiše se jednokratni kod sačinjen od slučajnog niza osam alfanumeričkih karaktera koji se šalje na mejl korisniku (Sl. 1). Potrebno je da korisnik ima pristup mejlu kako bi kompletirao prijavu tako što će preuzeti dospjeli kod i unijeti ga kao dodatni faktor autentifikacije (Sl. 2), a u slučaju nepodudaranja sa primljenim kodom, korisniku se ponovo prikazuje početna forma.

Na ovaj način koji je jednostavan jer ne koristi dodatni hardver već samo postojeću infrastrukturu mejl servera i koji se koristi u mnogim aplikacijama za potvrdu identiteta, povećana je zaštita korisničkog naloga jer i u slučaju kompromitovanja korisničkog imena i lozinke potencijalni napadač mora imati pristup elektronskoj pošti žrtve. Međutim, zavisnost od nivoa zaštite samog mejla i mogućih kašnjenja ili presretanja pri prenosu elektronske poruke čine prikazanu metodu ranjivom.



Slika 1. Sadržaj pristiglog mejla.



Slika 2. Polje za unos dodatnog faktora autentifikacije.

B. JWT

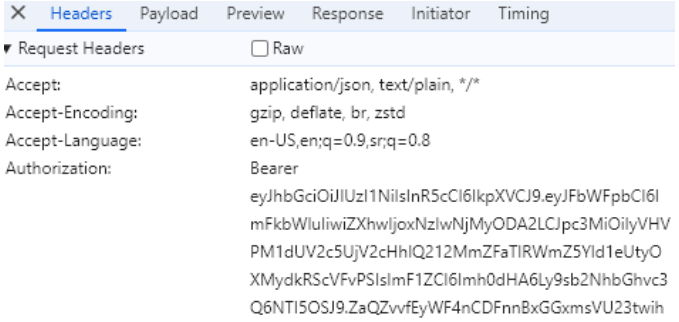
Za autentifikaciju, autorizaciju te efikasnu i sigurnu razmjenu podataka između dvije strane (najčešće klijenta i servera) u formi JSON objekata često se koristi *JSON Web Token – JWT*. JWT je otvoreni standard (RFC 7519) za prenos kodiranih i digitalno potpisanih informacija pomoću tajnog ključa ili preko para javnog i privatnog ključa. JWT obezbjeđuje potvrdu identiteta tako što se vrati klijentu nakon uspješne prijave. Kasnije se može koristiti za autorizaciju API poziva koji se šalju serveru pri čemu je zagarantovan integritet i autentičnost sadržaja tokena. Svoju primjenu nalazi u veb aplikacijama, mobilnim aplikacijama i raznim API servisima, a s obzirom da je u pitanju JSON format lako se parsira direktnim mapiranjem na objekte što podržavaju mnogi programski jezici te se pokazao kompaktnijim u odnosu na standarde za XML format kao što je SAML (engl. *Security Assertion Markup Language)* [6].

Strukturu tokena uključuju tri dijela odvojena znakom „ . “:

1. Zaglavlje (engl. *header*) – sadrži tip tokena i algoritam za potpisivanje (metapodaci).
2. Korisni podaci (engl. *payload*) – sadrže tvrdnje (engl. *claims*) što može biti ID korisnika, korisničko ime, mejl adresa, korisnička uloga, rok trajanja tokena i slično (ono što se želi prenijeti da bi se koristilo na odredišnoj strani).
3. Potpis (engl. *signature*) kojim se osigurava da sadržaj tokena nije izmijenjen pri prenosu.

U kreiranoj aplikaciji JWT se koristio za korisnike koji su administratori aplikacije. Generiše se na serverskoj strani nakon uspješne prijave, vraća se na klijentsku stranu i smiješta u lokalno skladište veb čitača odakle je pribavljan za autorizaciju zahtjeva i prikazivanje elemenata korisničkog interfejsa. Algoritam koji se koristio za potpisivanje tokena je HMAC-SHA256 (kombinacija *Hash-Based Message Authentication Code* za autentifikaciju poruke heš funkcijom sa tajnim ključem i *Secure Hashing Algorithm-256* koji, nezavisno od ulaza, jednosmjerno generiše fiksnih 256 bita na izlazu). U sklopu korisnih podataka vraćeni su podaci o korisniku dok je vrijeme isteka tokena ograničeno na pet časova. Svaki sljedeći HTTP zahtjev koji zahtjeva autorizaciju sadrži i token u zaglavlju (Sl. 3) što je realizovano *Bearer* šemom.

U opisanoj implementaciji osigurana je kontrola pristupa administratorskim opcijama u aplikaciji kao i validnost HTTP zahtjeva upućenih serveru sa nedostacima rizičnog čuvanja tokena u lokalnom skladištu zbog opasnosti od XSS (engl. *Cross Site Scripting*) napada injekcijom zlonamjernih skripti, zavisnošću od tajnog ključa i nešifrovanja podataka.



Slika 3. Prikaz zaglavlja autorizovanog HTTP zahtjeva.

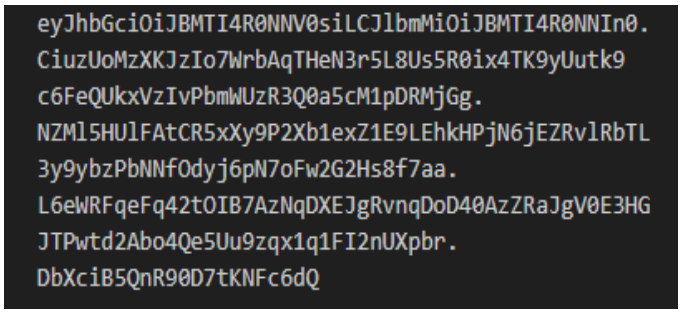
C. *JWE*

Iako je u većini aplikacija sasvim dovoljna upotreba JWT-a, u nekim slučajevima radi postizanja povjerljivosti podataka neophodno je da se podaci pri prenosu pored potpisivanja i šifruju što je moguće kreiranjem *JSON Web Encryption – JWE* tokena. JWE je IETF standard za šifrovanje podataka u JSON formatu simetričnim ili asimetričnim algoritmima koji ih šifruje na način da ih dešifrovati mogu samo oni entiteti kojima su zaista i namijenjeni. Pošto sigurnost JWE koncepta primarno zavisi od tajnosti kriptografskog ključa, on se mora adekvatno dinamički generisati ili upotrebljavati pomoću posebnih alata za upravljanje ključevima kako bi se spriječio neovlašćeni pristup trećim stranama [7].

Struktura šifrovanog tokena u odnosu na JWT je nešto složenija i uključuje pet dijelova odvojenih znakom „ . “ (Sl. 4):

1. Zaglavlje (engl. *header*) sa metapodacima o tokenu: tip tokena, algoritam za šifrovanje ključa/podataka i dr.
2. Šifrovani ključ (engl. *encrypted key*)
3. Vektor inicijalizacije (engl. *initialization vector*)
4. Šifrovani podaci (engl. *ciphertext*): korisni podaci u šifrovanom obliku.
5. Autentifikacioni tag (engl. *authentication tag*) koji štiti integritet tokena.

U aplikaciji su odabrani standardizovani algoritmi: AES-256-KW algoritam za šifrovanje ključa tokena i AES-256-CBC-HMAC-SHA512 kao kombinovani algoritam za šifrovanje i verifikaciju integriteta podataka tokena. Sa dužinama kriptografskih ključeva od 256 bita ovi algoritmi daju veoma visok nivo sigurnosti sa strane očuvanja privatnosti od neželjenog pristupa, krađe i potencijalnih manipulacija nad podacima sa nasumičnim ključevima čime se otežava njihovo otkrivanje. Takođe, kompatibilna je njihova primjena u raznim tehnologijama što olakšava implementaciju. Mana upotrebe JWE jeste složenost i intenzivne operacije nad podacima što može uticati na performanse kao i rizik od kompromitovanja dijeljenog ključa koji je ovdje korišćen. Dakle, iako se relativno jednostavno softverski realizuje uz pomoć ugrađenih biblioteka radnih okvira, JWE može unijeti dodatno opterećenje (engl. *overhead*) u obradi podataka.



Slika 4. Primjer JWE tokena.

D. *Primjer mrežne segmentacije*

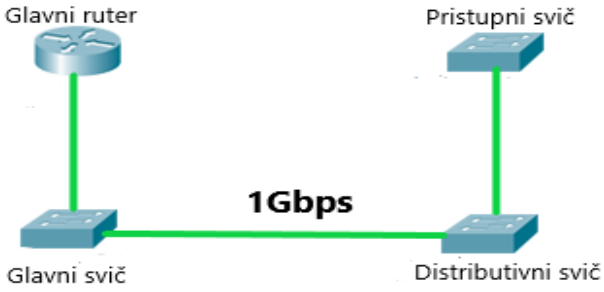
Elektrotehnički fakultet Univerziteta u Istočnom Sarajevu posjeduje sopstvenu računarsku mrežu sa mnoštvom povezanih uređaja shodno potrebama brojnih učionica, laboratorija, sala i kancelarija, a sve u svrhu sprovođenja raznih akademskih i administrativnih aktivnosti.

Fizička organizacija uređaja predstavljena je hibridnom topologijom kojom se kombinuju prednosti pojedinih topologija. Mnogim vezama među uređajima se postiže redundantnost i pouzdanost. Takođe, uređaji su organizovani hijerarhijski (Sl. 5), a radi lakšeg održavanja kreirani su manji segmenti pomoću rutera i svičeva. Centralni uređaj u mreži je svič nazvan *Core Switch* na koji su povezani ruteri koji omogućavaju dva izlaza na internet (podrazumijevani i rezervni) sa jedne strane i upravljivi svičevi distributivne uloge sa druge strane na koje su povezani obični, pristupni svičevi kojima se ne može upravljati, a na njih su dalje povezane pristupne tačke za bežično povezivanje i krajnji korisnički uređaji (računari, serveri, nadzorne kamere).

Sa gledišta logičke topologije bitne su virtuelne lokalne mreže kreirane tako što su portovima određenih svičeva dodijeljeni različiti opsezi IP adresa simulirajući time postojanje više lokalnih mreža dok se *trunk* kablovima vrši istovremeni, višestruki prenos signala. Izvršena je i segmentacija korisnika čime su poboljšane performanse redukcijom latencije i kolizija te regulisano opterećenje pošto postoje zasebne virtuelne mreže za menadžment, profesorske kancelarije, studentske laboratorije, klijente kojima se ustupa mrežni prostor i goste kako žičano tako i za Wi-Fi.

Što se tiče bezbjednosti treba, pored VLAN mreža na L2 komunikacionom sloju, navesti i prisustvo zaštitnih zidova u vidu kontrolnih lista pristupa i primjenu NAT tehnologije na ruterima, VPN PPTP server na jednom ruteru (L3 nivo), AES enkripciju verzije WPA/WPA2-PSK za WLAN i to da su diskovi servera postavljeni u RAID.

Kritički posmatrajući strukturu opisane mreže pored evidentnih prednosti ističe se mogućnost boljeg upravljanja inventarom, zavisnost od centralnih uređaja u izolovanim segmentima realizovanih topologijom zvijezde, mogućnost preopterećenja *trunk* kablova i nepostojanje rezervnog izlaza na internet za sve VLAN-ove.



Slika 5. Prikaz jedne hijerarhijske linije uređaja u mreži.

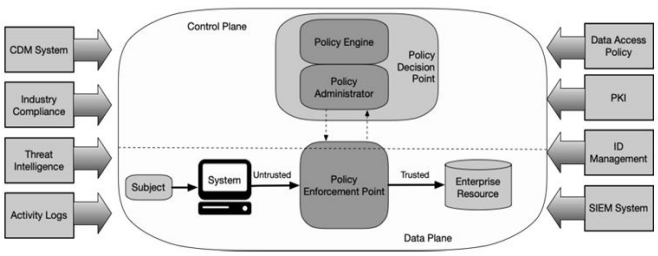
IV. ARHITEKTURA NULTOG POVJERENJA

Tradicionalne metode sajber bezbjednosti kao što su zaštitni zidovi, VPN i proksi serveri se oslanjaju na mrežni perimetar koji obavija mrežu i tako štiti njenu unutrašnjost u koju postoji implicitno povjerenje (stepen sigurnosti). Ovo je vremenom počelo da pokazuje svoje nedostatke sa sve sofisticiranijim prijetnjama hakera koji kada uspiju da se infiltriraju probivši perimetar, lako šire svoje dejstvo lateralnim kretanjem koristeći resurse i privilegije kompromitovanog korisnika. Ekstremnim povećanjem internih napada javila se ideja za robusnim i proaktivnim rješenjem koje bi uvelo deperimetrizaciju. 2010. godine prvi put se pod parolom "*never trust, always verify*" pojavio termin ZTA nakon čega postaje predmet brojnih istraživanja, a posebno u posljednjih nekoliko godina što je dovelo do potrebe za standardizacijom i konkretnim smjernicama za implementaciju. Tako ZTA sa svojim apstraktnim logičkim modelom i kombinacijom tehnologija, pristupa i korisnih praksi postaje zvanična NIST preporuka za sajber bezbjednosnu paradigmu (NIST SP 800-207) 2020. godine.

ZTA je sajber bezbjednosna arhitektura čija je premisa da se povjerenje ne može implicitno dodijeliti nijednom entitetu u mreži već je ono zasnovano na kontekstu. Fokus se stavlja na granularniju kontrolu pristupa, autentifikaciju i autorizaciju svakog zahtjeva i transakcije, princip najmanjih privilegija i kontinuiran monitoring sistema. Njena implementacija je spora jer su potrebna velika ulaganja za dodatnu administraciju kroz praćenje velikog broja parametara. Zato se preporučuje postepena implementacija u dužem vremenskom periodu. Sa druge strane, navedeni primjeri realizacije bezbjednosnih zahtjeva pokazuju kako se pojedini koncepti ZTA mogu primijeniti u bilo kojoj IT oblasti.

Suština strukture ZTA je data njenim logičkim modelom na Sl. 6. Tri glavna elementa su [8]:

1. Generator politika (engl. *Policy Engine – PE*): blok za donošenje odluka o pristupu resursima na osnovu ulaznih podataka.
2. Administrator politika (engl. *Policy Administrator – PA*): izvršni blok koji identifikuje korisnike tokenima ili kredencijalima i dozvoljava ili zabranjuje pristup resursima prema generisanim politikama.
3. Tačka upisavanja politika (engl. *Policy Enrollment Point - PEP*): blok za kontrolu i nadgledanje saobraćaja sa posredničkom ulogom između korisnika i sistemskih resursa.



Slika 6. Logički model ZTA [8].

Izvori ulaznih podataka za bogatu orkestraciju kojom se generišu sigurnosne politike mogu biti: sistem kontinuirane dijagnostike, sistem za usklađenost sa industrijskim standardima, sistem za skupljanje informacija o prijetnjama, logovi aktivnosti, pravila pristupa podacima, infrastruktura javnih ključeva, sistemi za upravljanje identitetom korisnika, informacijama i događajima.

Navedene komponente ne moraju biti jedinstveni sistemi jer jedan resurs može obavljati funkciju više logičkih komponenti i obrnuto iz čega proizilaze i varijacije modela: modeli zasnovani na gejtveju, portalu resursa, enklavama resursa ili na izolovanju aplikacija [8].

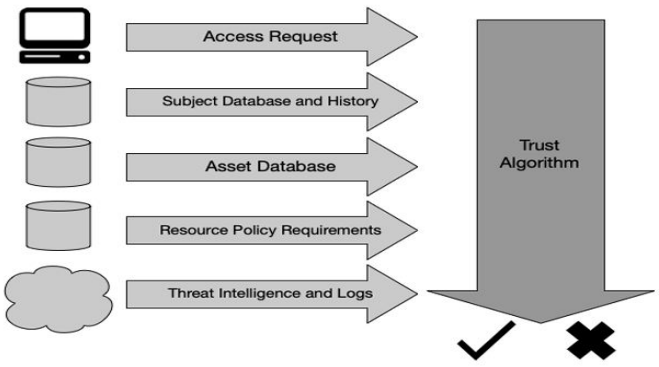
Sigurnosne politike se donose kao izlazi algoritma povjerenja (engl. *Trust Algorithm* – TA) koji konfiguriše tačke za upisivanje politika. Slanje rezultata može uzrokovati kratkotrajna pauziranja sesije radi sprovođenja ovog procesa što reguliše PA blok prema vremenskim ograničenjima radnog toka. Na Sl. 7 ilustrovani su ulazi algoritma povjerenja.

Prema načinu vrednovanja faktora TA može biti [8]:

1. Kriterijumski TA: forsira zadovoljenje svih kvalifikacionih atributa istovremeno.
2. Skorski TA: na osnovu specificiranih težinskih vrijednosti i ulaznih podataka računa nivo povjerenja koji se poredi sa deklarisanim pragom za pojedine akcije nad resursima.

Prema načinu vrednovanja zahtjeva TA mogu biti [8]:

1. Singularni TA: pojedinačno tretira svaki zahtjev bez uzimanja u obzir istorijskih podataka što ga čini brzim.
2. Kontekstualni TA: uzima u obzir akcije koje je subjekat izvodio ranije.



Slika 7. Ulazi algortima povjerenja [8].

U idealnom slučaju TA bi trebao biti kontekstualan, ali to ograničavaju infrastrukturne komponente, a i u praksi je pokazao da nekad može izazvati bespotrebna upozorenja. Administratori sistema zato pokušavaju razviti kriterijume i težinske faktore tako da balansiraju sigurnost, efikasnost, upotrebljivost i korisničko iskustvo.

V. ZAKLJUČAK

Digitalizacija i ekspanzija računarskih mreža nastala povezivanjem ogromnog broja uređaja putem različitih infrastruktura na globalnom nivou dovela je do zavisnosti mnogih poslovnih procesa od informacionih tehnologija. Stoga je značaj zaštite podataka veoma veliki, a posebno zbog katastrofalnih posljedica hakerskih napada.

U radu su predočeni osnovni zahtjevi iz ovog domena, navedeni su demonstrativni primjeri njihove realizacije uz obrazloženje prednosti, nedostataka i mogućnosti daljeg razvoja takvih rješenja nakon čega je opisana ZTA koja istovremeno integriše sve koncepte na naprednom nivou.

Arhitektura nultog povjerenja, iako se smatra „*network-driven*" rješenjem, može se primijeniti na bilo koju IT oblast jer su njeni koncepti univerzalni kada su u pitanju mnogi sistemi. Cilj rada je bio pokazati kako se u različitim okruženjima (veb aplikaciji i lokalnoj mreži) mogu primijeniti pojedine sigurnosne tehnike shodno mogućnostima i istaći arhitekturu nultog povjerenja kao moderan pristup koji objedinjuje sve te tehnike. Međutim, kompletnu implementaciju zasad samo nude poznate svjetske korporacije iz IT industrije (*Cisco*, *Google*, *Microsoft Azure* i druge). Ostaju otvorena pitanja da li ZTA implementacija unosi preveliko opterećenje sistemu i da li postoje nejasnoće u samom standardu jer za mnoge stavke nije striktno opisano kako se realizuju.

Primarni zaključak rada jeste da je proces zaštite od prijetnji u ozbiljnim informacionim sistemima neprestan i da se uvijek sve mjere zaštite mogu nadograđivati. Inicijalni sigurnosni zahtjevi su i do danas ostali isti, ali se tehnologije kojima se oni ispunjavaju konstantno modifikuju u stalnoj trci za prednostima u odnosu na hakere.

ZAHVALNICA

Posebna zahvalnost pripada mentoru prof. dr Danijelu Mijiću čiji su savjeti i sugestije u mnogome olakšale izradu ovoga rada koji je zasnovan na diplomskog radu autora iz jula 2024. godine.

LITERATURA

[1] European Union Agency for Network and Information Security (ENISA), (septembar 2024.), "ENISA Threat Landscape 2024", [Online] dostupno na: https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf, posjećeno 27.12.2024.

[2] Embroker, "Top 16 cybersecurity threats in 2024", [Online] dostupno na: https://www.embroker.com/blog/top-cybersecurity-threats/, posjećeno 27.12.2024.

[3] World Economic Forum, (WEF), (januar 2024.),"The global risks report 2024", 19th edition, [Online] dostupno na: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf, posjećeno 29.12.2024.

[4] Crowd Strike, "Crowd Strike 2024 Global Threat Report", [Online] dostupno na: https://www.crowdstrike.com/en-us/global-threat-report/, posjećeno 30.12.2024.

[5] A. Vidaković, "Arhitektura nultog povjerenja u savremenim korporativnim mrežama", Diplomski rad, Elektrotehnički fakultet Univerziteta u Istočnom Sarajevu, Bosna i Hercegovina, juli 2024.

[6] JWT.io, (Auth0), "Introduction to JSON Web Tokens", [Online] dostupno na: https://jwt.io/introduction, posjećeno 29.12.2024.

[7] M. Jones (Microsoft), J. Hilderbrand (Cisco), "RFC 7516 – JSON Web Encryption (JWE)", IETF , maj 2015, [Online] dostupno na: https://datatracker.ietf.org/doc/html/rfc7516, posjećeno 04.01.2025.

[8] S. Rose, S. Mitchell, S. Connelly, „Zero Trust Architecture", NIST SP 800-207, 2020.

ABSTRACT

The application of information systems is practiced to achieve efficient business digitalization, optimizing business processes and enabling greater control over resources. Given their significance in numerous economic activities, it is essential to focus on the aspect of information security in today's highly dynamic and unpredictable virtual environment, where data protection of potential threats becomes imperative. Following an introductory analysis of risks and statistical data, this paper provides an understanding of security concepts: authentication, authorization and access control, segmentation and encryption, accompanied by practical implementation in the example of a web application and local computer network. Particular emphasis is placed on the possibility of integrating these concepts at an advanced level, achieving a Zero Trust Architecture as a comprehensive solution.

CREATING SECURE SYSTEMS USING ZERO-TRUST CONCEPTS

Aleksandar Vidaković