Orxan Vaqif KAZIMOV
Qərbi Kaspi Universiteti, Idarəetmədə İnformasiya sistemləri, magistr
E-mail: orkhankazimli@gmail.com
ORCID ID: 0009-0007-4328-2430

UNİVERSİTETLƏR ÜÇÜN VAHİD MOBİL TƏTBİQ SİSTEMİNDƏ NPS SERVER ƏSASLI AUTENTİFİKASİYA MODELİNİN KONSEPTUAL İŞLƏNMƏSİ

Xülasə

Ali təhsil müəssisələrində rəqəmsal transformasiya prosesinin sürətlənməsi və "Smart Campus" konsepsiyasının tətbiqi, tədris və inzibati xidmətlərin mobil platformalara inteqrasiyasını zəruri etmişdir. Lakin çoxsaylı istifadəçi qruplarının (tələbələr, akademik heyət, inzibati personal) fərqli giriş icazələrinə malik olması, vahid və təhlükəsiz bir autentifikasiya modelinin qurulmasını tələb edir. Məqalədə universitetlər üçün nəzərdə tutulmuş vahid mobil tətbiq ekosistemi çərçivəsində Network Policy Server (NPS) əsaslı autentifikasiya modelinin konseptual strukturu və iş prinsipi təqdim olunur. Tədqiqatın əsas məqsədi RADIUS protokolu vasitəsilə mərkəzləşdirilmiş siyasətlərin tətbiqi və Active Directory (AD) infrastrukturu ilə mobil tətbiqlər arasında təhlükəsiz körpünün yaradılmasıdır. Təklif olunan model, istifadəçi məlumatlarının təhlükəsizliyini təmin etməklə yanaşı, sistem inzibatçıları üçün mərkəzləşdirilmiş idarəetmə və qlobal miqyaslana bilmə imkanları yaradır. Tədqiqat işində həmçinin NPS-in tətbiqi ilə autentifikasiya sorğularının optimallaşdırılması və kiber-təhdidlərə qarşı dayanıqlılığın artırılması məsələləri analiz edilmişdir

Açar sözləri: Mobil tətbiqlər, rəqəmsal universitet, NPS server, RADIUS protokolu, mərkəzləşdirilmiş autentifikasiya, identifikasiya idarəetməsi (IdM), informasiya təhlükəsizliyi.

UOT: 004.056:004.7
JEL: L86, I23, D83
DOI: https://doi.org/10.54414/MBAE2478

Giriş

Müasir dövrdə rəqəmsallaşma ali təhsil sistemində həm inzibati idarəetmə, həm də tədris proseslərinin köklü şəkildə elektron platformalara keçidini sürətləndirmişdir. Universitetlərin rəqəmsal ekosistemi genişləndikcə, tələbə və əməkdaşlara təqdim olunan xidmətlərin böyük əksəriyyəti bulud texnologiyaları və mürəkkəb informasiya sistemləri vasitəsilə həyata keçirilməyə başlanmışdır. Bu texnoloji inkişaf fonunda mobil tətbiqlər, təhsil resurslarına, fərdi akademik göstəricilərə və inzibati xidmətlərə yerindən və zamanından asılı olmayaraq 7/24 operativ çıxışı təmin edən ən strateji alətlərdən biri kimi ön plana çıxmışdır.

Buna baxmayaraq, mobil platformaların universitet mühitinə inteqrasiyası özü ilə bərabər ciddi kiber-təhlükəsizlik və infrastruktur çağırışları gətirir. Hazırda bir çox ali təhsil müəssisələrində "informasiya adacıqları" (information silos) problemi mövcuddur; yəni kitabxana sistemi, tədris idarəetmə sistemi (LMS) və maliyyə portalları fərqli verilənlər bazalarından və avtonom autentifikasiya üsullarından istifadə edir. Bu pərakəndəlik istifadəçilər üçün "şifrə yorğunluğu" (password fatigue) yaratmaqla yanaşı, təhlükəsizlik boşluqlarına, xüsusilə zəif autentifikasiya faktorlarına və icazəsiz giriş risklərinə yol açır.

Problemin həlli yolu kimi, Network Policy Server (NPS) texnologiyasının tətbiqi universitetin daxili şəbəkə təhlükəsizlik siyasətlərini mobil tətbiq mühitinə daşımağa imkan verir. Microsoft-un RADIUS (Remote Authentication Dial-In User Service) server həlli olan NPS, uzaqdan qoşulma sorğularını mərkəzi bir nöqtədən təsdiqləməyə, qruplar üzrə siyasətlər tətbiq etməyə və ətraflı audit

loqları aparmağa imkan yaradır. Bu məqalədə mobil tətbiqin backend hissəsi ilə universitetin əsas server infrastrukturu arasında NPS vasitəsilə qurulan konseptual model təhlil edilir. Tədqiqatın aktuallığı, universitetlərin heterogen şəbəkə mühitlərində vahid giriş (Single Sign-On - SSO) prinsiplərinə yaxın bir təhlükəsizlik arxitekturasının qurulması zərurəti ilə şərtlənir.

Problemin Qoyuluşu və Mövcud Vəziyyətin Analizi

Universitet ekosistemində istifadəçi bazasının (on minlərlə tələbə, müəllim və xarici tərəfdaşlar) genişliyi və rəqəmsal xidmətlərin (LMS, elektron kitabxana, maliyyə portalları) müxtəlifliyi autentifikasiya prosesini mürəkkəb bir struktura çevirmişdir. Müasir rəqəmsal təhsil mühitində mərkəzləşdirilməmiş (desentralizə olunmuş) autentifikasiya sistemləri artıq müasir kiber-təhlükəsizlik tələblərinə cavab vermir. Tədqiqat göstərir ki, pərakəndə idarəetmə modellərində aşağıdakı kritik problemlər sistemin dayanıqlılığını təhdid edir:

1. Məlumatların Təkrarlanması və Dayanıqlığı (Data Redundancy). İstifadəçi məlumatlarının müxtəlif sistemlərdə (SQL bazaları, lokal fayllar və s.) eyni vaxtda saxlanılması və yenilənməsi məlumat bütövlüyünü (Data Integrity) ciddi şəkildə pozur. Bir sistemdə şifrəsini yeniləyən istifadəçinin məlumatı digər sistemlərdə köhnə qalır ki, bu da sinxronizasiya xətalarına və mürəkkəb verilənlər bazası konfliktlərinə səbəb olur.

2. Vahid Təhlükəsizlik Siyasətinin Olmaması. Hər bir alt-sistemin (məsələn, kitabxana tətbiqi və ya tələbə portalı) öz şifrə mürəkkəbliyi, sessiya müddəti və kilidləmə (lock-out) qaydaları olur. Vahid siyasətin olmaması istifadəçilərin ən zəif qorunan sistem üzərindən "Phishing" və ya "Credential Stuffing" hücumlarına məruz qalmasına şərait yaradır. Şəbəkə inzibatçıları üçün isə bütün bu fərqli qaydaları eyni anda audit etmək praktiki olaraq qeyri-mümkündür.

3. İzolyasiya Olunmuş "İnformasiya Adacıqları". Mobil tətbiqlərin əksəriyyəti müstəqil (stand-alone) autentifikasiya bazası ilə işləyir. Bu cür izolyasiya mərkəzi identifikasiya idarəetməsini (Identity Management - IdM) mümkünsüz edir. Məsələn, universiteti tərk edən bir əməkdaşın mərkəzi bazada hesabı bağlansa da, onun izolyasiya olunmuş mobil tətbiq üzərindən daxili məlumatlara çıxışı aylarla aktiv qala bilər.

4. Genişlənmə (Scalability) və İnteqrasiya Çətinlikləri. Universitetin rəqəmsal ekosisteminə əlavə edilən hər bir yeni xidmət (məsələn, onlayn imtahan platforması) üçün sıfırdan autentifikasiya modulu qurmaq həm böyük zaman, həm də əlavə texniki resurs tələb edir. Bu, universitetin İT infrastrukturunun çevikliyini azaldır və innovativ həllərin tətbiqini ləngidir.

5. İstifadəçi Təcrübəsinin (UX) Aşağı Olması. Tələbə və müəllimlər fərqli xidmətlər üçün onlarla müxtəlif istifadəçi adı və şifrə yadda saxlamalı olurlar. Bu, "Password Fatigue" (şifrə yorğunluğu) yaradır və istifadəçiləri şifrələri qeyri-təhlükəsiz yerlərdə (məsələn, kağız üzərində və ya brauzerdə qorunmayan şəkildə) saxlamağa sövq edir. Bu kritik problemlərin aradan qaldırılması, istifadəçi təcrübəsinin yaxşılaşdırılması və ümumi şəbəkə təhlükəsizliyinin beynəlxalq standartlara uyğun artırılması məqsədilə NPS server əsaslı vahid və mərkəzləşdirilmiş autentifikasiya modelinin işlənib hazırlanması günümüzün ən aktual texnoloji zərurətinə çevrilmişdir.

Tədqiqatın Metodologiyası

Tədqiqatın əsas məqsədi müasir universitet ekosistemi daxilində heterogen istifadəçi qrupları (tələbə, professor-müəllim heyəti, inzibati və texniki personal) üçün Network Policy Server (NPS) texnologiyasına əsaslanan mərkəzləşdirilmiş autentifikasiya modelinin konseptual arxitekturasını işləyib hazırlamaqdır. Tədqiqatın metodoloji strukturunu formalaşdırmaq üçün sistemli analiz və kompleks elmi-texniki yanaşmalardan istifadə edilmişdir. Bu metodologiya təklif olunan modelin həm nəzəri-informativ əsaslarını, həm də praktiki tətbiq (deployment) imkanlarını əhatə edir.

Metodoloji baza kimi aşağıdakı elmi yanaşmalar və tədqiqat üsulları tətbiq edilmişdir:

1. Müqayisəli və Funksional Protokol Analizi (RADIUS, LDAP, OAuth) [8, 9]. Tədqiqatda müxtəlif autentifikasiya protokollarının universitetin mürəkkəb şəbəkə mühitindəki effektivliyi araşdırılmışdır.

- RADIUS (Remote Authentication Dial-In User Service) protokolunun genişmiqyaslı şəbəkə infrastrukturunda sorğuların emalı sürəti, UDP əsaslı iş prinsipi və AAA (Authentication, Authorization, Accounting) modelinə uyğunluğu təhlil edilmişdir.
- LDAP (Lightweight Directory Access Protocol) kataloq xidmətləri ilə müraciət zamanı yaranan gecikmələr (latency) və NPS-in bu sorğuları "RADIUS Proxy" kimi idarə etmə imkanları müqayisə edilmişdir [8, 9].
- Mobil tətbiq səviyyəsində OAuth 2.0 və OpenID Connect standartlarının NPS-lə sinxron fəaliyyət ssenariləri nəzərdən keçirilmişdir. Bu təhlil, NPS-in universitetin daxili şəbəkəsi ilə xarici mobil tətbiq mühiti arasında "təhlükəsizlik şlüzü" rolunu oynamasını əsaslandıran texniki arqumentləri formalaşdırmışdır [8, 9].

2. Mərkəzləşdirilmiş İdentifikasiya Modellərinin Struktur Analizi. Universitetlərdə mövcud olan izolyasiya edilmiş informasiya alt-sistemlərinin (LMS - Learning Management System, ERP, rəqəmsal kitabxana) vahid bir identifikasiya qovşağından asılılığı və bu sistemlər arasındakı "Trusted Connection" (etibarlı əlaqə) mexanizmləri analiz olunmuşdur. Struktur analiz vasitəsilə mərkəzləşdirilmiş idarəetmənin təhlükəsizlik siyasətlərinin (Policy Enforcement) tətbiqindəki rolu və hər bir alt-sistemin ayrı-ayrılıqda "Identity Provider" (IdP) kimi çıxış etməsinin yaratdığı risklər müəyyən edilmişdir [3].

3. Konseptual Sistem Modelləşdirilməsi və İnfrastruktur Dizaynı. Tədqiqat prosesində sistem komponentlərinin qarşılıqlı əlaqəsini və məlumat axınını təsvir etmək üçün abstrakt modelləşdirmədən istifadə edilmişdir.

- İstifadəçi - Mobil Tətbiq - API Gateway - NPS - Active Directory zənciri üzrə məlumatın hərəkət trayektoriyası və hər bir qovşaqda tətbiq olunan şifrələmə (TLS 1.3, RADIUS Shared Secret) qatları vizuallaşdırılmışdır.
- Bu yanaşma sistemin "tək bir uğursuzluq nöqtəsi" (Single Point of Failure) riskini analiz etməyə və yüksək əlçatanlıq (High Availability) üçün klasterləşmə ehtiyaclarını müəyyənləşdirməyə imkan vermişdir.

4. Şəbəkə Giriş Siyasətlərinin (Network Access Policies) Nəzəri Əsasları. Tədqiqat çərçivəsində mobil tətbiqin universitetin mövcud Active Directory (AD) infrastrukturu ilə inteqrasiyasının yalnız autentifikasiya (şifrə yoxlanışı) deyil, həm də dinamik avtorizasiya rollarını (tələbənin statusu, personalın icazə səviyyəsi) necə idarə edəcəyi işlənmişdir. Bu, "Role-Based Access Control" (RBAC) modelinin NPS vasitəsilə mobil mühitə adaptasiyasını təmin edir.

Aparılan kompleks metodoloji təhlil göstərir ki, seçilmiş yanaşma universitetlərdə rəqəmsal ekosistemin təhlükəsizliyinin artırılması, istifadəçi məlumatlarının bütövlüyü və inzibati idarəetmənin optimallaşdırılması üçün fundamental elmi-praktiki baza rolunu oynayır.

NPS server əsaslı autentifikasiya modelinin konseptual strukturu

Network Policy Server (NPS), Microsoft tərəfindən inkişaf etdirilən və sənaye standartı olan RADIUS (Remote Authentication Dial-In User Service) protokolu üzərində qurulmuş mərkəzləşdirilmiş autentifikasiya, avtorizasiya və hesab uçotu (AAA - Authentication, Authorization, and Accounting) sistemidir [1]. Universitet şəbəkələri kimi heterogen (müxtəlif tipli cihaz və istifadəçilərin olduğu) və çoxşaxəli infrastrukturlarda NPS, şəbəkə giriş sorğularını vahid bir təhlükəsizlik mərkəzindən filtrləməyə imkan verən strateji qovşaq rolunu oynayır. O, hər bir istifadəçi qrupu (tələbə, professor, inzibati heyət) üçün spesifik şəbəkə siyasətləri (Network Policies) təyin etməklə, resurslara müraciəti qranulyar (detallı) səviyyədə nəzarətdə saxlayır [6, 7].

Təklif olunan konseptual model, ali təhsil müəssisəsinin vahid mobil tətbiq ekosistemini təmin etmək üçün dörd fundamental layın (layer) iyerarxik və sinxron qarşılıqlı əlaqəsinə əsaslanır:

1. Mobil Tətbiq (Frontend Layer) – İstifadəçi İnterfeysi. Bu lay istifadəçinin (tələbə, müəllim və ya personal) sistemlə təmasda olduğu ilk nöqtədir. Konseptual modeldə bu komponent yalnız məlumatların toplanması və serverdən gələn nəticələrin

vizuallaşdırılması funksiyasını yerinə yetirir. Təhlükəsizlik arxitekturasının əsas şərti olaraq, "Zero Trust" (Heç kəsə inanma) prinsipi tətbiq edilir: kritik məlumatlar (şifrələr, həssas tokenlər və ya session ID-lər) mobil cihazın lokal yaddaşında (cache) saxlanılmır. Bu, mobil cihazın itməsi, oğurlanması və ya zərərli proqram təminatı ilə yoluxması zamanı universitetin daxili məlumat bazasına sızma riskini texniki olaraq sıfıra endirir.

2. Server Tərəfi (API/Backend Layer) – Vasitəçi Şlüz. Mobil tətbiqdən gələn şifrələnmiş HTTPS sorğularını qəbul edən bu mühit, daxili şəbəkə ilə xarici internet trafiki arasında "təhlükəsizlik proksisi" (Security Proxy) rolunu oynayır. Bu layın ən kritik funksiyası protokol konvertasiyasıdır: o, mobil tətbiqdən gələn tətbiq səviyyəli sorğuları RADIUS paketlərinə çevirir və NPS server üçün etibarlı bir RADIUS müştərisi (RADIUS Client) kimi çıxış edir. Bu keçid layı həm də "Rate Limiting" (sorğu sayının məhdudlaşdırılması) tətbiq edərək, daxili NPS serverini mümkün DoS/DDoS hücumlarından qoruyur [9].

3. NPS Server (Logic & Policy Layer) – Qərar Qəbuletmə Mərkəzi. Sistemin "intellektual mərkəzi" hesab olunan NPS, gələn sorğuları üç mərhələli süzgəcdən keçirir:

- Autentifikasiya: İstifadəçi məlumatlarının həqiqiliyinin yoxlanılması.
- Avtorizasiya: İstifadəçinin statusuna uyğun (məsələn, tələbənin yalnız öz qiymətlərinə, müəllimin isə jurnal sisteminə çıxışı) icazələrin müəyyənləşdirilməsi.
- Siyasət Tətbiqi (Policy Enforcement): Qoşulma zamanı cihazın növü, qoşulma vaxtı (məsələn, imtahan saatlarında xüsusi giriş hüququ) və IP ünvanı kimi şərtlər yoxlanılır. NPS, müxtəlif korporativ qaydaları tətbiq edərək girişi təsdiq edir və ya rədd edir [6].

4. Universitetin Daxili İstifadəçi Kataloqu (Identity Store). Bütün korporativ profillərin və təhlükəsizlik qruplarının mərkəzləşdirilmiş şəkildə saxlandığı Active Directory (AD) və ya LDAP əsaslı kataloq xidmətidir. NPS özü daxilində istifadəçi bazası saxlamır; o, yalnız sorğunu "Identity Store"-a yönləndirərək "Bəli/Xeyr" cavabını alır. Bu inteqrasiya imkan verir ki, tələbə universiteti bitirdikdə və ya əməkdaş işdən çıxdıqda, AD-də onun hesabı dondurulan kimi mobil tətbiqə girişi də avtomatik olaraq bütün sistemlərdə eyni anda ləğv edilsin [6].

Autentifikasiya prosesinin iş alqoritmi və texniki protokollar

Modelin effektivliyi məlumat axınının ciddi ardıcıllıqla və şifrələnmiş kanallarla həyata keçirilməsindən asılıdır. Proses aşağıdakı elmi-texniki mərhələlərlə icra olunur:

- Məlumat Girişi və İlkin Emal: İstifadəçi öz unikal identifikasiya nömrəsini (tələbə ID) və şifrəsini tətbiqə daxil edir. Mobil tətbiq daxilindəki skriptlər vasitəsilə məlumatların sintaktik düzgünlüyü yoxlanılır.
- Təhlükəsiz Translyasiya: Məlumatlar internet üzərindən backend serverə ötürülərkən TLS 1.3 (Transport Layer Security) protokolu ilə şifrələnir. Bu, "Man-in-the-Middle" (ortadakı adam) hücumlarının qarşısını almaq üçün vacibdir.
- RADIUS Sorğusunun Formalaşdırılması (Request): Backend server istifadəçi məlumatlarını RADIUS Access-Request paketi halına gətirir. Bu paketə backend və NPS arasında əvvəlcədən təyin edilmiş gizli açar (Shared Secret) əlavə olunur.
- Mərkəzi Validasiya: NPS server paketi deşifrə edir və Active Directory üzərindən istifadəçinin statusunu (aktiv/deaktiv) və şifrəsini çarpaz yoxlayır. Eyni zamanda, həmin istifadəçinin mobil tətbiqə giriş icazəsinin olub-olmadığına dair şəbəkə siyasətlərini (Policies) işə salır.
- Nəticənin Qaytarılması (Response): Yoxlamanın nəticəsindən asılı olaraq NPS Access-Accept (Giriş uğurlu) və ya Access-Reject (Giriş rədd edildi) cavabını backend-ə göndərir.
- Sessiyanın İdarə Edilməsi: Uğurlu autentifikasiya zamanı backend server mobil tətbiq üçün müvəqqəti və unikal bir JWT (JSON Web Token) yaradır. Bu token gələcək sorğuların təkrar şifrə daxil edilmədən icrasını təmin edir [4, 6].

Təhlükəsizlik üstünlükləri və inzibati effektivlik

Ali təhsil müəssisələrinin informasiya sistemlərində təhlükəsizlik yalnız texniki bir parametr deyil, həm də akademik reputasiyanı, fərdi məlumatların bütövlüyünü və istifadəçi məxfiliyini qoruyan strateji bir təminatdır. Təklif olunan NPS (Network Policy Server) əsaslı autentifikasiya modeli, universitetin kiber-təhlükəsizlik arxitekturasını aşağıdakı fundamental istiqamətlər üzrə gücləndirir:

1. Vahid Şifrə Siyasətinin (Unified Password Policy) və MFA İnteqrasiyası. Pərakəndə sistemlərdə ən böyük risklərdən biri "şifrə fraqmentasiyası"dır; yəni istifadəçilərin müxtəlif tətbiqlər üçün fərqli, çox vaxt asan təxmin edilən şifrələr təyin etməsidir. NPS modeli Active Directory (AD) ilə birbaşa inteqrasiya olunduğu üçün, universitet üzrə vahid şifrə mürəkkəbliyi (uzunluq, simvol kombinasiyası) və müntəzəm yenilənmə tələbləri bütün mobil ekosistemə şamil edilir. Bu, "Brute Force" (kobud qüvvə ilə sındırma) və "Credential Stuffing" hücumlarının effektivliyini minimuma endirir. Bundan əlavə, NPS vasitəsilə mobil tətbiqə Çoxfaktorlu Autentifikasiya (MFA) qatını əlavə etmək daha sadə və mərkəzləşdirilmiş şəkildə həyata keçirilir.

2. Kontekstual Giriş Nəzarəti və Şəbəkə Siyasətləri (Network Policies). NPS serveri inzibatçılara hər bir istifadəçi qrupu üçün "Conditional Access" (şərti giriş) qaydaları müəyyən etməyə imkan verir. Məsələn, tələbənin mobil tətbiq vasitəsilə daxili şəbəkə resurslarına müraciəti yalnız müəyyən edilmiş akademik saatlarda və ya yalnız universitetin təhlükəsiz Wi-Fi seqmentində (SSID) olduqda aktivləşdirilə bilər. Bu yanaşma, coğrafi və ya şəbəkə əsaslı məhdudiyyətlər qoymaqla "insider threat" (daxili təhdid) riskini azaldır və hər bir alt-tətbiq üçün ayrıca icazə mexanizmi qurmaq zərurətini aradan qaldıraraq sistemin mürəkkəbliyini azaldır [1].

3. Dərinləşdirilmiş Jurnallaşdırma (Advanced Logging) və Forensik Analiz. NPS serverinə gələn bütün RADIUS paketləri — hər bir uğurlu və uğursuz giriş cəhdi, sessiya müddəti, istifadəçi cihazının MAC/IP ünvanı — mərkəzi log serverlərdə (məsələn, SIEM sistemlərində) arxivlənir. Bu jurnallar kiber-insidentlərin araşdırılması (Digital Forensics) və şəbəkə anomaliyalarının (məsələn, eyni istifadəçinin qısa müddətdə fərqli coğrafi koordinatlardan daxil olması - "Impossible Travel") aşkarlanması üçün kritik məlumat mənbəyidir. Bu, universitetin İT təhlükəsizlik komandasına real vaxt rejimində monitorinq və proaktiv müdafiə imkanı verir [1].

4. "Ruh Hesablar" (Ghost Accounts) Riskinin Aradan Qaldırılması. Bir çox köhnə, desentralizə olunmuş sistemlərdə tələbə xaric olunduqda və ya əməkdaş işdən çıxdıqda, onun hər bir sistemdəki hesabını əllə bağlamaq böyük inzibati yük yaradır. Unudulan aktiv profillər ("ruh hesablar") kiber-cinayətkarlar üçün ən asan giriş qapısıdır. NPS modelində istifadəçi AD-də deaktiv edildiyi saniyədən etibarən, ona bağlı olan bütün mobil xidmətlərə giriş avtomatik olaraq bloklanır. Bu, məlumatların sinxronizasiyasını təmin edir və "tək bir həqiqət mənbəyi" (Single Source of Truth) prinsipini reallaşdırır.

5. İnzibati Effektivlik və İqtisadi Səmərəlilik. Bu model universitet rəhbərliyinə həm İT xərclərinə qənaət etməyə (hər alt-sistem üçün bahalı autentifikasiya lisenziyaları almamaq), həm də beynəlxalq informasiya təhlükəsizliyi standartlarına (məsələn, ISO/IEC 27001) uyğunlaşmağa imkan verir. İnzibati baxımdan, vahid panel üzərindən bütün mobil istifadəçi bazasını idarə etmək İT departamentinin operativliyini təxminən 40-50% artırır. Bu da resursların yeni təhsil texnologiyalarının inkişafına yönəldilməsinə şərait yaradır [4].

Təklif olunan modelin təhlükəsizlik üstünlükləri və idarəetmə səmərəliliyi

NPS server əsaslı autentifikasiya modelinin tətbiqi ali təhsil müəssisələrinin rəqəmsal ekosistemində sadəcə bir texnoloji yenilik deyil, həm də infrastrukturun dayanıqlığını təmin edən strateji bir addımdır. Bu model universitet mühitində kiber-təhdidlərin azaldılması və resursların səmərəli idarə olunması baxımından bir neçə həlledici üstünlüyə malikdir.

1. Kiber-təhdidlərin Minimallaşdırılması və Proaktiv Müdafiə. Mərkəzləşdirilmiş NPS arxitekturası fərdi istifadəçi məlumatlarının

qorunmasında "Zero Trust" (Heç kəsə inanma) prinsipinə yaxın bir müdafiə qatı yaradır.

- Vahid Siyasət İdarəetməsi (Policy-Based Defense): Pərakəndə sistemlərdən fərqli olaraq, NPS inzibatçılara vahid nöqtədən Network Access Policies tətbiq etməyə imkan verir. Bu, şifrə mürəkkəbliyi ilə yanaşı, qoşulma zamanı cihazın sağlamlıq vəziyyətini (anti-virusun aktivliyi, OS yenilənmələri) yoxlayan NAP (Network Access Protection) mexanizmlərini də aktivləşdirir [2].
- Brute-Force və Credential Stuffing-ə Qarşı Müqavimət: Autentifikasiya sorğuları Active Directory (AD) ilə sinxronlaşdığı üçün, hər hansı bir sistem üzərindən edilən uğursuz giriş cəhdləri dərhal mərkəzi hesabın bloklanması ilə nəticələnir. Bu, cinayətkarların fərqli mobil modullar üzərindən şifrə seçmə (brute-force) cəhdlərini səmərəsiz edir [1].
- İkiqat Şifrələmə Zolağı: Mobil tətbiq ilə API backend arasında HTTPS (TLS 1.3), backend ilə NPS arasında isə RADIUS protokolu daxilindəki "Shared Secret" mexanizmi məlumatların tranzit zamanı (data-in-motion) deşifrə olunma riskini minimuma endirir [2].

2. İnzibati Effektivlik və Resursların Optimallaşdırılması. Universitetlərdə minlərlə istifadəçinin olması İT departamentləri üçün böyük idarəetmə yükü yaradır. NPS modeli bu yükü avtomatlaşdırma hesabına azaldır.

- İstifadəçi Ömrünün İdarə Olunması (User Lifecycle Management): Bir tələbə universiteti bitirdikdə və ya xaric olunduqda, onun mərkəzi kataloqda (AD) deaktiv edilməsi kifayətdir. Bu zaman NPS vasitəsilə həmin istifadəçinin mobil tətbiqə, Wi-Fi şəbəkəsinə və digər daxili resurslara girişi eyni saniyədə kəsilir. Bu, unudulmuş profillərdən (Ghost Accounts) yarana biləcək təhlükəsizlik boşluqlarını tamamilə aradan qaldırır [2].
- Mərkəzi Audit və Hesabatlılıq (Advanced Logging): NPS-in RADIUS Accounting funksiyası hər bir sessiyanın başlanma və bitmə vaxtını, ötürülən məlumatın həcmini və istifadə olunan IP ünvanlarını qeyd edir. Bu, universitet rəhbərliyinə sistemin istifadə intensivliyini analiz etməyə və kiber-insidentləri dərhal araşdırmağa (Digital Forensics) imkan verir [1].

3. İqtisadi və Texniki Genişlənmə İmkanları. Yeni bir mobil modulun (məsələn, rəqəmsal kitabxana və ya tələbə yeməkxana sistemi) ümumi ekosistemə inteqrasiyası zamanı artıq sıfırdan autentifikasiya sistemi qurmağa ehtiyac qalmır. Yeni tətbiq sadəcə NPS-ə bir RADIUS Client kimi əlavə edilir [1]. Bu yanaşma:

1. Lisenziya xərclərinə qənaət edir (hər modul üçün ayrıca DB və ya auth sistemi alınmır).
2. İT heyətinin operativliyini 40-50% artırır.
3. Beynəlxalq ISO/IEC 27001 (İnformasiya Təhlükəsizliyi İdarəetmə Sistemi) standartlarına uyğunluğu asanlaşdırır.

Gələcək perspektivlər

Müzakirə predmeti olan NPS modelinin digər autentifikasiya metodları ilə müqayisəsində aşağıdakı texniki üstünlüklər xüsusi əhəmiyyət kəsb edir:

- RADIUS vs. Birbaşa LDAP İnteqrasiyası: Bir çox tətbiq birbaşa LDAP (Lightweight Directory Access Protocol) üzərindən istifadəçi bazasına müraciət edir. Lakin NPS (RADIUS) istifadə edildikdə, sorğular paket səviyyəsində şifrələnir və “Shared Secret” mexanizmi sayəsində backend-server ilə autentifikasiya serveri arasında etibarlı tunel yaradılır. Bundan əlavə, RADIUS protokolu cihazın MAC ünvanı, qoşulma protokolu və “Frame-Protocol” kimi atributlara görə filtrləmə aparmağa imkan verir ki, bu da birbaşa LDAP sorğularında mümkün deyil.
- Mərkəzləşdirilmiş Ölçəkləndirmə (Scalability): Təklif olunan model yalnız mobil tətbiq üçün deyil, gələcəkdə universitetin VPN xidmətləri, eduroam (təhsil müəssisələri üçün qlobal Wi-Fi rouminq xidməti) və 802.1X standartlı simli/simsiz şəbəkələri üçün vahid autentifikasiya mərkəzi (Single Authentication Hub) kimi xidmət edə bilər.

Gələcək tətbiq perspektivləri

Modelin gələcək tətbiq ssenariləri universitetlərdə tam rəqəmsal ekosistemin (Digital Campus) formalaşmasına fundamental töhfə verə bilər [5]:

1. Sertifikat Əsaslı Autentifikasiya (EAP-TLS): Mobil tətbiq daxilində sənəd dövriyyəsinin və akademik əməliyyatların təhlükəsizliyini təmin etmək üçün NPS bazasında rəqəmsal sertifikatların tətbiqi. Bu, istifadəçi adı və şifrə sındırılsa belə, fiziki cihaz sertifikatı olmadan girişin qarşısını alan ən yüksək təhlükəsizlik səviyyəsidir.
2. "Smart Campus" və IoT İnteqrasiyası: Tələbə kartlarının mobil tətbiqə (NFC/QR texnologiyası ilə) inteqrasiyası vasitəsilə imtahan otaqlarına, laboratoriyalara və kitabxana resurslarına girişin NPS üzərindən mərkəzləşdirilmiş idarə olunması. Bu, fiziki və rəqəmsal təhlükəsizliyin vahid mərkəzdən idarəsini təmin edir.
3. Dinamik Siyasət Təyini (Dynamic Policy Assignment): Süni intellekt (AI) alqoritmlərinin NPS logları ilə inteqrasiyası sayəsində istifadəçi davranış analizi (UEBA) apararaq, şübhəli girişləri avtomatik bloklayan "Ağıllı Təhlükəsizlik Şlüzü"nün qurulması.

Nəticə

Tədqiqat işində ali təhsil müəssisələri üçün vahid mobil tətbiq sistemində Network Policy Server (NPS) əsaslı autentifikasiya modelinin konseptual yanaşması və arxitekturası ətraflı şəkildə işlənmişdir. Təklif olunan modelin tətbiqi, mobil platformaların universitetin mövcud identifikasiya infrastrukturu ilə təhlükəsiz, mərkəzləşdirilmiş və şəffaf şəkildə inteqrasiyasını təmin etməklə, rəqəmsal ekosistemin dayanıqlılığını artırır.

Aparılan elmi-nəzəri təhlillərin və struktur qiymətləndirmələrinin nəticəsi olaraq belə qənaətə gəlmək olar ki:

- Məlumatların Bütövlüyü və Sinxronizasiyası: Mərkəzləşdirilmiş autentifikasiya modeli müxtəlif alt-sistemlərdə yaranan "data redundancy" (məlumat təkrarlanması) problemini kökündən həll edir. Bu, istifadəçi profillərinin tək bir mənbədən (Single Source of Truth) idarə olunmasını təmin edərək, məlumat sızıntısı riskini və inzibati xətaları minimuma endirir [6].
- Kiber-təhdidlərə qarşı Çoxyönlü Müdafiə: Vahid şəbəkə siyasətlərinin (Network Policies) tətbiqi, mobil mühitdə ən çox rast gəlinən kiberhücum risklərini (məsələn, Brute Force, Identity Theft) əhəmiyyətli dərəcədə azaldır. NPS vasitəsilə tətbiq olunan dinamik filtrləmə və audit imkanları universitetin daxili şəbəkəsini xarici mobil giriş nöqtələrindən gələ biləcək təhlükələrə qarşı izolyasiya edir.
- İnzibati və İqtisadi Səmərəlilik: Təklif olunan arxitektura, hər bir mobil tətbiq və ya modul üçün ayrı-ayrı autentifikasiya sistemlərinin qurulması zərurətini aradan qaldırır. Bu isə inzibati idarəetmədə vaxta qənaət olunmasına, İT resurslarının optimallaşdırılmasına və texniki dəstək xərclərinin azalmasına nail olmağa imkan verir.

Yekun olaraq qeyd etmək olar ki, bu yanaşma müasir universitet mühitində mobil xidmətlərin təhlükəsizliyinin artırılması, "Smart Campus" hədəflərinə çatılması və idarəetmənin rəqəmsal optimallaşdırılması baxımından ən effektiv və perspektivli elmi-praktiki modellərdən biridir. Tədqiqatda irəli sürülən konseptual model, ali təhsil müəssisələrində genişmiqyaslı rəqəmsal transformasiyanın təhlükəsizlik təməli kimi çıxış edə bilər.

ƏDƏBİYYAT SİYAHISI:

1. Stallings W. Network Security Essentials: Applications and Standards. 2016.
2. Rigney C., Willens S., Rubens A., Simpson W. Remote Authentication Dial In User Service (RADIUS). RFC 2865. 2000.
3. Agudo I. Digital Identity and Identity Management Technologies. 2010.
4. ISO/IEC 27001: Information security, cybersecurity and privacy protection — Information security management systems — Requirements. 2022.
5. Zheng Y., Ni J. Smart Campus Security Framework based on Unified

Authentication. IEEE Xplore Digital Library. 2019.
6. Microsoft Documentation. Network Policy Server Overview. 2025.
7. Bishop M. Computer Security: Art and Science. 2018.
8. Google Scholar elmi verilənlər bazası: Mobil şəbəkələrdə autentifikasiya və təhlükəsizlik standartları üzrə resurslar. URL: https://scholar.google.com
9. IEEE Xplore Digital Library: Texniki arxitektura və şəbəkə siyasətlərinin (Network Policies) idarə olunması üzrə elmi tədqiqatlar. URL: https://ieeexplore.ieee.org
.

Orkhan Vagif KAZIMOV
Master's student at Information Systems in Management, Western Caspian University

CONCEPTUAL DEVELOPMENT OF AN NPS SERVER-BASED AUTHENTICATION MODEL IN A UNIFIED MOBILE APPLICATION SYSTEM FOR UNIVERSITIES

Summary

The acceleration of the digital transformation process in higher education institutions has necessitated the widespread use of mobile applications. The secure and centralized management of services provided through mobile platforms requires the improvement of authentication mechanisms. The article presents a conceptual approach to a Network Policy Server (NPS) based authentication model within a unified mobile application system for universities. The proposed model ensures the integration of mobile applications with the university's existing identification infrastructure and creates advantages in terms of security, management, and scalability.

Keywords: mobile applications, university information systems, NPS server, centralized authentication, information security.

Орхан Вагиф КАЗИМОВ
Магистр по Информационным Системам в Управлении, Западно-Каспийский Университет

КОНЦЕПТУАЛЬНАЯ РАЗРАБОТКА МОДЕЛИ АУТЕНТИФИКАЦИИ НА БАЗЕ NPS-СЕРВЕРА В ЕДИНОЙ МОБИЛЬНОЙ ПРИКЛАДНОЙ СИСТЕМЕ ДЛЯ УНИВЕРСИТЕТОВ

Резюме

Ускорение процессов цифровой трансформации в высших учебных заведениях сделало необходимым широкое внедрение мобильных приложений. Безопасное и централизованное управление услугами, предоставляемыми через мобильные платформы, требует совершенствования механизмов аутентификации. В статье представлен концептуальный подход к модели аутентификации на базе сервера сетевых политик (NPS) в рамках единой системы мобильных приложений для университетов. Предложенная модель обеспечивает интеграцию мобильных приложений с существующей инфраструктурой идентификации университета и создает преимущества с точки зрения безопасности, управления и масштабируемости.

Ключевые слова: мобильные приложения, информационные системы университета, сервер NPS, централизованная аутентификация, информационная безопасность.

Daxil olub: 26.02.2026