DOI: https://doi.org/10.36719/2663-4619/114/276-279

Sevil Haqverdiyeva
Azərbaycan Dövlət Aqrar Universiteti
https://orcid.org/0009-0000-1238-8338
sevil.haqverdiyeva@gmail.com
Elnarə Orucova
Azərbaycan Dövlət Aqrar Universiteti
https://orcid.org/0009-0001-3876-3682
orucovaelnara@gmail.com
Anar Quliyev
Azərbaycan Dövlət Aqrar Universiteti
https://orcid.org/0009-0002-5549-4063
anar_quliyev74@mail.ru
Gültəkin Muradlı
Azərbaycan Dövlət Aqrar Universiteti
https://orcid.org/0009-0002-8904-9507
gultekin.qedimli@mail.ru

Korporativ şəbəkələrdə AAA təhlükəsizliyə nəzarət xidməti

Xülasə

Məqalədə identifikasiya (authentication), autentifikasiya (authorization) və avtorizasiya (accounting) xidmətlərini göstərən AAA təhlükəsiz korporativ şəbəkə girişi təmin edən təhlükəsizlik komponenti araşdırılmışdır. Başqa sözlə, o, istifadəçilərin identifikasiyası, sorğuların autentifikasiyasının işlənməsi və avtorizasiya məlumatlarının toplanmasını həyata keçirir. Autentifikasiya tələb edən proqramların xüsusi modulu olan AAA server interfeysləri korporasiyanın resursları idarə edir. Tipik olaraq AAA server şəbəkəyə giriş keçid yolu serverləri (network access gateway server), verilənlər bazası və istifadəçi məlumatlarının saxlandığı kataloqlarla qarşılıqlı əlaqədə olur. AAA server şəbəkə resurslarına "ağıllı" nəzarət girişi, siyasətin yerinə yetirilməsi, auditin istifadəsi və xidmətlər üçün lazımi hesablama məlumatlarını təmin edir. Bu proseslərin kombinasiyası effektiv korporativ şəbəkənin idarəsi və təhlükəsizliyi üçün vacib hesab olunur.

AAA xidmətləri əsasən ana AAA server (dedicated AAA server) vasitəsilə təmin edilir. AAA server ilə proqramlar və ya şəbəkə qurğularının əlaqəsi aparıcı əsas standart olan RADIUS-dur (Remote Authentication Dial-in User Service).

İdentifikasiya serveri AAA server kimi ana şəbəkə qurğusudur (dedicated network device). Bu qorunulan şəbəkə sistemlərinə və resurslarına daxil olan trafik üçün doğrulama xidməti təmin edir. İdentifikasiya serveri ilə korporativ proxy təhlükəsizlik divarı birləşdirilir. Belə ki, doğrulama və giriş nəzarət xidmətləri ayrılmış doğrulama serverinə göndərilir. Bu yolla giriş nəzarət siyasəti korporativ şəbəkənin bütün trafikinə uyğunlaşdırıla və tətbiq oluna bilər.

Açar sözlər: *korporativ şəbəkə, şəbəkə nəzarəti, təhlükəsizlik, identifikasiya, gizlilik*

Sevil Hagverdiyeva
Azerbaijan State Agrarian University
https://orcid.org/0009-0000-1238-8338
sevil.haqverdiyeva@gmail.com
Elnara Orujova
Azerbaijan State Agrarian University
https://orcid.org/0009-0001-3876-3682
orucovaelnara@gmail.com

Anar Guliyev
Azerbaijan State Agrarian University
https://orcid.org/0009-0002-5549-4063
anar_guliyev74@mail.ru
Gultekin Muradli
Azerbaijan State Agrarian University
https://orcid.org/0009-0002-8904-9507
gultekin.qedimli@mail.ru

AAA Security Control Service in Corporate Networks

Abstrct

The article examines the security component that provides AAA secure corporate network access, which provides authentication, authorization, and accounting services. In other words, it performs user identification, authentication processing of requests, and collection of authorization data. The AAA server interfaces, which are special modules of programs requiring authentication, to manage corporate resources. Typically, the AAA server interacts with network access gateway servers, databases, and directories where user data is stored. The AAA server provides "intelligent" control access to network resources, policy enforcement, audit usage, and accounting information necessary for services. The combination of these processes is considered essential for effective corporate network management and security.

AAA services are mainly provided by a dedicated AAA server. The main standard for communication between applications or network devices with the AAA server is RADIUS (Remote Authentication Dial-in User Service).

The identification server is a dedicated network device, such as the AAA server. It provides authentication services for traffic entering protected network systems and resources. The identity server is integrated with the corporate proxy firewall. Thus, authentication and access control services are sent to a dedicated authentication server. In this way, access control policies can be customized and applied to all traffic in the corporate network.

Keywords: *corporate network, network control, security, identification, privacy*

Giriş

AAA təhlükəsiz korporativ şəbəkə girişi üçün identifikasiya (authentication), autentifikasiya (authorization) və avtorizasiya (accounting) xidmətləri təmin edən önəmli şəbəkə təhlükəsizliyi komponentidir. Başqa sözlə, o, istifadəçilərin identifikasiyası, sorğuların autentifikasiyasının işlənməsi və avtorizasiya məlumatlarının toplanmasını həyata keçirir (Cole, 2011).

Authentication (Identifikasiya) – istifadəçinin real müəyyən olunma prosesinə istinad edir. Bunu istifadəçinin sistemə daxil olması üçün subyektin (istifadəçinin) sistemdə unikal, təkrarlanmayan məlumat vasitəsilə identifikasiyası kimi başa düşmək olar. Tipik olaraq keçərli adın (valid name) və uyğun gələn parolun daxil edilməsindən sonra girişə icazə verilir. Doğrulama unikal kimlik məlumatları qrupu (unique set of credentials) olan hər kəsə girişə icazə verir (Kiza, 2005). Identifikasiya əməliyyatında AAA server istifadəçinin doğrulanması üçün "credential" ilə məlumat bazasından oğurlanmış digər istifadəçilərin "credential"lərini qarşılaşdırır. Əgər bu "credential" doğrudursa, istifadəçi şəbəkəyə giriş qazanır. Yox əgər uğursuzdursa, doğrulama baş tutmur və şəbəkəyə giriş qadağan olunur. "Credential"in növlərinə misal olaraq parol, birdəfəlik nişanlar, rəqəmsal credential və biometrik ölçmələr aiddir (Cole, 2011).

Tədqiqat

İndentifikasiya Standartları: Bu standarlar şəbəkəyə daxil olmaq istəyənlərin (entity) indentifikasiyasını təmin edə bilirlər. Bu standartlara aşağıdakılar aiddir (Panko, 2010):

- Password-Based Authentication

- Challenge-Response Authentication

Parol əsaslı identifikasiya – password-based authentication: Bu standart çox sadədir və "entity"-nin (bunu subyekt kimi də başa düşmək olar) doğrulanmasının qədim metodudur.

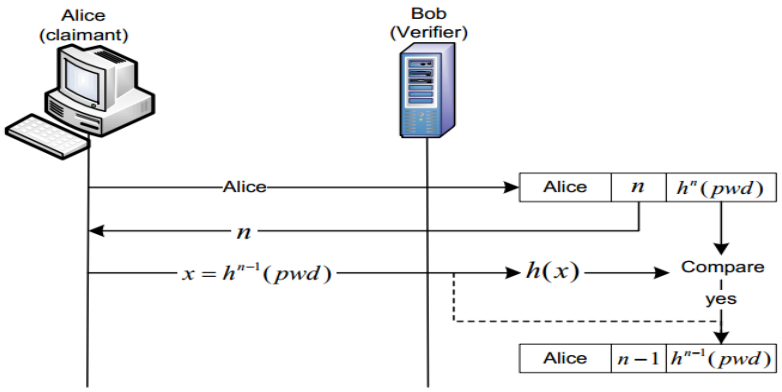
Burada parol dedikdə iddiaçının (Alice) bildiyi nə isə bir şey başa düşülür. Parol sistem resurslarına giriş əldə etmək üçün istifadə olunur. Parol əsaslı identifikasiya standartının sxeminə birdəfəlik parol (one-time password) və sabit parollar (fixed password) daxildir. Sabit parol hər bir giriş üçün dəfələrlə istifadə olunan, dəyişdirilməyən paroldur (Goldwasser, Bellare, 2008).

One-time password: Bu, bir parol identifikasiya sistemidir. Bu sistemdə hər bir parol yalnız bir dəfə istifadə olunur. Birdəfəlik parol sistemi parolların gizlincə dinlənilməsinin qarşısını alır, çünki bu parol yenidən istifadə olunmur. Buna görə də birdəfəlik parol sistemi təkrar hücumların qarşısını alır (Gupta, 2015).

İstifadəçi və sistem orijinal parol **pwd** və sayğac **n** üzərində razılaşırlar. Sistem $\mathbf{h^n(pwd)}$ hesablayır. Burada $\mathbf{h^n(pwd)}$ mənası...

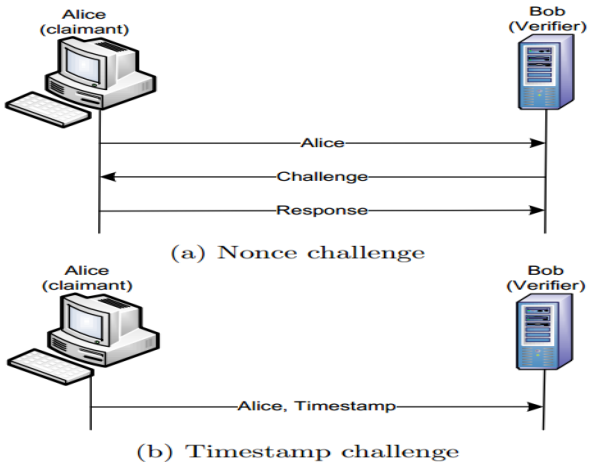
$$h^n(pwd)=h(h^{n-1}(pwd)) \text{ – dir.}$$

Sistem istifadəçi eyniliyini n-in qiymətini və $h^n(pwd)$ qiymətini özündə saxlayır. Şəkil 1-də istifadəçinin ilk dəfə sistemə giriş əldə etdiyi göstərilib (John, Dominic, 2006).



Şəkil 1. Lomport-un Hash-əsaslı Birdəfəlik parolu

Challenge-Response Authentication (Yoxlama –cavab doğrulaması): Parol indentifikasiyasında Alisan bilavasitə parolu bildiyini nümayiş etdirməklə Boba öz kimliyini təsdiq etmiş olur. Buna baxmayaraq, Alisa bu sirri göndərəndə bu rəqib tərəfin daha tez əldə edilə bilər (Katz, Lindell, 2007).



Şəkil 2. Timestamp Yoxlama

Challenge-Response Authentication standartında Alisa sirri göndərmədən sirri bildiyini sübut edir. Başqa sözlə, Alisa Boba gizli parolu göndərmir; Bob asanlıqla bura giriş əldə edə bilər. **Challenge** (yoxlama) dəyişən dəyərdir, Bob tərəfindən göndərilən təsadüfi nömrə (random number) və ya vaxt dəyişən dəyəridir (time-varying value) (Newman, 2009).

Bu, şəkil 2-də göstərildiyi kimi, Alisa (claimant) yoxlama funksiyasını istifadə edir və cavab kimi alınan nəticəni Boba (verifier) göndərir. Bu nəticə, yəni cavab, göstərir ki, Alisa bu sirri bilir. Təsadüfi nömrə (say) ssenarisində Bob tez-tez yalnız bir dəfə istifadə olunan birdəfəlik təsadüfi nömrəni göndərir. Bu hal isə proqramların təkrar hücumlarından effektiv qorunmasını təmin edir.

Dəyişən vaxt ssenarisində Alisa adətən tarix və/ya müəyyən bir hadisənin ardıcıl formada baş vermə zamanını göndərir. Buna **timestamp** deyilir (Oppliger, 2005). Timestamp müəyyən vaxtda təkrar hücumun qarşısını alan sorğuların mövcud olduğunu göstərmək üçün istifadə olunur. **Keyed-hash** funksiyaları və asimmetrik açar şifrələməsi kimi kriptoqrafik alqoritmlər kriptoqrafiya əsaslı identifikasiyanı yaratmaq üçün istifadə oluna bilər (Stallings, 2013).

Ümumiyyətlə, kriptoqrafiya əsaslı identifikasiya parol-əsaslı identifikasiyadan daha təhlükəsizdir. Əsas ideyası odur ki, identifikasiya yoxlamasının əsasında gizli kriptoqrafik əməliyyatların yerinə yetirilməsi durur (Stinson, 2006).

Nəticə

Authorization – Avtorizasiya – İstifadəçi şəbəkəyə giriş əldə etmək üçün doğrulamadan sonra avtorizasiyadan keçməlidir. Bu, subyekt tərəfindən təqdim edilmiş eyniləşdirmə məlumatlarının həqiqiliyinin yoxlanması prosesidir. Bu, adətən giriş nəzarət siyahıları (Access Control Lists – ACLs) ilə istifadəçi identifikasiyasından sonra yoxlanılır. ACLs özündə time-of-day məhdudlaşdırmasını, fiziki yerləşmə məhdudlaşdırmasını və ya eyni istifadəçi tərəfindən müxtəlif tipli logların yaradılmasının məhdudlaşdırılmasını daxil edir.

Adətən avtorizasiya identifikasiya konteksində baş verir. Çox vaxt üstünlüyün təyin edilməsi xidmətlərin müəyyən növünü istifadə etmə bacarığı ilə müəyyən edilir. Aşağıdakı xidmət növlərini özündə saxlayır, amma onlarla məhdudlaşmır: IP ünvan filtrləmə, ünvan təyin etmə, marşrutun müəyyən edilməsi, QoS / müxtəlif xidmətlər, buraxılış zonasına nəzarət / trafikin idarə olunması və şifrələmə.

Accounting – Hesabatlıq – AAA strukturunda son mərhələ hesabatlıqdır. Yəni yuxarıda qeyd olunan proseslərin ardından, subyektin (istifadəçinin) obyekt üzərində öncədən müəyyən edilmiş səlahiyyətlərinin təmin olunması və bu fəaliyyətlərin qeydiyyatının aparılması prosesidir.

Ədəbiyyat

1. Cole, E. (2011). *Network security bible*. Wiley.
2. Cole, E. (2011). *Network security*. Wiley.
3. Goldwasser, S., Bellare, M. (2008). *Lecture notes on cryptography*. Cambridge, Massachusetts.
4. Gupta, P. C. (2015). *Cryptography and network security*.
5. John, T., Dominic, W. (2006). *Complexity and cryptography*. Cambridge University Press.
6. Katz, J., Lindell, Y. (2007). *Introduction to modern cryptography*. CRC Press.
7. Kiza, J. M. (2005). *Computer network security*.
8. Newman, R. C. (2009). *Computer security*.
9. Oppliger, R. (2005). *Contemporary cryptography*. Artech House.
10. Panko, R. R. (2010). *Corporate computer and network security*.
11. Stallings, W. (2013). *Cryptography and network security*.
12. Stinson, D. R. (2006). *Cryptography: Theory and practice (3rd ed.)*. Chapman & Hall/CRC.

Daxil oldu: 25.11.2024
Qəbul edildi: 27.02.2025