SDN texnologiyasının səviyyələrində təhlükəsizlik məsələləri və həlli yolları

Orxan Mənsimzadə
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
orxan@iit.science.az

***Xülasə*— Proqramla idarə olunan şəbəkə texnologiyası (SDN – Software Defined Network) şəbəkə proqram təminatı olaraq gələcək şəbəkə arxitekturasını ənənəvi şəbəkələrdə tətbiq edir, SDN şəbəkə idarəçiliyi üçün sadəlik, proqramlaşdırma və elastiklik baxımından perspektiv imkanlar yaradır. SDN texnologiyasını tətbiq edərkən öndə duran ən vacib məsələlərdən biri də təhlükəsizlik. Məqalədə OpenFlow əsasında qurulan SDN texnologiyasının təhlukəsizlik məsəsləri və həlli yolları haqqında məlumat verilmişdir. SDN texnologiyası əsasında qurulan şəbəkəyə edilən hücumlar və bu hücumlardan mudafiə olunmaq üçün tətbiq olunan üsullar təhlil edilmişdir.**

Açar sözlər— SDN; OpenFlow; DoS; şəbəkə;

I. GİRİŞ

Rəqəmsal cəmiyyət böyüdükcə internetin əhatə dairəsi genişlənir və istifadəçilər hər tərəfdən məlumatları rahat əldə əldə edə bilirlər. İstifadəçilərin şəbəkə xidmətlərində tələbatının artması şəbəkəni qurmaq və idarə etməkdə çətinliklər yaradır. Proqramla idarə olunan şəbəkə (SDN) texnologiyası, şəbəkəyə nəzarəti asanlaşdırmaq və mərkəzdən şəbəkəni idarə etmək və şəbəkəni proqramlaşdırmaqla şəbəkənin genişlənməsinə imkan verir. Proqramla idarə olunan şəbəkə arxitekturası çox sayda marşrutlayıcı, kommutatorlar, və müxtəlif növ şəbəkə qurğuları ilə mərkəzləşdirilmiş idarəedici altında işləyən bir şəbəkələrarası ekran kimi qurulmuşdur və bunları idarə etmək üçün istifadə olunan çox sayda mürəkkəb protokollar mövcuddur. Proqramla idarə olunan şəbəkə texnologiyası şəbəkə funksiyasını virtuallaşdırmaq üçün ən yaxşı texnologiya hesab edilən yeni və inqilabi şəbəkə arxitekturasına malikdir. SDN şəbəkəyə nəzarəti idarəetmə səviyyəsi və verilənlərin ötürülməsi səviyyəsinə bölməklə şəbəkədə yüksək çevikliyə malik şəbəkə idarəetməsinin sadələşdirilməsi və təkmilləşdirilməsi üçün nəzərdə tutulmuş bir texnologiyadır. Əsas məqsəd kompleks idarəetmə məntiqini bütün şəbəkə modellərindən ləğv etmək və paket ötürülməsinə nəzarət etmək üçün məntiqi nəzarət mərkəzi təşkil etməkdir. Bu, mövcud şəbəkə texnologiyasını dəyişdirmədən tətbiqi proqramlar vasitəsilə bütün şəbəkə trafikini sərbəst şəkildə idarə etmək məqsədi daşıyır. OpenFlow SDN-də idarəetmə səviyyəsi və verilənlərin ötürülməsi səviyyəsi arasında əlaqəni təmin edən bir protokoldur. OpenFlow idarəedicidə, kommutatorda və bir-biri ilə bağlı olan kanalda tətbiq olunur. OpenFlow əsasında qurulan SDN-də şəbəkəyə olan hücumların qarşısının alınması üçün təhlükəsizliyə daha çox önəm verilməlidir. Verilənlərin ötürülməsi səviyyəsi SDN arxitekturasının alt səviyyəsində yerləşir və bir-birinə qoşulan minlərlə kommutatordan ibarətdir. Bu kommutatorların əsas işi paketlərin ötürülməsidir. Bir kommutatora hücum olunarsa göndərilən paketlər düzgün ötürülmür. Kommutatorlar istifadəçilərin şəbəkəyə qoşulması üçün birbaşa giriş nöqtəsidir və bədniyyətlilər giriş portuna sadəcə keçid edərək hücum edə bilərlər. Bunun üçün də kommutatorlarda təhlükəsizlik tədbirlərini gücləndirmək lazımdır. Əsas təhlükə məqamları inzibatçı və kommutator arasında verilən qaydaların dəyişdirilməsi və kommutatorlarla istifadəçilər arasında ötürülən paketlərə edilən DoS hücumlardır. OpenFlow idarəedicisi SDN arxitekturasında ən vacib protokollardan biri hesab olunur, burada OpenFlow açarlarına paket ötürmə qaydalarını yeniləmək və bütün şəbəkənin işini nəzarət etmək üçün şəbəkə vəziyyətini ələ almaq lazımdır. Məqalədə OpenFlow idarəedici əsaslı SDN-in müxtəlif təhlükəsizlik məsələləri və SDN şəbəkəsini təhdid edən problemlər nəzərdən keçirilmişdir. SDN təhlükəsizlik hücumlarını dəf etmək üçün müxtəlif üsulları təmin edən problem və problemlərin mövcud əks tədbirləri analiz edilmişdir [1–3].

II. “OPENFLOW” ƏSASINDA QURULAN SDN TEXNOLOGİYASINDA TƏHLÜKƏSİZLİK MƏSƏLƏLƏRİ

OpenFlow idarəedicisinə əsaslanan SDN-də əsasən bədniyyətlinin SDN-nin idarəetmə səviyyəsindəki boşluqları aşkarlayıb istismar etməsi əsas təhlükəsizlik problemlərindən biridir. İdarəedici gələn şəbəkə paketlərinin axınlarına nəzarət etməkdə məsul olduğundan o, çoxsaylı hücumların əsas hədəfinə çevrilir.

A. “**Daşqın” və “Xidmətdən imtina” hücumları**. Nəzarətçinin əsas vəzifəsi daşqın və xidmətdən imtina hücumlarını (DoS) dəf etməkdir. SDN-də idarəetmə səviyyəsi bilinməyən (idarə edə bilmədiyi) şəbəkə paketlərini qəbul edərkən axın qaydalarını təmin etmək üçün ötürücü səviyyəsindən sorğu almaq məcburiyyətindədir. Bədniyyətli bir nəzarətçini sıradan çıxarmaq üçün DoS hücumu və ya başqa bir vasitə tətbiq edə bilər. Məsələn, bədniyyətlilər nəzarətçinın işini yavaşlatmaq üçün onun üzərində bəzi resurs tükətmə metodlarını tətbiq edə bilər. Beləliklə nəzarətçi cavab gələn paketlərə qarşı yavaş işləyəcək və xidmətdən imtina edəcək.

DOI: 10.25045/NCInfoSec.2019.41

SDN şəbəkəsində DoS hücumlarının qarşısının alınması üçün 2 prinsip irəli sürülür:

- Verilmiş bir şəbəkənin SDN OpenFlow açarlarını istifadə etdiyini araşdırmalı;
- Resurs tükətmə hücumunu həyata keçirməli, çünki bədniyyətli şəbəkənin əvvəlcədən nəzərdə tutulmuş axın qaydalarının vəziyyətini bilir.

B. Host oğurlanma hücumu (Host hijacking attack). Host oğurlanma hücumu Host İzləmə Xidmətini (Host Tracking Service, HTS) OpenFlow şəbəkəsində istifadə edən bir hücumdur. Host İzləmə Xidməti şəbəkənin geniş görünüşündə və SDN nəzarətçisində istifadə olunan vacib bir xidmətdir. Şəbəkədə HTS ilə bağlı əsas məsələ, ev sahibi kimi davranması və DoS hücumu nəticəsində şəbəkənin işini pozmaqdır. Bədniyyətli nəzarətçinin bütün şəbəkə məlumatlarının idarə edilməsindən xəbərdardır. Buna görə də şəbəkə haqqında bütün məlumatları əldə etmək və SDN fəaliyyətini yavaşladacaq kritik məlumat və konfiqurasiyaları dəyişdirmək üçün darama üsulundan istifadə edə bilər. Bədniyyətli təhlükəsizlik sistemindən uğurla keçsə parol və rabitə məlumatları kimi kritik məlumatları idarə edə, dəyişdirə bilər və ya trafiki istənilən yerə yönləndirə bilər. Bu vəziyyətdə OpenFlow şəbəkəsinə hücum edən bədniyyətli üçün məlumatları əldə etmək daha asan olacaq. Bu təhlükənin qarşısının alınmasında istifadəçinin fərdi məlumatlarının OpenFlow nəzarətçisində gizlətmək üçün “Host location hacking attack” tətbiqindən istifadə etmək mümkündür.

Aldatma hücumu: Bədniyyətli aldatma hücumundan istifadə edərək nəzarətçini təqlid edə bilər. Bu hücum uğurlu olarsa, bədniyyətli SDN şəbəkə komponentlərində axın cədvəlinin girişlərini yarada və yeniləyə bilər. Şəbəkə mütəxəssisləri idarəedicidə bu axınlar barədə heç bir məlumat əldə edə bilməzlər. Beləliklə, təcavüzkar şəbəkəni tamamilə idarə etmək hüququna yiyələnir [4–7].

III. SDN TEXNOLOGİYASINDA TƏHDİDLƏRDƏN QORUNMA ÜSULLARIN TƏHLİLİ

OpenFlow nəzarətçisinə əsaslanan SDN-in müxtəlif təhdidlərdən qorumaq üçün və hücumların qarşısının alınması üçün bir çox yanaşma və tədqiqatlar aparılmışdır.

Hiper axını (Hyperflow): Şəbəkənin genişlənməsinə imkan yaradır və şəbəkənın mərkəzi nəzarət sistemini qoruyur. Hiper axını tətbiqi OpenFlow idarəedicisində işləyir və idarəedicinin vəziyyətinə təsir edən əməliyyatlar apararaq bütün şəbəkənin görünüşünü sinxronizasiya edir. Hiper axını fərqli idarəedicilərdə qərar qəbul etmə icazəsini ləğv edir. Beləliklə, verilənlərin ötürülməsi səviyyəsinin sorğusuna cavab müddəti idarəetmə səviyyəsi tərəfindən minimuma endirilir. Ayrıca özü-özünü idarə edən OpenFlow şəbəkələri arasındakı əlaqə yaratmağa imkan verir və bu OpenFlow şəbəkə sistemlərində mövcud olmayan bir xarakterdir. Bu idarəetmə qurğusunun DoS hücumlarından qorunmasını təmin edir. DoS hücumu, idarəedicinin əməliyyatlarını asanlıqla idarə edən və MAC cədvəllərinin dolmasına imkan verən bir hücum kimi də tanınır.

SDN-Mühavizə (SDN-Guard): Yenilikçi bir üsul, şəbəkəyə zərər verə biləcək trafik axını istiqamətləndirir zərərli, trafik üçün axın qaydalarının tətbiq olunmasını uzadır və SDN idarəedicisini qoruyaraq güvənli hala gətirib cixardır. SDN-Guard, idarəetmə səviyyəsinin genişliyinin DoS hücumu zamanı azalmasının minimuma endirməyə kömək edir. SDN idarəedicisi II hissədə danışdığımız host izləmə xidmətindəki təhdidlərdən dinamik olaraq qorunur və bu aşağıdakı üç faktordan ibarətdir:

- Port İdarəedici (Port Manager) : Trafik yaradan hostu müəyyənləşdirmək üçün məsuliyyət daşıyır. Ayrıca, MAC ünvanı ilə eyni olan host siyahısını özündə qeyd edir.
- Host sınamaq (Host Probing) : ICMP tələbini təmin etməklə hostun əlçatan olub olmadığını yoxlamaq üçün məsuliyyət daşıyır.
- Host yoxlamaq (Host Checker) : Hostun köçürülməsinin mümkünlüyünün yoxlaması və ARP sorğularının qarşısını alınması.

FlowSec: SDN idarəedisinə DoS hücumların qarşısının alınması üçün FlowSec strategiyası da irəli sürülüb. FlowSec idarəedicinin ötürmə qabiliyyətinin yığılan statistikasını dinamik olaraq hesablayır. Əgər hücum aşkar edilərsə, kommutatorun ümumi statistikasına cavabdeh olan Floodlight modulundan istifadə edərək kommutatoru yavaşlamağa məcbur edir.

FloodGuard: FloodGuard iki yanaşma əsasında işləyir. Birinci yanaşma, aktiv bir axın qaydası analizatorudur. Dinamik proaktiv axın qaydaları yaratmaq və bu qaydaları verilənlərin ötürülməsi səviyyəsində kommutatora yükləməklə şəbəkə siyasətinin qorunması üçün verilmişdir. İkinci yanaşma paketin köçürülməsidir. İdarəedicinin işini davam etdirmək üçün Round-Robin alqoritmindən istifadə edərək daşqın paketlərini tutduqdan sonra OpenFlow idarəedicisinə ötürmək üçün istifadə olunur.

FlowTrApp: Data mərkəzə aşağı və yüksək dərəcəli DDoS hücumunu aşkar edir və yüngülləşdirir. Gələn hücum trafikini ardıcıl axın qaydaları ilə uyğunlaşdıraraq təsnif edir.

TopoGuard: TopoGuard, şəbəkə hücumlarını üçün real vaxt rejimində aşkarlanmasını təmin edən təhlükəsizlik vasitəsidir.

SDN şəbəkəsinə olan hücumlara qarşı əks tədbirlərdən bəhs edildi. Bu əks tədbirlər tədqiqatçılar üçün ən yeni üsullar, o cümlədən quruluşlar və həllər barədə biliklərə sahib olmaq, OpenFlow idarəedicisinə əsaslanaraq SDN şəbəkəsinə olan təhdidlərə yeni əks tədbirlər hazırlamağa çalışmaq üçün daha faydalıdır. OpenFlow və SDN şəbəkə monitorinqini böyük dərəcədə asanlaşdıracağını və proqramlaşdırılmış şəbəkələri tətbiq etməklə şəbəkəyə yeniliklər qatacağını vəd edir. Beləliklə, bu, tədqiqatçılara digər təhlükəsizlik məsələlərini yüngülləşdirməyə və inkişafını asanlaşdırmağa kömək edir [8–10].

NƏTİCƏ

SDN idarəetmə və verilənlərin ötürülməsi səviyyələrinə ayrılmaqla, şəbəkə idarəçiliyini asanlaşdırır və bəzi yeni qaydalar və siyasətləri tətbiq etmək üçün xarici tətbiqetmələrdən istifadə şəbəkənin proqramla idarə olunmasını artırır. Şəbəkənin mərkəzləşdirilməsi və proqramlılığı təhlükəsizlik məsələlərinə diqqəti dahada artırır. OpenFlow SDN – də tətbiq olunan ən son protokoldur. Bu məqalədə OpenFlow idarəedici əsaslı SDN şəbəkəsinin təhlükəsizlik məsələlərinə baxdıq. SDN təhlükəsizlik hücumlarını dəf etmək üçün müxtəlif üsullardan bəhs etdik və bu üsullardan düzgün metodun seçilib tətbiq olunmasını müzakirə etdik.

İSTİNADLAR

[1] B. A. A. Nunes, M.Mendonca, X.-N. Nguyen, K. Obraczka, and T. Turletti, “A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks”, IEEE Communications Surveys & Tutorials, Vol. 16, Issue: 3, 2014, pp. 1617-1634.

[2] S. Sezer, B. Fraser, D. Lake, “Are We Ready for SDN? Implementation Challenges for Software-Defined Networks”, IEEE Communications Magazine, Vol. 51, Issue: 7, 2013, pp. 36-43.

[3] Shu Z., Wan J., Di Li, “Security in Software-Defined Networking: Threats and Countermeasures”, Mobile Network and Applications, Vol. 21, No. 8, 2016, pp. 764-776.

[4] W. Li, W. Meng, L. F. Kwok, “A Survey on OpenFlow-based Software Defined Networks: Security Challenges and Countermeasures”, Journal of Network and Computer Applications, Vol. 68, 2016, pp. 126-139.

[5] S. Hong, L. Xu, H.Wang, G. Gu, “Poisoning Network Visibility in Sof tware-Defined Networks: New Attacks and Countermeasures”, In: Proceedings of NDSS, San Diego, 2015, pp.126-139.

[6] S. Shin, G. GU, “Attacking Software-Defined Networks: A First Feasibility Study”, In: Proceedings of the 2ndWorkshop on Hot topics in Software Defined Networks (HotSDN), Hong Kong, 2013, pp. 165-166.

[7] A. Tootoonchian, Y. Ganjali, “HyperFlow: A DistributedControl Plane for OpenFlow”, In: Proceedings of the Internet Network Management Workshop/Workshop on Research on Enterprise Networking (INM/WREN), San Jose, 2010, pp. 1-6.

[8] L. Dridi, M. Faten Zhani, “SDN-Guard: DoS Attacks Mitigation in SDN Networks”, 5th IEEE International Conference on Cloud Networking, 2016, pp. 212-217

[9] Tri-Hai Nguyen, M. Yoo, “Attacks on Host Tracker in SDN Controller: Investigation and Prevention”, Information and Communication Technology Convergence (ICTC), International Conference, 2016, pp. 610-612.

[10] N. Gude, T. Koponen and J. Pettit, “NOX: Towards an Operating System for Networks”, ACM SIGCOMM Computer Communication Review archive Vol. 38 Issue 3, 2008, pp. 105-110.

SECURITY ISSUES AND SOLUTIONS AT SDN TECHNOLOGY LEVELS

Orkhan Mansimzada

Institute of Information Technology of ANAS, Baku, Azerbaijan

orxan@iit.science.az

Abstract– Software defined network technology (SDN) as a networking software implements future network architecture in traditional networks.SDN offers promising opportunities for network management in terms of simplicity, programming and flexibility. One of the most important issues facing SDN technology is security. This article provides an overview of security solutions of SDN technology and solutions which is build based on OpenFlow. Detailed information on network attacks based on SDN technology and the methods used to protect justify these attacks are provided.

Keywords– *SDN, OpenFlow, network, DoS*