Əşyaların İnterneti texnologiyaları əsasında yaradılan şəbəkə mühitində hücumların təhlili

Məmməd Həşimov
İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
mamedhashimov@gmail.com

***Xülasə*— Məqalədə əşyaların İnternetinin (IoT) bəzi təhlükəsizlik məsələləri araşdırılmışdır. IoT qurğuları vasitəsi ilə həyata keçirilən hücümlar göstərilmişdir. IoT şəbəkəsində istifadə olunan mövcud qurğularda yüksək təhlükəsizliy həllərinin tətbiq edilə bilməməsi ilə bağlı məhdudiyyətlər təhlil edilmişdir. IoT şəbəkəsinin təhlükəsiz fəaliyyət göstərməsinə təsir edən hücumların təsnifatı verilmişdir.**

Açar sözlər— əşyaların İnterneti (IoT), IoT təhlükəsizliyi, IoT qurğuları, IoT hücumları.

I. GIRIŞ

Hazırda internet, insanların gündəlik həyatının ayrılmaz bir hissəsinə çevrilmişdir. İnternetdən istifadə insanlar arasındakı ünsiyyəti, məlumat paylaşmasını və qarşılıqlı təsiri artıraraq gündəlik həyatımızı əhəmiyyətli ölçüdə dəyişdirdiyi artıq qaçılmaz bir gerçəklikdir. Bizi əhatə edən bütün faydalı əşyaların İnternet şəbəkəsinə qoşulması “Əşyaların İnterneti” terminin (ing, Internet of Things, IoT) yaradılmasına gətirib çıxarmışdır. IoT şəbəkəsində təkcə insanlarla əşyalar arasında deyil, həmçinin əşyaların öz aralarında da qarşılıqlı əlaqələrinin qurulması nəzərdə tutulur [1]. IoT konsepsiyasının mahiyyəti ondan ibarətdir ki, bizi əhatə edən predmet və ya əşyalar (planşet, smartfon, fitnes üçün qurğu, ev avadanlıqları, geyimlər, avtomobillər, istehsal avadanlıqları, tibbi avadanlıqlar, dərman preparatları və s.) miniatür identifikasiya və sensor (həssas) qurğularla təmin olunaraq naqilli və naqilsiz əlaqələr (sputnik, mobil əlaqə, Wi-Fi və Bluetooth) vasitəsilə qarşılıqlı əlaqədə olur və proseslərin tamamilə avtomatik yerinə yetirilməsini təmin edir [2].

IoT Dünya İqtisadi Forumunun qiymətləndirməsində dünyanı dəyişdirəcək texnologiyalar arasında ilk sıralarda yer alır və bu texnologiyanın yaxın 10 ildə dünya iqtisadiyyatında əsas trend olacağı proqnozlaşdırılır. IoT qurğularının sayı 2017-ci ildə 31% artaraq 8.4 milyarda çatmış və 2020-ci ildə bu sayın 30 milyarda çatacağı gözlənilir [3].

IoT texnologiyası əsasən aşağıdakı sahələrdə tətbiq edilir və yaxın onilliklər ərzində bizi əhatə edən hər şeyə təsir edəcəyi gözlənilir [4]:

- neft-qaz sənayesi: neft məhsullarının kəşfiyyatı, hasilatı, emalı, nəqli və satışı proseslərinin idarə edilməsi;
- şəhərlərdə: nəqliyyatın idarə edilməsi, işıqlandırma, dayanacaq, ağıllı ofis binaları, tullantıların idarə edilməsi;
- avtomobillərdə: prediktiv texniki təminat, toqquşmanın qarşısının alınması, öz-özünü idarə edən vasitələr;
- enerji istehsalı və paylanmasında: smart qrid, mikroqrid, elektrik stansiyalarının idarəetmə sistemləri;
- kənd təsərrüfatında: səmərəli hasilat, suvarma və gübrələmə;
- ətraf mühitdə: meşə yanğınlarının əvvəlcədən aşkarlanması, nəsli kəsilməkdə olan heyvanların izlənilməsi;
- tibdə: məsafədən diaqnostika, yaşlı və xəstə insanların monitorinqi;
- və s.

IoT tətbiqləri və qurğularının sürətlə artması ilə yanaşı, kiber hücumlar da təkmilləşdirilərək təhlükəsizlik və məxfilik ilə əlaqədar daha da ciddi təhdidlər yaradır. Bu qurğuların əksəriyyəti kiber hücumlara qarşı dayanıqsızdır. Belə qurğular hakerlər üçün mühüm əhəmiyyət kəsb etməyə bilər. Ancaq hakerlər ciddi sistemlərə hücum məqsədilə botnetlərin (“robot” və “network” sözlərinin birləşməsindən yaranmışdır, zərərli proqramlarla yoluxmuş və bədniyyətli tərəfindən idarə edilə bilən kompüterlər şəbəkəsidir [5]) yaradılması üçün belə qurğulara müdaxilə edirlər.

II. ƏŞYALARIN İNTERNETİNDƏ TƏHLÜKƏSİZLİK MƏSƏLƏLƏRİ

Gündən-günə artan IoT qurğularının yeni növləri geniş yayılmağa başlamışdır, lakin onların təhlükəsizlikə bağlı bir sıra çatışmazlıqları mövcuddur. Məşhur elektron ticarət şirkəti “*Alibaba”-nın* mobil təhlükəsizlik qrupunun apardığı araşdırmalara əsasən, IoT qurğularının proqram təminatının 90%-dən çoxu təhlükəsizlik hücumlarına məruz qalır. Onların 94%-də isə hakerlər tərəfindən asanlıqla istifadə oluna bilən veb interfeyslərində təhlükəsizlik boşluqları vardır [6]. Təhlükəsizlik mütəxəssislərinin fikirlərinə əsasən artıq ağıllı qurğuların təhlükəsizliyi çox ciddi məsələdir, bu, mümkün təhlükə deyil, real təhlükədir [7]. Çox hallarda hakerlər böyük iqtisadi ziyana səbəb olmasalar da fiziki şəxslərin həyatına təhlükə yarada bilən implantasiya qurğularına və ya intellektual avtomobillərə distant olaraq təhlükə törədir. Bundan əlavə, IoT qurğuları sənaye, hərbi və digər əsas sahələrdə geniş istifadə edildiyinə görə, hakerlər ictimai və milli təhlükəsizliyə təhdid hesab edilə bilər.

DOI: 10.25045/NCInfoSec.2018.47

2013-cü ilin dekabr ayında müəssisələrin təhlükəsizliyi ilə məşğul olan Proofpoint şirkətinin tədqiqatçısı ilk IoT botnetini aşkar etmişdir. Proofpoint şirkətinin məlumatına əsasən, burada ağıllı televizorlar, uşaq monitorları və digər ağıllı məişət texnikasından istifadə olunmuşdur [8]. 21 oktyabr 2016-cı il tarixində Domain Name System provayderi olan Dyn-ə qarşı hücum edilmişdi. Həmin hücum nəticəsində GitHub, Twitter və başqaları kimi saytlara giriş dayandırılmışdı [6]. Bu hücum, printer, IP kamera, şəbəkə keçidləri və monitorları və s. daxil olmaqla çoxsaylı IoT qurğularından ibarət olan botnet vasitəsilə həyata keçirilmişdir.

“Kaspersky Lab” şirkətinin mütəxəssisləri tərəfindən hazırlanan hesabata əsasən 2017-ci ilin əvvəlindən ağıllı qurğular üçün zərərli proqramların sayı iki dəfə artıb və hücumların sayı 7 mini ötüb [9]. Kibercinayətkarlar ağıllı qurğuların sistemlərini qırmaqla istifadəçiləri izləyə bilir, onları şantaj edir və hər hansı bir cinayət törətmək üçün onların qurğularından bir vasitə kimi yararlanırlar.

IoT qurğuları və şəbəkələri təbii resurs baxımından məhduddur. Şərti təhlükəsizlik həllərinin IoT əsaslı sistemlərə tətbiq edilə bilməməsi üçün əsas məhdudiyyətlər aşağıdakılardır [10, 11]:

- IoT qurğularında adətən aşağı sürətli Mərkəzi Prosessor (CPU, ing, Central Processing Unit) dan istifadə edildiyindən, bu qurğular daha çox batareya ilə idarə olunurlar. Müasir kriptoqrafik alqoritmlər isə sürətli hesablama tələb etdiyinə görə həmin qurğulara birbaşa ötürülə bilmir.
- Telefon və noutbuklarla müqayisədə, IoT qurğularında yaddaş məhdud həcmdədir. Şərti təhlükəsizlik arxitekturaları isə məhdud yaddaşa malik qurğular üçün nəzərdə tutulmamışdır.
- IoT qurğuları adətən rabitə qurmaq üçün aşağı səviyyəli rabitə interfeyslərindən istifadə edirlər. Aşağı sürətli kommunikasiya mühiti səbəbindən ənənəvi təhlükəsizlik sxemləri IoT əsaslı sistemlərə tətbiq edilə bilmirlər.
- Mobil IoT qurğuları əvvəlcədən konfiqurasiya edilmədən şəbəkəyə qoşula və ya qəflətən şəbəkəni tərk edə bilər. Şəbəkə topologiyalarında bu tip ani dəyişiklik mövcud təhlükəsizlik sxemlərinin fəaliyyətinə təsir edir. Nəticədə, bu sxemlər IoT mühitinə tətbiq edilə bilməz.
- IoT mühitində qurğular müxtəlif növ naqilsiz protokollardan *(RFID, WiFi, Zigbee, Z-Wave, Bluetooth və s.)* ibarətdir. Mövcud təhlükəsizlik həlləri arasında, müxtəlif qurğulara kompleks həll tapmaq çətindir.

Son zamanlarda IoT qurğularının təhlükəsizliyini təmin etmək üçün bu problemlərə qarşı mübarizə aparmaq, həmin riskləri minimallaşdırmaq və ya aradan qaldırmaq məqsədilə daha yaxşı metodların hazırlanması istiqamətində bir çox tədbirlər həyata keçirilir. Avropa Komissiyası IoT-un kibertəhlükəsizliyinin təmini üçün tədbirlər kompleksi hazırlamağı planlaşdırır [12]. Avropa Birliyinə üzv ölkələr tərəfindən dövlət səviyyəsində qəbul ediləcək qərarlar internetə qoşulma imkanına malik bütün qurğular üçün sertifikatlaşdırma və ya analoji prosedurun tətbiqini nəzərdə tutur.

III. ƏŞYALARIN İNTERNETİ ŞƏBƏKƏSİNƏ OLUNAN HÜCUMLARIN TƏSNİFATI

IoT mühitində baş verə biləcək müxtəlif növ hücumları aşağıdakı kimi qrulaşdırmaq olar [10, 13, 14]:

Hücumların təsirinə görə təsnifatı (ing, Classification of Attack Severities)

- **Yüksək təsirli hücumlar:** bu hücumlar IoT əsaslı sistemi bütövlükdə təhlükə altına sala bilər. Hücum edən autentifikasiya etmədən IoT şəbəkəsinə və sisteminə daxil ola bilər. Bu cür hücumlar məlumatların məxfilik və bütövlüyünü tamamilə poza və IoT xidmətlərini dayandıra bilər.
- **Orta təsirli hücumlar:** bu hücumlar, hücuma məruz qalmış IoT əsaslı sistemin fəaliyyətinin qismən pozulmasına səbəb olur. Hücumlar sistemə yüksək təsir göstərsə də hücum edənin imkanları məhdud olur (məsələn, hücum edən müxtəlif imtiyazlara malik ola bilər, lakin bütün sistemə tam nəzarət edə bilmir).
- **Aşağı təsirli hücumlar:** bu hücumlara kiçik təhdidlər aiddir. Demək olar ki, bütün hallarda, edilən hücum IoT xidmətlərinin təmin edilməsinə təsir göstərmir.

Qurğu əsaslı hücumlar (ing, Attacks Based on Device Property)

- **Aşağı səviyyəli qurğu sinfinə edilən hücumlar:** hücum edən və hədəf IoT qurğusu olub, eyni yaddaş və CPU sürəti kimi oxşar konfiqurasiyalara və imkanlara malikdir. Məsələn, zərərli proqram təminatı ehtiva edən ağıllı saat və ya ağıllı televizora avtorizasiyasız daxil olur, daha sonra ağıllı televizordan spam e-poçtları göndərir.
- **Yüksək səviyyəli qurğu sinfinə edilən hücumlar:** bu zaman, hücum edən qurğu hücum edilən qurğudan daha güclü olur. Hücum edən IoT şəbəkəsinə və ağıllı qurğulara çıxış əldə etmək üçün fərdi kompüterlərdən, dizüstü kompüterlərdən və ya virtual maşın qismində tam təchiz edilmiş qurğulardan istifadə edərək zərərli fəaliyyətlər həyata keçirir.

Məkana bağlı hücumlar (ing, Attacks Based on Adversary Location)

- **Daxili hücum:** hücum edən və hücum edilmiş qurğu eyni şəbəkə daxilindədir. Hücum edən həmin şəbəkə daxilində hər hansı bir komponent tərəfindən hücumlar həyata keçirdir. Məsələn, o, evin təhlükəsizlik sistemini söndürmək üçün qurğular arasında mövcud olan etibarlılıq əlaqələrindən istifadə edərək bir ağıllı qurğudan digərinə keçə bilər.
- **Xarici hücum:** düşmən və hücum edilmiş qurğu müxtəlif şəbəkələrdə yerləşir. Hücum edən hər yerdə yerləşdirilə bilər. Məsələn, düşmən avtorizasiya sisteminin zəifliklərindən istifadə edərək ev şəbəkələrinə distant olaraq daxil olur, daha sonra ağıllı qurğulara hücum etməyə başlayır.

Hücum strategiyalarına əsaslanan hücumlar (ing, Attacks Based on Attack Strategy)

- **Fiziki hücumlar:** bu hücumlar fiziki ziyana səbəb olur, qurğunun xüsusiyyət və konfiqurasiyalarını dəyişir. Məsələn, düşmən qurğuya zərərli kodları və saxta məlumatları daxil etməklə hücum edir.

Zərərli kodun daxil edilməsi hücumu (ing. Malicious code Injection Attacks) – hücum edən cihazın yaddaşına zərərli kodu salmaqla onu idarə edə bilər. Həmin zərərli kod yalnız spesifik funksiyaları yerinə yetirmir, həm də IoT sisteminə hücum edənin çıxışını və hətta onun IoT sisteminə tam nəzarət etməsini təmin edə bilər.

Saxta məlumatın daxil edilməsi hücumları (ing. False Data Injection Attacks) – IoT-dakı qurğuların ələ keçirilməsi ilə, hücum edən həmin qurğudan alınmış normal məlumatların yerinə saxta məlumatlar yerləşdirə və saxta məlumatları IoT tətbiqlərinə ötürə bilər. Saxta məlumatlar alındıqdan sonra, IoT proqramları yanlış əks əlaqə əmrlərini geri göndərə və ya yanlış xidmətlər təqdim edə bilər ki, bu da IoT proqram və şəbəkələrinin effektivliyinə təsir edə bilər.

- **Məntiqi hücumlar:** bu hücumlar IoT qurğusuna heç bir fiziki ziyan vurmadan onların fəaliyyətini dayandırır (yəni hücuma məruz qalmış qurğu real zaman rejimində məlumatların ötürülməsini dayandırır).

Giriş səviyyəsinə əsaslanan hücumlar (ing, Attacks Based on Access Level)

- **Aktiv hücumlar:** hücum edən IoT-un qurğu və şəbəkələrinin normal funksiyasını pozur. Resursların tükənməsi və yüklənməsi kimi müxtəlif növ *xidmətdən imtina hücumları (ing, Deniel-of-service attacks, DoS)* aktiv hücumlar hesab edilir. DoS hücumları şəbəkə protokollarına hücum etməklə və ya şəbəkəni izafi trafiklə yükləməklə IoT sistemlərinin xidmətlərini yararsız hala sala bilir. DoS hücumu ən çox yayılmış hücumlardan biri hesab edilir. DoS hücumları *Ping of Death, TearDrop, UDP, SYN, Land Attack və s.* kimi hücum sxemlərinin vasitəsi ilə yaradılır.
- **Passiv hücumlar:** hücum edən səlahiyyətli IoT qurğusu olub, şəbəkənin funksiyasını pozmadan əlaqə kanalının monitorinqini aparmaqla və trafikini təhlil etməklə etibarlı şəxslərdən məlumat toplamaq üçün qeyri-qanuni fəaliyyət göstərir. Bu növ hücumlar IoT-un məxfiliyinə təhlükə yaradır.

İnformasiya təhlükəsi səviyyəsinə əsaslanan hücumlar (ing, Attacks Based on Information Damage Level)

- **Fasilələr:** fasilələrin yaradılması ilə həyata keçirilən hücumlar IoT xidmətlərinə qarşı edilir. Bu növ hücumlar xidmətin keyfiyyətini aşağı salır və ya onların qanuni istifadəçilər tərəfindən istifadəsinə imkan vermir.
- **Gizli dinləmə:** ücum edən istənilən əlaqə kanalına icazəsiz giriş əldə edir və şəxsi əlaqə vasitəsilə aparılan mesajları "dinləyir". Bu növ hücum məlumatların məxfiliyinə qarşı edilir.
- **Modifikasiya:** bu, hücum edənin məlumatı dəyişdirmək (dəyişiklik, əlavə, silinmə) cəhdidir. Bu növ hücum şəbəkədəki əlaqə kanallarının qarışıqlığına və dəyişik düşməsinə səbəb olur. Modifikasiya hücumları məlumatın bütövlüyünə təhdid hesab edilir.
- **Saxtalaşdırma:** hücum edən saxta məlumat daxil etməklə və ya saxta fəaliyyət göstərməklə kommunikasiyada iştirak edən elementlər arasında qarışıqlıq yaradan mesaj göndərir. Bu növ hücumlar mesajın orijinallığına təhlükə yaradır.
- **Ortada adam hücumu *(ing, Man-in-the-middle Attack):*** hücum edən autentifikasiya olunan və autentifikasiya edən qurğular arasında yerləşərək onlar arasında ötürülən verilənləri ələ keçirə və dəyişə bilər. Həmin iki normal qurğu araya daxil olan qurğunu aşkar edə bilmir və hətta bir-birləri ilə birbaşa ünsiyyət qurduqlarını ehtimal edirlər. Bu hücum iki normal qurğu arasındakı əlaqəni izləmək, dinləmək, təhrif etmək və nəzarət etməklə IoT-dakı məlumatların gizliliyini, bütövlüyünü və məxfiliyini poza bilər.

Host əsaslı hücumlar (ing, Host Based Attacks)

- **İstifadəçi təhdidləri:** istifadəçilər şəxsi məlumatlarını (ad və ya doğum tarixi) və ya təhlükəsizlik məlumatlarını (açar, şifrə) qeyri-təhlükəsiz vasitələrlə təqdim etməyə təhrik edilirlər. Şifrələnməmiş mesajların və zəif kriptoqrafik sxemlərin qeyri-təhlükəsiz vasitələrlə ötürülməsi istifadəçilərə qarşı edilən hücumlara səbəb olur.
- **Proqram təminatına təhdid:** hücum edən IoT qurğularının proqram təminatının boşluqlarından istifadə edir. Məsələn, hər hansı zərərli qurğu hücum edilən qurğuya dayanmadan əlaqə sorğusu göndərməklə onu "donmuş" vəziyyətə salır. Bu proses hücum edilən qurğunun hücum edən qurğunu bloka salmaq kimi xüsusiyyətə malik olmadığı halda baş verə bilər.
- **Texniki təminata təhdid:** verilənlər, açar və proqram kodları kimi həssas məlumatlar IoT qurğusunun özündə saxlanılır. Hücum edən fiziki qurğuya giriş tələb edən texniki təminatı təhrif edərək həmin sənədləri əldə edir. O, müəyyən qurğu üzərində mikro yoxlama və əks mühəndislik kimi zərərli fəaliyyətlər həyata keçirir.

NƏTİCƏ

IoT gündəlik həyatımızda bizi böyük faydaları ilə təmin etsə də, müxtəlif təhlükəsizlik təhdidlərinə meyillidir. Bu texnologiyanın geniş yayılması və tətbiqi ilə bağlı ən mühüm problemlərdən biri də məhz təhlükəsizlik məsələləridir. Əsasən istifadə edilən "əşyaların" (qurğuların) minimal yaddaş həcmi, aşağı sürətli CPU-dan istifadə edilməsi, naqilsiz şəbəkə protokolları vasitəsilə əlaqə qurulması, obyektlərin fiziki əlyetərliyi və sistemlərin açıq olması nəticəsində təhlükəsizlik hücumları IoT üçün daha da böyük problemə çevrilir. Kibercinayətkarların da bu cür boşluqlardan faydalanması təhlükəsizlik problemlərinin həllini daha da mürəkkəbləşdirir. İnternetə qoşulmuş qurğuların hücumlara qarşı müdafiəsini təmin etmək üçün həmin riskləri minimallaşdırmaq və ya aradan qaldırmaq məqsədilə daha yaxşı və müasir metodların işlənilib hazırlanmasına ehtiyac vardır.

ƏDƏBİYYAT

[1] R.M. Əliquliyev, R.Ş. Mahmudov, Əşyaların İnterneti: mahiyyəti, imkanlari və problemləri, İnformasiya cəmiyyəti problemləri, 2011, №2(4), s.29-40.
[2] M.H. Məmmədova, Z.Q. Cəbrayılova, Dəniz neft platformasinda personalin fizioloji vəziyyətinin və coğrafi mövqeyinin monitorinqində əşyalarin internetinin imkanlari, 2018, №2, s.3-17.
[3] Report-internet of things. http://reports.weforum.org/industrial-internet-of-things/general-findings/2-1-the-state-of-the-market/
[4] C.R. Baudoin. Deploying the Industrial Internet in Oil & Gas: Challenges and Opportunities // Society of Petroleum Engineers, 2016, pp.1-11.
[5] Y.N. İmamverdiyev, G.B. Qarayeva, Botnetlər və onların aşkarlanması üsulları, İnformasiya texnologiyaları problemləri, 2017, №1,s.100–111.
[6] W.Zhou, Y.Jia, A.Peng, Y.Zhang, P.Liu, The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved, IEEE Internet of Things Journal, 2015.
[7] Malware ‘loving’ smart devices. www.pressreader.com/uae/khaleej times/20170708/282497183695817
[8] Y.Yang, L.Wu, G.Yin, L.Li and H.Zhao, A Survey on Security and Privacy Issues in Internet-of-Things, IEEE Internet of Things Journal, 2017, vol.4, issue.5, pp. 1250– 1258.
[9] Ловушки «интернета вещей». https://securelist.ru/honeypots-and-the-internet-of-things/30874/
[10] A.Haritha, A.Lavanya, Internet of Things: Security Issues, International Journal of Engineering Science Invention, 2017, vol. 6 Issue 11, pp. 45-52.
[11] L.S. Sayana, B.K. Joshi, Securıty Issues ın Internet of Thıngs, UGC Sponsored National Conference on Global Challenges – Role of Sciences & Technology in Imparting their Solutions (GCRSTS 2016), April 2016.
[12] How the EU cybersecurity act could set standards that impact legal liability and cross-border data flows. https://www.itproportal.com/features/how-the-eu-cybersecurity-act could-set-standards-that-impact-legal-liability-and-cross-border-data-flows/
[13] M.Nawir, A.Amir, N.Yaakob, O.B.Lynn, Internet of Things (IoT): Taxonomy of Security Attacks, 3rd International Conference on Electronic Design (ICED), pp. 321-326. August 11-12, 2016.
[14] J.Deogirikar, A.Vidhate, Security Attacks in IoT: A Survey, International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC 2017), pp. 32-37, 2017.

ANALYSIS OF THE ATTACKS TO NETWORK ENVIRONMENT BASED ON IoT TECHNOLOGY

Mammad Hashimov
Institute of Information Technology of ANAS, Baku,
mamedhashimov@gmail.com

Abstarct - The article examines the some safety issues of the Internet of Things (IOT). It highlights the attacks through IoT devices. It analyzes the restrictions related to the unavailability of applying high-security sollutions in existing IoT devices used in IoT networks. The article also classifies the attacks affecting the safe functioning of IoT network.

Keywords - Internet of Things (IoT), IoT security, IoT devices, IoT attacks.