Əşyaların İnternetinin təhlükəsizlik məsələləri

Məmməd Həşimov
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
mhashimov@iit.ab.az

***Xülasə*— Əşyaların interneti dedikdə müxtəlif əşyaların internet üzərindən bir-birilə əlaqə qura bilməsi başa düşülür. Bunun üçün müxtəlif arxitektur səviyyələrindən istifadə olunur. Məqalədə əşyaların internetinin arxitekturası təhlil edilmiş və əsas səviyyələri (sensor, şəbəkə, tətbiqi) haqqında məlumat verilmişdir. Qeyd edilən səviyyələrdə meydana çıxan bir sıra təhlükəsizlik məsələləri analiz edilmiş və onların həlli yolları göstərilmişdir.**

Açar sözlər*— *əşyaların interneti, əşyaların internetinin arxitekturası, sensor səviyyəsi, şəbəkə səviyyəsi, tətbiqi səviyyə, əşyaların internetinin təhlükəsizliyi, virus.

I. GİRİŞ

İnternet sürətlə inkişaf etməklə, əhatə dairəsini genişləndirməklə, bütün fəaliyyət sferalarına daha dərindən nüfuz etməklə insan həyatına hər gün yeni reallıqlar bəxş etməkdədir [1]. Hazırda internet, insanların gündəlik həyatlarının ayrılmaz bir hissəsinə çevrilmişdir. İnternet istifadəsinin insanlar arasındakı ünsiyyəti, məlumat paylaşmasını və qarşılıqlı təsiri artıraraq gündəlik həyatımızı əhəmiyyətli ölçüdə dəyişdirdiyi artıq qaçılmaz bir gerçəklikdir. Bizi əhatə edən bütün faydalı əşyaların (məişət avadanlıqlarının, elektrik cihazlarının, gündəlik istehlak mallarının, nəqliyyat vasitələrinin, istehsal qurğularının, əmək alətlərinin, informasiya daşıyıcılarının, tibbi ləvazimatların, mühafizə və nəzarət sistemlərinin, bitki və heyvanat aləminin) İnternet şəbəkəsinə qoşulması “Əşyaların İnterneti” termininin (*Internet of Things – IoT)* yaradılmasına gətirib çıxarmışdır [1]. Əşyaların İnterneti (Əİ) bizi sürətlə “ağıllı məhsullar”ın bütünlüklə həyatımıza tətbiqinə aparır. Bu gün özümüz də dərk etmədən televizorların, evlərin, sənaye avadanlıqlarının internetə qoşulduğunu görürük. Onlar öz aralarında məlumatları mübadilə edir və bizə göndərirlər. Bunlar həyatımızın rahatlığını təmin edir. Hətta smartfonlar belə internetə qoşularaq öz aralarında şəbəkələr yaradırlar[2].

Əİ-nə artıq gündəlik həyatımızın hər bir fəaliyyət sahəsində rast gəlinir. Onlardan əsasən ev, xəstəxana və digər yerlərdə baş verən dəyişikliklərin distant olaraq idarə olunması, yanğınların qarşısının alınması və digər faydalı funksionallığın təmin edilməsi məqsədi ilə istifadə olunur [3]. Əgər hər hansı bir qurğu və ya obyekt internetə qoşula bilirsə onu “Əşyaların İnterneti”-nin bir hissəsi hesab etmək olar. Təəssüf ki, bu qurğuların və əlavələrin (proqramların) əksəriyyəti hakerlər tərəfindən hədəfə çevrilirlər. Aparılan qiymətləndirmələrə əsasən, Əİ cihazlarının 70%-na hücum etmək çox asan olduğu qeyd olunur [4]. Buna görə də, internetə qoşulmuş cihazların hücumlara qarşı müdafiəsini təmin etmək üçün səmərəli bir mexanizmə ehtiyac vardır. Hazırda Əİ cihazlarının təhlükəsizliyini təmin etmək üçün bu problemlərə qarşı mübarizə aparmaq, həmin riskləri minimallaşdırmaq və ya aradan qaldırmaq məqsədilə daha yaxşı metodların hazırlanması istiqamətində bir çox araşdırmalar aparılır.

II. ƏŞYALARIN İNTERNETİNİN ARXİTEKTURASI

Əİ elektronika, proqram təminatı, sensor və İnternet vasitəsilə məlumatların toplanması və mübadiləsini həyata keçirən "əşyalar" toplusudur [4]. Əİ müxtəlif əşyaların insan müdaxiləsi olmadan bir-biri ilə IP qoşulması üzərindən qarşılıqlı əlaqəyə girdiyi şəbəkədir. Əİ-nin əsas xüsusiyyəti onların insan iştirakı olmadan avtonom işləməsidir.

“Əşyaların İnterneti” termini ilk dəfə 1999-cu ildə MİT Avto-İD mərkəzinin təsisçisi və icraçı direktoru Kevin Eşton tərəfindən işlədilib [5]. “Əşyaların İnterneti” termini 2005-ci ildə Beynəlxalq Telekommunikasiya İttifaqının analitiklər qrupunun İnternetin vəziyyətinə həsr olunmuş hesabatında işlədildikdən sonra diqqəti cəlb etməyə başladı [1].

Beynəlxalq Verilənlər Korporasiyasının (IDC) 2013-cü il üçün təqdim etdiyi hesabatına əsasən, istifadə olunan Əİ cihazlarının sayının 2020-ci ildə 41 milyarda çatacağı gözlənilir [3].

Əİ milyardlarla obyektləri internet üzərindən birləşdirmək (əlaqələndirmə) qabiliyyətinə malik olmalıdır, bunun üçün də çevik arxitektur səviyyələrinə ehtiyac var.

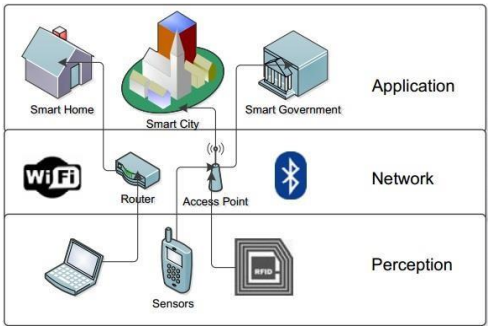
Əİ-də hər bir səviyyə öz funksiyaları və bu səviyyədə istifadə olunan cihazlar ilə müəyyən edilir. Əİ-də səviyyələrin sayı ilə bağlı müxtəlif fikirlər var. Aparılan, bir çox tədqiqatlara əsasən demək olar ki, Əİ əsasən *perception layer* (qavrama və ya sensor səviyyəsi), *network layer* (şəbəkə səviyyəsi) və *application layer* (tətbiqi səviyyə) kimi adlandırılan üç səviyyə üzərində fəaliyyət göstərir [6] (Şəkil1).

Perception layer - qavrama səviyyəsi, həmçinin sensor səviyyəsi kimi də başa düşülür. Sensor səviyyənin əsas məqsədi sensorların köməyi ilə fiziki aləmdən məlumatları toplamaq və mübadilə etməkdən ibarətdir. Bu səviyyə məlumatları (temperatur, səs, vibrasiya, təzyiq və s.) aşkarlayır, toplayır, emal edir və sonra şəbəkə səviyyəsinə ötürür.

Sensor səviyyəsi iki hissəyə bölünür: sensor qovşağı (sensorlar və ya nəzarətçilər və s.) və marşrutlama şəbəkəsi ilə əlaqələndirilmiş sensor şəbəkəsi. Sensor qovşağı məlumatların əldə edilməsi və idarəetməsi üçün istifadə olunur, marşrutlama şəbəkəsi isə alınan məlumatları şəbəkə keçidinə göndərir. Sensor səviyyəsi texnologiyalarına naqilsiz sensor şəbəkələri (WSNs), implantasiya edilə bilən tibbi cihazlar (IMD'ler),

DOI: 10.25045/NCInfoSec.2017.25

Radio Frequency Identification - radiotezlik identifikasiyası (RFID), Global Positioning System - qlobal yerləşdirmə sistemi (GPS) və s. daxildir [3].



Şəkil 1. Əşyaların İnternetinin arxitekturası

Network layer - şəbəkə səviyyəsi, həmçinin ötürücü səviyyə kimi tanınır və Əİ arxitekturunda orta səviyyə kimi tətbiq olunur. Şəbəkə səviyyəsi məlumatların marşrutlaşdırma funksiyasına xidmət edir. Şəbəkə səviyyəsinin vəzifəsi sensor səviyyəsi tərəfindən toplanmış məlumatları qəbul etmək və həmin məlumatları Əİ qurğularına və tətbiqlərinə ötürmək üçün inteqrasiya olunmuş şəbəkələr vasitəsilə marşrutları müəyyən etməkdən ibarətdir [7].

Şəbəkə səviyyəsi Əİ-nin arxitekturunun ən mühüm səviyyəsidir, çünki müxtəlif qurğular (hub), kommutasiya (switching), şlüz (gateway), cloud computing performansı və s., həmçinin müxtəlif kommunikasiya texnologiyaları da (Bluetooth, WiFi, 3G, LTE və s.) bu səviyyədə inteqrasiya olunur.

Application layer - tətbiqi səviyyə, həmçinin biznes səviyyəsi kimi də tanınır və Əİ ən üst səviyyəsi kimi həyata keçirilir. Tətbiqi səviyyə şəbəkə səviyyəsindən ötürülən məlumatları alır və lazımi xidmətləri və əməliyyatları təmin etmək üçün həmin məlumatları istifadə edir. Məsələn, tətbiqi səviyyə alınan məlumatların ehtiyat nüsxələrini verilənlər bazasında saxlamaq üçün xidməti təmin edə bilər və ya fiziki qurğuların gələcək vəziyyətini proqnozlaşdırmaq üçün alınan məlumatların qiymətləndirməsini həyata keçirə bilər. Bu səviyyədə müxtəlif tələblərə malik bir sıra tətbiqlər mövcuddur. Misal olaraq smart şəbəkə, smart nəqliyyat, ağıllı şəhərlər və s. daxildir. Tətbiqi səviyyə məlumatların həqiqiliyini, tamlığını və gizliliyini təmin edir. Bu səviyyədə məqsəd ağıllı bir mühitin yaradılmasının təmin edilməsidir [8].

III. ƏŞYALARIN İNTERNETİNİN TƏHLÜKƏSİZLİYİ

Əşyaların interneti ilə ənənəvi İnternet arasındakı fərq burada insanın rolunun olmamasından ibarətdir. Əİ qurğuları fərdin davranışları haqqında məlumatı toplaya, təhlil edə və tədbir görə bilir [3]. Əİ tətbiqləri ilə təmin edilən xidmətlər insan həyatına böyük fayda verməklə yanaşı fərdi məxfilik və təhlükəsizliyi böyük riskə ata bilər.

Əİ istehsalçıları həmin qurğulara dayanıqlı təhlükəsizlik sistemini tətbiq edə bilmədikləri səbəbindən təhlükəsizlik sahəsinin mütəxəssisləri İnternet bağlantısı olan çoxsaylı təhlükəli cihazların potensial riskləri barəsində bir neçə dəfə xəbərdarlıq etmişlər. 2013-cü ilin dekabr ayında müəssisələrintəhlükəsizliyi ilə məşğul olan Proofpoint şirkətinin tədqiqatçısı ilk Əİ botnetini (“robot” və “network” sözlərinin birləşməsindən yaranmışdır, zərərli proqramlarla yoluxmuş və bədniyyətli tərəfindən idarə edilə bilən kompüterlər şəbəkəsidir [9]) aşkar etmişdir. Proofpoint şirkətinin məlumatına əsasən, botnetin 25 faizindən çoxu kompüterlərdən başqa, ağıllı televizorlar, uşaq monitorları və digər məişət texnikasıdan ibarət idi [3].

Əİ-nin arxitekturunun hər bir səviyyəsi təhlükəsizlik təhdidlərinə və hücumlarına qarşı həssasdır. Bu hücumlar aktiv və ya passiv ola bilər, xarici mənbələrdən və daxili şəbəkədən təşkil edilən hücum nəticəsində meydana gələ bilər. Aktiv hücum birbaşa xidməti dayandırır, passiv hücum isə xidməti dayandırmadan şəbəkə məlumatlarına nəzarət edir. Hər bir səviyyədə Əİ-nin cihaz və xidmətləri DoS hücumlarına qarşı həssasdır. Bu növ hücumlar səlahiyyətli istifadəçilərin cihaz, resurs və ya şəbəkədən istifadəsini əngəlləyir [8]. Aşağıdakı bölmələrdə hər bir səviyyə üzrə təhlükəsizlik məsələlərinin ətraflı təhlili verilmişdir.

Sensor səviyyəsinin təhlükəsizlik məsələləri.

Sensor səviyyəsində üç təhlükəsizlik məsələsi mövcuddur [8]. Birinci məsələ naqilsiz siqnalların gücü ilə əlaqədardır. Siqnallar əsasən sensor qovşaqları arasında naqilsiz texnologiyaların istifadəsi ilə ötürülür. Bu zaman effektivlik kənar dalğalar tərəfindən təhlükəyə məruz qala bilər. İkinci məsələ Əİ-nin cihazlarındakı sensor qovşağına yalnız sahibi tərəfindən deyil, həm də hücumçular tərəfindən müdaxilə oluna bilməsi ilə əlqədardır. Belə ki, qovşaqların xarici və açıq mühitlərdə fəaliyyət göstərməsi sensor və cihazların fiziki hücumlara məruz qalmasına səbəb olur. Bu isə hücumçuların avadanlıqların aparat təminatının komponentlərinə müdaxiləsi ilə nəticələnə bilir. Üçüncü məsələ isə şəbəkə topologiyasının xarakterik cəhəti olan dinamikliyi ilə əlaqədardır. Belə ki, Əİ qovşaqlarının yeri tez-tez dəyişdirilir. Əİ sensor səviyyəsi əsasən sensorlar və RFID-lərdən ibarətdir. Onların saxlama qabiliyyəti, enerji istehlakı və hesablama qabiliyyəti çox məhdud olduğundan bir çox təhdid və hücumlara qarşı həssas olur.

Node Capture Attacks (Qovşağın tutulma hücumu). Bir çox qurğular ərazilərdə statik şəkildə yerləşdirilir, bu da onların fiziki cəhətdən təhlükəyə məruz qalmasına səbəb ola bilər [10]. Hər hansı bir qovşaq hücuma məruz qalarsa, mühüm məlumatlar (qrupun rabitə açarı, radio açarı, uyğunluq siqnalı və s.) hücum edən tərəfindən ələ keçirilə bilər. Hücum edən, həmçinin ələ keçirilən qovşaqla bağlı bütün vacib məlumatları ziyanlı qovşağa köçürə bilər və daha sonra, Əİ şəbəkəsinə və ya sisteminə qoşulmaq məqsədilə ziyanlı qovşağı icazəli qovşaq kimi göstərə bilər. Bu hücum, qovşağın replikasiya hücumu olaraq da ifadə edilir. Qovşaq tutma hücumu şəbəkəyə ciddi təsir göstərə bilər. Belə hücumlardan qorunmaq üçün zərərli qovşaqların monitorinqi və aşkar edilməsi sahəsində effektiv sxemlər öyrənilməlidir.

Malicious code Injection Attacks (Zərərli kodun daxil edilməsi hücumu) – Qovşağın tutulma hücumuna əlavə olaraq, hücum edən cihazın yaddaşına zərərli kodu salmaqla onu idarə edə bilər. Həmin zərərli kod yalnız spesifik funksiyaları yerinə yetirmir, həm də Əİ sisteminə hücum edənin çıxışını təmin edə

və hətta onun Əİ sisteminə tam nəzarət etməsini təmin edə bilər [11]. Zərərli kod daxil edilmə hücumundan qorunnmaq üçün, effektiv kod identifikasiyası sxemlərinin layihələndirilməsi və Əİ-yə inteqrasiya edilməsi lazımdır.

False Data Injection Attacks (*Saxta məlumatın daxil edilməsi hücumları)* – Əİ-dəki qovşaq və ya cihazların ələ keçirilməsi ilə, hücum edən tutduğu qovşaq və ya cihazdan alınmış normal məlumatların yerinə saxta məlumatlar yerləşdirə və saxta məlumatları Əİ tətbiqlərinə ötürə bilər. Saxta məlumatlar alındıqdan sonra, Əİ proqramları yanlış əks əlaqə əmrlərini geri göndərə və ya yanlış xidmətlər təqdim edə bilər ki, bu da Əİ proqram və şəbəkələrinin effektivliyinə təsir edə bilər. Belə zərərli hücumdan müdafiə olunmaq üçün yalnış məlumatların Əİ tətbiqləri tərəfindən qəbul edilməzdən əvvəl səmərəli şəkildə təsbit edə və geri ötürə bilən metodlar (saxta məlumatın filtrlənməsi sxemi və s.) hazırlanmalıdır [12].

Sleep Deprivation Attacks (yuxu məhrumetmə hücumu)- Əİ-də əksər qurğu və ya qovşaqların elektrik imkanları az olur. Cihaz və qovşaqların istismar müddətini uzatmaq üçün cihaz və ya qovşaqlar elə proqramlaşdırılmışdır ki, onların enerji istehlakını azaltmaq üçün yuxu rejimini təqib etmək mümkün olsun. Bununla belə, yuxu məhrumetmə hücumu proqramlaşdırılmış yuxu rejimlərini poza bilər ki, bu da həmin qurğunun sönənədək fasiləsiz işləməsinə səbəb ola bilər [10]. Bu cihaz və qovşaqların ömrünü uzatmağın bir həll yolu vardır ki, o da onların xarici mühitdən (günəş, külək və s.) enerji yığa bilmək qabiliyyətləridir.

Şəbəkə səviyyəsinin təhlükəsizlik məsələləri

Əİ-də şəbəkə səviyyəsinin əsas məqsədi toplanmış məlumatların ötürülməsi olduğu üçün, bu səviyyədəki təhlükəsizlik problemləri şəbəkə resurslarının təsirinə əsaslanır. Bundan əlavə, əksər Əİ cihazları naqilsiz rabitə əlaqələri vasitəsilə Əİ şəbəkələrinə qoşulur. Beləliklə, bu səviyyədəki əksər təhlükəsizlik problemləri naqilsiz şəbəkələrlə bağlıdır.

Deniel-of-service attacks (Xidmətdən imtina hücumları) - DoS hücumları şəbəkə protokollarına hücum etməklə və ya şəbəkəni izafi trafiklə yükləməklə Əİ sistemlərinin xidmətlərini yararsız hala sala bilər. DoS hücumu ən çox yayılmış hücumlardan biri hesab edilir. Beləliklə, DoS hücumları, Ping of Death, TearDrop, UDP, SYN, Land Attack və s. kimi hücum sxemlərinin vasitəsi ilə yaradıla bilər [12]. DoS hücumlarından qorunmaq üçün hücum sxemləri əvvəlcə diqqətlə araşdırılmalı və daha sonra Əİ sistemlərinin təhlükəsizliyini təmin etmək məqsədilə hücumların azaldılması üçün effektiv müdafiə sxemləri yaradılmalıdır.

Spoofing attacks (Spufinq hücumlar) - Spufinq hücumlarının məqsədi hücum edənin Əİ sisteminə tam giriş əldə etməsini təmin etmək və sistemə zərərli məlumatlar göndərməkdir. Əİ-dəki spufinq hücumlarına IP spufinq, RFID spufinq və s. nümunə göstərmək olar. IP spufinq hücumunda, hücum edən şəbəkədə mövcud olan digər icazəli qurğulardakı etibarlı IP ünvanını saxtalaşdıra və qeyd edə bilər. Daha sonra isə o, Əİ sisteminə daxil olaraq zərərli məlumatları etibarlı kimi göstərərək onları etibarlı IP ünvanları vasitəsilə göndərə bilər. RFID spufinq hücumunda isə hücum edən etibarlı RFID nişanı haqqında məlumatları gizli saxlaya və qeyd edə və daha sonra həmin etibarlı ID (identification – identifikasiya) nişanı ilə Əİ sisteminə zərərli məlumatlar göndərə bilər [10, 12]. Spufinq hücumlarından müdafiə olunmaq məqsədilə təhlükəsiz etibarlı idarəetmə, identifikasiya və autentifikasiya həllərindən istifadə etmək olar [12].

Sinkhole hücumları - Bu hücum zamanı hücum edən, zərərli qovşağın digər qovşaqlar üçün cəlbedici görünməsini təmin edir. Belə ki, hər hansı konkret qovşaqdan gələn bütün məlumat axını təhlükəli qovşağa yönləndirilir ki, bu da paketlərin düşməsinə səbəb olur, yəni bütün trafik dayandırılır və sistem məlumatın qarşı tərəfdə qəbul olunduğuna inanır [10]. Qeyd etmək lazımdır ki, sinkhole hücumu yalnız çatdırılan məlumatların məxfiliyinin pozulması üçün deyil, həm də əlavə hücumların (DoS hücumu və s.) həyata keçirilməsi üçün təşkil edilə bilər. Bu isə daha çox enerji istehlakına səbəb olur. Sinkhole hücumundan qorunmaq məqsədilə təhlükəsiz marşrutlaşdırma protokolu kimi üsulların araşdırılıb tətbiq edilməsi tələb olunur.

Man-in-the-middle hücumu - Bu halda hücum edən tərəfindən nəzarət edilən zərərli cihaz şəbəkədə iki kommunikasiya qurğusu arasında virtual olaraq yerləşdirilə bilər. Zərərli qurğu iki normal cihazın təsbit məlumatlarını oğurlamaqla, həmin cihazların arasına daxil olub onlar arasında ötürülən bütün məlumatları saxlaya və yönləndirə bilər [13]. Həmin iki normal cihaz araya daxil olan qurğunu aşkar edə bilmir və hətta bir-birləri ilə birbaşa ünsiyyət qurduqlarını ehtimal edirlər. Bu hücum iki normal cihaz arasındakı əlaqəni izləmək, dinləmək, təhrif etmək və nəzarət etməklə Əİ-dəki məlumatların gizliliyini, bütövlüyünü və məxfiliyini poza bilər. Cihazların aparat təminatı vasitəsilə fiziki cəhətdən qovşaqlara edilən hücumlarından fərqli olaraq, qeyd edilən hücum yalnız Əİ şəbəkələrində istifadə olunan rabitə protokollarına əsaslanmaqla həyata keçirilə bilər. Normal cihazların hücum edən tərəfindən müəyyənləşdirilməməsi və əsas məlumatların sızmamasını təmin edən təhlükəsiz rabitə protokolları və əsas idarəetmə sxemləri effektiv müdafiə üsullarına daxildir [12].

Routing Information Attacks (*Marşrutlandırma məlumatları hücumları)* – Bu hücumlar əsasən Əİ sistemlərindəki marşrutlaşdırma protokollarına yönəldilir. Burada marşrutlaşdırma məlumatları hücum edən tərəfindən manipulyasiya edilə və yenidən göndərilərək şəbəkədə qapanma (loop) yarada bilər. Bu isə mənbə ilə bağlı informasiyanın şişməsinə və Əİ şəbəkəsində artan gecikmələrə səbəb ola bilər. Bu hücumdan qorunmaq məqsədilə cihazlar arasında təhlükəsiz əlaqənin yaradılması, həmçinin identifikasiya məlumatı və IP ünvanlarının hücum edənə sızdırılmaması üçün təhlükəsiz marşrutlaşdırma protokollarından və etibarlı idarəetmədən istifadə etmək olar [12].

Sybil Attacks (*Sibil hücumları)* - Sibil hücumu zamanı hər hansı zərərli qurğu, yəni sibil cihaz, şəbəkədəki digər qovşaqlara bir neçə identifikasiya təqdim edir və beləliklə də hücum edən eyni zamanda bir çox yerdə yerləşə bilər [13]. Sibil cihaz bir sıra qanuni identifikatora (şəxsiyyətə) malik olduğundan, sibil cihaz tərəfindən göndərilən yalan məlumatlar qonşu cihazlar tərəfindən asanlıqla qəbul edilə bilər. Bundan əlavə, sibil cihazlarını yönləndirici qovşaq kimi seçən

marşrutlar, bir neçə fərqli kəsişmə yolunun müəyyənləşdirildiyini ehtimal edə bilər. Əslində isə yalnız bir yol müəyyən edilir və ötürülən bütün məlumatların sibil cihazından keçməsi tələb olunur. Sibil hücumlarından qorunmaq üçün Əİ sistemləri üçün təhlükəsiz identifikasiya və autentifikasiya mexanizmləri hazırlanmalıdır.

Unauthorized Access (icazəsiz giriş) – Əİ-də RFID ən mühüm texnologiyalardan biridir. RFID əsaslı qurğuların əksəriyyətinin Əİ-yə inteqrasiya olunduğuna və RFID-lərin əksəriyyətində müvafiq identifikasiya mexanizmlərinin olmadığına görə, hücum edən tərəfindən RFID nişanlarına giriş əldə edilə və orada saxlanılan məlumatlar mənimsənilə, dəyişdirilə və silinə bilər. Beləliklə, Əİ-də RFID əsaslı cihazların icazəli giriş və autentifikasiya mexanizmləri daha da inkişaf etdirilməlidir [12].

Tətbiqi səviyyənin təhlükəsizlik məsələləri -

Tətbiqi səviyyənin əsas məqsədi istifadəçilər tərəfindən göndərilən istənilən sorğunu dəstəkləməkdir. Beləliklə, tətbiqi səviyyədəki problemlər proqram təminatına edilən hücumlarla əlaqəlidir. Tətbiqi səviyyənin bir neçə mümkün problemləri aşağıda verilmişdir:

Phishing Attack (fişinq hücum) – Burada hücum edən virusla yoluxmuş e-poçt və fişinq veb saytları vasitəsilə istifadəçilərin identifikasiya məlumatlarını saxtalaşdırmaqla, istifadəçilərin şəxsiyyət və parol kimi gizli məlumatlarını ələ keçirə bilər [11]. Təhlükəsiz avtorizasiya girişi, identifikasiya və autentifikasiya isə fişinq hücumlarını azalda bilər. Buna baxmayaraq, ən səmərəli yol istifadəçilərin internetdə sörf (gəzərkən) edərkən həmişə diqqətli olmalarıdır [12].

Malicious Virus/worm (təhlükəli virus/soxulcan) - Əİ tətbiqləri üçün digər problemlərdən biri zərərli virus və ya soxulcanlardır. Hücum edən, Əİ proqramlarını zərərli (soxulcan, Troyan atı və s.) viruslar ilə yoluxdurmaqla məxfi məlumatları əldə edə və ya təhrif edə bilər [10]. Əİ proqramlarında zərərli virus və ya soxulcan hücumları ilə mübarizə aparmaq üçün etibarlı firewall, virus aşkarlanması və digər müdafiə mexanizmləri yerləşdirilməlidir.

Malicious Scripts (Zərərli skriptlər) - Əİ sisteminin funksiyalarına zərər vurmaq məqsədi ilə proqram təminatına əlavə edilir, proqram təminatında dəyişikliklər edir və proqram təminatından silinirlər. Bütün Əİ tətbiqləri internetə qoşulduğu üçün, hücum edən zərərli skriptlərlə (java hücum proqramları, aktiv-x skriptlər və s.) İnternet vasitəsilə xidmətlər tələb edən müştəriləri asanlıqla aldada bilər. Zərərli skriptlər gizli məlumatların sızması və hətta, tam bir sistemin bağlanmasına səbəb ola bilər. Zərərli skriptlərdən müdafiə olunmaq üçün Əİ sistemlərində effektiv skript aşkarlama üsulları, honeypot texnikaları da daxil olmaqla, statik kodların və dinamik hərəkətlərin aşkarlanması üsulları tətbiq olunmalıdır [12].

NƏTİCƏ

Rəqəmsallaşan və hər keçən gün daha çox texnologiyanın istifadə edildiyi bir dövrdə bizi əhatə edən bir çox əşyaların internetə qoşulması insanların həyatını getdikcə asanlaşdırmaqdadır. Əşyaların İnterneti gündəlik həyatımızda bizi böyük faydaları ilə təmin etsə də, müxtəlif təhlükəsizlik təhdidlərinə meyllidir. Nəzərə alsaq ki, bu texnologiyanın geniş yayılması və tətbiqi ilə bağlı ən mühüm problemlərdən biri də məhz təhlükəsizlik məsələləridir, hazırda bu istiqamətdə intensiv tədqiqat işləri aparılır. Bu məqsədlə məqalədə əşyaların internetinin arxitekturasının müxtəlif səviyyələrində meydana çıxan bir sıra təhlükəsizlik məsələləri analiz edilmiş və onların həlli yolları göstərilmişdir.

ƏDƏBİYYAT

[1] R.M. Əliquliyev, R.Ş. Mahmudov, Əşyaların İnterneti: mahiyyəti, imkanlari və problemləri, İnformasiya cəmiyyəti problemləri, 2011, №2(4), s.29-40.

[2] http://technimum.com/company/bakcell/blog/5946.html

[3] 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.

[4] M.A. Razzaq, M.A. Qureshi, S.H. Gill and S. Ullah, Security Issues in the Internet of Things (IoT): A Comprehensive Study, International Journal of Advanced Computer Science and Applications, 2017, vol.8, no.6, pp. 383– 388.

[5] http://www.rfidjournal.com/articles/view?4986

[6] C. Suchitra., C.P. Vandana, Internet of Things and Security Issues, International Journal of Computer Science and Mobile Computing, 2016, vol.1, issue.1, pp. 133– 139.

[7] M. Wu, T.l. Lu, F.Y Ling, J. Sun and H.Y. Du, Research on the architecture of Internet of things, 3rd International Conference on Advanced Computer Theory and Engineering, 2010, pp. 484-487.

[8] R. Mahmoud, T. Yousuf, F. Aloul and I. Zualkernan, Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures, The 10th International Conference for Internet Technology and Secured Transactions, 2015, pp. 336-341.

[9] Y.N. İmamverdiyev, G.B. Qarayeva, Botnetlər və onların aşkarlanması üsulları, İnformasiya texnologiyaları problemləri, 2017, №1, s.100–111.

[10] B.Sasikala, M. Rajanarajana, B. Geethavani, Internet of Things: A Survey on Security Issues Analysis and Countermeasures, International Journal Of Engineering And Computer Science, 2017, vol.6, no.5, pp. 21435-21442.

[11] M.U. Farooq, M. Waseem, A. Khairi, S. Mazhar, A Critical Analysis on the Security Concerns of Internet of Things (IoT), International Journal of Computer Applications, 2015, vol.111, no.7, pp. 1-6.

[12] J. Lin, W. Yuy, N. Zhangz, X. Yang, H. Zhangx and W. Zhao, A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications, IEEE Internet of Things Journal, 2017, vol.4, no.5, pp. 1125–1142.

[13] E. Leloglu, A Review of Security Concerns in Internet of Things, Journal of Computer and Communications, 2017, vol.5, 121-136.

SECURITY ISSUES OF THE INTERNET OF THINGS

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

Abstract – The internet o things contains the items (things) can communicate through the internet. Various architecture layers are used for this. This article analyzes the architecture of the internet of things and provides detailed information about the main layers (sensor, network, application). It also explores security issues of the mentioned layers and provides their solution ways.

Keywords – Internet of Things, IoT, architecture of IoT, sensor layer, network layer, application layer, security of IoT