Müasir şəbəkə təhlükəsizliyi və inam problemləri

Ramiz Şıxəliyev
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
ramiz@science.az

***Xülasə* — Məqalədə müasir şəbəkə təhlükəsizliyi və inam məsələləri analiz olunmuşdur. Əsasən, İnternetdə mövcud olan yeni şəbəkə xidmətlərinin təhlükəsizlik və inam məsələləri analiz edilmişdir. Xüsusilə də bulud hesablamaları, əşyaların İnerneti və sosial şəbəkə xidmətlərində meydana çıxan təhlükəsizlik məsələləri analiz edilmişdir.**

Açar sözlər — şəbəkə təhlükəsizliyi, şəbəkə xidmətləri, bulud hesablamaları, əşyaların İnterneti, sosial şəbəkə xidmətləri

I. GİRİŞ

Bu gün fərdlərin, təşkilatların və dövlətlərin mövcud şəbəkə infrastukturundan, xüsusilə də İnternetdən asılılığı artıq təsdiq olunmuş faktdır. Xüsusilə də, onlar şəbəkə infrastrukturunun təhlükəsizliyi və inam dərəcəsindən çox asılıdırlar. Çünki, hücumların, təhlükələrin, verilənlərin oğurlanması və xidmətlərin dayanması hallarının tez-tez baş verməsi onların normal fəaliyyətini pozur. Bununla yanaşı, qlobal əlaqələrin genişlənməsi, xüsusilə İnternetin genişlənməsi, mobil İnternetin, naqilsiz şəbəkələrin, IoT (Internet of Things), Cloud Computing, Grid Computing, sosial şəbək xidmətlərinin (SŞX) və s. müxtəlif şəbəkə xidmətlərinin və tətbiqlərinin, həmçinin yeni protokolların yaranması ayrı-ayrı fərdlər və təşkilatlar arasında qarşılıqlı əlaqəni genişləndirmiş və dərinləşdirmişdir. Nəticədə fərdlər və təşkilatlar informasiyanın saxlanılması və ötürülməsi sistemlərindən tam asılı vəziyyətə düşmüşdür.

İlk hesablama sistemlərinin işinə kompüter təhlükəsizliyinin təsir etməsinə baxmayaraq, o, bilik sahəsi kimi 1970-ci illərin əvvəllərində öyrənilməyə başlanımışdır. Ənənəvi olaraq, kompüter təhlükəsizliyinin əsas məqsədi informasiyanın və sistemin resurslarının məxfiliyinin, bütövlüyünün və əlyetərliyinin təmin edilməsi idi. Bu zaman məxfiliyin təmin edilməsinin məqsədi informasiya və resurslara ancaq icazəsi olan şəxslərin girişinin təmin edilməsindən ibarət idi. Bütövlüyün təmin edilməsinin məqsədi informasiyanın saxlanıması və ötürülməsi zamanı saxtalaşdırılmasının qarşısının alınması idi. Əlyetərliyin məqsədi isə istənilən zaman səlahiyyətli şəxlərin informasiyaya və resurslara girişinin təmin edilməsi idi.

İnternet yaranana qədər, ənənəvi təhlükəsizlik modelləri və mexanizmləri qapalı hesablama sistemləri üçün nəzərdə tutulmuşdur və əsasən sistemin perimetri daxilində təhlükəsizliyini təmin edirdi. Bu zaman sistemin təhlükəsizlik perimetri daxilində ümumi təhlükəsizlik infrastrukturu və təhlükəsizlik siyasəti istifadə edilirdi.

Lakin bu gün İnternetin geniş istifadəsi, şəbəkələrin funksionallığının genişləndirməsi, infrastrukturunun dəyişməsi, dinamikliyi, istifadə edilən texnologiyaların müxtəlifliyi ənənvi mono-texnoloji təhlükəsizlik paradiqmasının istifadəsini qeyri-mümkün edir və şəbəkələrə inamı azaldır. Çünki bu gün şəbəkə təhlükəsizliyində əsaslı trendlər baş verir [1]. Buna görə də, mövcud şəbəkə infrastrukturuna və şəbəkələrin funksionallığına müvafiq olaraq yeni şəbəkə təhlükəsizliyi paradiqmasının yaradılması və şəbəkələrin təhlükəsizliyinə inamın artırılması və bunun üçün multi-texnoloji təhlükəsizlik paradiqmasının yaradılması çox aktual məsələdir.

İnam (ing. trustworthy) bir konsepsiya olaraq təhlükəsizliklə bərabər şəbəkələrin gözlənilən (normal) fəaliyyətinə təminat verən dayanıqlıq və digər xüsusiyyətləri əhatə edir. İnamlı şəbəkə termininin mənası Avropa Birliyinin FP7 tədqiqat proqramında daha dəqiq göstərilmişdir və şəbəkənin inamlı qəbul edilməsi üçün o, təhlükəsiz, hücumlara və dayanmalara qarşı etibarlı və dayanıqlı olmalıdır [2]. Bundan başqa, xidmət keyfiyyəti təmin olunmalıdır, kofidensiallıq təmin edilməklə istifadəçi verilənləri mühafizə edilməlidir və bunun üçün istifadəçilərin verilənlərin təhlükəsizliyinin idarə edilməsində iştirakı üçün faydalı və etibarlı alətlər təmin edilməlidir.

Təqdim edilən məqalənin əsas məqsədi müasir şəbəkə təhlükəsizliyi və inam məsələlərinin analizidir.

II. ŞƏBƏKƏ TƏHLÜKƏSİZLİYİ VƏ İNAM

Ümumiyyətlə, şəbəkə təhlükəsizliyi və inam həm şəbəkə istifadəçilərinin, həm də şəbəkə infrastrukturunun təhlükəsizlik və inam məsələlərini əhatə edir. İstifadəçilərin təhlükəsizliyi və inam məsələləri insanların şəxsi həyatının mühafizəsi, mobil xidmətlərin təhlükəsizliyi, verilənlərin və təhlükəsizlik siyasətinin menecmenti əhatə edir. Şəbəkə infrastrukturunun təhlükəsizliyi və inam məsələləri ziyankar proqramların aşkar edilməsi və aradan qaldırılması, müdaxilələrin aşkarlanması və qarşısının alınması, şəbəkələrə və avadanlıqlara inam, proqram təminatının təhlükəsizliyi, xüsusi təyinatlı sistemlərin təhlükəsizliyi və təhlükəsiz əməliyyat mərkəzlərinin yaradılmasını əhatə edir. Lakin bu iki sinif məsələlər bir-biri ilə sıx bağlıdır və çox zaman ikinci sinif məsələləri həll etmədən birincini həll etmək qeyri-mümkündür.

Müasir şəbəkə təhlükəsizliyinin analizi göstərir ki, kiberhücumların trendi, əsasən, tətbiq səviyyəsi hücumları,

DOI: 10.25045/NCInfoSec.2018.14

sosial mühəndislik, hədəf hücumları, informasiyanın sızması və daxili istifadəçi hücumları, şifirləmə, IPv6 hücumları, bulud hesablamaları və sosial şəbəkə hücumlarından ibarətdir. Demək olar ki, bu gün şəbəkə təhlükəsizliyi sahəsində baş verən başlıca trend ondan ibarətdir ki, hücumlar, əsasən, şəbəkə infrastrukturunun və ya qovşaqlarının sıradan çıxarılmasına deyil, informasiyanın (verilənlərin, məsələn, korporativ, fərdi və s verilənlərin) əldə edilməsinə yönəlmişdir. Şəxsi həyatın toxunulmazlığına və verilənlərin oğurlanmasına yönəlmiş hücumlar əsas təhlükəsizlik trendlərinə aid edilir. Təhlükəsizliyin təmin edilməsində əsas yanaşma sistemin təhlükəsizliyi ilə bərabər informasiyanın (verilənlərin) təhlükəsizliyinin təmin edilməsindən ibarətdir [1]. Bu gün demək olar ki, əsas hücum hədəfi İnternetdə istifadə edilən yeni xidmətlərdir, xüsusilə də bulud hesablamaları, əşyaların İnterneti, sosial şıbəkə və s. xidmətlərdir.

Bulud hesablamaları xidmətlərinin təhlükəsizliyi və inam. Bulud hesablamaları proqramlaşdırma metodologiyalarının, verilənlər bazası texnologiyalarının, kommunikasiya şəbəkələrinin və İnternetin inteqrasiyasından ibarət olan yeni bir sahədir və sorğu əsasında istifadəçilərə resursların verilməsini təmin edir. Bu gün bulud hesablamaları artıq vacib şəbəkə xidmətinə çevrilmişdir. Müəssisə və təşkilatlar xərcləri azaltmaq və effektivliyi artırmaq üçün işlərini bulud hesablamaları mühitinə keçirirlər. Bu və ya digər bulud hesablamaları xidmətinin seçilməsi zamanı təhlükəsizlik və inam faktorlarlarının nəzərə alınması çox vacibdir.

Bulud hesablamaları xidmətləri resursların geniş miqyasda ümumi istifadəsini və qarşılıqlı əlaqsəni təmin edir. Buna görə də təhlükəsizlik bulud hesablamaları xidmətləri infrastrukturunun çox vacib elementi sayılır, çünki bu mühitə giriş idarə edilməli və təhlükəsiz fəaliyyət təmin olunmalıdır. Həmçinin, bulud hesablamaları mühitində xidmət alan və xidmət göstərənin bir-birinə inamı olmalıdır və bu əsas məsələlərdən biridir.

Bulud hesablamaları müxtəlif lokal sistemlərdən təşkil olunduğu və tərkibinə müxtəlif mühitlərdən elementlər daxil olduğu üçün buludda təhlükəsizliyin təmin edilməsi çətinləşir. Bir tərəfdən təhlükəsizlik mexanizmi istifadəçilərin təhlükəsizliyinə zəmanət verməlidir, digər tərəfdən isə istifadəçilərin işində çətinlik yaratmamaq üçün o qədər mürəkkəb olmamalıdır. Beləliklə, təhlükəsizlik və rahatlıq arasında müəyyən balans olmalıdır. Etibarlı və təhlükəsiz hesablamaya təhlükəsizlik və məxfilikdən başqa, həmçinin həqiqilik, əlyetərlik, və bütövlük daxildir [3]. Bulud hesablamaları təhlükəsizliyi mexanizmlərinin geniş imkanalara malik olmasına baxmayaraq, müəyyən çatışmazlıqları mövcuddur. Məsələn, bulud hesablamaları sistemində aparat səviyyəsində etibarlı hesablamanı dəstəkləyən mexanizmlər yoxdur. Həmçinin bulud hesablamaları mühitində inamın əsası dəqiq müəyyən olunmayıb və sertifikatların yaradılması və mühafizəsi o qədər təhlükəsiz deyil. Digər tərəfdən, istifadəçilərin fəaliyyətinin monitorinqı mexanizmi yoxdur [4].

Şəbəkə səviyyəsində təhlükəsizlik təmin edilərkən açıq (public) və xüsusi (private) buludları fəraləndirmək çox vacibdir. Əgər xüsusi buludların xidmətlərinə yeni hücumlar yosdursa və onlarda boşluqalar müəyyən edilməyibsə, onda onun topologiyasının dəyişdirilməsinə ehtiyac yoxdur. Lakin açıq bulud xidmətlərinin istifadəsi zamanı təhlükəsizlik tələblərinin dəyişməsi şəbəkənin topologiyasının dəişdirilməsini tələb edir.

Host səviyyəsində təhlükəsizliyin təmin edilməsi və risklərin qiymətləndirilməsi zamanı həm xidmət növləri (SaaS (Software as a service), PaaS (Platform as a Service), və IaaS (Infrastructure as a service)), həm də buludların növləri (açıq (public), xüsusi (private) və hibrid) nəzərə alınmalıdır. Bu zaman SaaS və PaaS xidmətlərində hostların təhlükəsizliyi bulud xidmətlərini göstərən provayder tərəfindən həyata keçirilməlidir. Lakin IaaS xidmətində isə təqdim edilmiş hostların təhlükəsizliyinə kliyentlər cavabdehdirlər [5].

Bulud xidmətlərinə inamın qiymətləndirilməsi sahəsindəki tədqiqatların nəticələri bulud xidmətlərinə inamı tam şəkildə qiymətləndirməyə imkan vermir. Çünki müxtəlif tədqiqatçılar bulud xidmətlərinə inamı qiymətləndirmək üçün müxtəlif atributlar istifadə edirlər [6]. İnam müşahidə olunan faktlara və sübutlara əsaslanan subyektiv bir konsepsiyadir. Təşkilatlardan asılı olaraq bulud xidmətlərinə inamın tərifi dəyişir [7].

IoT təhlükəsizliyi və inam. Bu gün IoT tətbiqləri demək olar ki, insan həyatının bütün sahələrində, məsələn, səhiyyədə, binaların və ev təsərrüfatının avtomatlaşdırılması, ətraf mütinin monitorinqi, enerji və nəqliyyat infrastrukturunun idarə edilməsi və s. sahələrdə mövcuddur və onların fəaliyyətində cox vacib rol oynayır. IoT-un inkişafının geniş yayılmasının əsas səbəbi naqilsiz şəbəkə texnologiyalarının (məsələn, RFID (Radio Frequency Identification – Radiotezlik əsasında identifikasiya), WiFi, 4G, IEEE 802.15.x) mikroelektronikanın və s. sahələrin sürətlə inkişafı oldu [8]. Artıq 2020-ci ilə IoT-a qoşulmuş naqilsiz qurğuların sayı 26 milyarda çatacağı proqnozlaşdırılır [9]. Lakin çoxlu sayda avtonom sistemlərin IoT tətbiqləri vasitəsilə İnternetə qoşulması geniş miqyasda və diapazonda təhlükəsizlik problemləri yaradır, xüsusilə də fərdi məlumatların mühafizəsi ilə bağlı ciddi problemlər yaradır [10]. IoT qurğularının inamsız İnternet vasitəsi ilə qarşılıqlı əlaqəsi təhlükəsizlik sahəsində yeni problemlərin yaranmasına gətirib çıxarır. Məsələn, hər-hansı IoT qurğusunun təhlükəsizliyinin pozulması digər sistemlərə hücum edilməsinə imkan verir və bu da həm fiziki aləmdə (insanların fiziki təhlükəsizliyi), həm də virtual aləmdə (İnternetdə) insanlara ziyan vurulması üçün istifadə edilə bilər. Fərdi məlumatlara icazəsiz giriş, onların sizmasına və bəd niyyətlərlə istifadə edilməsinə gətirib çıxara bilər. Ənənəvi təhlükəsizlik mexanizmləri müəyyən problemləri həl etməyə imkan verir, lakin IoT-un təhlükəsizliyi ilə bağlı xüsusi aspektlər mövcuddur və onlar IoT-un təhlükəsizliyinin təmin edilməsi üçün geniş və bütöv yanaşma tələb edirlər. Çünki IoT qurğuları

adətən naqilsiz əlaqədən istifadə edir və bu da təhlükələr yaradır.

IoT qurğular müxtəlif naqilsiz əlaqə vasitəsi ilə (məsələn, Wireless Sensor Network (WSN), Global System for Mobile Communications (GSM), Code Division Multiple Access (CDMA), Bluetooth və Wi-Fi) qoşulduğu üçün IoT-un təhlükəsizlik məsələləri də fərqlənir [11].

.*Sosial şəbəkə xidmətlərinin təhlükəsizliyi və inam.* Sosial şəbəkə xidmətləri (SŞX) İnternetdə insanların müəyyən maraqlar və ya fəaliyyət çərçivəsində onlayn icmalarının yaradılmasına yönəlmişdir. SŞX insanlara bir-biri ilə əlaqə yaratmağa və informasiya mübadiləsi etməyə imkan verir. Hal-hazırda İnternetdə çoxlu sayda SŞX mövcuddur. Bununla yanaşı, SŞX istifadəçilərin şəxşi həyatının toxunulmazlığı və informasiya təhlükəsizliyi ilə bağlı yeni problemlər yaradır. Yəni SŞX-nin yaranması İnternet mühitində təhlükəsizlik risklərinin artmasına gətirib çıxarmışdır. Bu risklər ziyanlı proqramların və spamların yayılması, sosial mühəndislik və sosial şəbəkə hesablarına hücumların həyata keçirilməsi, eləcə də, izləmə, aldatma, şantaj, qarayaxma və s. kimi müxtəlif aspektli təhlükələrlə bağlıdır [12].

SŞX-də inam informasiya mübadiləsi və yeni münasibətlərin yaradılması üçün həlledici faktordur. SŞX-ə inam bir tərəfin, digər tərəfin əməllərinə qarşı həssas olması ilə müəyyən edilir. Yəni nəzarət imkanından asılı olmayaraq, bir tərəf digər tərəfdən inamlı şəxsə xas olan əməllər gözləyir [13].

NƏTİCƏ

Məqalə müasir şəbəkə təhlükəsizliyi və inam məsələlərinin analizinə həsr olunmuşdur. Müasir şəbəkələr, xüsusilə İnternet infrastrukturu həm texnoloji, həm də xidmət müxtəlifliyi baxımından çox dəyişmişdir. Bununla yanaşı yeni təhlükələr və hücum növləri meydana çıxmışdır və nəticədə təhlükəsizlik məsələlərinin həlli çox mürrəkkəblişmişdir və şəbəkələrə inam azalmışdır. Bu şəraitdə mövcud təhlükəsizlik paradiqmaları o qədər də effektiv deyil və buna görə də yeni təhlükəsizlik paradiqmalarının yaradılması aktual məsələdir.

ƏDƏBİYYAT

[1] Şıxəliyev R.H. Müasir kompüter şəbəkələrinin təhlükəsizlik trendləri haqqında // İnformasiya cəmiyyəti problemləri, 2015, №: 2, s. 82-86.

[2] http://cordis.europa.eu/fp7/ict/security/

[3] Avizienis A., Laprie J.-C., Randell B., and Landwehr C. Basic Concepts and Taxonomy of Dependable and Secure Computing // IEEE transactions on dependable and secure computing, 2004, vol.1, no.1, pp. 11-33.

[4] Shen Z., Li L., Yan F., Wu X. Cloud Computing System Based on Trusted Computing Platform / Proceedings of the International Conference on Intelligent Computation Technology and Automation, 2010, pp. 942-945.

[5] Mather, T., Kumaraswamy, S., Latif, S.: Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance. O'Reilly Media, Inc., 2009.

[6] Pandey S., Daniel A.K. Fuzzy Logic Based Cloud Service Trustworthiness Model / Proceedings of the 2nd IEEE International Conference on Engineering and Technology (ICETECH), 2016, pp. 73-78.

[7] Edward A. , et al. A process-oriented methodology for assessing and improving software trustworthiness / Proceedings of the 2nd ACM Conference on Computer and communications security. ACM, 1994, pp. 39-50.

[8] Atzori L., Iera A., Morabito G. The Internet of Things: A Survey // Computer Networks 2010, vol. 54, pp. 2787–2805.

[9] Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020; Gartner Inc.: Stamford, CT, USA, 2013.

[10] Federal Trade Commission. Internet of Things – Privacy and Security in a Connected World; FTC: Seattle, WA, USA, 2013. 8. Şıxəliyev , R.H. Sosial şəbəkələrdə təhlükəsizlik problemləri // İnformasiya Cəmiyyəti Problemləri, 2016, № 2, s. 80-88.

[11] Şıxəliyev R.H. Sosial şəbəkələrdə təhlükəsizlik problemləri // İnformasiya Cəmiyyəti Problemləri, 2016, № 2, s. 80-88.

[12] Shin D.-H. The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption // Interacting with Computers 2010, vol. 22, no. 5, pp. 428-438.

[13] Baig Z.A. Securing the internet of things infrastructure – standards and techniques / Proceedings of the Australian Information Security Management Conference, 2014, pp. 75-81.

MODERN NETWORKS SECURITY AND TRUSTWORTHINESS

Ramiz Shikhaliyev
Institute Information Technology ANAS, Baku, Azerbaijan
ramiz@science.az

Abstract – The article analyzes modern network security and trustworthiness issues. Basically, the security and trustworthiness issues of the new network services available on the Internet have been analyzed. In particular, cloud computing, Internet of things and social networking services have been analyzed.

Keywords – network security, network services, cloud compuring, Internet of things, social network services