Mobil avadanlıqlarda fərdi məlumatların təhlükəsizliyi məsələləri

Oqtay Ələkbərov
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
oqtayalakbarov@iit.science.az

***Xülasə*— Son dövrlərdə mobil istifadəçilər mobil avadanlıqlardan bank ödəmələri, internet xidmətləri, e-poçt xidmətləri, çoxsaylı proqram əlavələri, video, foto və audio məlumatların saxlanması və s. kimi istiqamətlərdə geniş istifadə edilir. Qeyd edilən xidmətlərdən istifadə vaxtı mobil qurğular haker hücumlarına məruz qalır. Məqalədə mobil qurğularda yerləşən fərdi məlumatların təhlükəsizliyi və təhdidlərin təsnifatı təhlil edilmiş və meydana çıxan problemlər analiz edilmişdir. Fərdi məlumatların təhlükəsizliyinin təmin olunması üçün tövsiyələr təklif edilmişdir.**

***Açar sözlər*— mobil qurğular, təhdidlər, biometrik təhlükəsizlik, məxfilik, gizlilik**

I. GİRİŞ

Son dövrlərdə texnologiyanın inkşafı mobil qurğulara olan tələbatı da artırmışdır. İstifadəçilərin gündəlik həyatda mobil qurğulardan (smartfonlar, planşetlər) istifadəsi onların təhlükəsizliyi məsələlərini gündəmə gətirir. Əksər ekspertlər mobil qurğularda saxlanan məlumatların xakerlər tərəfindən daha asan əldə edilməsini qeyd edirlər. Hal hazırda mobil avadanlıqlardan bank ödəmələri, internet, e-poçt xidmətləri, çoxsaylı proqram əlavələri, video, foto və audio məlumatların saxlanması və s. kimi istiqamətlərdə geniş istifadə edilir. İstifadəçi mobil avadanlıqlardan istifadə etdikdə bir çox riskləri nəzərə almırlar. Araşdırmalar göstərir ki, əksər istifadəçilər mobil qurğulardan istifadə zamanı təhlükəsizlik siyasətinə əməl etmirlər. Amerika Birləşmiş Ştatlarında 1000-ə yaxın istifadəçi arasında aparılmış sorğu nəticəsində məlum olmuşdur ki, istifadəçilərin sadəcə 12%-i mobil qurğuların təhlükəsizlik siyasətinə əməl edirlər. Mobil telefonlarda müxtəlif proqram əlavələrinin olması, mobil telefonların daima internet şəbəkəsində onlayn olması onların təhlükəsizlik məsələlərini daima aktual edir.

II. MOBIL QURĞULARDA FƏRDİ MƏLUMATLARA TƏHDİDLƏRININ TƏSNİFATI

Mobil telefonların təhlükəsizliyinin əsas funksiyası mobil telefonlarda saxlanan şəxsi və işgüzar məlumatların etibarlılığını təmin etməkdir. Mobil qurğulardan geniş istifadə olunması onlarda saxlanan məlumatlara hakerlər tərəfindən hücum edilməsinə səbəb olur. Haker hücumları əsasən sms mətnlərinin ötürülməsi, multimedia məlumatlarının mübadiləsi və əlaqə kanallarından istifadə zamanı baş verir. Mobil avadanlıqların təhlükəsizliyinə təsir edən təhdidlər aşağıdakılardır [1].

Fiziki təhdidlər- Mobil qurğuların balaca və yüngül olması onların oğurlanması və ya itirilməsi ehtimalını artırır. Juniper şirkətinin keçirdiyi sorğuya əsasən hər 20 mobil telefon istifadəçisindən 1-i mobil qurğunun itirilməsi və ya oğurlanması halları ilə rastlaşır. İstifadəçi mobil telefonun itirərsə və onu PİN kod və ya parol vasitəsi ilə bloklamasa, mobil telefonu əldə edən digər istifadəçi aşağıdakı məlumatları əldə etməsinə imkan yaradır [2].

- Elektron poçtda yerləşən məlumatlara;
- Sosial şəbəkələrdəki (Facebook, Google, Twitter) qeydiyyat məlumatlarını;
- Brauzerlərdə saxlanan parollara;
- Parol və kredit kartı haqqında məlumat;
- Elektron poçtun ünvanı və əlaqədə olduğu şəxslərin telefon nömrələri;
- Video, audio və fotoşəkillər haqqında məlumat.

Şəbəkə təhdidləri. Bildiyimiz kimi mobil qurğular müxtəlif növ naqilsiz şəbəkə texnologiyaları (wi-fi, bluetooth, nfc) ilə təchiz olunmuşdur. Hakerlər tərəfindən hücümlar ilkin olaraq məhz şəbəkə texnologiyalarına olunur. Bu hücumlar zamanı əsasən SMS, MMS və səsli zəng xidmətlərindən istifadə edilir. Hakerlər adətən şəbəkə təhdidləri zamani Smishing və Vishing hücumlarından istifadə edirlər. Smishing hücum SMS xidmətləri, Vishing hücumu isə səsli zəng xidmətləri vasitəsi ilə həyata keçirilir [3].

Sistem təhdidləri. İstifadə olunan əməliyyat sistemlərində istehsalçı tərəfindən buraxılmış boşluqlara görə mobil avadanlıqlarda çox ciddi təhlükəsizlik problemləri baş verə bilər. Məsələn, 2015-ci ildə Samsung şirkətinin istehsal etdiyi bəzi qurğularda istifadə olunur. SwiftKey-də aşkarlanan boşluq, istifadəçinin yazışmalarının digər şəxslər tərəfindən rahatlıqla əldə olunmasına şərait yaratmışdır.

Proqram əlavələri təhdidləri. Mobil telefonlarda müxtəlif növ proqram əlavalərindən istifadə olunur. İstifadəçi istənilən proqramı mobil telefona yükləyərkən təhlükəsizlik siyasətinə ciddi qaydada əməl etməlidir. Təcrübələr göstərir ki,

DOI: 10.25045/NCInfoSec.2019.36

kibercinayətkarlar sosial mühəndisliyin müxtəlif növlərindən istifadə etməklə, istifadəçinin məlumatlarını asanlıqla ələ keçirə bilirlər. Proqram əlavələri təhdidləri, əsasən, aşağıdakı kateqoriyalardan ibarət olur:

- casus proqramları;
- zərərli proqramlar;
- məxfiliyi təhdid edən proqramlar;
- proqram boşluqları.

Mobil telefonların proqramlarında boşluqların olması demək olar ki, mobil telefonların müxtəlif hücumlara qarşı zəif olmasına səbəb olur. Adətən bu cür boşluqlar zamanı hakerlər müxtəlif zərərli virus və ya proqram təminatlarından istifadə edirlər. Bunlara aşağıdakı hücum növlərini misal göstərə bilərik:

Troyan atı ilə hücumlar zamanı, adətən, istifadəçinin şəxsi məlumatları oğurlanmaqla yanaşı, müxtəlif zərərli proqram təminatları mobil qurğuya yüklənə bilər

Botnet hücumları zamanı mobil avadanlığın hesablama resurslarından istifadə olunur. Çox vaxt istifadəçinin belə hücumlardan xəbəri olmur.

Soxulcan hücumları zamanı virus sistemdə yaranan boşluqlardan istifadə etməklə daha çox zərər yetirmək qabilliyətində olur. Mobil avadanlıqlarda belə tip viruslar əsasən istifadəçinin maliyyə məlumatlarını oğurlanması üçün istifadə olunur

Rootkit zərərli proqram təminatı olub, istifadəçinin xəbəri olmadan onun mobil telefonuna daxil olur. Bu tip zərərli proqram əlavaləri mobil qurğunun əməliyyat sisteminin əsas funksiyalarını özunə lazımı formada idarə edir.

Mobil telefonlara olunan təhdidlərin sayının artmasının başqa bir səbəbi mobil ödəniş sistemlərinin geniş sferada istifadə olunmasıdır. Belə ki, istifaçilərin gündəlik həyatında ödənişlərin çox bir hissəsini mobil telefonlar vasitəsi ilə həyata keçirirlər. Belə təhdidlər zamanı, adətən istifadəçilər sadə üsullarla aldadılırlar. McAfee Lab şirkətinin araşdırmaları göstərir ki, müxtəlif saxta URL ünvanlardan istifadə eləməklə istifadəçilər zərərli veb saytlara yönləndirillər. İstifadəçiyə hədiyyə vauçerlər, məşhur brendlərə endirimlər və ya müxtəlif xidmətlər göstərən hər hansi bir saytın xidmətlərinə böyük endirimlər təklif etməklə istifadəçini zərərli saytlara keçid etməyə yönləndirlər edir. Statistikaya görə hər 100 müraciətin 51-i məhz zərərli saytlara yönləndirilir.

III. MOBİL AVADANLIQLARDA FƏRDİ MƏLUMATLARIN TƏHLÜKƏSİZLİYİNİN TƏMİN OLUNMASI YOLLARI

Mobil telefonlarda fərdi məlumatların təhlükəsizliyinin təmin olunmasında 2 cür yanaşma mövcuddur. 1-ci yanaşmada mobil telefonların fərdi məlumatlarının təhlükəsizliyini istifadəçi özü təmin edirsə, 2ci yanaşmada bu proses mobil avadanlıq istehsalçısının birbaşa özündən asılı olur. Mobil telefon istifadəçisinin fərdi məlumatları qorumaq üçün bir neçə təhlükəsizlik tələblərinə riayət etməlidir. [4]

Şifrələmə. Əgər mobil telefonda xüsusi məlumatlar olarsa, bu mütləq şəkildə şifrələnməlidir. Fərdi məlumatların şifrələnməsi onları kənar şəxslərin müdaxiləsindən qoruyur. Eyni zamanda şifrələnmiş fayllar məxfilik siyasətinin tam qorunmasına kömək edir.

Standartlaşdırma və ya Sertifikatlaşdırma - bu proses mobil telefonun təhlükəsizlik faktorlarını təmin edir. Belə ki, standartlara cavab verən mobil telefonlar istifadəçinin fərdi məlumatlarının təhlükəsizliyi üçün kilid sistemləri, antivirus proqramları və ehtiyat nüsxə yaddaşı ilə təmin olunur

Şəbəkəyə giriş idarəetməsi- (ing. Network Access Control)- Bu xidmətin olması şəbəkəyə qoşulan bütun qurğuların qeydiyyatını təmin edir. Belə ki, şəbəkədə olan mobil telefonlardan hər hansı birində virus aşkarlanarsa həmin qurğunun şəbəkəyə girişi blok olunur. Çünki istənilən hücumun uğurlu alınması üçün əsas faktor virusa yoluxmuş və ya zərərli proqram yüklənmiş mobil telefonun internet şəbəkəsində uzun müddət qalmasıdır.

Yuxarıda qeyd etdiyimiz kimi mobil telefonlarda fərdi məlumatların təhlükəsizliyini istifadəçilərlə yanaşı mobil avadanlıqların istehsalçıları da təmin edir. Fərdi məlumatları qorumaq üçün istehsalçı şirkətlər bir sıra təhlükəsizlik siyasətlərinə əməl etməlidirlər. [6]

Proqram əlavələri bazası. Adətən, belə bazalarda sertfikatlaşdırılmış proqram tətbiqləri yerləşdirilir. İstehsalçı tərəfindən daima belə bazalara ciddi nəzarət olur. Hər hansı proqram əlavələrində virus və ya boşluq aşkarlanarsa həmin tətbiq dərhal bazadan çıxarılır. Hal hazırda bu tip proqram bazaları olan Play Store, Apple Store, Galaxy Store geniş istifadə olunur. İstehsalçı şirkətlər demək olar ki, hər gun təhlükəsizlik siyasətində yeniləmə aparmaqla belə bazalarda yarana biləcək problemlərin qarşısını alırlar.

Əməliyyat sistemləri İstehsalçı şirkətlər ilk növbədə mobil telefonların əməliyyat sistemində təhlükəsizlik məsələlərinə daha çox diqqət yetirirlər. Belə ki əməliyyat sistemləri proqramçılar tərəfindən yazılarkən bütün fərdi məlumatların təhlükəsizliyini qorumaq üçün mümkün standartların hamısından istifadə edirlər. Eyni zamanda mobil telefon istehsalçıları hər ay mobil qurğularda təhlükəsizlik siyasətinin yenilənməsi ilə bağlı istifadəçilərə bildirişlər göndərirlər.

Proqram təminatçıları İstehsalçı şirkətlər mobil telefondan istifadəni daha da asan etmək üçün bir sıra mobil qurğulara əlavə proqram təminatları yükləyirlər. Bu proqram əlavaləri proqramçılar tərəfindən yazılarkən istehsalçı tərəfindən müəyyən təhlükəsizlik şərtləri qoyulur. Belə ki, yazılmış proqram təminatında fərdi məlumatların gizlilik şərtlərini qorumaq üçün məhz proqram təminatçısına məhdudiyyətlər qoyulur.

Biometrik təhlükəsizlik Son dövrlərdə texnologiyanın daha da inkişafı artıq mobil telefonlarda da biometrik təhlükəsizlik texnologiyalarından istifadə üçün zərurət yaratmışdır.

Biometrik təhlükəsizlik mobil qurğularda adətən 2 mərhələdən ibarət olur: qeydiyyat və autentifikasiya mərhələləri.

Qeydiyyat mərhələsində istifadəçinin fizioloji informasiyaları götürülür. Bura biz barmaqların skan olunmasını, üz cizgilərinin oxunması, göz bəbəyinin oxunması və s. texnologiyaları aid edə bilərik.

Autentifikasiya zamanı isə klaviaturada hər hansı simvolun yığılması, imza və ya istifadəçinin səsindən istifadə olunur. [5]

Yuxarıda qeyd olunan faktorlar bizə əsas verir ki, mobil qurğularda istifadəçilərin fərdi məlumatlarının təhlükəsizliyini qorumaq üçün bəzi şərtlərə əməl edək [7]:

- Məlumatları yükləyərkən mütləq antivirus proqramlarından istifadə etmək;
- Proqram əlavələrini yoxlanılmış bazalardan yükləmək;
- Rəsmi olmayan, pulsuz təklif olunan proqram əlavələrindən istifadə etməmək;
- Məlumat mübadiləsi zamanı gecikmələri diqqətdə saxlamaq;
- Əməliyyat sistemində tez tez yeniləmə aparmaq;
- Biometrik məlumatları məxfi saxlamaq.

NƏTİCƏ

Son dövrlərdə texnologiyaların inkişafı mobil avadanlıqlarada təsirsiz ötüşməmişdir. Məqalədə mobil telefonlarda yerləşən fərdi məlumatların təhlükəsizliyinə təhdid yaradan məsələlər və onların həlli yolları analiz və təhlil edilmişdir. Mobil qurğularda fərdi məlumatlara təhdidlərin təsnifatı təhlil edilmişdir. Eyni zamanda mobil avadanlıqlarda fərdi məlumatların təhlükəsizliyinin təmin edilməsi və həlli yolları təklif edilmişdir. Mobil avadanlıqların sürətli inkşafı ilə yanaşı zərərli proqramların sayının artması, hər proqram əlavələrinə görə fərqli təhdidlərin olması onların təhlükəsizlik məsələlərini diqqət mərkəzində saxlayır. Apardığımız araşdırmalar onu göstərir ki, istifadəçilər mobil telefonlarda təhlükəsizlik siyasətini mütəmadi olaraq yeniləməli, mobil telefonlarını kənar şəxslərə etibar etməməlidirlər.

İSTİNADLAR

[1] M. Sujitra, G. Padmavathi, “A Survey on Mobile Device Threats, Vulnerabilities and their Defensive Mechanism”, İnternational Journal of Computer Applications, New-york, vol. 56, No. 14 pp. 27-29, October, 2019.

[2] I.Mavridis, G. Pangalos, “Security Issues in a Mobile Computing Paradigm”, Communication and Multimedia Security, Athens, vol 3, pp. 61-75, 2012.

[3] R. Prodanovic and D. Simic, “A Survey of Wireless Security,” Journal of Computing and Information Technology, vol. 15, no. 3, p. 237, Sep. 2007.

[4] S. Toyssy, M. Helenius, “About malicious software in smartphones”, Journal in Computer Virology, vol. 2, no. 2, pp. 109–119, 2006.

[5] D. Liu, N. Zhang, and K. Hu, “A Survey on Smartphone Security”, International Journal of Advanced Computer Science and Applications, vol. 7, pp. 61–65, August. 2013.

[6] D. Venugopal, G. Hu, and N. Roman, “Intelligent virus detection on mobile devices”, Proceedings of the International Conference on Privacy, Security and Trust. New York, pp. 1–4, 2006.

[7] G. Delac, M. Silic, and J. Krolo, “Emerging security threats for mobile platforms”, in MIPRO, Proceedings of the 34th International Convention. IEEE, pp. 1468–1473. 2011

PERSONAL DATA SECURİTY ON MOBİLE DEVİCES

Ogtay Alakbarov

Institute of Information Technology of ANAS, Baku, Azerbaijan

oqtayalakbarov@iit.science.az

Abstract— Recently, mobile users have been widely using mobile devices for banking, internet services, email services, numerous applications, storage of video, photo and audio information and for other operations. Mobile devices are exposed to hacker attacks when using these services. This paper analyzes the security of personal data stored on mobile devices and the classification of threats and analyzes emerging problems. The recommendations on personal data security are provided**.**

Keywords— *mobile devices, threats, biometric security, privacy, confidentiality*