Smartfonlarda informasiya təhlükəsizliyi riskləri

Şüşə Kərimova

AMEA İnformasiya Texnologiyaları İnstitutu

shusha_az@rambler.ru

***Xülasə*— Smartfonlar geniş imkana malikdirlər: sensor massivi, çoxkanallı radio, şəbəkə interfeysi, qiqabaytlı yaddaş və güclü prosessor. Belə xüsusiyyətlərinə görə smartfonlar artıq gündəlik həyatımızın bir hissəsinə çevrilib. Smartfonlar həm də informasiya mənbəyidir. Şəxsi həyatımız, işimiz, bir sözlə özümüzlə bağlı olan bu informasiyanın təhlükəsizliyini də nəzərə almaq üçün bir sıra tədbirlər görmək lazımdır. Bu işin məqsədi smartfonlarda informasiya təhlükəsizliyini və smartfon istifadəçilərinin gizlilik risklərini göstərmək və təhlükəsizliyi qorumaq üçün istifadəçilərə praktiki məsləhətlər verməkdir. Işdə smartfon istifadəçilərinin informasiya təhlükəsizliyi üçün 10 risk qiymətləndirilir.**

Açar sözlər*— *smartfon; fərdi məlumatlar; informasiya təhlükəsizliyi; risk.

I. GİRİŞ

Smartfonlar cəmiyyətin bütün təbəqələri, hökumət rəsmiləri, biznes və istehlakçılar üçün mühüm vasitədir [1]. Tək Böyük Britaniya, Almaniya, Fransa, İspaniya və İtaliyada, smartfon istifadəçilərinin sayı 61 milyonu artıb [2]. Smartfonlarda Android, İOS, Windows Phone, Black Berry, Firefox OS, Sailfish OS, Tizen, Ubuntu Touch OS əməliyyat sistemləri var [3]. Android əməliyyat sistemi istifadəçilər üçün geniş imkanlar yaradır. Eyni zamanda bu sistemlər çoxsaylı hücumlara məruz qalır. Tədqiqatlar göstərir ki, təhlükəsizlik baxımından Android-də çatışmazlıq mövcuddur, hansı ki, təcavüzkara Secure Digital JavaScript və ya HTML vasitəsilə SD kartında olan faylları yükləməyə icazə verir [4]. Digər məsələ Androidlərin Troyan vurusuna yoluxmasıdır. “Kaspersky Securiry Bulletin” dərc olunmuş məlumatına əsasən hər ay orta hesabla zərərverici proqramların 6300 yeni mobil nümunəsi müəyyən edilir. Bütovlükdə, Android üçün məlum zərərverici nümunələrin sayı səkkiz dəfədən çox artıb [5].

IPhone əməliyyat sistemi IOS**.** Bu əməliyyat sistemi həmçinin Apple-ın Ipad və ya Ipod kimi başqa mobil qurğularında istifadə olunur. Təhlükəsizliyin təmin olunması üçün hər bir istifadəçi şifrləmə açarının generasiyası üçün unikal koda malik olmalıdır. Kodlaşdirma üçün 3DES və ya AES-128 alqoritimindən istifadə olunur [4]. Bu iPhone-da saxlanılan şəxsi informasiyanın müdafiəsi üçün istifadə olunur. Parol siyasəti ilə yanaşı iPhone qurğuda məhdudiyyətlərin qurulmasını dəstəkləyir. Məsələn, bu YouTube-u məhdudlaşdıra bilər, kamera, səs (yığım) və s. yolla Apple qurğunun təhlükəsizliyinə nəzarət edə bilər. Bundan başqa, iPhone IPsec, L2TP, Cisco və PPTP kimi Virtual Private Network texnologiyanı (VPN-nı) dəstəkləyir. iPhone həmçinin Secure Sockets Layer (SSL) VPN-ı dəstəkləyir, hansı ki, məlumatların ötürülməsi üçün təhlükəsizliyin daha yüksək səviyyəsini təmin edir. İnternetin təhlükəsiz istifadəsini təmin etmək üçün iPhone iki yanaşma vasitəsilə veb-trafik təhlükəsizliyi təmin edir: SSL v3 və Transport Layer Security (TLS) v1.0.

Smartfonların digər bir növü olan BlackBerry-nin əməliyyat sistemi C++-da yazılmış OS BlackBerry -dir. Bu əməliyyat sistemi WAP1.2-i dəstəkləyir. BlackBerry əməliyyat sistemi öz simsiz daşıyıcıları vasitəsilə avtomatik yenilənə bilər.

Smartfonlar - barkod oxuyucu cihaz, peyk naviqasiya sistemi, e-poçt, sosial şəbəkə, Wi-Fi giriş nöqtəsi və zəng etmək üçün istifadə edilə bilər. Smartfonların artan əhəmiyyətini nəzərə alaraq, bu cihazların məxfilik və təhlükəsizlik risklərini qiymətləndirmək vacibdir. Işdə smartfon istifadəçiləri üçün əsas informasiya təhlükəsizliyi riskləri göstərilir. Qeyd edilir ki, risklər smartfonların potensial gəlirinə uyğun balanslaşdırılmalıdır.[1] Buna sadə bir misal göstərək ki, smartfonlar evdə tək qalan ürək xəstələrinin təhlükəsizliyini təmin edə bilər. Onların ürək problemlərini yoxlamaq və nəzarət etmək üçün tibbi heyətə imkan yarada bilər. Belə formada smartfonlar pasiyentin həyat keyfiyyətini yaxşılaşdıra bilər, eyni zamanda səhiyyə xərclərini azalda bilər [6] .

II. İNFORMASİYA TƏHLÜKƏSİZLİYİ RİSKLƏRİ

Bu bölmədə smartfonların istifadəsi ilə bağlı daha vacib informasiya təhlükəsizliyi riskləri haqqında ümumi məlumat verilir.

2.1 İstifadə ssenariləri

Risklər smartfonun necə istifadə olunmasından asılı olaraq dəyişir. Buna görə də üç müxtəlif istifadə ssenarisi müəyyən edilir və hər bir ssenari üçün risk və tövsiyələr təsvir etməyə cəhd edilir.

İstifadə ssenariləri	Təsvir
Istehlakçı (C)	Smartfon insanların gündəlik həyatının ayrılmaz hissəsidir - məsələn, telefon zəngləri, sosial şəbəkə, mesaj, naviqasiya, oyun, online bank, yer əsaslı xidmətlər, internet, mikro-bloq, e-poçt, fotoqrafiya, video, qeyd, e-səhiyyə, və s.
Işçi (E)	Smartfon əməkdaş tərəfindən biznes və ya hökumət təşkilatlarında istifadə olunur. Işdə telefon zəngləri üçün istifadə olunur, mobil Internet, korporativ e-poçt, xərclərin, müştəri əlaqələrinin menecmenti, səyahət zamanı

	yardım, əlaqəli idarəetmə və biznes sosial şəbəkə, video konfrans, vəzifələri planlaşdırmaq və sənədləri oxumaq. Bəzi hallarda işlə əlaqədar olaraq formaları doldurmaq üçün də smartfonlardan istifadə olunur. Bu ssenari istifadə olunduqda rəsmi işəgötürən tərəfindən müəyyən informasiya təhlükəsizliyi siyasəti tətbiq olunur. Smartfon məhdud şəkildə şəxsi məqsədlər üçün istifadə olunur.
Yüksəkvəzifəli şəxs (H)	Smartfon biznes və ya hökumət təşkilatlarında yüksək səviyyəli rəsmi və ya onun köməkçisi tərəfindən istifadə olunur. Həssas informasiya və ya vəzifələrin icrası ilə bağlı informasiya işlənərsə, təhlükəsizlik siyasəti daxil edilir və smartfonun funksiyaları məhdudlaşdırıla bilər və zəngin qorunması üçün kriptoqrafik modullar – məxfilik əlavə oluna bilər.

Qeyd edək ki, fərdi smartfonlar və smartfon istifadəçiləri tez-tez başqa bir istifadə ssenarisində də kəsişirlər. Bu özlüyündə təhlükəsizlik risklərinin idarəedilməsində mühümdür. Məsələn, həssas müştəri məlumatları olan biznes smartfonu bayram günündə ölkədən kənara götürülə bilər. Smartfon həftəsonu şəxsi sosial şəbəkə kimi (C ssenarisi) və iş günlərində həssas elektron müraciətlər (ssenari E) üçün istifadə oluna bilər. Tövsiyyələrdə bəzi konkret məsələləri ünvnlamaq üçün bəzi məsləhətlər veriləcək. Ümumilikdə, istifadəçilər üçün təhlükəsizlik təhdidlərinin idarə edilməsi əməkdaşlara və yüksək vəzifəli əməkdaşlara tətbiq olunmalıdır.

III. RİSKLƏRİN QİYMƏTLƏNDİRİLMƏSİNƏ YANAŞMA

Informasiya təhlükəsizliyində risk fərdi informasiya aktivlərinə təsir edir və ehtimalla əlaqəlidir [7]. Təhlükələr bir və ya daha artıq boşluqdan istifadə edir. Təhlükələrin təsiri təhlükəyə məruz qalmış aktivlərin qiyməti ilə təyin oluna bilər. Bu işdə müəyyən qədər zərər çəkmiş aktivlərin aşağıdakı siyahısından istifadə edirik:

- Şəxsi məlumat
- Korporativ intellektual mülkiyyət
- Konfidensial məlumat
- Maliyyə aktivləri
- Qurğu və xidmətin əlyetərliliyi və funksiyaları
- Şəxsi və siyasi reputasiya (nüfuz)

Risklər ekspert qrupunun müzakirəsindən sonra təyin olunur. Sonra hər bir riskin orta qiyməti haqqında məlumat verilir.

Risklərin qiymətləndirilməsinin məqsədi istifadəçilərə risklər haqqında məlumat verməkdir ki, onlar öz təsirlərini minimuma endirsinlər. Ona görə də təhlükə ehtimalı və təsirinə heç bir mütləq dəyər qoyulmur. Ona görə də "Yüksək" ehtimal neçə dəfə deyil, təhlükənin ildə baş verəcəyi ilə qiymətləndirilir. Həmçinin eyni funksiyanı yerinə yetirən digər texnologiyalar ilə müqayisədə smartfon istifadəsinin müqayisəli risklərin qiymətləndirilməsini təklif edilmir. Qeyd etmək lazımdır ki, boşluq və risklər müxtəlif smartfon modelləri arasında, fiziki şəxslər və təşkilatlar arasında çox fərqli ola bilər (gizli pin nömrələri və ya parol, müştəri əlaqələri). Məsələn, müəyyən təşkilatların müəyyən əməkdaşları üçün smartfonun ünvan kitabçasına təsir edən məxfiliyin pozulması böyük təsir göstərə bilər (ailə və dostları, telefon nömrələri aşkar oluna bilər). Fiziki şəxslər və təşkilatlara öz fərdi risk qiymətləndirmələrindən çəkinmək və fərdi halda potensial faydalarını risklərlə müqayisə etmək tövsiyə olunur.

IV. RİSKLƏRİN İCMALI

Risklər müxtəlif istifadə ssenarilərində orta qiymətinə görə sıralanıb.

R1. Qurğunun itməsi və ya oğurlanması

Təhlükə təsviri	Smartfon oğurlanır və ya itirilir. Onun yaddaşının mühafizə edilməməsi və ya sökülən media müdafiəsizliyi orada saxlanılan məlumatlara hücumçunun çıxış əldə etməsinə imkan verir.

Smartfonlar, qiymətli və cib ölçülü olmaqla, həm də oğurlanmış və ya itirilmiş ola bilər.

Son ötən il Böyük Britaniya hökuməti 2% mobil telefon məlumatının oğurlanması araşdırılmışdır. [8]. Smartfonun yaddaş və ya media daşıyıcısı kifayət qədər (şifrələmə ilə) qorunmursa, onda təcavüzkar bu məlumatları əldə edə bilər. Smartfonlarda kredit kartının Pin-kodu, bank hesabı, parol kimi və s. qiymətli informasiya ola bilər. Iş telefonlarında tez-tez korporativ e-poçt və sənəd və həssas olan məlumat ola bilər. H ssenarisi halında təsir çox yüksəkdir, smartfonda məxfi məlumat ola bilər, məsələn gizli e-poçt. E və H ssenarilərində ehtimal qiymətləndirilməsi aşağıdır, çünki istifadəçilər oğurluq və itirilmə haqqında bilirlər, yaddaşın kodlaşdırılması, qurğunun avtobloklanması kimi müdafiə tədbirləri tez-tez İT mütəxəsisləri tərəfindən yerinə yetirilir. Qeyd edək ki, hətta şifrləmə tamamlandıqda belə, hücum zəif smartfonlarda şifrələmə həyata keçirilməsində mövcud ola bilər [9].

R2. Məlumatların bilmədən yayılması

Təhlükə təsviri	Smartfon istifadəçisi bilmədən telefonun-dakı məlumatları açıqlayır.

İstifadəçilər heç də həmişə smartfonların bütün əlavə funksiyalarını bilmirlər. Istifadəçilər hətta bilmirlər ki, bu əlavələr onlar haqqında şəxsi məlumatlar toplayır. Ünvan məlumatları, məsələn, tez-tez istifadə edilən məlumatlar və ya yüklənmiş foto məlumatları sosial şəbəkələrdə istifadə olunur. Ünvan məlumatlarının bilərəkdən yayılması və izlənilməsi hücumçulara kömək edə bilər. Şübhəsiz ki, bu cür təhlil (əgər bu birmənalı istifadəçiyə aiddirsə) insanın şəxsi hüququnu

poza bilər, necə ki, Avropa məlumatların mühafizəsi haqqında qanunda qeyd olunur ki, müəyyən fərdin məxfilik hüququnun qorunmasına diqqət yetirmək lazımdır, eyni zamanda quldurluq və ya qiymətli mallar olan yük avtomobillərinin qaçırılması ilə bağlı təqiblər edilməsinə icazə vermək olar [9]. Verilənlər bazasının tipinin müəyyən edilməsi qərarın dəyişməsini qəbul etməyə malik olmadan özünü istifadəçi razılığı ilə inteqrasiyada göstərir. Məsələn, ünvan məlumatları tez-tez şəkil fayllarına daxil edilir. İstifadəçi əlavə proqramdan istifadə etməklə bilərəkdən onların yerinin açılmasına icazə vermiş ola bilər. Açıqlanan informasiyanın maraqlı nümayişi internet səhifəsi icanstalku.com tərəfindən təmin edilir, hansı ki, bu təsvirlərdə quraşdırılmış (maarifləndirmə məqsədləri üçün) GPS məlumatları vasitəsilə üstü açılıb[9].

R3. Istismardan çıxan smartfonlara hücumlar

Təhlükə təsviri	Smartfon istismardan çıxarılır, təcavüzkarın cihazdakı məlumatlara baxmaq imkanı olur.

Identifik verilənlərin oğurluğu haqqında məlumatların genişlənməsinə əsasən bir çox istifadəçilər və təşkilatlar indi kompüteri istismardan çıxarmamışdan əvvəl onun sərt diskini məhv edir və ya silir. Eyni fikir hələ smartfonlarla baş verməmişdir. Çünki, smartfonlar təkrar istifadə olunur. ABI bazar analitiklərinin tədqiqatına görə 2012-ci ildən başlayaraq 100 milyondan artıq mobil telefonlar hər il təkrar istifadə üçün emal olunur [11]. Qeyd etdiyimz kimi, smartfonlar böyük həcmdə həssas informasiyaya malik ola bilər, hansı ki, təcavüzkar üçün dəyərli ola bilər.

R4. Fişinq hücumları

Təhlükə təsviri	Təcavüzkar həqiqi görünən saxta apps və ya (SMS, e-poçt) mesajlar vasitəsilə (məsələn, parol və kredit kartı nömrələri kimi) istifadəçi etimadnaməsini toplayır.

Fişinq-hücumları ənənəvi fərdi kompüter istifadəçiləri üçün tanınmış təhlükədir. Fişinq-hücumların platforması müstəqildir, çünki təcavüzkarın hər hansı bir şəkildə istifadəçinin cihazına hücum etməsi lazım deyil. Fişinq riskinin smarfon istifadəçilər üçün vacib olma səbəbləri var.

Smartfon kiçik ekranın olması deməkdir. Bu isə təcavüzkara daha asanlıqla etibarlı maskalanmağa imkan verir. Belə ki, istifadəçi gələn siqnalı qəbul edir və bu siqnalın SSL veb saytdan istifadə olunub-olunmadığını yoxlamaq məqsədilə göndərildiyi qeyd olunur.

R5. Casus hücumları

Təhlükə təsviri	Smartfonlarda şəxsi məlumatlar əldə etmək və ya nəticə çıxarmaq üçün hücumçuya imkan verən casus hücumları quraşdırılıb.

Casus proqram təminatı - ziyanlı proqram təminatıdır, istifadəçilər və onların fəaliyyətləri haqqında gizlicə informasiya toplayır və bundan reklam elanlarında marketinq məqsədi ilə istifadə edir. Belə casus proqram təminatı istifadəçinin razılığı ilə yüklənmiş yardımçı proqram təminatı kimi görünə bilər. Smartfonlardakı yadda saxlanılmış və emal olunmuş şəxsi məlumatlar, həssas sənəd, etimadnamələr toplusu smartfonları casus proqram təminatları üçün maraqlı edir. Bundan əlavə, smartfonlar gizli kanallarla təmin olunur, hücumçu tərəfindən verilənlər aşkarlana bilər. Hətta əlavəyə doğrudan da ehtiyac olduqda məlumatı təyin olunmuş kanalla göndərdikdə belə smartfon modeli heç də həmişə istifadəçini kifayət qədər mənfi ünsürlərdən qoruya bilmir. Məsələn, proqram havanı təyin etmək üçün yer verilənindən istifadə etmək və Internetə qoşulmaq üçün icazə xahiş edə bilər. Əlavə proqram bundan mənfi ünsür kimi istifadə edə bilər, yer ünvanını marketinq məqsədi ilə reklam serverinə göndərə bilər. Belə ki, son araşdırmalarda qeyd olunur ki, 30 smartfonda əlavələr oxunub [12]. Heç bir halda istifadəçi razılığı əldə edilməyib. Başqa bir misal, S-Mobile təsvir edir ki, 48, 694 sifarişlərin Android bazarında öyrənilməsi özəl və ya məxfi məlumatlara icazə üçün hər beş əlavədən bir məlumat xahiş edir, onları hücumçu qərəzli məqsədlər üçün istifadə edə bilər [13].

R6. Şəbəkəyə sızma hücumları

Təhlükə təsviri	Təcavüzkar ziyankar şəbəkəyə giriş nöqtəsi (Wi-Fi və ya GSM) tapır. Təcavüzkar daha sonra əlaqəni kəsir, belə halda istifadəçi üçün fişinq hücumları həyata keçirmək olar.

Wi-Fi və Bluetooth vasitəsilə smartfonlar şəbəkəsinə müdaxilə edilə bilər. Dolandırıcının Internet portal adları smartfonlarda zərərli SMS mesajı ilə konfiqurasiya edilə bilər. Bu giriş nöqtəsindən Wi-Fi və Bluetoothdan istifadə etməklə smartfonun şəbəkə kommunikasiyasına təsir etmək olar [14]. Daha mürəkkəb sızma hücumu ziyankarın GSM baza stansiyası quraşdırmasına əsaslanır. Bu hücum 3G şəbəkələri üçün mümkün deyil. Dolandırıcının Wi-Fi nöqtəsindən və ya digər şəbəkə qovşaqlarından digər bir neçə hücumu həyata keçirmək üçün bir vasitə kimi istifadə edilə bilər.

R7. Müşahidə hücumları

Təhlükə təsviri	Hücumçu müəyyən olunmuş istifadəçini smartfon vasitəsilə müşahidə edir.

Smartfonlar müəyyən adamı müşahidə altında saxlamaq üçün də istifadə oluna bilər. Smartfonda mikrofon, kamera, KS və GPS kimi bir çox sensorlar vardır. Bu imkanlar smartfonu fərd ilə bağlayaraq, həm də onu casusluq aləti edir [15]. Bəzən istifadəçi hücumçunu ziyanlı əlavə yükləməklə aldada bilər. Buna sadə bir misal, app Tap Snake – guya ki, sadə Snake oyunudur, GPS ilə ünvan məlumatları əldə edə bilər [16].

R8. Nömrəyığan hücumu

Təhlükə təsviri	Hücumçu istifadəçidən ziyanlı proqram təminatı ilə pulları oğurlayır, hansı ki,

SMS xidməti ilə gizli istifadə edir.

Müəyyən zənglər üçün, məsələn SMS, mikroödənişlər, o cümlədən telefon zəngləri və ölçülən GSM/UMTS və s. üçün istifadəçi smartfonlarda pul xərcləyir. Əgər hücumçu istifadəçi smartfonunda əlavə proqramlar quraşdıra bilsə, gizli şəkildə bunları istifadəçinin öz razılığı ilə həyata keçirə bilər. Bu hücumun riski yüksək qiymətləndirilir, çünki, bu hücumlar istənilən büdcədə yerləşə bilər.

R9. Zərərli maliyyə hücumları

Təhlükə təsviri	Smartfon zərəli proqram təminatı ilə yoluxur, bilərəkdən kredit kartının nömrəsinin, distant bank xidmətinin oğurlanması üçün yönəlib.

Maliyyə zərərli proqram təminatı şəxsi məlumatları oğurlamağa yönəlmiş, orta səviyyəli insanın maliyyə əlavələrinə və ya veb-servislərinə hücum edən proqram təminatıdır. Maliyyə zərərli proqram təminatı konkret mandat oğurlamaq və ya maliyyə ərizə və ya internet xidmətlərində hücumlar yerinə yetirilməsi üçün nəzərdə tutulmuş proqram təminatıdır. Maliyyə zərərli proqramlar - kredit kartı nömrələri yığmağa, onlayn bank ərizəsi üçün SMS identifikasiya kodları ələ keçirmək üçün hücum ola bilər.

R10. Şəbəkənin yüklənməsi

Təhlükə təsviri	Smartfondan istifadəyə görə şəbəkə resursunun yüklənməsi

Smartfonların və mobil internetin tətbiqi şəbəkə yüklənməsi riskini artırır. Şəbəkənin yüklənməsi iki yolla baş verə bilər:

Siqnal yüklənmə: Smartfonun daimi əlavələri həmişə yeniləşmiş məlumat üçün şəbəkəni soruşurlar. Göndərilən məlumatın hər bir biti üçün çoxlu sayda siqnal göndərilir (məsələn, iş qabiliyyətini yoxlamaq məlumatları). Tipik smartfon 8 dəfə artıq siqnal trafikini ümumiləşdirir, nəinki noutbuk USB aparat açarı ilə [17].

İnformasiya yüklənməsi: Cisco qiymətləndirmələrinə görə, mobil məlumatların trafiki hər il artaraq 2009 və 2014 arasında 39 dəfə artmışdır [18].

NƏTİCƏ

Bu işdə smartfonların daha çox yayılmış növləri, onlarda olan əməliyyat sistemləri haqqında qısa məlumat verildi. Smartfonların getdikcə imkanlarının daha da genişləndiyini və onların insanların gündəlik həyatının ayrılmaz hissəsi olduğunu qeyd etdik. Eyni zamanda smartfonların imkanları və bu imkanlarla yanaşı bu günümüzdə istifadəçilər üçün informasiya təhlükəsizliyi barədə məlumat verdik. Bu istifadəçilərin hansı hücumlara məruz qala biləcəyini göstərdik. Qeyd etdiyimiz kimi işdə smartfon istifadəçilərinin informasiya təhlükəsizliyi üçün 10 risk qiymətləndirilir. Əsas risklərin icmalını verdik, istifadəçiləri risklərlə məlumatlandırdıq.

ƏDƏBİYYAT

[1] Computerwoche. Die Kanzlerin bekommt ihr Merkel-Phone.[Online] http://www.computerwoche.de/netzwerke/mobile-wireless/1910789/

[2] comScore .European Smarthone Market Grows 41 Percent in Past Year.2010.
http://www.comscore.com/Press_Releases/2010/9/European_Smarthone_Market_Grows_41_Percent_in_Past_Year

[3] http://en.wikipedia.org/wiki/Mobile_operating_system

[4] Mobile Security Device
www.cse.wustl.edu/~jain/cse571-11/ftp/mobiles/#SmarThread

[5] www.kaspersky.com/about/new/virus/2013/99_of_all_mobile_threats_target_Android

[6] The Tech Journal. Monitor your Body On Your Android Cellphones. 2010.
http://www.thetechjournal.com/tech-news/monitor-your-body-on-your-android-cellphones.xhtml

[7] International Organization for Standardization. ISO.IEC 27005.2008.

[8] Government calls for action on mobile phone crime. BBC. Cellan-Jones, Rory. 2010.
http://news.bbc.co.uk/2/hi/technology/8509299.stm.

[9] ENISA. Cloud computing Security Risk Assesment. [Online]
http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment.

[10] Marienfeldt.B. Iphone business security framework. [Online] 2010
http://www.marienfeldt.wordpress.com/2010/03/22/iphone-business-security-framework/.

[11] http://www.abiresearch.com/press/1015-Recycled+Handset+
+Shipments+to+Exceed+100+Million+Units+in+2012.

[12] F-Secure. Warning On Possible Android mobile Trojans. [Online] January 2010http://www.f-secure.com/weblog/archives/00001852.html.

[13] SMobile Systems. Threat Analysis of the Android Market. [Online] 2010.
http://threatcenter.smobilesystems.com/wp-content/uploads/2010/06/Android- Market-Threat-Analysis-6-22-10-v1.pdf.

[14] Mobile Security Lab. Hijacking Mobile Data Connections. s.l:Blackhat, 2008

[15] TSH Soft Group. The SPY Phone.com [Online] http://www.thespyphone.com/.

[16] PCWorld. Android Game is a Spy App in Disguise. [Online] 2010.
http://www.pcworld.com/article/203512/android_game_is_a_spy_app_in_disguise.html?+k=hp_new.

[17] Airvana. Solving the mobile netwirk signalling overload. [Online] 2010. http://viewer.zmags.co.uk/publication/d5f7ecee#/d5f7ecee/4.

[18] CISCO. Visual Networking Index: Global Mobile Data Traffic Forecast Update. [Online]2010
http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.html