СИГУРНОСТТА В МОБИЛНИЯ СВЯТ

Николай Касъклиев

ПУ „Паисий Хилендарски“ , гр. Пловдив, ул. „Цар Асен“ 24
kasakliev@uni-plovdiv.bg

***Резюме**: Развитието на технологиите и в частност на мобилните устройства, подобряването на техните технически характеристики и все по-богатата им функционалност и достъпност, засилват необходимостта за потребителите и разработчиците на мобилни приложения да обръщат все по-голямо внимание на въпросите, касаещи сигурността. В работата е направен анализ на рисковете по отношение на сигурността и опит да се систематизират добри практики и препоръки, които следва да се спазват както от обикновените потребители, така и от разработчици на средства за осигуряване на висока степен на сигурност.*

***Ключови думи**: мобилни приложения, компютърна сигурност, мобилни устройства*

Увод

В наши дни почти всеки използва някакво мобилно устройство (смартфон, таблет, лаптоп и др.) в ежедневието, независимо дали за работа, обучение или за забавление. Според някои статистически данни вече 90% от населението на земята разполага с мобилен телефон, повече от 50% използва смартфон, половината от потребителите на мобилни устройства използват устройствата си за Интернет, около 80% използват мобилни приложения а половината от притежателите на таблети и смартфони пазаруват чрез тях.

Всички тези данни показват една ясна тенденция на бързо нарастване на броя на мобилни устройства сред потребителите и все по-широката им употреба, вкл. за пазаруване, обучение, банкиране, търсене на информация, социални контакти и много други.

Предимствата за обикновения потребител се изразяват в бързо и лесно намиране на информация, достъп до интернет услуги по всяко време и от почти всяка точка на земното кълбо. Наред с предимствата все по-отчетливо се откроява и необходимостта да се обръща по-голямо внимание и на въпросите, касаещи сигурността. От техническа гледна точка това са: антивирусна защита, кодиране на информацията, защита чрез биометрични данни и др.

Колкото мобилните устройства стават „по-умни“, толкова повече и по-цена информация се съхранява на тях. Лични данни, данни за кредитни и дебитни карти, пароли, сертификати за сигурност, документи, електронна поща и много

друга важна информация се съхранява и използва от потребителя, което значително увеличава риска от нейната кражба или загуба.

Целта на настоящата работа е да се изследват рисковете за сигурността пред мобилните устройства и информацията и да се посочат добри практики, препоръки и политики за повишаване на сигурността, както от гледна точка на обикновения потребител, така и от тази на разработчика на приложения за мобилни устройства.

1. Опасности

Повечето от настолните компютри, с които работим днес са относително защитени от рискове, свързани с различни опасности - това е така, защото повечето разработчици на операционни системи и потребителски софтуер проектират и вграждат, като стандарт, механизми и инструменти за защита, вкл. защитни стени, антивирусни програми, инструменти за криптиране и контролиран достъп и др..

При мобилните устройства, обаче, нещата са различни. Повечето от тях не разполагат с вградена програма за сигурност или ако има, то тя не е активна. От друга страна потребителите на мобилни устройства много често игнорират рисковете.

Според Symantec[ISTR] в сравнение между 2011 и 2012 година увеличението на атаките срещу мобилни устройства е с 59%. Според друго изследване на Kaspersky [KSB12] увеличението е с 34%. Макар и стойностите да не са много близки, вижда се една ясна тенденция към увеличаване на заплахите пред потребителите на мобилни устройства. Най-застрашени в момента са потребителите на устройства с Android, тъй като за тях са идентифицирани най-много видове заплахи. Най-атакувани, обаче, са устройства, базирани на Apple iOs, а устройствата с Windows Phone са атакувани най-малко в момента.

Статистиката показва, че атаките към мобилните устройства са в следните направления:

1. Около 32% от атаките са свързани с кражба на информация;
2. 25% са традиционни заплахи, като изтриване, отказ от работа и др.;
3. 15% касаят проследяване на потребителя;
4. 13% касаят изпращане на съдържание от устройството;
5. 8% преконфигуриране на устройството;
6. и 8% нежелани реклами.

Мобилните устройства могат да бъдат подложени на атаки по различни начини, но можем да ги обобщим в следните три категории.

а). Атаки от Интернет. Една от основните характеристики на съвременните мобилни устройства е Интернет свързаността. Независимо дали сърфираме,

изпращаме или получаваме поща, ние сме застрашени пак от червеи, вируси или троянски коне по същия начин, както са застрашени и настолните компютри. Интересен факт е, че първите вируси за мобилни устройства, разпространени по Интернет, са идентифицирани през 2004г., създадени за популярната по онова време Symbian OS.

б). Атака, чрез свързан с кабел десктоп компютър. Друга отличителна характеристика на умните устройства е възможността за синхронизация. Синхронизацията може да бъде на електронната поща, на календара или на различни потребителски файлове. Тъй като, по принцип, мобилните устройства осъществяват т.н. “trust” връзка с настолния компютър, то рискът от пренасяне на вирус е дост голям. Друга ситуация е когато потребителя инсталира приложения или дори операционна система т.н. jailbreaking или rooting по кабел.

в). Атака през мрежа. Тъй като съвременните мобилни устройства са неизменно свързани с някой доставчик на гласови или услуги за пренос на данни, то в тази мрежа също могат да се крият рискове за сигурността, най-често чрез кратки или мултимедийни съобщения. Също така съвременните мобилни устройства разполагат с функции за достъп до безжични компютърни мрежи, които също могат да бъдат източник на атака.

Мобилните устройства са изложени на редица рискове по отношение на сигурността, сходни с тези за десктоп компютрите, като тук ще посочим основните.

Mobile Malware - зловреден софтуер. В тази категория се включват вируси, червей, троянски коне и други програми. Този вид рискове главно касаят кражба на ценна информация, като пароли, пин кодове, но и могат да записват глас или да използват вградената камера. Опасността е голяма, тъй като потребителите все по-често използват мобилни устройства за бизнес, банкиране и пазаруване.

Кражба и изгубване. Характерно за мобилните устройства е техния малък размер. От тази гледна точка те са лесна мишена на крадци или лесно могат да се загубят. Наред с рисковете посочени в предишната категория и по-конкретно за мобилните телефони съществува риск от натрупване на значителна телефонна сметка от проведени международни или продължителни разговори или пренос на данни.

Друга вид касае **риск за съдържанието**. Например, , мобилните устройства разполагат с камера, чрез която могат да се сканират QR кодове. Съдържанието, което се крие зад тези кодове, може да бъде текст, имейл адрес или интернет адрес, посещението на който може да доведе до риск.

Риск от проследяване. Голяма част от мобилните устройства имат вграден GPS приемник, който позволява да се използват услуги, като напр.

навигация. Някои приложения, като тези за социалните медии, също използват услугите за установяване на местоположението на потребителя, което води до риск от физическо проследяване.

Риск в облака. В последните няколко години се наблюдава увеличаване на използване от обикновения потребител на все повече облачни услуги. Доставчиците на такива услуги се увеличават значително,като се започне от утвърдени компании в бранша и се стигне до не там сигурни малки компании с ограничен потенциал за осигуряване на високо ниво на сигурност. В най-голяма степен облака се използва като хранилище на документи, като в редица случаи потребителите съхраняват и документи, които съдържат лична информация, която може да бъде откраднатa.

От представеното дотук може да заключим, че тенденцията на разпространение на мобилни устройства с разширени технически характеристики и функционалност сред потребителите ще се запази и в бъдеще, като някои дори прогнозират и скорошен край на традиционните десктоп компютри. Наред с това, обаче, опасностите, свързани с такива устройства, се увеличават и изискват все по-голямо внимание, както от обикновения потребител така и от разработчиците на приложения за тях.

2. Сигурност

Тук се предлагат добри практики и препоръки за повишаване на сигурността по отношение на представените вече опасности. Разглеждат се от две гледни точки - на обикновен потребител и на разработчик на приложения за мобилни устройства.

2.1. Обикновен потребител

За обикновения потребител е важно да си отговори на следния въпрос: Какво да направя за да повиша сигурността?

Отговорът на този въпрос може да бъде много обстоен. Съществуват много източници на информация по темата - от производителите на мобилни устройства през разработчиците на мобилни операционни системи и приложения до обикновени потребители, сблъсквали се с подобни проблеми. По-долу са представени част от препоръките, общи за различните типове мобилни устройства и различни мобилни платформи (Android, IPhone, Windows Phone и др.).

- Конфигуриране на мобилното устройство с код за достъп или пин код, ако позволява. Това ще ограничи използването му при изгубване или кражба.
- Конфигуриране за автоматично заключване.

- Регулярно актуализиране на инсталираната мобилна операционна система и мобилните приложения. Позволява защита от открити бъгове или дупки в сигурността.
- Инсталиране или активиране на антивирусен софтуер.
- Инсталиране и използване само на мобилни приложения от сигурен интернет магазин за приложения. В противен случай риска се увеличава значително.
- Ако устройството позволява да се използва криптиране на информацията. Могат да се използват софтуерни инструменти като Norton Mobile Security, Lookout, и др.
- Използване на устройството само в мрежи с високо ниво на защита.
- Конфигуриране на интернет браузърите адекватно.
- Периодично създаване на бакъп.
- Използване на приложения от типа Find my Phone.
- Особено внимание при отваряне на Email, SMS, QR кодове от непроверени източници.
- Изтриване на цялата информация ако устройството се продава, дава за ремонт или изхвърля.
- Деактивиране на всички функции на устройството, които не се използват в даден момент или дълготрайно.

2.2. Разработчик на мобилни приложения

Тук ще разгледаме препоръки, които могат да се спазват от разработчици на приложения, за да бъдат с по-малък риск за сигурността. Ще разгледаме три от основните платформи с доминиращ дял (около 94%) на пазара на мобилни устройства Android, iOs и Windows Phone.

В помощ на разработчиците на Android [BPSP], Apple [SCG] и Microsoft [SDC] приложения са публикувани добри практически съвети и препоръки. Наред с официалните източници в специализираната литература за разработчици също могат да се намерят такива. В допълнение компаниите верифицират предложените от разработчиците приложения за съответната платформа преди да ги публикуват на официалните специализирани интернет магазини .

Платформите разполагат с вградени средства и механизми за осигуряване на висока сигурност. За улеснение на разработчиците, платформите са така разработени, че да осигурят добро ниво на сигурност по подразбиране.

След направен анализ се установи, че и трите платформи имат сходни средства и механизми. Някои от вградените свойства са:

- Sandbox механизъм, който осигурява изолиране на данните и изпълнението на програмата за отделните приложения. По този начин всяко приложение е предпазено от интервенция от друго.
- Работна рамка, осигуряваща имплементация на най-често използваните методи за сигурност, като криптиране, защита при интерпроцесната комуникация и ограничен достъп.
- Файлова система, позволяваща криптиране на информацията.
- Ограничаване на достъпа до системни функции и данни на базата на категории потребители.
- Дефиниране на ограничения на принципа за всяко приложение отделно.

При разработка на мобилни приложения основният въпрос, касаещ сигурността, е мястото и начина на съхранение на данните и ограничаване на достъпа до тях. При мобилните устройства данните се съхраняват или на вътрешната или на външната памет. По принцип когато данните се съхраняват на вътрешната памет и те са защитени от достъп само за съответното приложение. Когато обаче данните се съхраняват на външна памет, като SD карта, те са достъпни за четене и промяна от всички. Тъй като такава карта може да се премахне, то не се препоръчва изпълними файлове и важна информация да се съхранява там или картата да се криптира.

Що се касае до ограничаване на достъпа се използва механизма на т.н. позволения (permissions). Главната препоръка за разработчиците е да се създават приложения, които не изискват специални позволения или те са малко. Самите платформи дефинират стандартни позволения, които могат да се използват при почти всяка ситуация. Особено внимание трябва да се обръща на системните и споделени файлове, ако някое приложение изисква работа с тях, то за приложението трябва да се дадат позволения само за четене. Също така трябва да се избягва функционалност, позволяваща промяна на самите позволения.

Друга важна област, касаеща сигурността, са мрежовите комуникации. Голяма част от мобилните устройства се използват именно в такава среда. Заплахата идва от това, че при тези комуникации често се изпраща важна лична информация, което крие голям риск. Добрите практики сочат използването на подходящия протокол, когато се обменя такава информация по мрежа. Например, когато се предава чувствителна(?) информация да се използва HTTPS протокола за да се осигури защитен уеб пренос. В допълнение приложенията трябва да използват цифрови сървърни сертификати само от познати източници или т.н. Certificate Authorities (CAs), в противен случай трябва или да се извежда предупреждаващо съобщение на потребителя или да не се осъществи комуникация. Що се касае до клиентските сертификати, някои типове приложения задължително трябва да ги изискват.,

Такива са приложенията, изискващи финансови транзакции, като интернет банкиране, разплащания при покупки, приложения позволяващи достъп до корпоративни мрежи и други.

Друга препоръка за разработчиците е да избягват разработка на приложения на базата на SMS протокола. Вместо това да се използват облачни услуги за съобщения и известяване като Google Cloud Messaging, Windows Push Notification Services и iOS Push Notifications, за да се предават съобщения между уеб сървър и клиентско приложение. Чрез използване на кратки съобщения могат да се изпраща спам до произволен потребител от телефонната книга или от компрометирана мрежа на оператор. Други видове атаки, чрез кратко съобщение е нежелано използване на услуги с добавена стойност, фишинг, малуер и други.

Не по-маловажна мярка за повишаване на сигурността при разработка на приложения за мобилни устройства е валидиране на данните, които потребителя ще въвежда, използвайки дадено приложение. Опасностите могат да бъдат препълване на буфера и отказ от обслужване. Друг от примерите е свързан с използване на скриптови езици, като JavaScript и SQL. Голяма част от мобилните приложения използват SQL бази данни за да съхраняват информацията, която потребителя въвежда или пък изисква справка, което води до риск от т.н. SQL injection или с други думи внедряване на SQL код в потребителския вход. Решението е да се използват средствата на различните платформи за правилното форматиране на входните за програмата стрингове.

Поредния въпрос, с който трябва да се съобразяват разработчиците на приложения, но който е от изключителна важност, е този за съблюдаване на законодателството и нормативните рамки на страната или региона за който е предназначено това приложение. В много страни има строги ограничения за това каква информация може да се изисква от потребителя, квалифицира се като лична, и е предмет на защита от съответните закони. Други примери, които могат да се посочат, са приложения подходящи само за определена възрастова група, например деца, приложения, които позволяват проследяване на местоположението на потребителя и други. В тези случаи разработчикът трябва да осигури подходяща форма за запознаване на потребителя с това каква информация ще се събира и съхранява, дали ще се използва и за какви цели и то преди приложението да бъде инсталирано или използвано за първи път.

Заключение

След направения анализ на видовете рискове пред мобилните устройства и засилването на атаките, на които са подложени от една страна и все по-честото им използване в практиката за пазаруване, банкиране и лична кореспонденция от друга, на все по-преден план излизат аспектите относно

сигурността. От особена важност за потребителите днес е да осъзнаят сериозността на проблема и да вземат съответните мерки. За разработчиците на приложения за мобилни устройства остава важната задача да създават такива приложения, които са с висока степен на защита, следвайки наложените добри практики и препоръки и в съзвучие с законовата рамка за съответния регион.

Благодарности

Работата е частично финансирана по проекти BG051PO001-4.3.04-0064, Пловдивски електронен университет (ПеУ): национален еталон за провеждане на качествено е-обучение в системата на висшето образование, ЕСФ (2012 – 2014) и BG051PO001-3.1.08-0041 „Стандартизиране и интегриране на разнотипни информационни и управленски университетски системи (СИРИУС)“, финансиран от ОП „Развитие на човешките ресурси“, ЕСФ (3013-2014).

Литература

1. [BPSP] Best Practices for Security & Privacy, http://developer.android.com/training/best-security.html.
2. [ISTR] Internet security tread report, http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf.
3. [KSB12] Kaspersky Security Bulletin 2012, http://www.securelist.com/en/analysis/204792255/Kaspersky_Security_Bulletin_2012_The_overall_statistics_for_2012.
4. [SCG] Secure Coding Guide, https://developer.apple.com/library/ios/documentation/Security/Conceptual/SecureCodingGuide/Introduction.html.
5. [SDC] Security Developer Center, http://msdn.microsoft.com/en-US/security/default.aspx.

SECURITY IN THE MOBILE WORLD

Nikolay Kasakliev

Plovdiv University "Paisii Hilendarski", Plovdiv, "Tsar Asen"str. 24
kasakliev@uni-plovdiv.bg

Abstract: *The evolution of the technologies, particularly mobile devices, improvement of their performance and increasing their rich functionality and affordability, increase the need for users and developers of mobile applications to pay more attention to the issues concerning security. This paper cover an analysis of the risks to the security and attempt to codify best practices and recommendations that should be respected by both ordinary users and developers to provide a high level of security.*