УДК 004.9

Ю. Ф. Петяк
Українська академія друкарства

ФАКТОРИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ МОБІЛЬНИХ ПРИСТРОЇВ

Розглянуто фактори загроз інформаційної безпеки мобільних пристроїв, які впливають на можливість проведення атак, спрямованих на витік даних.

Інформаційна безпека, витоки даних, мобільні пристрої, фактор, атака, зловмисник, програмне забезпечення, мобільна операційна система

Мобільні пристрої (МП) відіграють важливу роль у нашому житті. Складно уявити сучасну ділову людину без смартфона, за допомогою якого вона вирішує свої повсякденні завдання, як бізнесові, так і приватного характеру. За останні роки спосіб використання мобільних пристроїв докорінно змінився. Вони застосовуються не лише як засоби комунікації, а й як пристрої збереження та обробки важливої і цінної інформації. Ріст популярності МП та їх повсюдне застосування зробило ці пристрої ідеальною мішенню для зловмисників. Як зазначають експерти з інформаційної безпеки (ІБ), останніми роками помітно зросла кількість цілеспрямованих атак саме на мобільні пристрої [3].

Наявні методики захисту даних на МП суттєво поступаються технологіям, застосовуваним на персональних комп'ютерах. Це зумовлено передусім особливостями мобільної платформи, технічними характеристиками та класичним позиціюванням МП лише як засобу спілкування. Недооцінювання користувачами та бізнесом прихованих загроз, які несуть у собі МП, може призвести до фінансових втрат та втрати репутації. Навпаки, кіберзлочинці зрозуміли можливості мобільних телефонів й активно використовують їх для своєї діяльності.

Популярними видами атак на МП є використання шкідливих програм для крадіжок грошей у системах мобільного банкінгу та SMS–віруси. Інформаційна безпека (ІБ) має два чинники. Перший — це те, яку архітектуру безпеки має система. Другий — поширеність цієї системи. Чим менше система розповсюджена, тим менше буде на неї атак. Атакують переважно ОС Android, тому що це вигідніше порівняно з іншими системами. Останнім часом спостерігається збільшення атак, метою яких є крадіжка конфіденційних даних [3]. Особливо гостро ця проблема постає з поширенням підходу Bring Your Own Device (BYOD), коли приватні МП працівників компаній використовуються для опрацювання корпоративних даних [2]. Існують різні підходи до впровадження BYOD, кожна компанія вибирає свій шлях, власні правила використ-

тання МП на роботі. Великий та середній бізнес часто будують власну інфраструктуру із застосуванням систем Mobile Device Management (MDM). Однак впровадження системи MDM економічно невиправдане для малих компаній, що змушує їх шукати альтернативні шляхи забезпечення належного рівня ІБ при використанні персональних МП. Однак причиною витоків даних може бути сам користувач. Необізнаність у сфері інформаційних технологій та недотримання елементарних правил ІБ призводить до втрати МП і в подальшому до їх несанкціонованого використання для доступу до конфіденційних даних [5].

Тому важливим практичним завданням є розроблення та впровадження інформаційних технологій і заходів, спрямованих на підвищення рівня захисту персональних і корпоративних даних на МП. Для розв'язання поставленої задачі слід насамперед визначити фактори впливу на можливість здійснення атак на МП, спрямованих на витік інформації.

Фактори інформаційної безпеки — це причини, що призводять до порушення ІБ на конкретних МП й обумовлені недоліками їх функціонування, властивостями архітектури безпеки МП, застосовуваними програмним забезпеченням і апаратною платформою, умовами експлуатації [1]. Фактори ІБ можна умовно поділити на людські, технологічні та організаційні. Людський фактор визначається досвідом і поведінкою користувача, його розумінням можливих загроз ІБ. Може мати навмисний або ненавмисний характер. Технологічні фактори мають недоліки в програмно-апаратній платформі й комунікаційні засоби. Організаційні фактори описують вимоги до архітектури ІБ, заходи та політики для забезпечення необхідного рівня захисту даних на МП.

Фактори інформаційної безпеки

1. *Несанкціоноване розробником втручання (НВ) користувача* в роботу пристрою шляхом внесення змін у системні налаштування, прямий доступ до функцій ядра системи та системних файлів, оминаючи вбудовані механізми безпеки [7]. Це значно підвищує вірогідність зараження мобільної операційної системи (МОС) шкідливим програмним забезпеченням (ПЗ) і ставить під загрозу конфіденційні дані чи корпоративні ресурси. Більше того, отримавши необмежений і неконтрольований доступ до пристрою, користувач має такий же рівень доступу для троянських програм. При цьому порушується ліцензійна угода, в результаті чого власник пристрою позбавляється права на технічну підтримку від розробника та гарантійних зобов'язань. Експертами використовуються терміни, якими описується процедура отримання адміністративних прав користувачем на своєму пристрої — «device rooting» для систем на базі Android та «jailbreak» для систем на базі iOS. Існують різні причини, з яких користувачі здійснюють таке втручання. Найчастіше користувачі отримують можливість: встановлювати стороннє ПЗ на пристрій, що в іншому разі було б неможливо; змінювати ОС пристрою на альтернативні; розширювати функціональні можливості пристрою. Даний фактор є найважливішим серед інших,

адже користувач свідомо йде на цей крок, часто не розуміючи, до яких наслідків це може призвести.

2. *Наявність каналів передачі даних (КПД).* Сучасні мобільні пристрої наділені різноманітними комунікаційними технологіями. Передовсім це бездротовий зв'язок Wi-Fi та мобільна передача даних 2G/3G/4G, популярна і технологія Bluetooth. Наявність комунікаційних можливостей дозволяє зловмисникам здійснювати віддалені мережеві атаки на мобільні пристрої, а шкідливому ПЗ непомітно передавати конфіденційну інформацію за межі пристрою. Однак відмовитися від використання цих технологій неможливо, тому необхідно контролювати передачу каналами зв'язку конфіденційних даних та реагувати на мережеві атаки. Для цього використовують різні підходи. Наприклад, можна дозволяти передачу важливих даних лише в межах приміщень, де канали передачі надійно захищені від прослуховування чи зовнішнього втручання. Цей фактор важливий з огляду на те, що наявність КПД суттєво спрощує атаки, спрямовані на витік інформації.

3. *Локація (Л).* Дозволяє визначити, в якому середовищі та місці перебуває мобільний пристрій і на основі цієї інформації приймати обґрунтоване рішення щодо заборони чи дозволу про опрацювання або передачу важливих даних. Більше того, МП можуть бути загублені або викрадені, що, у свою чергу, призведе до компрометації даних. Для запобігання цьому можна використовувати бездротові сенсорні мережі чи систему GPS [4]. Однак важливо розуміти, що розповсюдження даних про розміщення пристрою в системах геолокації зумовить створення додаткових загроз ІБ, адже зловмисники можуть з великою точністю визначити розташування пристрою, що полегшить їм вибір вектора атаки.

4. *Кваліфікація користувача (КК).* Визначає рівень володіння ним сучасними ІТ і вміння застосовувати їх для безпечного опрацювання та передачі даних. Користувачі мусять чітко слідувати правилам політики ІБ, прийнятої на корпоративному рівні, постійно контролювати свої дії. Проте це не завжди допомагає, що призводить до витоків важливої інформації. Людина стає тією слабкою ланкою, яка визначає загальний рівень ІБ системи [6]. Зловмисники використовують це для здійснення атак методами соціальної інженерії, що часто є ефективнішим і швидшим способом крадіжки даних. На думку фахівців, подібні атаки займатимуть провідне місце серед інших типів атак і їх кількість буде неухильно зростати. Протистояти таким атакам можна, використовуючи системи DLP.

5. *Технічна підтримка (ТП) розробника МП.* Кожен МП складається з двох основних частин — апаратної та програмної. Апаратний пристрій працює під управлінням МОС. При створенні МП розробники проводять всебічне тестування апаратної частини, тому атаки на МП або крадіжка даних з них у результаті вразливостей на апаратному рівні є малопоширеними. Помилки при написанні коду МОС можуть мати більш критичні наслідки. Саме вони ство-

рюють можливість проведення різноманітних атак як на рівні ядра чи системних компонент ОС, так і на рівні ПЗ. Існують методики ще на стадії тестування МОС виявляти більшість помилок, проте значна їх кількість залишається непоміченою. Зловмисники відшукують ці помилки і проводять за допомогою їх 0day-атаки, які є найбільш небезпечними. Ураховуючи це, розробники як МП, так і МОС постійно оновлюють системне та прикладне ПЗ, виправляючи в них знайдені помилки та вразливості. Відомі виробники створюють ефективну інфраструктуру підтримки своєї продукції, а маловідомі не приділяють достатньо уваги даному питанню, що призводить до появи на ринку продукції, підтримка якій не надається. Ці пристрої насамперед стають жертвами атак зловмисників. Зважаючи на це, великий і середній бізнес намагається використовувати в своїй діяльності продукцію відомих фірм — Samsung, Apple, BlackBerry й інших. Однак з розповсюдженням BYOD вони змушені враховувати специфіку кожного мобільного пристрою. До того ж слід пам'ятати, що після втручання користувача в роботу пристрою втрачається змога отримання технічної підтримки, а оновлення МОС стає неможливим. Цей фактор також важливий при проектуванні систем ІБ.

6. *Наявність засобів інформаційної безпеки (ЗІБ)* безпосередньо впливає на загальний рівень захисту даних на мобільному пристрої. До цих засобів відносяться: антивіруси, міжмережевий екран (firewall), системи шифрування даних тощо [5]. Подібне ПЗ необхідно встановлювати користувачем самотужки. Відомі виробники систем захисту мають рішення як для комп'ютерних платформ, так і для МП. Однак часто для того щоб встановити ЗІБ на МП та забезпечити ефективну протидію загрозам, потрібно надати цим програмам найвищі адміністративні права, що неможливо без втручання у функціонування МП. Рівень захисту, який ЗІБ надають користувачеві, залежить від його правильного налаштування. Таким чином, даний фактор залежить від фактора РК, а його значення є достатньо важливим.

7. *Інтегрований показник надійності встановленого ПЗ (ІПН)*. Цей фактор обчислюється за методикою, прийнятою розробником МОС. Для платформи Android використовується рейтинг ПЗ на Google Play. Ще однією складовою зазначеного фактора є права, отримані програмами при інсталяції чи запуску. ПЗ може одержувати та використовувати ресурси МП та МОС лише згідно з правами, явно заданими розробником ПЗ. Винятком є шкідливе ПЗ, яке обходить це обмеження, експлуатуючи помилки в розробці МОС, або неправильне налаштування пристрою. Цей показник має середню вагу, оскільки розробники МОС постійно удосконалюють свої методики визначення «ненадійності» ПЗ сторонніх виробників, тому випадків зараження МП зазначеним способом стає все менше.

8. *Можливість встановлення ПЗ із сторонніх джерел (СД)*. На МП можна встановлювати ПЗ з офіційного джерела та сторонніх джерел. Для платформи Android офіційним джерелом ПЗ є Google Play, для iOS — App Store. ПЗ

у цих джерелах є перевіреним розробником МОС, тому користувач має певну гарантію, що МП матиме високий рівень захисту. Щоправда, іноді в офіційних джерелах знаходили ПЗ з ознаками деструктивних дій, тому і Google, і Apple змушені були посилити вимоги до якості ПЗ сторонніх розробників. Розробники МП рекомендують не встановлювати ПЗ зі сторонніх джерел, окрім офіційних або довірених. Цей фактор має важливе значення, оскільки прецедентів зараження МП сторонніми програмами, встановлених з неофіційних джерел, стає все більше.

Визначення факторів, які впливають на ІБ мобільних платформ, є першим кроком у створенні надійних систем безпеки МП. У подальшому має бути експертне оцінювання запропонованих факторів і визначення їх пріоритетності для обчислення інтегрального числового показника надійності системи захисту МП.

1. Вихорев С. В. Классификация угроз информационной безопасности [Электронный ресурс] // Годовой обзор «Сетевые атаки и системы информационной безопасности 2001»: [сайт]. — Режим доступа: http://www.cnews.ru/reviews/free/oldcom/security/elvis_class.shtml (23.10.14). — Название с экрана. 2. Петяк Ю. Ф. Вплив BYOD на безпеку корпоративних даних / Ю. Ф. Петяк // Тези доп. 17-ї міжнар. наук.-практ. конф. з проблем видавничо-поліграфічної галузі: 19 лист. 2013 р. — К. : УкрНДІСВД, 2013. — С. 27. 3. Петяк Ю. Ф. Методи боротьби з мережевими атаками в ОС Android / Ю. Ф. Петяк // Тези доп. наук.-техн. конф. проф.-викл. складу, наук. прац. і асп.: 5–8 лют. 2014 р. — Львів: Укр. акад. друкарства, 2014. — С. 118. 4. Семенов А. Беспроводные сенсорные сети — новые модели использования [Электронный ресурс] // А. Семенов / BYTE Россия. — № 12 (88), дек. 2005: [сайт]. — Режим доступа: http://www.bytemag.ru/articles/detail.php?ID=8780 (23.10.14). — Название с экрана. 5. Якушин П. Безопасность мобильного предприятия / П. Якушин // Открытые системы. — 2013. — № 1. — С. 22–25. 6. Recommendations for Data Loss Prevention in a Mobile Environment [Электронный ресурс] // ZONESE7EN: [сайт]. — Режим доступа: http://zonese7en.com/6-recommendations-for-data-loss-prevention-in-a-mobile-environment/ (21.10.14). — Название с экрана. 7. Sheldon Robert. Rooted Android device risks include network access, data theft [Электронный ресурс] / Robert Sheldon // Офіційний сайт TECHTARGET.COM: [сайт]. — Режим доступа: http://searchconsumerization.techtarget.com/tip/Rooted-Android-device-risks-include-network-access-data-theft (20.10.14). — Название с экрана.

ФАКТОРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МОБИЛЬНЫХ УСТРОЙСТВ

Рассмотрены факторы угроз информационной безопасности мобильных устройств, влияющих на возможность проведения атак, направленных на утечку данных.

FACTORS INFORMATION SECURITY MOBILE

Considered the factors of information security threats to mobile devices, which influence the possibility of attacks aimed at data leakage.

Стаття надійшла 19.10.2014