Пірог О.В., к.т.н., доцент
Державний університет «Житомирська політехніка»

СТАНДАРТИ ВЕРИФІКАЦІЇ БЕЗПЕКИ МОБІЛЬНИХ ДОДАТКІВ

У квітні 2023 року вийшов реліз версії 2.0.0 Стандарту верифікації безпеки мобільних додатків OWASP (OWASP Mobile Application Security Verification Standard – MASVS) [1]. Основними напрямками забезпечення безпеки мобільних додатків визначено: зберігання даних, криптографічні методи, аутентифікація та авторизація, мережевий зв'язок, взаємодія платформ, якість коду, стійкість до зворотного проектування та втручання.

Мобільні додатки обробляють широкий спектр конфіденційних даних, таких як персональні дані (PII), криптографічний матеріал, секрети та ключі API, які часто потрібно зберігати локально. Ці конфіденційні дані можуть зберігатися у пам'яті додатку. Також конфіденційні дані зберігаються або розкриваються у загальнодоступних місцях (використання API, резервне копіювання, журнали). Тому потрібний контроль, що гарантує належний захист конфіденційних даних, що зберігаються додатком, та всіх їх витоків.

Криптографія є важливою для мобільних додатків, оскільки мобільні пристрої дуже портативні і їх можна легко втратити або вкрасти. Зловмисник, який отримує фізичний доступ до пристрою, потенційно може отримати доступ до всіх конфіденційних даних, що зберігаються на ньому (паролі, фінансова інформація та особиста інформація). Криптографія є засобом захисту цих конфіденційних даних шляхом їх шифрування, щоб неавторизований користувач не міг їх прочитати. Також необхідно керувати криптографічними ключами протягом усього їх життєвого циклу (генерація, зберігання та захист ключів). Погане керування ключами може поставити під загрозу навіть найнадійнішу криптографію. Тому потрібно переконатися, що додаток використовує криптографію відповідно до передових галузевих практик, які визначені в стандартах, таких як NIST.SP.800-175B [2] і NIST.SP.800-57 [3].

Аутентифікація та авторизація є важливими компонентами мобільних додатків. Важливо, щоб додаток дотримувалася найкращих практик, щоб забезпечити безпечне використання протоколів. Мобільні додатки, щоб підтвердити особу користувача, використовують різні форми аутентифікації (біометрія, PIN-код, багатофакторна аутентифікація). Ці механізми мають бути реалізовані правильно, щоб забезпечити їх ефективність у запобіганні несанкціонованому доступу. Безпеку віддаленої кінцевої точки слід перевіряти за допомогою галузевих стандартів, таких як OWASP Application Security Verification Standard (ASVS) [4].

Забезпечення мережевої безпеки є критично важливим аспектом безпеки мобільних додатків. Щоб забезпечити конфіденційність і цілісність даних, що передаються, розробники зазвичай покладаються на шифрування, наприклад, за допомогою TLS. Однак існують способи вимкнення безпечних параметрів за замовчуванням або їх обходу (з використанням API або бібліотек сторонніх розробників). Мобільний додаток повинен встановлювати безпечні зашифровані з'єднання та перевіряти це. Розробник може довіряти лише певним центрам сертифікації (CA).

Безпека мобільних додатків значною мірою залежить від їх взаємодії з платформою, що передбачає розкриття даних за допомогою наданих платформою механізмів взаємодії між процесами (IPC), що можуть використовуватися зловмисниками. Конфіденційні дані (паролі, дані кредитних карток і одноразові паролі в сповіщеннях) відображаються в інтерфейсі користувача. Важливо переконатися, що ці дані не витікають через механізми платформи (автоматично створені знімки екрана), розкриття за допомогою «серфінгу через плече» або під час спільного використання пристрою. Тому потрібно безпечно використовувати надані платформою механізми IPC та безпечно відображати конфіденційні дані в інтерфейсі користувача.

Мобільні додатки мають точки введення даних (інтерфейс користувача, IPC, мережа та файлова система). Потрібно розглядати ці вхідні дані як ненадійні. Загрозами є ін'єкційні атаки (ін'єкція SQL, XSS або незахищена десеріалізація). Дефекти пам'яті, важко виявити під час тестування на проникнення, але їх можна запобігти за допомогою безпечної архітектури програмування. Існують вразливості програмування, які виникають із зовнішніх джерел (ОС і компоненти ПЗ сторонніх розробників). Розробники повинні дотримуватися найкращих практик, таких як OWASP Software Assurance Maturity Model (SAMM) [5] і NIST.SP.800-218 Secure Software Development Framework (SSDF) [6], перевіряти та дезінфікувати всі вхідні дані, щоб запобігти атакам ін'єкцій, а також забезпечувати оновлення додатків і платформ, щоб захистити від відомих вразливостей.

Заходи поглибленого захисту (обфускація коду, anti-debugging, anti-tampering тощо) важливі для підвищення стійкості додатків до зворотного проектування. Вони створюють нові рівні контролю безпеки, що ускладнює зловмисникам зворотне проектування. Такий захист перешкоджає з'ясуванню того, як додаток працює за допомогою статичного аналізу, запобігає динамічному аналізу. Ці заходи створюють додатковий захист.

Список використаних джерел

1. OWASP Mobile Application Security Verification Standard URL: https://mas.owasp.org/MASVS/11-MASVS-RESILIENCE/
2. NIST.SP.800-175B Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms URL: https://csrc.nist.gov/pubs/sp/800/175/b/r1/final
3. NIST.SP.800-57 Recommendation for Key Management URL: https://csrc.nist.gov/pubs/sp/800/57/pt1/r5/final
4. OWASP Application Security Verification Standard URL: https://owasp.org/www-project-application-security-verification-standard/
5. OWASP Software Assurance Maturity Model URL: https://owaspsamm.org/model/
6. NIST.SP.800-218 Secure Software Development Framework URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf