БЕЗПЕКА МОБІЛЬНИХ ДОДАТКІВ

Бреславець О.Ю., к.ф-м.н., доц. Черних О.П., д.т.н., проф. Носков В.І., Гугнін В.М.
Національний технічний університет «ХПІ», Харків

У наш час використання мобільних телефонів стало повсюдним і повсякденним. Завдяки можливостям мобільних додатків, швидкому зростанню обчислювальної потужності смартфонів та все зростаючої доступності мобільних пристроїв програмне забезпечення для смартфонів вимагає все більше часу на тестування та більшої відповідальності у розробці.

З ростом популярності мобільних додатків у користувачів зростає їх популярність і у зловмисників. Додатки на кожній платформі мають як свою специфіку написання, так і свої специфічні загрози, реалізація яких може призвести як до крадіжки особистих даних, в тому числі банківських, так і до проникнення в корпоративну мережу.

Основні проблеми безпеки пов'язані з тим, що різноманітність ОС для мобільних пристроїв дуже велика, так як і кількість їх версій в одному сімействі.

Були розглянуті уразливості, які найбільш часто зустрічаються та включені в список OWASP Mobile Top Ten Risks. Основними проблемами, які легко усуваються на етапі розробки, є:

– небезпечне зберігання даних;
– недостатній захист каналів передачі інформації;
– слабка авторизація та аутентифікація;
– небезпечне управління сесіями.

Для захисту мобільних додатків від вразливостей необхідно:

– не зберігати дані на SD карті;
– вимикати логування;
– переглядати конфігураційні файли додатків користувача на предмет забутих даних.

Таким чином, швидке розширення функціоналу веде за собою велику складність і меншу захищеність мобільних пристроїв. Розглянуті проблеми переважно виникають при неправильній організації процесів розробки і тестування.