ВРАЗЛИВІСТЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В IOS-ДОДАТКУ

магістр О.Ю. Колесник, д-р техн. наук., проф. С.Г. Семенов, канд. фіз.-мат. наук, доц. О.П. Черних, Національний технічний університет "Харківський політехнічний інститут", м. Харків

Якщо потрібно програмувати банківський додаток або гру, якщо програма використовує мережу, вони повинні бути безпечними. Для всіх, крім самих штрихових даних, програмне забезпечення не може визначити – чи є дані користувача конфіденційними, незручними або навіть небезпечними. Велика кількість незначних частин інформації може сукупно стати набагато більшою проблемою, ніж сума його частин.

З наведених причин завжди слід припускати, що кожна частка даних, з якими зустрічається розроблена програма, могла би містити номер банківського рахунку або пароль, вона повинна бути захищена відповідно.

Деякими атаками, з якими стикається програма, можуть бути:

Snooping-Attacks – коли третя сторона переглядає дані програми під час транзиту. Атака "Людина посередині"– атака, в яких третя сторона переносить свій комп'ютер між програмою та сервером. Напад "Людина посередині" включає: spoofing and phishing – створення фальшивих серверів, які маскуються як легітимні сервери. Уловлювання – зміна даних між сервером та програмою. Викрадення сеансу – захоплення інформації про автентифікацію та використання її для позиціонування користувачів.

Ін'єкційні атаки – атаки, в яких спеціально створені дані можуть призвести до виконання клієнтом чи серверним програмним забезпеченням інших команд, крім перевірених. Це зазвичай трапляється, коли програма говорить за інтерпретатора скриптів, наприклад, оболонки або сервера баз даних SQL.

Переповнення буферу та числові переповнення – атаки, в яких спеціально створені дані приводять до того, що програма може читати чи записувати дані в частинах свого адресного простору, де це не повинно бути, що може призвести до виконання довільного виконуваного коду, розкриття приватної інформації.

Кількість застосовуваних рівнів захисту залежить від конкретного додатка. Вибір і узгодження рівня захищеності в додатку, що розробляється, повинні виконуватися на самих ранніх етапах проектування.