Лаетін Д.А., здобувач
Варганова Д.О., ст. викладач
Державний університет "Житомирська політехніка"

РЕАЛІЗАЦІЯ ТА АНАЛІЗ МЕТОДІВ БЕЗПЕКИ В КРОСПЛАТФОРМЕННИХ .NET ДОДАТКАХ З ВИКОРИСТАННЯМ MAUI

В сучасних реаліях розробки безпека програмного забезпечення стає критично важливою проблемою. В контексті технології кросплатформенної розробки .NET MAUI є доволі якісним рішенням з високими стандартами безпеки. Крім того, через постійні оновлення та підтримку від Microsoft середовище .NET будь-які вразливості або помилки оперативно виправляються.

MAUI дає можливість створити єдину кодову базу для платформ Adnroid, Windows, iOS та macOS і являє собою найновіший інструмент для кросплатформеної розробки. Основні принципи базуються на .NET 6+ та використовують різні API для роботи з локальними функціями різних ОС.

Методи підтримки безпеки MAUI:

1. Захист даних:
   - Secure Storage [1] – API, який використовується для зберігання важливих даних, які мають бути зашифровані: токени, паролі, персональні дані.
   - Використання бібліотек .NET для захисту даних, наприклад: System.Security.Cryptography дозволяє надійно зашифрувати дані, перед їхнім зберіганням та передачею.
2. Авторизація:
   - Дозволяє інтегрувати функції біометричної аутентифікації, такі як Face ID, Touch ID для iOS та macOS, або Android BiometricPrompt
   - Використання токена JWT [2] дозволяє керувати сесіями користувачів.
3. Мережева безпека:
   - Використання протоколу HTTPS дозволяє уникнути атак типу MITM.
   - Інтеграція з платформою Microsoft Entra ID [3] для керування доступом до корпоративних ресурсів.
   - Для веб-контенту наявне налаштування CSP [4], що обмежує застосування потенційно небезпечного коду та підключення до незахищених ресурсів.
4. Логування та моніторинг:
   - Azure Application Insights надає можливість відстежувати різноманітні безпекові події та зберігати журнали аудиту.
5. Кросплатформенна адаптація безпеки:
   - Безпекові механізми кожної платформи потребують окремих налаштувань та спеціальної адаптації. Наприклад, Android потребує налаштування Network Security Configuration, а iOS використання лише HTTPS.
   - Підтримка Dependency Injection дозволяє створювати безпечну архітектуру, з легкою можливістю майбутнього розширення кодової бази.
6. Інструменти для перевірки безпеки:
   - Інструменти подібні до SonarQube [5] або Snyk можуть автоматично перевіряти код на наявність потенційних вразливостей. Наприклад необроблені виключення або некоректне використання API.
   - Використання комбінації емуляторів (Anroid Emulator чи Xcode Simulator) та спеціалізованих інструментів пентестингу (Burp Suite, OWASP ZAP).

Отже, можна впевнено сказати, що MAUI має справді високі стандарти безпеки, тому може бути використана навіть при розробці критично важливих застосунків. Адаптація до специфічних вимог кожної платформи забезпечує надійність додатка у будь-яких умовах. Разом з інструментами тестування та моніторингу, можлива реалізація високого рівня безпеки, навіть з обмеженими ресурсами.

Список використаних джерел

1. Secure storage. MAUI Documentation. URL: https://learn.microsoft.com. (дата звернення: 21.11.2024).
2. SON Web Tokens. URL: https://jwt.io. (дата звернення: 21.11.2024).
3. Microsoft Entra ID. URL: https://www.microsoft.com. (дата звернення: 21.11.2024).