ВИКОРИСТАННЯ HTTPS В IOS ДОДАТКУ

Колесник О.Ю, Черних О.П.
Національний технічний університет «Харківський політехнічний інститут», м. Харків

Найчастіше адресний рядок не привертає уваги, якщо не потрібне перейти за посиланням, яке скопійоване звідкілясь в буфер обміну.

App Transport Security (ATS) – це настройка iOS. Вона впливає на те, який протокол для передачі даних будуть використовувати мобільні додатки.

Якщо ATS вимкнена, то використовується звичайний протокол HTTP, а якщо включена – то HTTPS, в якому всі дані між додатком і сервером шифруються, так що сторонні спостерігачі не зможуть дізнатися, що саме передається. Протокол HTTPS – розширення протоколу HTTP, що підтримує шифрування за протоколами SSL і TLS, забезпечує криптографічний захист.

Якщо дані не захищені по SSL, то запущена в якийсь момент програма-перехоплювач дозволяє скористатися ними зловмисникові. Технічна реалізація HTTPS трохи складніше: для цього захищуваний сайт повинен мати в користуванні сертифікат сервера, який користувач приймає або не приймає. Такий сертифікат встановлюється на сервер, що обробляє з'єднання. Шифруються і дані, отримані клієнтом, і дані, отримані від нього. Для перевірки, чи той клієнт їх отримує і надає, використовуються ключі шифрування.

За замовчуванням ATS активована вже в iOS 9, проте розробники до сих пір можуть відключати цю можливість і передавати дані по HTTP.

Для кращого захисту призначених для користувача даних Apple вимагає від усіх додатків в App Store з 2017 року підтримувати ATS.

Але навіть при використанні HTTPS-з'єднань залишається можливість перегляду даних при обміні з сервером, наприклад, в публічних мережах є можливість відстежувати трафік за допомогою атаки «людина посередині», коли між додатком і сервером з'являється посередник. Боротися з цим можна за допомогою SSL-піннінга – в цьому випадку додаток знає SSL-сертифікат сервера, який використовується для HTTPS-з'єднання, і не довіряє іншим сертифікатам. При отриманні від сервера невідомого сертифіката (як у випадку з атакою "людина посередині") з'єднання обривається. Для цього в додатку зберігається публічний ключ сертифіката – тоді при оновленні сертифіката сервера не доведеться випускати нову зборку додатка, так як публічний ключ залишиться колишнім.

Застосування HTTPS в розроблюваних і застосованих iOS додатках допоможе забезпечити захист від кібератак, таким чином, не дасть зловмисникам перехопити дані.