БЕЗПЕКА У ANDROID

д.т.н., проф. Кучук Г.А., Гугнін В.М., Межерицький С.Г.,
Мельников О.С.
Національний технічний університет «ХПІ», Харків

Найбільшу долю операційних систем на ринку смартфонів займає Android (станом на 2016 року – 86.2%), що покладає на Google відповідальність за безпеку даних всіх користувачів.

Нещодавно професор криптографії Метью Грін з університету Джона Хопкінса стверджував, що Android відстає в плані безпеки від iOS як мінімум на шість років.

При цьому директор з безпеки Android Адріан Людвіг нещодавно заявив, що число Android-смартфонів, на яких встановлено потенційно небезпечні програми, становить менше 1%.

Побачивши ці заяви ми вирішили дізнатися більше про безпеку Android та дослідити розвиток та нововведення.

У докладі розглянуто особливості безпеки ядра Android, яке побудовано на базі ядра Linux.

Безпека ядра Linux заснована на користувальницькій моделі повноважень, ізоляції процесів, механізмі для безпечного IPC та можливості видалення непотрібних та потенційно небезпечних частин ядра.

Android має середовище стилю UNIX, що гарантує, що один користувач не може змінити файли іншого користувача, тобто кожен застосунок, яких вже на 2015 рік було 1,6 мільйонів, працює як власний користувач файлової системи.

Android забезпечує ряд криптографічних API, що включають реалізацію стандарту і зазвичай використовують криптографічні примітиви, такі як AES, RSA, DSA і SHA.

Крім того, API забезпечено для високорівневих протоколів, таких як SSL і HTTPS.

У останній версії Android 7.0 було введено десятки змін, деякі з яких – це засноване на файлі шифрування, рандомизація порядку завантаження бібліотеки і схема v2 підпису APK.

Розглянуті параметри безпеки та її нововведення у системі Android демонструють, що компанія Google піклується за безпеку користувачів та займає гідний рівень серед систем на ринку.