**Report about researched media covert channels for mobile devices, known attacks with utilization of covert channels for mobiles.**

Приховані канали - це шляхи передачі інформації між процесами системи, які порушують політику безпеки. Користувач може не мати дозволу на обробку даних, які його цікавлять, але він шукає обхідні шляхи. Оскільки будь-яка дія в системі викликає зміни стану інших складових системи, то за умови спостережливості і знання цих зв’язків можна відновити першопричину події хоча б частково.

Сьогодні користувачі смартфонів встановлюють безліч програм, яким надають доступ до персональної інформації користувачів, включаючи кредитну картку, медичні записи, телефонні контакти, страхові картки тощо. Безпека даних цієї конфіденційної інформації стала критичною проблемою для цих користувачів. Операційна система Android (ОС) успадковує інфраструктуру безпеки Linux, де програми встановлюються та виконуються в її індивідуальному віртуальному середовищі або пісочниці . ОС використовує модель дозволів на основі політики безпеки для управління доступом до спільних ресурсів, і програма повинна шукати явні дозволи на доступ до них під час встановлення. Зловмисник, зацікавлений в отриманні приватних даних користувача, повинен обходити ці політики безпеки, які запобігають незаконному доступу. В Android приховані канали можуть використовуватися зловмисними програмами для такої атаки. Прихований канал - це середовище, через яке дві сутності спілкуються без використання звичайних методів (наприклад, намірів).Зокрема, додаток, що має доступ до приватних даних користувача, може перенести його в іншу програму на тому самому пристрої або на зовнішній сервер за допомогою цих нетрадиційних каналів.

Приховані канали можна класифікувати як канали синхронізації або зберігання. У каналі синхронізації інформація між двома змованими програмами передається за допомогою спільних ресурсів, що не мають можливості зберігання (наприклад, центрального процесора) протягом певного періоду часу. Кодування та декодування інформації виконується з точною синхронізацією часу між двома програмами. На відміну від цього, канал зберігання передбачає використання спільних ресурсів, що мають можливість зберігання (наприклад, файлова система). Це забезпечуєсинхронне кодування та декодування інформації.

Як приклад прихованого каналу:  
 Мобільні пристрої зазвичай мають літій-іонну батарею з обмеженою ємністю заряду. Паралельне використання декількох ресурсів розряджає акумулятор з різною швидкістю, залежно від використовуваного компонента. Ця властивість може бути використана для кодування інформації для формування прихованого каналу. Зокрема, API BatteryManager надає трансляційний намір , повідомляючи програмі (незначний фільтр, зареєстрований в ACTION BATTERY CHANGED) про кожні 1% зміни рівня заряду акумулятора. Шкідливий додаток може виконувати двійкове кодування

потрібну інформацію, виконуючи паралельні операції на поєднанні ресурсів, таких як процесор та яскравість екрану, для досягнення заздалегідь визначеної швидкості розряду. Adecoder оцінює швидкість розряду за точний проміжок часу, використовуючи трансляційний намір, тим самим формуючи прихований канал.

Список джерел:  
1. <https://sites.google.com/site/zagrozu/to-dos>  
2. https://www.researchgate.net/publication/286292726\_Towards\_a\_Systematic\_Study\_of\_the\_Covert\_Channel\_Attacks\_in\_Smartphones