У комп'ютерної безпеки , прихований канал представляє собою тип атаки , який створює можливості для інформаційних об'єктів передачі між процесами, які не повинні бути дозволено спілкуватися з допомогою політики безпеки комп'ютера . Термін, утворений в 1973 році Батлером Лампсоном , визначається як канали, "не призначені взагалі для передачі інформації , наприклад, вплив сервісної програми на завантаження системи ", щоб відрізнити його від законних каналів, які підлягають контролю доступу COMPUSEC . Програма, що має доступ до особистих даних користувача, може передавати їх іншій програмі на тому самому пристрої або на зовнішній сервер, використовуючи ці нетрадиційні канали. Вважається, що прихований канал з пропускною здатністю > 100 біт/с є собою серйозну загрозу безпеці даних в системі. Тому наявність прихованих каналів з великою пропускною здатністю створює високий ризик збереження призначених для користувача особистих даних на мобільному пристрої.

Троянська атака працює у чотири фази. Спочатку встановлюється шкідливе програмне забезпечення користувачем на своєму особистому пристрої. Потім воно отримує доступ до деякої конфіденційної інформації, таку як відстеження місцезнаходження користувача GPS. Шкідливий компонент програми кодує інформацію та надсилає її через фізичний пристрій. В той самий час, використовується другий компонент додатка, керований зловмисником у фоновому режимі для збору зразків із відповідного датчик. Цей другий компонент програми декодує сигнал від датчика, отримуючи вихідні дані. Нарешті, компонент програми-одержувача надсилає цю інформацію на деякий хост, керований зловмисником в Інтернеті.

Прикладом троянського додатка може бути фітнес-програма Jog-Log, яка допомагає користувачам відстежувати свій прогрес в бігу. Мета нападника - отримати домашню адресу користувача. Додаток реалізує простий журнал бігу, який визначає, коли і як довго, і де користувач бігає, щоб відстежувати свій прогрес. Коли користувач хоче почати пробіжку, він запускає додаток, і додаток використовує GPS для відстеження пробіжки. Додаток запрошує дозвіл на доступ до GPS, але воно не запитує дозволу на доступ в Інтернет. Додаток також запитує доступ до мікрофона, щоб дозволити користувачу додавати прості «голосові замітки» до своїх записів журналу. Вночі, коли користувач спить, додаток використовує ScheduleExecutorService для пробудження і використання PMCC(The Progressive Multi-Channel Correlation Method спочатку розроблений для сейсмічних масивів, виявився ефективним при виявленні низькоамплітудних когерентних інфразвукових сигналів в межах некогерентного шуму) для передавання інформації про місцезнаходження, зібрану раніше під час останнього запуск. Зловмисник налаштовує спеціальний веб-сервер для відповіді на ці запити шляхом запису параметрів CGI в пов'язаний файл з IP-адресою користувача. Як тільки дані потрапляють на хост

зловмисника, зловмисник може знайти найближчу адресу координати GPS, записану на початку і кінці маршруту користувача, що, ймовірно, є домашньою адресою.

Динамік та акселерометр. Динамік на більшості інтелектуальних пристроїв може спричинити вібрацію всього пристрою, якщо тони відтворюються з досить великою гучністю. Ми використовуємо динамік як джерело сигналу, відтворюючи стандартні двотонові багаточастотні (DTMF) звуки та акселерометр для вимірювання вібрації телефону, яка буде резонувати з відтворюваними тонами. Потім ми виконуємо двійковий амплітудний зсув для модуляції даних. Кодування DTMF використовуються, оскільки смартфони спроектовані так, щоб добре його здійснювати, і воно менш помітне в цьому контексті. Це демонструє, що два довільні датчики можна об'єднати, щоб сформувати прихований канал.

1. https://en.wikipedia.org/wiki/Covert_channel#Identifying_covert_channels
2. Towards a Systematic Study of the Covert Channel Attacks in Smartphones Swarup Chandra , Zhiqiang Lin , Ashish Kundu , and Latifur Khan
3. Physical Media Covert Channels on Smart Mobile Devices Ed Novak Yutao Tang Zijiang Hao Qun Li, Yifan Zhang