Атака «ручкой» или как KNOB-атака способна взломать Bluetooth и украсть ваши данные.

KNOB (Key Negotiation of Bluetooth) Attack – это серьезный инцидент в IT-сфере, который затронул множество устройств, использующих беспроводную технологию Bluetooth для обмена данными. Инцидент связан с ошибкой в процессе согласования ключей (key negotiation) между устройствами Bluetooth. В спецификациях Bluetooth два устройства, устанавливающие между собой защищенное соединение, могут выбирать длину ключа в пределах от 1 до 16 байт. В случае однобайтового ключа взломать его можно достаточно быстро простым брутфорсом – системным перебором всех возможных комбинаций. Это и делает подобное соединение уязвимым и даёт возможность хакерам получить доступ к различным устройствам. Злоумышленники могут использовать эту уязвимость для атаки на широкий спектр устройств, включая смартфоны, ноутбуки, наушники и другие Bluetooth-гаджеты.

Обобщение до класса проблем: Инцидент KNOB Attack поднимает общую проблему в области криптографии и безопасности: недостаточное внимание к длине ключей и уровню шифрования. Это также является напоминанием о важности периодического аудита и усовершенствования стандартов безопасности в ответ на появление новых угроз.

Мораль и выводы:

**Безопасность должна быть приоритетом**: Уязвимости, даже на первый взгляд незначительные, могут стать серьезным источником угрозы.

**Регулярное аудирование и обновление протоколов**: Индустрия должна уделять больше внимания периодическому аудиту и обновлению криптографических протоколов и стандартов безопасности, чтобы учесть новые угрозы и ситуации.

**Ограничение длины ключа:** Необходимо ввести ограничение на длину ключа энтропии, чтобы устранить возможность брутфорса.

**Обучение и осведомленность**: Инженеры и пользователи должны быть осведомлены о существующих угрозах и правильных методах защиты, чтобы соблюдать лучшие практики безопасности.

**Сотрудничество с сообществом**: Индустрия должна поощрять сотрудничество между разработчиками, исследователями уязвимостей и производителями устройств для обнаружения и устранения угроз.

Ссылки на источники

<https://francozappa.github.io/publication/knob/slides.pdf>

[Security Week 34: неординарные уязвимости в Windows / Хабр (habr.com)](https://habr.com/ru/companies/kaspersky/articles/464365/)

[Ошибка безопасности Bluetooth (KNOB) позволяет хакерам захватить динамики (inform.click)](https://vpn.inform.click/oshibka-bezopasnosti-bluetooth-knob-pozvoljaet-hakeram-zahvatit-dinamiki-vpn-inform/?ysclid=lm6jpbklm1816774853)

Вопрос на экзамен:

Как работает KNOB-атака? Почему так просто взломать Bluetooth- соединение, имеющее восьмибитный ключ?

План доклада:

1. Что такое Bluetooth, Bluetooth BR/EDR and Bluetooth Low Energy
2. Как работает соединение – этапы
3. KNOB
4. Что с этим делать