ПРИМЕНЕНИЕ РЕЖИМА ШИФРОВАНИЯ SL3 КАРТ MIFARE НА ПРИМЕРЕ ДОМОФОНОВ ОТ ГК ПИК.

ЭТАПЫ СТРОИТЕЛЬСТВА СКУД В МКД

- Разработка технического задания на строительство, которому будет соответствовать готовая, построенная система СКУД (Mifare Plus уровня безопасности SL3)
- Строительство дома со СКУД в котором участвуют: проектировщик, застройщик, подрядчик, суб-подрядчик, производитель оборудования
- Приёмка дома в эксплуатацию управляющей компанией

Как не допустить утечку кода шифрования выбранного для шифрования ?

ТЕХНОЛОГИИ БЕСКОНТАКТНЫХ КАРТ (ФОРМАТЫ ИДЕНТИФИКАТОРОВ)

- EM Marine (StandProx, ANGstrem, SlimProx, MiniTag)125 КГц
- Mifare от NXP (Classic,Plus, UltraLight, DESfire) (Mifare 1k, 4k) 13,56 МГц
- HID производитель HID Corporation(ProxCard II, ISOProx-II, ProxKey II) 125 КГц
- iCLASS и iCLASS SE (производитель HID Corporation,) 13,56 МГц
- Indala® (Motorolla), Nedap, Farpointe, Kantech, UHF (860-960 МГц)

MIFARE SL1 VS SL3

Mifare SL1	Mifare SL3
Crypto-1 — проприетарный алгоритм шифрования, созданный NXP Semiconductors для использования в RFID-картах стандарта Mifare Classic	Advanced Encryption Standard (AES) — симметричный алгоритм блочного шифрования, принятый в качестве стандарта шифрования правительством США по результатам конкурса AES.
Тип Чипа - Plus\Classic	Тип Чипа - Plus

ИЗВЕСТНЫЕ УЯЗВИМОСТИ MIFARE CLASSIC

- Криптография карты хорошо исследована. Найдена уязвимость реализации генератора псевдослучайных чисел (ГПСЧ) карты и уязвимости алгоритма CRYPTO1. На практике эти уязвимости используются в следующих атаках:

  Dark side — атака использует уязвимость ГПСЧ. Работает на картах MIFARE Classic поколения до EV1 (в EV1 уязвимость ГПСЧ уже устранена). Для атаки нужна только карта, знать ключи не нужно.

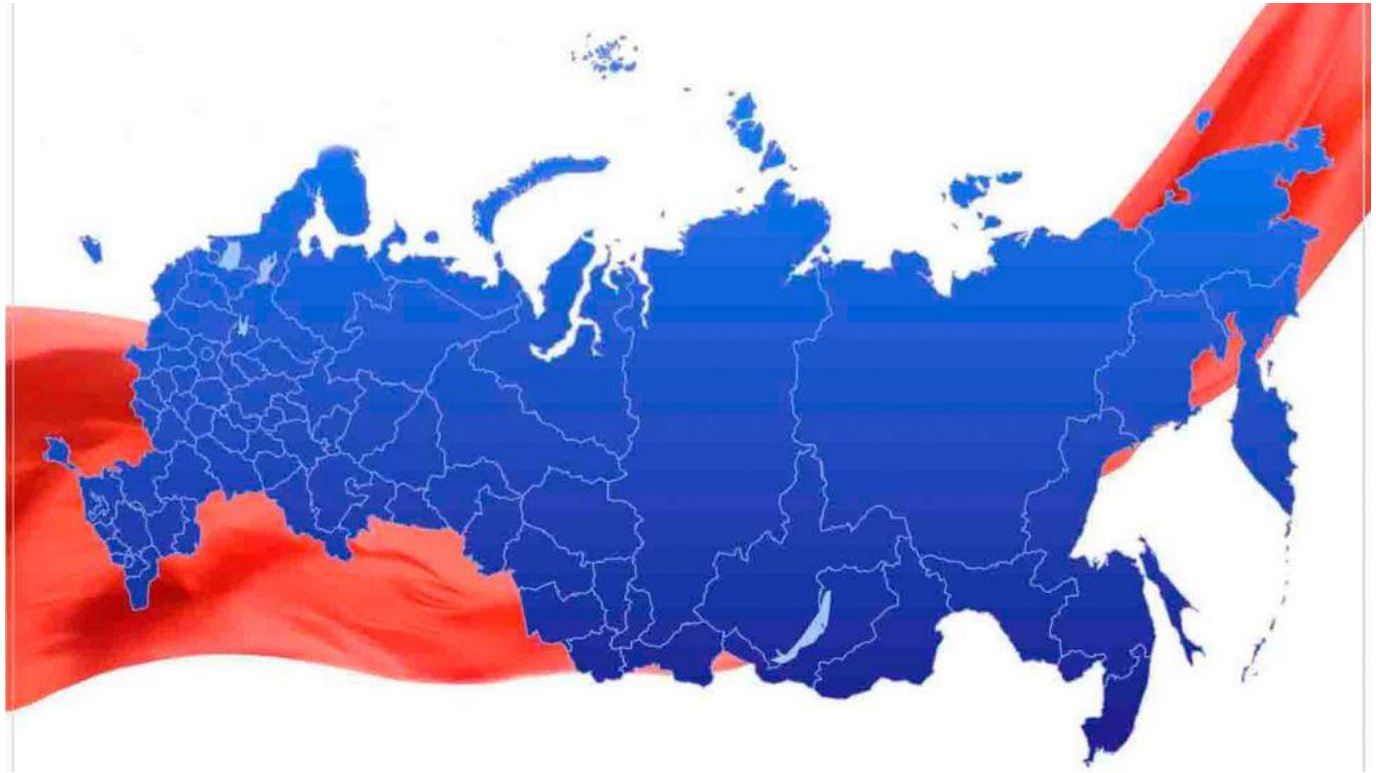
- *Nested* – атака использует уязвимость CRYPTO1. Атака производится на вторичные авторизации, поэтому для атаки нужно знать один валидный ключ карты. На практике для нулевого сектора часто используют стандартные ключи для работы MAD – с него и начинают. Работает для любых карт на CRYPTO1 (MIFARE Classic и его эмуляции). Атака продемонстрирована на ХабраХабре в статье про Уязвимость карты Подорожник
- *Атака прослушиванием обмена* – атака использует уязвимость CRYPTO1. Для атаки нужно подслушать первичную авторизацию между устройством чтения и картой. Для этого необходимо специальное оборудование. Работает для любых карт на CRYPTO1 (MIFARE Classic и его эмуляции Атака продемонстрирована на ХабраХабре в статье «Взлом транспортных карт «Ситикард»

ШИФРОВАНИЕ И СЧИТЫВАНИЕ С ПРИМЕНЕНИЕМ КЛЮЧА

- Шифрование происходит на заводе изготовителе. По заранее утверждённому заказу с использованием заранее определённых секторов карты памяти.
- А считывание происходит на считывателе, заранее настроенном. Считыватель обращается к только ему известному сектору карты с определённым ключом и получает в ответ данные хранящиеся в карте. Считанные данные считыватель посылает в контроллер который сверяет наличие такого идентификатора в базе данных и принимает решение об открытии\не открытии точки прохода.

ГЕОГРАФИЯ ПРИСУТСТВИЯ

- Москва
- Московская Область
- Обнинск
- Калуга
- Санкт-Петербург
- Новороссийск



ОБОРУДОВАНИЕ ДЛЯ СКУД

Большинство производителей оборудования работают в режиме чтения UID

Некоторые поддерживают SL1, который уже скомпрометирован в далёком 2008 году.

И лишь некоторые ведущие бренды используют поддержку SL3, на их оборудовании и построена наша система.

РИСКИ ПРИ ОБОРОТЕ БОЛЕЕ 200 ТЫС. ЭКЗЕМПЛЯРОВ КАРТ

- Риски со стороны жильцов – доверяя делать копию ключа «мастеру», дамп ключа жильца попадает в его базу данных, и «мастер» получает возможность ходить в подъезд, да и пользоваться паркингом или машиноместо жильца.
- Коммерческие риски: при розничной стоимости карты в 300 рублей – потеря рынка продажи дополнительных карт является не маленькой потерей. Даже если на одном ЖК появляется «Мастер» по копированию ключей убытки компании могут исчисляться сотнями тысяч и миллионами рублей.
- Эстетические свойства: абсолютно все копии производятся на болванках низкого качества. Качество оригинала я думаю многим из вас знакомо.

В ЗАКЛЮЧЕНИИ

- СКУД в МКД - единственная слаботочная система, с которой житель сталкивается по несколько раз в день.
- И я надеюсь, что она у нас получается достойной :)