Сигурност на системи от физическия свят

трагедия в три действия

Васил Колев <vasil@ludost.net>

Уводни думи

- Продължение на “Светлината в края на тунела е влак”
- Бургас(conf) ми действа зле
  - пясък
  - море (мокро)
  - морски лешояди
    - повече познати като гларуси
  - слънце
  - все се будя рано
    - сутринта беше по-светло, отколкото сега

Проблемът в internet

- Всеки може да ви атакува
  - (почти) анонимно
- Почти всеки го прави
- Ако човек не се подсигурява, бързо му се случва нещо

Последици от проблема

- Много research
- Много добри идеи
- Като цяло, доста здрава система
- Би трябвало да се поучим от нея

Физическия свят

- По-труден за масово атакуване
- С по-тежки последствия
- Няма натиск за подобряване
- Механиката е гадна работа
- Няма математическа теория, която да помага

Текущ изглед

- Сигурността в системите от физическия свят е трагична
- Основно security through obscurity
  - "Ако никой не знае за него, не може да се счупи"
  - Вижте колко добра работа свърши в internet...
- Елементарна (и счупена) криптография
- Липса на сериозен (академичен) research
- Оправдание: "може да се намери извършителят на всичко"
  - good luck with that.

Spoiler alert

- По-лесно е да ви оберат къщата, отколкото да ви свалят домашното порно
- Всички са/сме идиоти

Секретни ключалки

- Отварят се с отвертка и кламер
- Bump key

Защита

- Няма.
- Говорете си с някой приятел ключар кое колко време отнема да се отвори.
- Много често е по-лесно да се атакува самата врата
- Четете, забавно е

Сейфове

- По-голяма трагедия
  - “For example, Bulldog BD 1500 could be opened with the metal shank method, or by inserting a coat hangar into the battery port, causing it to short out and open”
  - “The Gun Vault GV2000S, obviously designed to hold firearms, is crackable by once again peeling off a cheap rubber cover, and pushing a wire through the exposed holes on the top.”

RFID системи

- Генерален начин за безжично удостоверяване
  - ще го срещнем пак, извън картите
- Срещат се къде ли не

Безконтактни карти

- Контрол на достъпа
- Безконтактни, удобни
- Гаражи, офиси, метро

Начин на работа

- Безжично захранване
- Излъчване на идентификатор, или
- Двупосочна комуникация (Mifare)

Ниво на сигурност

- Повечето са просто едно число
- Елементарни за записване и replay
- Картите за метрото са по-сигурни от картите за достъп до офиса ви
- Повечето такива карти са прекрасен начин да ви следят

Защита

- Не разчитайте само на тях
- “Tinfoil-hat” тип портфейл

Вратите като цяло

- Системи, удобни за hack-ване
- Много side channel-и
  - панти, каса, под прага...
- Youtube е пълен с примери

Охранителни системи за коли

- Сензори за различни неща
- Достатъчно захранване да вият много време
- Имобилайзери
- RFID

Тривиални атаки

- Шокова палка
- Заглушаване на сигнала към системата

Още по-тривиални атаки

- Записване отдалеч на сигнала от системата
- Декриптиране на (малкото), които използват криптография
  - “40 бита трябва да са достатъчни”
- Ползване на ключа за колата да ви следят
  - RFID . . .
- Намира се някакъв академичен research

малко отклонение

- Всичко с под 128-битово криптиране не трябва да му се вярва:
  - rainbow tables
  - FPGA
  - Математическо развитие
  - Закон на Мур
- На всичко, което не е отворено и не е проверено, също.

Целта на повечето мерки за сигурност...

- ... е да ни накара да се почувстваме сигурни.
- Връзката с истинската сигурност е инцидентна.
- “Ключалките ни пазят от честни хора”

Летища

- Бутилки с течности
- Засилени проверки
- Дребни остри предмети

Големи събития

- Олимпиадата в Лондон и противовъздушните ракети

За домашно

- Безконтактни плащания (банкови карти)
- Карти за метро
- Всякакви карти за отстъпки
- Паспортни RFID
- GPS
- Всякакви забавни неща в ефира
- In-app плащания, sms плащания
- Social engineering :)

В заключение

- Security is a mindset
- Security is a trade-off
- Имаме навика да вярваме твърде много на неща, които не обмисляме

Благодаря за вниманието

- Въпроси?