MFCUK

Mi**F**are **C**lassic **U**niversal tool**K**it

26C3, Lightning Talk

Andrei Costin, Pavol Luptak, Norbert Szetei

MFCUK – Intro

- Mifare Classic – short biography:
  - Possibly the most production-deployed RFID card
    - Check your credit card
    - Check your transport card
    - Check your student/ISIC card
    - Check your building-access card
  - More than 200 mil estimated in use
  - RFID Standard 14443A 13.56 MHz
  - Under “microscope” since 2007 (directly&indirectly ☺)
  - Completely broken as implementation and protocol
    - Proved theoretically and practically since 2007 till 2009

MFCUK – Intro (2)

- Trying to build a MiFare Classic Universal toolKit
  - Open-source, GPL, portable code
  - Hopefully to be included in some security/forensic distro
  - To merge MFOC from Nethemba team
    - Implements Nested Authentication attack
    - Need to know at least 1 valid keyA/keyB of any valid sector
    - Or need to be lucky enough to have default keys on card :)
    - If above are satisfied, it can recover all other sectors keys
  - To merge "MiFare Classic DarkSide Key Recovery tool" from Andrei Costin
    - Implements DarkSide attack, uses Crapto1 library as support
    - Name given by well-known "Dark Side" paper from Nicolas Courtois
    - Can recover any/all the keys without:
      - Being lucky to have "default key" as a gift
      - Knowing any of the valid keys

MFCUK – Intro (3)

- To include (wish-list – any volunteers to help?)
  - MiFare Classic SoftTag Emulation tool
    - To achieve 100% MiFare Classic 1K/4K Emulation
    - Including Manufacturer Block and UID :)
    - To run on cheapest (ACR122/Touchatag) readers
      - Proxmark3 is still too expensive for this
    - To be as simple as loading a file with dumped card contents
    - Act exactly as if it was the real dumped card (is it possible?)
  - Any other crazy-but-still-useful ideas with ACR122/libnfc/crapto1?!
    - 100% Mifare Classic Emulation PoC for Nokia's NFC 6131/6212 (patched?) Phones and associated (patched?) SDKs

MFCUK – Contact Us

- Project URLs:
  - code.google.com/p/mfcuk
  - groups.google.com/group/mfcuk