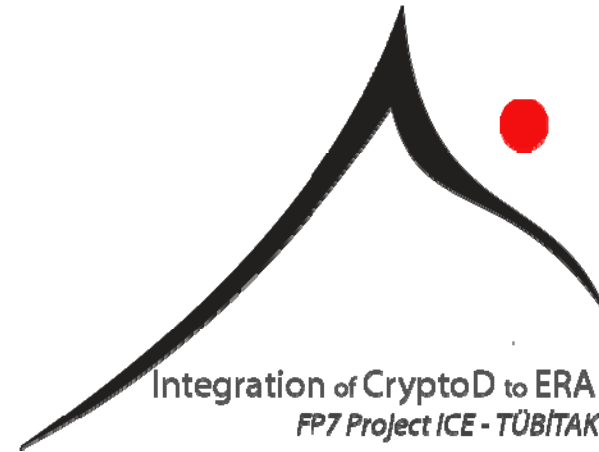


MIFARE Klasik Kart ve Saldırıları

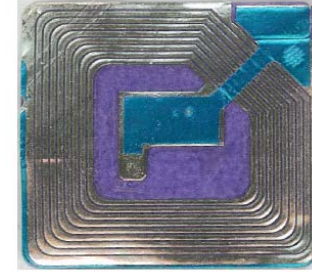


Taslak

- Mifare Klasik
 - Özellikleri
- Diğer MIFARE Kartlar
 - UltraLight, DESFIRE, SmartMX
- MIFARE Klasik Kartların Kullanım alanları
- Saldırılar
 - Tersine Mühendislik ile Mifare Klasik
 - Karakteristikleri
 - Asıllama Protokolü
 - Crypto I Şifreleme
 - Mifare Kripto-analizi
 - Saldırı 1
 - Saldırı 2
- Sonuç

Klasik Kart

- RFID teknolojisi Philips Austria tarafından tasarlanmış
 - Bünyesinde bir mikro-işlemci ve yazılım gömülüdür
 - Sudan, güneşten ve manyetik alandan etkilenmez
 - 13.56 MHz frekansta çalışır
 - ISO 14443 –Type A Bölüm 3e kadarki standardını destekler
- Patentli doğrulama ve şifreleme için gerekli güvenlik protokollerini barındırır.
 - Crypto I stream cipher



MIFARE Kartlar

- Mifare UltraLight
 - Klasik kartlardan tek farkı şifreleme mekanizması yoktur.
- Mifare – Pro, ProX, SmartMx,
 - Farklı etiket çeşitlerinde hafıza farklı A, B anahtarları tarafından korunur.
 - DES, AES, RSA bulunduran modelleri bulunmaktadır
- DESFire
 - ISO 14443-4 standardına uyumludur.
 - Okuyucu ile iletişimde uyumludur, okuma/yazma da uyumlu değildir
 - Microprocessor olarak MIFARE ProX/SmartMX dayanır.
 - 4 çeşidi vardır : 1KB Triple Des, 2-4-8KB AES
 - Okuma/yazma uzaklığı 10 cm
 - DESFire EV1(2006)
 - 2KB, 4KB, 8KB hafıza
 - Rastgele ID
 - 128-Bit AES
- Mifare + : Mart 2008'de Mifare Klasikteki açıklıktan ötürü üretilmiştir
 - 7-byte UID
 - 128-Bit AES
 - Okuyucu tarafında AES desteklenmediği için saldırılara karşı kapılar açık bırakılmıştır
 - Rastgele sayı üretme saldırılarına karşı bir yapılamamıştır

MIFARE Klasik Kartların Kullanım Alanları

- Dünya üzerinde 1 milyardan fazla Mifare Kart satıldı
 - Bunlardan 200 Milyonu Mifare klasik kart oluşturur
- Kullanım alanları
 - Üniversite girişlerinde
 - Ofis ve resmi daire girişlerinde
 - Halk taşımacılık sistemlerinde
 - OV-Chipkaart – Hollanda
 - Oystercard – Londra
 - Smartrider – Australia
 - Schipol Havalimanı Personel girişlerinde (Amsterdam)
 - Asya'da ödeme sistemlerinde

MIFARE Klasik Kartların Güvenliđi

- Aralık 2007, Henryk Plötz ve Karsten Nohl Mifare - Klasik kartın tersine mühendislik ile kullanılan algoritmaları ortaya çıkardı
- Mart 2008, Klasik kartların kopyalanması ve içindeki verilerin yapısının deđiştirilmesi gerçeklendi
 - A Practical Attack on the MIFARE Classic,
 - Dismantling MIFARE Classic.



Sorular ?