Nethemba
all about security

Check your RFID

Trendy v internetové bezpečnosti 2010

Ing. Pavol Lupták, CISSP, CEH
Lead Security Consultant

Nethemba

- **certifikovaní IT security experti** (CISSP, CEH, SCSecA), aktívni v OWASP, SOIT
- **náš hlavný business** – penetračné testy a hĺbkové bezpečnostné audity webových aplikácií, bezpečnostné konzultácie
- **aktívni v bezpečnostnom výskume** – demonštrovanie zraniteľností v „SMS jízdenkách“ (Praha, Bratislava, Viedeň, Varšava)

Aktuálny výskum

- bezpečnostná analýza OBU jednotiek (e-mýto)
- analýza možnosti útokov na slovenské biometrické pasy cez postranné kanály
- vývoj MFCUK – univerzálny nástroj na lámanie Mifare Classic

Prelomenie Mifare Classic

- teoreticky prelomený už od roku 2007
- **ako prví na svete** sme napísali a pod GNU GPLv2 zverejnili nástroj MFOC na prelomenie / získanie **všetkých kľúčov Mifare Classic**
- EMTEST (hlavný dodávateľ) bol 3 mesiace dopredu informovaný
- MFOC umožňuje získať kľúče k 1 miliarde kariet na svete, a viac ako 1 miliónu na Slovensku (!!!)

MFOC – spätná väzba

- odozvy od z celého sveta, stále masívne používané, získané kľúče pre:
- DP (Londýn, Bratislava, Varšava, Krakov, Malmo, Holandské mestá, Luxemburgsko, Sofia, Bukurešť, Cyprus)
- ISIC/univerzitné preukazy (všetky české/slovenské)
- parkovacie preukazy (Bratislava, Varšava, Krakov, Plzeň)

MiFare Classic Universal toolKit (MFCUK)

- integrácia s MiFare Classic DarkSide Key Recovery Tool napísaným Andreiom Costinom
- prvý draft prezentovaný na CCC v Berlíne
- umožňuje rýchlo a 100%-tne prelomiť všetky Mifare Classic karty (aj také, ktoré neobsahujú „default“ A/B kľúče)
- opensource, GPL, multiplatformový

100% emulácia Mifare SoftTag

- **univerzálna Mifare Ultralight/Classic/DESFire emulácia celého obsahu vrátane UID**
- ACR122/Touchatag čítačky (nfc-emulate.c)
- Proxmark 3 (stále príliš drahý)
- Nokia NFC 6131/6212 s cracknutým NFC SDK
- ďalšie možnosti?

Budúce plány

- analyzovať bezpečnosti HITAG čipov („badge“ karty, kľúčiky do áut Renault / Opel / Peugeot / Citroen ..)
- praktická demonštrácia prelomenia A5/1 (GSM) v slovenských/českých podmienkach

Ďakujem za Vašu pozornosť!