Nethemba
all about security

Nové trendy zraniteľností vo verejne nasadzovaných technológiách

Ing. Pavol Lupták, CISSP, CEH
Lead Security Consultant

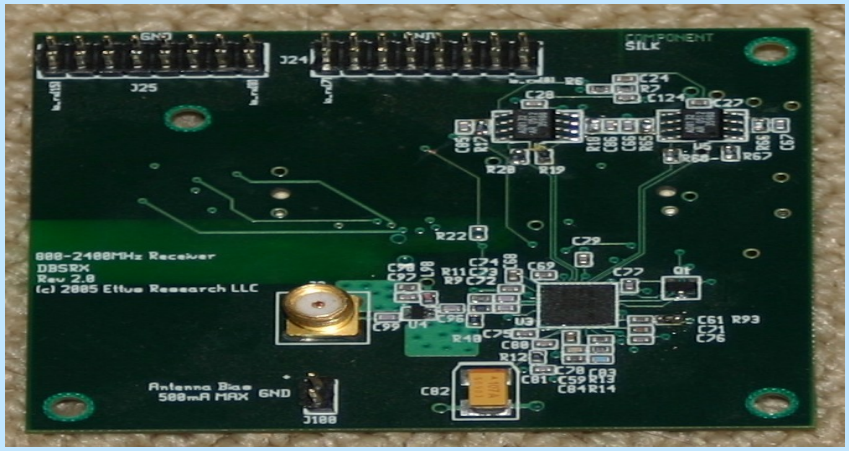
Nethemba

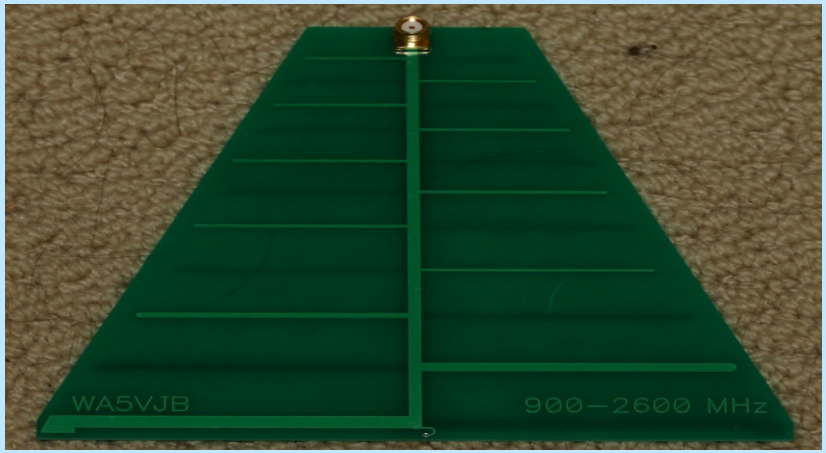
- **Certifikovaní IT security experti** (CISSP, CEH, SCSecA)
- **Zameranie:** všetky druhy penetračných testov, hĺbkové bezpečnostné audity webových aplikácií, bezpečnostné audity wifi sietí, operačných systémov, bezpečnostné konzultácie, návrh komplexných cloud computing riešení a clustrov, bezpečnej VoIP telefónie, forenzné analýzy
- **Ako jediní v ČR/SR ponúkame:**
  - bezpečnostné audity **čipových kariet**
  - demonštračné penetračné testy pre **všetkých**
  - aktívny bezpečnostný výskum (referencie – **zraniteľnosti v SMS lístkoch, praktické prelomenie najpoužívanejších čipových kariet Mifare Classic**)
- **Bezpečnostný výskum v množstve oblastí**

Prelomený GSM alebo ako kohokoľvek jednoducho odpočúvať

- Praktická demonštrácia možného zneužitia GSM na CCC konferencii v Berlíne bola zrušená
- Vaša komunikácia medzi mobilným telefónom a BTS stanicou je šifrovaná A5/1, ktorá bola teoreticky prelomená v roku 1997, prakticky pred vyše dvomi rokmi Steve Dhultom
- Je možné vypočítať špeciálne „rainbow“ tabuľky, ktoré je možné použiť na rýchle prelomenie zachyteného šifrovaného hovoru
- Pomocou verejne dostupného zariadenia (USRP2) a príslušných „daughterboard“ GSM prijímacích kariet (za rádovo $2000) je možné kompletne pasívne (bez možnosti detekcie!) zachytiť a prelomiť ľubovoľnú GSM komunikáciu
- USRP2 je možné použiť aj na vytvorenie vlastnej BTS stanice pomocou voľne dostupnej OpenBTS implementácie a jednoducho získať plnú kontrolu nad GSM telefónmi komunikujúcim s mobilnou sieťou
- Bezpečnosť GSM je **prelomená**, **mobilní operátori tento fakt ale ignorujú** a vystavujú Vás riziku možnosti triviálneho odpočúvania (ohrozených 4 miliardy ľudí v 200 krajinách sveta)
- Riešenie – použiť „bezpečnejšie“ A5/3 šifrovanie

USRP2 a „daughter board“ GSM karty





Prelomené „bezpečné“ šifrovanie v 3G sieťach (A5/3 Kasumi)

- A5/3 Kasumi je „bezpečnejšie“ vylepšenie tzv. „MISTY“ kryptosystému používané v 3G sieťach
- Adi Shamir (autor RSA) pred pár mesiacmi publikoval útok na A5/3 Kasumi
- Paradoxne útok funguje len na „bezpečnejší“ A5/3 Kasumi, ale nie na „menej bezpečný“ MISTY
- Možnosť prelomiť 3G komunikáciu behom 2 hodín na bežnom počítači
- Ohrozené sú všetky 3G siete a momentálne **neexistuje bezpečné riešenie**

Ešte stále veríte Vašej mobilnej GSM/3G komunikácii?

Čipové karty Mifare Classic

- Najpoužívanejšie karty na svete (1 miliarda čipov v obehu, len 1 milión na Slovensku)
- Dopravné podniky v Londýne, **Bratislave**, Varšave, Krakove, Sofii, Bukurešti, Malme, v Holandských mestách, v Luxemburgsku..
- Všetky **slovenské a české ISIC** a univerzitné preukazy
- Parkovacie karty v **Bratislave, Plzni,** Krakove, Varšave, …
- Vstupy do budov, platených parkovísk, **plavární**
- Prvé zraniteľnosti zverejnené už v roku 2007 na CCC konferencii v Berlíne
- Prvý veľký hack Londýnskych „Oyster“ kariet výskumníkmi z Holandskej univerzity Radboud
- **Nethemba s.r.o. ako prví na svete publikovali Mifare Classic bezpečnostný nástroj (pod otvorenou licenciou GNU GPLv2) umožňujúci prelomiť a získať kľúče pre všetky Mifare Classic karty**
- Spoločnosť EMTEST (hlavný slovenský dodávateľ uvedených kariet) bol 3 mesiace dopredu informovaný

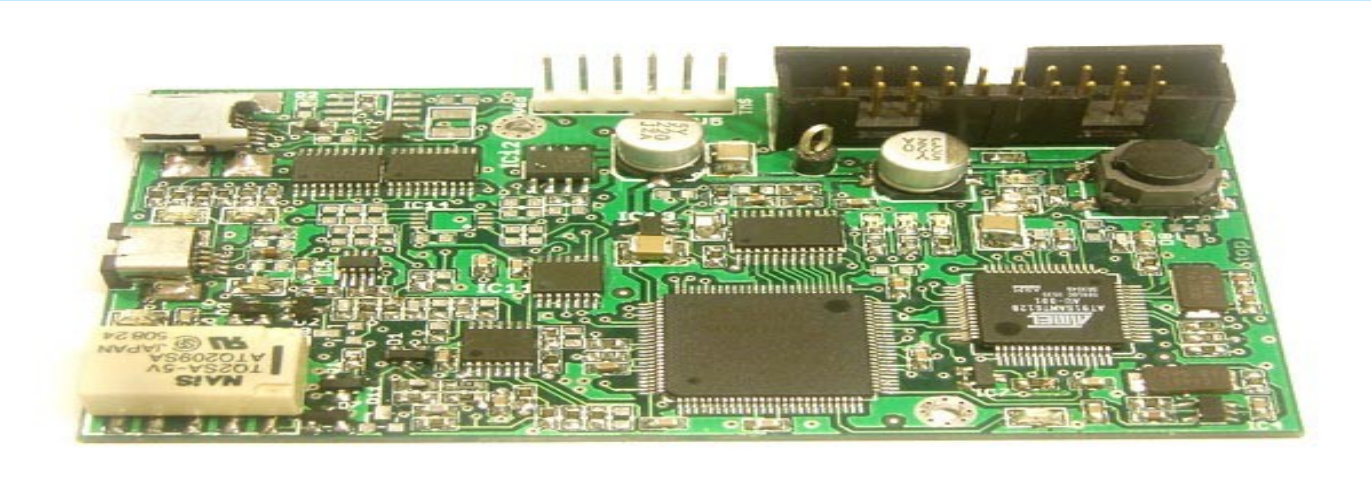
Mifare Classic 1kB/4kB karty

Potenciálne zneužitie Mifare Classic kariet alebo čo je všetko možné

- Vytvoriť si ľubovoľné množstvo kópií danej karty
- Dobiť si kredit podľa ľubovôle
- Emulovať karty pomocou špecializovaných zariadení (Proxmark3, Nokia NFC)
- Prečítať citlivé informácie (ako mená, priezviská, rodné čísla, stačí sa „poprechádzať“ po električke)
- Nenávratne zničiť karty ich používateľov (napríklad pasažierov v MHD)
- Monitorovať pohyb pasažierov v priestore

Útočník má plnú kontrolu nad obsahom čipových kariet Mifare Classic!

Proxmark III a Touchatag čítačka



Biometrické RFID pasy

- Všetky nové EU pasy (vrátane slovenských) obsahujú RFID 72kB čip, obsahujúci množstvo citlivých údajov (vaša JPEG fotografia, všetky osobné údaje z pasu, odtlačok prsta, …)
- Pri znalosti MRZ kódu (ktorý je zložený z čísla pasu, dátumu narodenia a expirácie pasu) je možné prečítať takmer celý obsah pasu (okrem EAC a odtlačku prsta) lacnou a verejne dostupnou čítačkou Touchatag za 30 €
- Dátum narodenia sa dá obvykle verejne zistiť, expirácia pasu je 10 rokov (takže maximálne 3650 možností), akým spôsobom je generované číslo pasu?
- Staršie pasy (bez EAC) je možné kompletne vyklonovať, prípadne odemulovať na Nokia NFC telefóne
- Na načítanie odtlačku prstu, AA Public Key Info je nutné poznať špeciálny kľúč – je ho možné získať útokmi cez postranné kanály (časová analýza zmeny napätia pri výpočte RSA), v prípade potenciálneho prelomenia, **bude možné čítať vaše odtlačky prstov a iné citlivé osobné informácie!**

Stále sa cítite s biometrickými RFID pasmi bezpečnejšie?

Biometrické RFID pasy s odtlačkom prsta

Prečítanie biometrického pasu

Slovenská polícia tvrdí, že sa to nedá. *„Údaje je možné čítať iba špeciálnou čítačkou priloženou priamo k pasu, čip je pasívny prvok,“* tvrdil včera František Blanárik z Národného bezpečnostného úradu (NBÚ).

Ďalšie prelomené RFID technológie

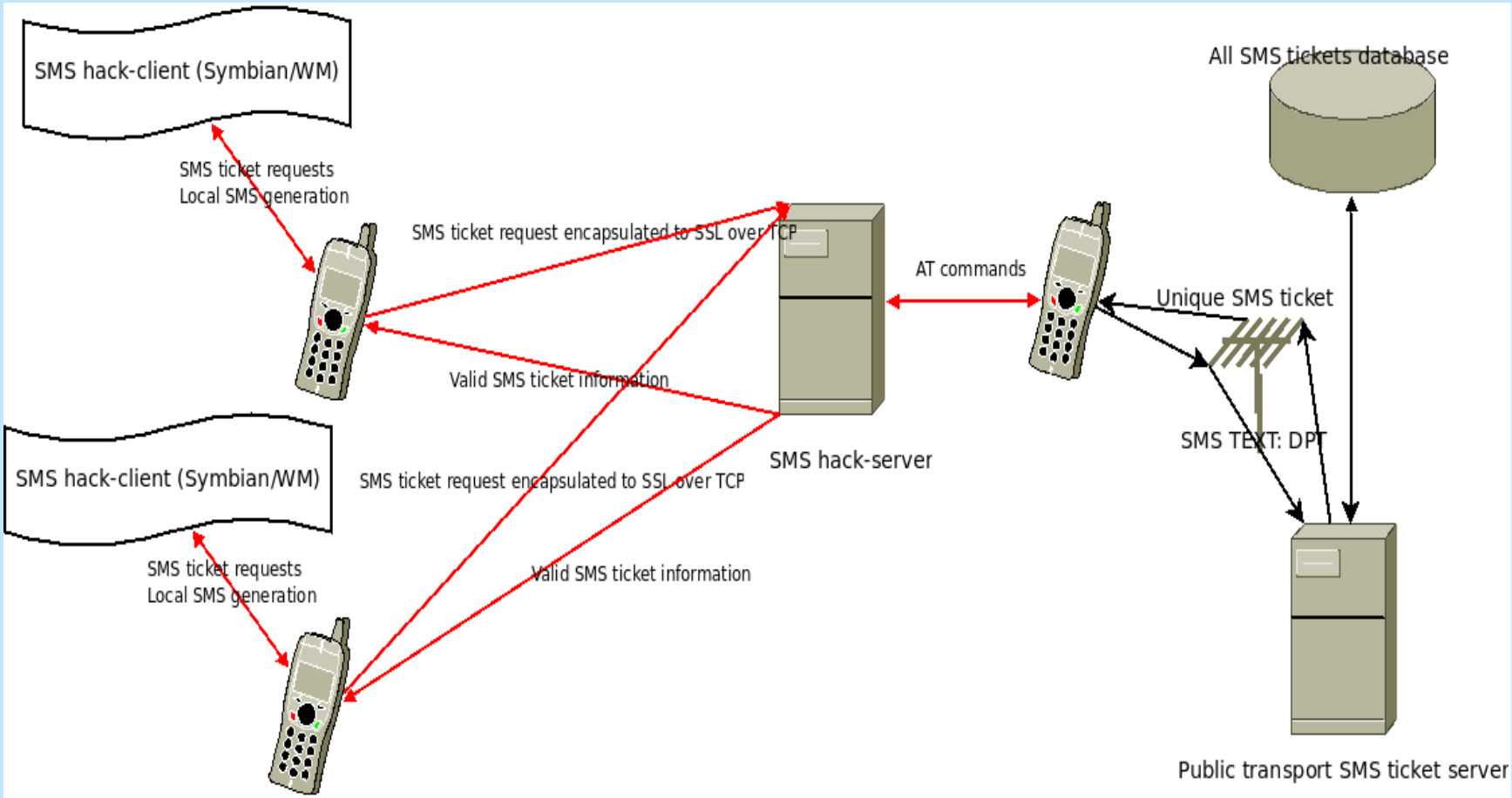
- **Hitag2** - „badge“ karty, kľúčiky do áut Renault / Opel / Peugeut / Citroen
- **Legic Prime** – platobné karty
- **Mifare UltraLight** – karty na lyžiarske vleky
- **HID Prox** – široké použitie
- **Biometrické pasy** – všetky, ktoré nepodporujú EAC, je možné vyklonovať

Neexistujú bezpečné RFID karty, len zatiaľ neprelomené...

Zraniteľnosti v SMS lístkoch

- Typická ukážka **chybne navrhnutej bezpečnostnej architektúry** – chýba jednoduché zviazanie pasažiera s SMS lístkom
- SMS lístok je možné jednoducho vygenerovať, distribuovať a zdielať veľkým množstvom ľudí
- Pri použití sofistikovanej detekcie geografických kolízií, možnosti podvrhnúť zdrojové číslo v SMS ako aj hovore je **takmer nemožné uvedený útok odhaliť (a určite neekonomické zo strany DP)**
- Zraniteľné DP veľkých miest – Bratislava, Praha, Viedeň, Varšava, …
- Bratislavský dopravný podnik bol z našej strany o danej zraniteľnosti informovaný ešte pred samotným nasadením zraniteľných SMS lístkov (!), Pražský dopravný podnik sa nám vyhrážal žalobou
- Bratislava zaviedla „celodenný“ SMS lístok, čo **výrazne znížilo náročnosť na implementáciu popisovaného SMS útoku**

Architektúra hacknutých SMS lístkov



Bezpečnosť elektronického mýta

- Extrémne drahý netransparentný projekt zaplatený daňovými poplatníkmi
- Spoločnosť Skytoll sme kontaktovali ohľadom **možnej bezpečnostnej analýzy v snahe získať ďalšie bezpečnostné informácie** – našu žiadosť prijali, ale **doteraz žiadna reakcia**
- **Proprietárny projekt, neverejná proprietárna uzavretá bezpečnosť –** môžeme sa len dohadovať, ako to celé z bezpečnostného hľadiska funguje
- Nezávisle od toho, či je dané riešenie bezpečné alebo nie (čo bez otvorenej analýzy nie je možné vedieť) **spolieha sa na inherentne nebezpečné a už prelomené technológie:**
  - **GSM –** ktoré je možné v reálnom čase rušiť, prelomiť, odpočúvať, podvrhnúť
  - **GPS –** ktoré je možné rušiť, resp. podvrhnúť (GPS spoofing)

Nevyhnutnosť otvorenosti všetkých verejných projektov dotovaných zo štátnych peňazí (dostupná bezpečnostná špecifikácia, použité protokoly, algoritmy, šifry, ..)

Palubná OBU jednotka

Vyhnúť sa poplatkom je možné pomocou jednoduchých verejne dostupných GPS rušičiek!

Záver

- S rastúcou komplexnosťou informačných technológii rastie aj množstvo potenciálnych útokov
- V prípade bezpečných technológií sa objavujú nové „**teoretické“ útoky**
- Z „teoretických útokov“ sa **stávajú prakticky realizovateľné hrozby**
- Veľa technológii je zraniteľných práve preto lebo sú **proprietárne a neverejné,** kedy chýba spätná väzba zo strany technickej verejnosti a nezávislých bezpečnostných špecialistov
- V prípade masovo používaných technológií je vždy nutný **objektívny nezávislý audit**

Len **otvorené technológie**

dokážu byť skutočne **bezpečné**

(inak si totiž bezpečnosťou

nemôžete byť „nikdy“ istý)