Bezkontaktní chytré karty a Datová úložiště

Marek Bukáček

výzkumná skupina GAMS při KM
KM FJFI ČVUT v Praze

23. duben 2012

Obsah

Bezkontaktní chytré karty

Elektronický pas

Datová úložiště

Představení

- pasivní bezkontaktní zařízení
- účelem je předat krátkou informaci

Představení

- pasivní bezkontaktní zařízení
- účelem je předat krátkou informaci
- vyvinuly se z karet s čárovým kódem
- obecně více typů karet, budeme uvažovat karty schopné kryptologických operací $\rightarrow$ chytré

Představení

- pasivní bezkontaktní zařízení
- účelem je předat krátkou informaci
- vyvinuly se z karet s čárovým kódem
- obecně více typů karet, budeme uvažovat karty schopné kryptologických operací $\rightarrow$ chytré
- použití: vstupní karty, platební karty, elektronický pas, opencard

Fyzikální pozadí

- radiová komunikace
- bez vlastního napájení $\rightarrow$ EM pole zdroje
- anténa karty a anténa terminálu pracují na principu vysokofrekvenčního transformátoru

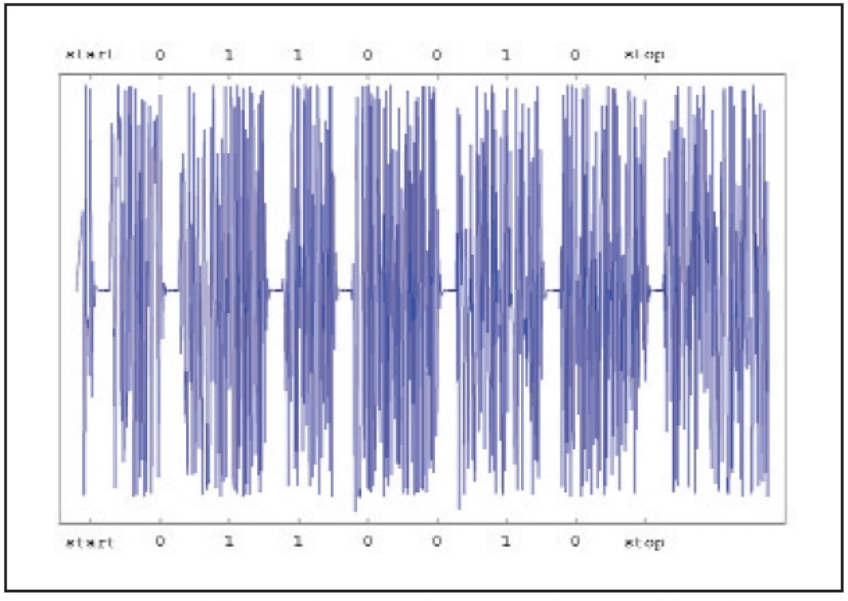
Fyzikální pozadí

- radiová komunikace
- bez vlastního napájení $\rightarrow$ EM pole zdroje
- anténa karty a anténa terminálu pracují na principu vysokofrekvenčního transformátoru
- přenos energie $\sim \frac{1}{r^3} \rightarrow$ komunikace na krátkou vzdálenost
- pro napájení sinusový signál 13,56 MHz (základní nosná vlna)
- pro přenos terminál - karta: amplitudová modulace nosné vlny (106 Kb/s)
- pro přenos karta - terminál: metoda modulace zátěží (napájecí zátěž 13,56 MHz x 847,5 kHz účelová zátěž)

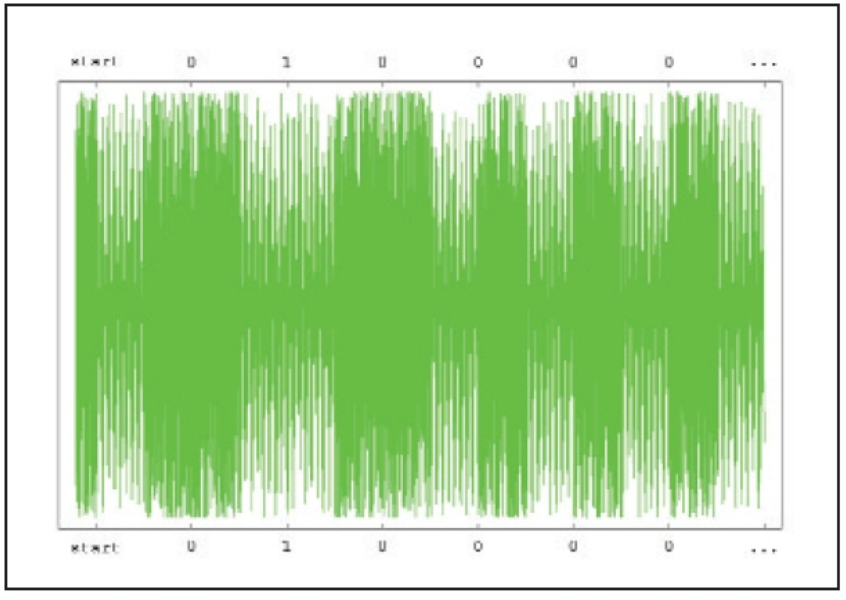
Fyzikální pozadí

- radiová komunikace
- bez vlastního napájení $\rightarrow$ EM pole zdroje
- anténa karty a anténa terminálu pracují na principu vysokofrekvenčního transformátoru
- přenos energie $\sim \frac{1}{r^3} \rightarrow$ komunikace na krátkou vzdálenost
- pro napájení sinusový signál 13,56 MHz (základní nosná vlna)
- pro přenos terminál - karta: amplitudová modulace nosné vlny (106 Kb/s)
- pro přenos karta - terminál: metoda modulace zátěží (napájecí zátěž 13,56 MHz x 847,5 kHz účelová zátěž)
- fyzikální možnosti útoku:
  - proměnná zátěž antény karty indukuje signál odpovídající modulované nosné vlně
  - aktivní vyslání správné vlny je pro terminál nerozlišitelné od zatěžování kartou

Ukázka komunikace - pozdravení



Obr. 1 Přenos dat z terminálu do karty (REQA)



Obr. 2 Přenos dat z karty do terminálu (ATQA)

- terminál vysílá příkaz REQA – výzva ke kartám v poli
- karta odpovídá příkazem ATQA – připravenost na komunikaci

MYFARE

- 1994 – společnost NXP Semiconductors, od roku 2006 majetkem Philips
- protokol MYFARE spolu s šifrovacím algoritmem KRYPTO1
- použití: vstupy do objektů, elektronické peněženky, dopravní a městské karty (opencard, OysterCard – Londýn, Moskva, Boston, Peking . . .) – 70 % trhu

MYFARE

- 1994 – společnost NXP Semiconductors, od roku 2006 majetkem Philips
- protokol MYFARE spolu s šifrovacím algoritmem KRYPTO1
- použití: vstupy do objektů, elektronické peněženky, dopravní a městské karty (opencard, OysterCard – Londýn, Moskva, Boston, Peking . . .) – 70 % trhu
- kapacita 1 - 4 KB v blocích po 16 bajtech, bloky seskupené do sektorů
- každý sektor má zaváděcí blok (4B)
- přístup k sektorům po prokázání klíče (48 bitů)
- různé typy přístupů (čtení, zápis, ++, . . .) $\rightarrow$ 2 různé klíče pro každý sektor
- blok 0 sektoru 0 nese informace od výrobce – např. číslo karty

MYFARE – jak kartu nepoužívat

- účel karty je pouze vstup do objektu
- terminál má seznam karet čísel karet, které vpouští
- proběhne pouze úvodní konverzace

MYFARE – jak kartu nepoužívat

- účel karty je pouze vstup do objektu
- terminál má seznam karet čísel karet, které vpouští
- proběhne pouze úvodní konverzace

- zdá se, že pro vstup je nutné ukrást kartu nebo seznam
- odposlech karty není reálný
- ale terminál opakuje číslo karty při úvodní konverzaci (podle standardu ISO) $\rightarrow$ odposlech na desítky metrů

MYFARE – jak kartu nepoužívat

- účel karty je pouze vstup do objektu
- terminál má seznam karet čísel karet, které vpouští
- proběhne pouze úvodní konverzace
- zdá se, že pro vstup je nutné ukrást kartu nebo seznam
- odposlech karty není reálný
- ale terminál opakuje číslo karty při úvodní konverzaci (podle standardu ISO) $\rightarrow$ odposlech na desítky metrů
- měnit implicitní hodnoty klíčů A0A1A2A3A4A5 resp. B0B1B2B3B4B5

MYFARE – vývoj

- prosinec 2007 – teoreticky popsán postup pro zkopírování MYFARE Classic
- duben 2008 – praktická metoda pomocí „běžné“ čtečky, 200 sec
- říjen 2008 – čtečka + notebook, 50 ms (= jedno načtení)
- duben 2009 – bezdrátové zkopírování karty do 10 sec

MYFARE – vývoj

- prosinec 2007 – teoreticky popsán postup pro zkopírování MYFARE Classic
- duben 2008 – praktická metoda pomocí „běžné“ čtečky, 200 sec
- říjen 2008 – čtečka + notebook, 50 ms (= jedno načtení)
- duben 2009 – bezdrátové zkopírování karty do 10 sec

- útoky využívají slabost parity bitu – každý odeslaný bit doprovázen dalším (podle standardu)
- MYFARE Classic ale vypočítává parity bit z otevřeného textu
- navíc ho používá k zašifrování dalšího bitu

MYFARE – vývoj

- prosinec 2007 – teoreticky popsán postup pro zkopírování MYFARE Classic
- duben 2008 – praktická metoda pomocí „běžné“ čtečky, 200 sec
- říjen 2008 – čtečka + notebook, 50 ms (= jedno načtení)
- duben 2009 – bezdrátové zkopírování karty do 10 sec

- útoky využívají slabost parity bitu – každý odeslaný bit doprovázen dalším (podle standardu)
- MYFARE Classic ale vypočítává parity bit z otevřeného textu
- navíc ho používá k zašifrování dalšího bitu

- F. D. Garcia at all: Wirelessly Pickpocketing a Mifare Classic Card, Netherlands

MYFARE DESFire

- od roku 2006
- varianty Triple-DES se 4 KB nebo AES se 2, 4 nebo 8 KB

MYFARE DESFire

- od roku 2006
- varianty Triple-DES se 4 KB nebo AES se 2, 4 nebo 8 KB
- situace v Praze
  - v době zahájení (2007) vydávány MYFARE Classic
  - rok 2008: přechod k MYFARE DESFire
  - možné přečtení karty stejně odhalí pouze číslo karty a datum narození držitele (+ data PID)
  - držitelé karet MYFARE Classic si je můžou zdarma vyměnit

Elektronický pas

- v ČR od druhé poloviny roku 2006
- standardy vydává Mezinárodní organizace pro civilní letectví – ICAO
- Chip Philips
- 15 souborů s daty „uživatele“ (kopie strojově čitelné zóny, fotografie, . . . , veřejný klíč)
- soubory s technickými údaji o kartě

Elektronický pas

- v ČR od druhé poloviny roku 2006
- standardy vydává Mezinárodní organizace pro civilní letectví – ICAO
- Chip Philips
- 15 souborů s daty „uživatele“ (kopie strojově čitelné zóny, fotografie, . . . , veřejný klíč)
- soubory s technickými údaji o kartě
- bezpečnost:
  - hodnota identifikátoru UID volena náhodně → znemožněno sledování pohybu
  - pro autentizaci přístupu k uživatelským souborům nutný digitální podpis
  - autentizace čipu protokolem „výzva – odpověď“ . . . volitelné
  - přístup k souborům prostřednictvím BAC

Elektronický pas – útoky

- možnosti odposlechu :
  - aktivní komunikace s pasem – desítky cm
  - odposlech – terminál i pas – jednotky cm
  - odposlech – pouze terminál – desítky m
  - aktivní komunikace s terminálem – desítky m

Elektronický pas – útoky

- možnosti odposlechu :
  - aktivní komunikace s pasem – desítky cm
  - odposlech – terminál i pas – jednotky cm
  - odposlech – pouze terminál – desítky m
  - aktivní komunikace s terminálem – desítky m
- „drncavý“ útok – dostat čtečku do dosahu karty fyzickým kontaktem
- EM pole dost silné pro komunikaci na 25cm může poškodit okolní elektroniku

Elektronický pas – útoky

- možnosti odposlechu :
  - aktivní komunikace s pasem – desítky cm
  - odposlech – terminál i pas – jednotky cm
  - odposlech – pouze terminál – desítky m
  - aktivní komunikace s terminálem – desítky m
- „drncavý“ útok – dostat čtečku do dosahu karty fyzickým kontaktem
- EM pole dost silné pro komunikaci na 25cm může poškodit okolní elektroniku
- útok metodou emulace postranních pásem

Elektronický pas – počátek komunikace

SEL ID: 08 94 34 37
T_1: E0 50 BC A5
P_1: 0E 78 77 A5 02 80 91 E1 65 77 01 02 01 01 D0 4A
T_2: 02 **00 A4 04 0C 07 A0 00 00 02 47 10 01** 98 B8
P_2: 02 **90 00** F1 09
T_3: 03 **00 A4 02 0C 02 01 1E** A7 9B
P_3: 03 **69 82** 27 5F

- pas si generuje identifikátor
- terminál iniciuje komunikaci
- pas odpovídá konfigurační strukturou
- terminál vybírá aplikaci zasláním AID
- pas hlásí úspěch (90 00)
- pokus o přístup do souboru EF.COM (služební data)
- odmítnutí (69 82) a požadavek kryptografické autentizace

Elektronický pas – Autentizace pasu

- Pasivní část:
  - vychází z RSA
  - soubor s veřejným klíčem od terminálu je uložen na kartě
  - délky klíčů: 3Kb + 2Kb (vydávají státní orgány)
  - nemůže rozlišit pravý pas od kopie

Elektronický pas – Autentizace pasu

- Pasivní část:
  - vychází z RSA
  - soubor s veřejným klíčem od terminálu je uložen na kartě
  - délky klíčů: 3Kb + 2Kb (vydávají státní orgány)
  - nemůže rozlišit pravý pas od kopie
- Aktivní část (ČR a . . .):
  - přidán soukromý klíč
  - terminál vyšle náhodné číslo V (8B)
  - karta generuje U náhodné o délce 106 B a vypočte hash $w = SHA - 1(U||V)$
  - vypočte $m = 6A||U||w||BC$ o délce 128 B
  - transformace RSA: $s = m^d$ mod N, kde N je modul a d soukromý exponent
  - odesláno do terminálu, ten ověří párovost s veřejným klíčem
  - záznam výzvy a správné odpovědi může sloužit jako důkaz výskytu na místě

Elektronický pas – BAC

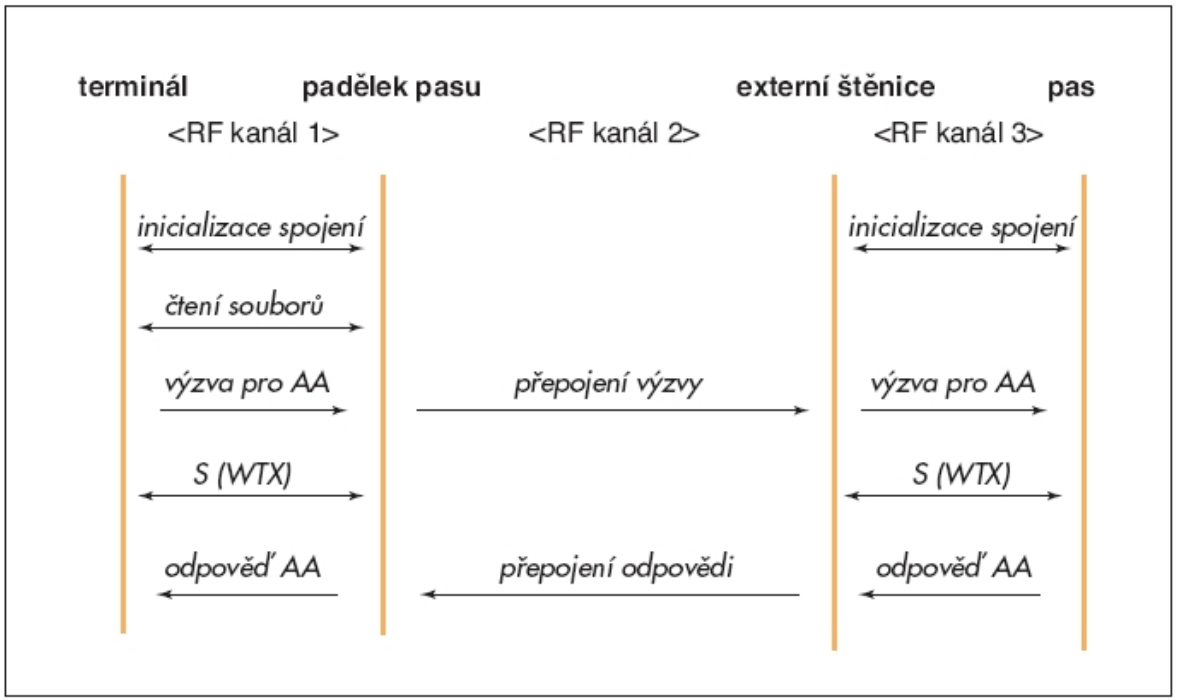
- Basic Access Control, pro autentizovaného žadatele
- heslo pro BAC je tvořeno z tištěných údajů v pasu (primární heslo W: číslo pasu, datum narození, datum exspirace)
- výpočet S jako prvních 16 B zleva z hodnoty SHA–1(W) – terminál
- výpočet dvou 16B klíčů K_E a K_M pro 3DES a pro kontrolní kód MAC – terminál

Elektronický pas – BAC

- Basic Access Control, pro autentizovaného žadatele
- heslo pro BAC je tvořeno z tištěných údajů v pasu (primární heslo W: číslo pasu, datum narození, datum exspirace)
- výpočet S jako prvních 16 B zleva z hodnoty SHA–1(W) – terminál
- výpočet dvou 16B klíčů K_E a K_M pro 3DES a pro kontrolní kód MAC – terminál
- terminál si řekne o kontrolních 8B $\rightarrow$ karta odešle otevřený text
- pomocí 3DES a MAC je terminál zašifruje (spolu s vlastními náhodnými 8B) a vrátí
- karta dešifruje, ověří vlastních kontrolních 8B
- identifikuje a zašifruje kontrolních 8B od terminálu, odešle

Elektronický pas – útok

- pas může požádat terminál o prodloužení čekání na odpověď (i 16ti násobek běžné doby, 5s)



Elektronický pas – slabiny

- krátké heslo S – stačí na drcavý útok
- na základě odposlechu terminálu hrubá síla prolomí
- $\rightarrow$ znalost W na příště, popřípadě detekování osoby podle S
- plánovaná metoda na použití dat z otisků prstů
- šifrování nechrání hlavičky příkazů a chybové hlášky

Elektronický pas – slabiny

- krátké heslo S – stačí na drcavý útok
- na základě odposlechu terminálu hrubá síla prolomí
- $\rightarrow$ znalost W na příště, popřípadě detekování osoby podle S
- plánovaná metoda na použití dat z otisků prstů
- šifrování nechrání hlavičky příkazů a chybové hlášky
- všechny možné útoky za cenu bezkontaktnosti

Elektronický pas – slabiny

- krátké heslo S – stačí na drcavý útok
- na základě odposlechu terminálu hrubá síla prolomí
- $\rightarrow$ znalost W na příště, popřípadě detekování osoby podle S
- plánovaná metoda na použití dat z otisků prstů
- šifrování nechrání hlavičky příkazů a chybové hlášky
- všechny možné útoky za cenu bezkontaktnosti
- závěr – je ochrana digitálních pasů dostačující?

Šifrování datových úložišť

- ochrana při archivování stejně důležitá jako při komunikaci
- velké množství citlivých dat

Šifrování datových úložišť

- ochrana při archivování stejně důležitá jako při komunikaci
- velké množství citlivých dat
- základní myšlenka:
  - sektor rozdělit na bloky po 16B (= „písmena“)
  - na ně použít AES s klíčem K

Šifrování datových úložišť

- ochrana při archivování stejně důležitá jako při komunikaci
- velké množství citlivých dat
- základní myšlenka:
  - sektor rozdělit na bloky po 16B (= „písmena“)
  - na ně použít AES s klíčem K
  - AES pro abecedu o 26 písmenech je slabý
  - zde je 2^{128} různých písmen

Možné útoky

- i zašifrovaná data nabízejí několik možností:

1. hodně bloků se stejnou hodnotou ukazuje na prázdné místo $\rightarrow$ odhad délky dat, přírůstků
2. možnost výměny bloků (silné, pokud známe pozice informací)
3. smazaní bloku (silné, pokud známe pozice informací)

Možné útoky

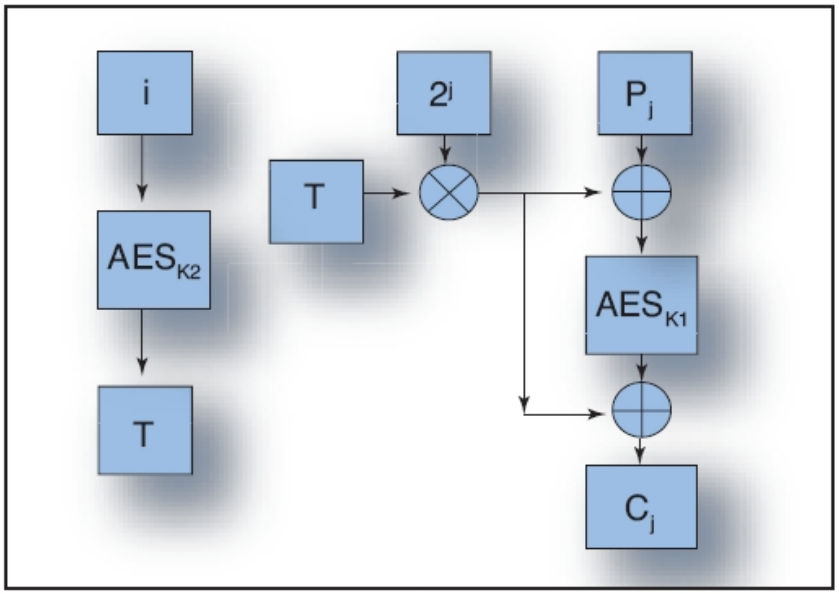
- i zašifrovaná data nabízejí několik možností:

1. hodně bloků se stejnou hodnotou ukazuje na prázdné místo → odhad délky dat, přírůstků
2. možnost výměny bloků (silné, pokud známe pozice informací)
3. smazaní bloku (silné, pokud známe pozice informací)
4. odeslat vlastní zprávu, podívat se, jak a kde byla uložena a poté s ní manipulovat

- nový standart požaduje šifrovat bloky různými způsoby → znemožnění přesunů

XTS–AES

- klíč má 2 části:
  - klíč pro AES (128B – 256B)
  - modifikační hodnota pro další sektory (128B)



- pro každý sektor *i* výpočet šumu *T*
- každý blok *j* sektoru *i* se šifruje již zašuměný

Flash disky

- 4GB flash disk jako záložní médium menší firmy nebo projektu
- chráněn vlastním tělem
- šifrování pro případ ztráty nebo krádeže
- stejné postup i pro paměťové karty v telefonech, ...

Flash disky

- 4GB flash disk jako záložní médium menší firmy nebo projektu
- chráněn vlastním tělem
- šifrování pro případ ztráty nebo krádeže
- stejné postup i pro paměťové karty v telefonech, ...
- šifrovací program TrueCrypt
  - první verze 2004 (založen na E4M – 1997)
  - freeware, www.truecrypt.org
  - šifrování souboru i diskového oddílu

Flash disky

- 4GB flash disk jako záložní médium menší firmy nebo projektu
- chráněn vlastním tělem
- šifrování pro případ ztráty nebo krádeže
- stejné postup i pro paměťové karty v telefonech, ...
- šifrovací program TrueCrypt
  - první verze 2004 (založen na E4M – 1997)
  - freeware, www.truecrypt.org
  - šifrování souboru i diskového oddílu
  - využívá AES, Twofish, Serpent pro šifrování
  - možnost připojit Blowfish, DES, Triple DES a CAST-128
  - pro hashování využívá RIPEMD-160, SHA-512 a Whirlpool

TrueCrypt

- máme zvolenou blokovou šifru a její klíč k_1
- šifrovaná oblast tvoří 1 soubor – datová a hlavičková část
- k_1 spolu s přídavným klíčem k_2 uloženy v hlavičce
- hlavička je zašifrovaná pomocí soli a hesla uživatele

TrueCrypt

- máme zvolenou blokovou šifru a její klíč k_1
- šifrovaná oblast tvoří 1 soubor – datová a hlavičková část
- k_1 spolu s přídavným klíčem k_2 uloženy v hlavičce
- hlavička je zašifrovaná pomocí soli a hesla uživatele
- data šifrována po 128b odděleně a s jiným klíčem (model Liskov-Rivest-Wagner)
- $C_i = E_{k_1}(P_i \oplus (k_2 \otimes i)) \oplus (k_2 \otimes i)$

TrueCrypt

- máme zvolenou blokovou šifru a její klíč k_1
- šifrovaná oblast tvoří 1 soubor – datová a hlavičková část
- k_1 spolu s přídavným klíčem k_2 uloženy v hlavičce
- hlavička je zašifrovaná pomocí soli a hesla uživatele
- data šifrována po 128b odděleně a s jiným klíčem (model Liskov-Rivest-Wagner)
- $C_i = E_{k_1}(P_i \oplus (k_2 \otimes i)) \oplus (k_2 \otimes i)$
- heslo a sůl zpracovány funkcí PBKDF2 – hash 2000 za sebou
- možnost šifrovat pomocí veřejného souboru
- cílem těchto operací je zdržet útok hrubou silou na heslo

TrueCrypt

- máme zvolenou blokovou šifru a její klíč k_1
- šifrovaná oblast tvoří 1 soubor – datová a hlavičková část
- k_1 spolu s přídavným klíčem k_2 uloženy v hlavičce
- hlavička je zašifrovaná pomocí soli a hesla uživatele
- data šifrována po 128b odděleně a s jiným klíčem (model Liskov-Rivest-Wagner)
- $C_i = E_{k_1}(P_i \oplus (k_2 \otimes i)) \oplus (k_2 \otimes i)$
- heslo a sůl zpracovány funkcí PBKDF2 – hash 2000 za sebou
- možnost šifrovat pomocí veřejného souboru
- cílem těchto operací je zdržet útok hrubou silou na heslo
- heslo by mělo obsahovat min. 20 znaků (včetně symbolů . . .)
- nezaplňovat celý prostor chráněnou oblastí – pro případ nezabezpečeného přístupu

Zdroje

- V. Klíma, T. Rosa: Kryptologie pro praxi (díly 1–5/2007 a 7,8/2007)
- T. Rosa: Bezpečnost RFID v praxi (prezentace 2008)
- F. D. Garcia at all: Wirelessly Pickpocketing a Mifare Classic Card
- Wikipedia – MYFARE, TrueCrypt
- http://opencard.praha.eu

Zdroje

- V. Klíma, T. Rosa: Kryptologie pro praxi (díly 1–5/2007 a 7,8/2007)
- T. Rosa: Bezpečnost RFID v praxi (prezentace 2008)
- F. D. Garcia at all: Wirelessly Pickpocketing a Mifare Classic Card
- Wikipedia – MYFARE, TrueCrypt
- http://opencard.praha.eu

Děkuji za pozornost