

Autentizace uživatelů tokeny



Metody autentizace uživatele

- Metody autentizace
 - něco, co známe (PIN, heslo)
 - **něco, co máme (klíč, čipová karta)**
 - něco, co jsme (biometriky)
- Třífaktorová autentizace
 - Token – čipová karta
 - PIN / heslo
 - Biometrika načtená a zpracovaná přímo tokenem

Token / Předmět

- *Něco, co uživatel má...*
- Předmět, token
- Token (angl.)
 - Projev, znamení, upomínka, památka
 - Znamka pravosti
 - *By the token...* Na důkaz toho
 - *Token money...* Mince kryté zlatem

Tokeny

- Jako u tajných informací je cílem autentizace (ověření identity) uživatele
 - co nejsnáze pro autorizované uživatele;
 - co nejkomplicovaněji pro neautorizované uživatele.
- Je potřeba řešit mj. otázky
 - obtížnosti vytvoření a kopírování,
 - průběhu kontroly,
 - práce s tokeny v „neočekávaných případech“,
 - co se má stát, je-li karta vyjmuta ze čtečky

Dilema

- **Cena výroby** jednoho kusu při výrobě mnohkusové série (co nejmenší cena)

versus

- **Cena padělání** jednoho kusu za účelem vniknutí do systému (co největší cena)
 - Přestává platit v případech, kdy se vyplatí produkce mnohkusové série (padělků)

Z historie

- Amulet
- Pečeť
- Bankovka se specifickým číslem nebo specificky roztržená bankovka



- Klíč!
- Peníze



Cena výroby

- Ekonomická „klasika“
- V přepočtu na kus klesá při výrobě větších sérií
 - Může být důležité pro uživatele prvních sérií, kdy následně cena výroby klesá a tím i bariéra pro ty, kdo zvažují padělání

Cena padělání

- Platí to, co pro cenu výroby, ale navíc
 - Je důležité to, zda (potenciální) útočník získá stejně výrobou jednoho nebo více padělků či nikoliv – motivace útočníka
 - Jak dlouho (a případně kolik) musí mít k dispozici původní(ch) token(ů)
 - Zda existuje legislativní postih padělání jako takového (bez ohledu na útok na systém)

Další omezení

- Prevence
 - Dostupnost vybavení
 - Modifikace běžně dostupného vybavení, např. barevné kopírky
 - Nekopírují přesně určité barvy
 - Také vnášejí svůj identifikátor do obrazu
 - Kontrola a licence živností atd.
- Utajení určitých informací (k používání nebo vlastní konstrukci tokenu)

Nejčastější tokeny v IT/IS

- Karty
 - S magnetickým proužkem
 - Čipové
 - Kontaktní / bezkontaktní
 - Čtečka na straně dotazovatele / kontrolovaného (mobil)
- Autentizační kalkulátory
 - S tajnou informací
 - S hodinami
 - Způsob vstupu/výstupu



Karta s magnetickým proužkem

- 3stopý proužek ~ 250 B (spolehlivě)
- Poměrně jednoduše se kopírují
 - Falešné bankomaty, čtečky ap.
 - např. nedávná „Libanonská smyčka“
 - Posun částí stop nepříliš účinný
 - Hologramy se obtížně kontrolují (autom.?)
 - Lze vytvářet charakteristiky individuálních magn. proužků
 - U každé karty zvlášť
 - Dochází k mírné změně v čase
 - Různá citlivost různých čtecích/kontrolních zařízení
- Podvody s PINy na kartách (čtení, přehrání) běžné



Čipové karty

- Co umí?
 - Paměťové (*chipcard*)
 - Paměťové se speciální logikou (ochrana PINem, čítače atd.)
 - Procesorové (*smartcard*)
- Jak s nimi komunikovat?
 - Kontaktní – nutný kontakt se čtečkou (zdroj energie)
 - Bezkontaktní
 - Nemůže použít externí zdroj energie – omezení
 - Operace mohou být prováděny bez vědomí uživatele
 - Vhodná pro fyzickou kontrolu přístupu ap.

Podoby čipové karty

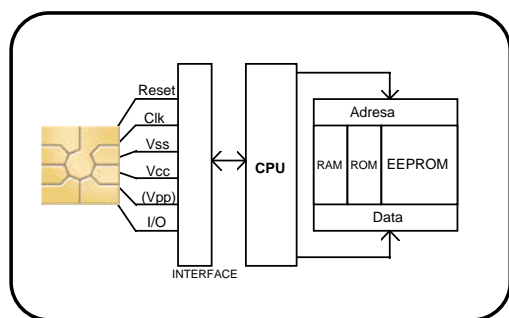
- Obvyklá karta – bankomatová ap.
- SIM karta (telefony GSM)
- USB token



Čipová karta s procesorem

- Dále jen „čipová karta“
- A samozřejmě i s pamětí
 - RAM (Random Access Memory) – x KB
 - ROM (Read Only Memory) – x.10-10² KB – OS ap.
 - EEPROM (Electrically Erasable Programmable Read Only Memory) – x.10 KB
- Různá složitost výpočtů, ideálně i náročné kryptografické operace

Kontaktní procesorová čipová karta



Logická struktura karty

- Po personalizaci karty je přístup dat možný pouze přes logickou strukturu souborů a adresářů.
- Data na čipové kartě se jeví podobně jako data na pevném disku
 - kořenový adresář → hlavní soubor - master file (MF)
 - adresáře → dedikovaný soubor - dedicated file (DF)
 - soubory → elementární soubor - elementary file (EF)
- Počátečně se pracuje s MF, další soubor nebo adresář pro práci lze vybrat
 - 2-bajtovým identifikátorem EF/DF/MF
 - zřetěžením jmen DF/EF

Typy dat

- Lineární záznamy
 - pevná délka
 - variabilní délka
- Cyklické záznamy
- Transparentní (nestrukturovaná) data

Řízení přístupu

- Řízení přístupu k datům na kartě je tvořeno především řízením přístupu k souborům.
- S každým souborem je svázána hlavička souboru, která určuje přístupová práva k souboru.
- Základním principem řízení přístupu je zadávání PINů a jejich management.
- Přístup k souboru může být například vázán na splnění některé z těchto podmínek:
 - ALW (vždy povolen přístup)
 - CHV1 (nutné zadat PIN uživatele 1)
 - CHV2 (nutné zadat PIN uživatele 2)
 - NEV (přístup nepovolen)

PIN management

- PINy jsou ukládány v samostatných souborech (EF). Přístupová práva k těmto souborům určují možnost změny těchto PINů.
- Při změně PINu je požadavek provázen starým a novým PINem.
- Počet neúspěšných pokusů bývá omezen. Po překročení limitu (3 - 5) je PIN blokován.
- Pro odblokování je třeba zadat PIN a odblokovací PIN.
- I počet neúspěšných odblokování je omezen.

Čipová karta jako aktivní prvek

- Čipové karty mají i nezanedbatelnou výpočetní sílu.
- Na čipové kartě je možné implementovat kryptografické algoritmy i protokoly.
- Je možné na kartě provádět operace s citlivými daty tak, že tato data nemusí opustit čipovou kartu (např. vytváření digitálního podpisu).
- Symetrické šifrovací algoritmy běží v prostředí čipové karty bez problémů (často též speciální HW akcelerátory - např. DES, 3DES, AES).
- Asymetrické kryptografické algoritmy jsou řádově náročnější, proto vyžadují specifické koprocesory.

Příklad moderní čipové karty

Infineon SLE 88CX642S

- 32-bitový RISC mikroprocesor (0,22 μm CMOS technologie)
- paměť ROM: 192 kB
- paměť RAM: 6 kB
- paměť EEPROM: 72 kB
 - doba zápisu: 4,5 ms
 - max. počet zápisových cyklů: 500 000
 - max. doba uchování dat: 10 let

Infineon SLE88CX642S

- Příklad časů pro nejvyšší pracovní frekvenci 55 MHz

Operace	Modulus	Exponent	Doba trvání operace
Podpis RSA (bez využití CRT)*	1024 bitů	1024 bitů	78 ms
Podpis RSA (bez využití CRT)*	2048 bitů	2048 bitů	6,9 s
Podpis RSA (s využitím CRT)*	1024 bitů	1024 bitů	25,2 ms
Podpis RSA (s využitím CRT)*	2048 bitů	2048 bitů	0,17s
Ověření RSA	1024 bitů	32 bitů	2,8 ms
Ověření RSA	2048 bitů		38 ms
Generování klíče RSA	1024 bitů		1,56 s
Generování klíče RSA	2048 bitů		14,4 s
Podpis EC DSA (over GF(p))	160 bitů	160 bitů	24 ms
Ověření EC DSA (over GF(p))	160 bitů	160 bitů	50 ms

Bezpečnost čipových karet

- **Základní pojmy:**
 - **Fyzická bezpečnost** (physical security) - překážka umístěná kolem počítačového systému za účelem ztížení neautorizovaného fyzického přístupu k tomuto počítačovému systému.
 - **Odolnost vůči narušení** (tamper resistance) - vlastnost části systému, která je chráněna proti neautorizované modifikaci způsobem zajišťujícím podstatně vyšší úroveň ochrany než ostatní části systému.
 - **Zjistitelnost narušení:** systém, u kterého jakákoliv neautorizovaná modifikace zanechává zjistitelné stopy.
 - **Detekce narušení:** automatické zjištění pokusu o narušení fyzické bezpečnosti.
 - **Odpověď na narušení:** automatická akce provedená chráněnou částí při zjištění pokusu o narušení.

Klasifikace útočníků

- Rozdělení možných útočníků podle jejich znalostí, schopností, finančních možností, přístupu ke speciálnímu vybavení apod.
- Klasifikace firmy IBM:
 - třída I - chytří nezavěšení útočníci
 - často velmi inteligentní, nedostatečné znalosti systému, přístup pouze ke středně sofistikovanému vybavení
 - třída II - zaslíbení insideri
 - mají značné specializované technické vzdělání i zkušenosti
 - třída III - dobře finančně podporované organizace
 - schopné vytvořit týmy specialistů, zajištěné dobrými finančními zdroji, provádí detailní analýzy systému

Útoky na čipové karty

- Fyzické útoky
 - invazivní
 - semi-invazivní
- Logické útoky
 - monitorování činnosti karty
 - časové analýzy
 - výkonové analýzy
 - indukce chyb během činnosti
 - programové útoky přes API

Fyzické útoky

- Reverzní inženýring – dochází k nevratné změně karty, případně čipu. Narušení je viditelné.
- Vyžadují nákladné vybavení, specializované přístroje a znalosti (třídy 3 klasifikace).
- Invazivní útoky
 - preparace čipu
 - rekonstrukce a analýza návrhu čipu
 - testování čipu s využitím mikrosond
 - čtení paměti čipu
- Semi-invazivní
 - nedochází k přímému zničení čipu
 - využívá záření, laseru, elektromagnetických polí, ...

Logické útoky

- Vyžadují detailní znalosti o struktuře karty (často zjištěné předchozím fyzickým útokem).
- Nevyžadují speciální a nákladné vybavení.
- Typy útoků:
 - monitorování činnosti karty
 - časová analýza
 - výkonová analýza
 - indukce chyb během činnosti
 - programové útoky přes API

Monitorování - časové analýzy

- Čas nutný pro vykonání rutiny v algoritmu závisí na známém vstupu a na datech uložených na kartě.
- Na základě znalosti vstupu a algoritmu (jeho implementace, optimalizací apod.) a nutného času k výpočtu můžeme odvodit použitá kryptografická data.
- Podstata obrany proti těmto typům útoku spočívá v minimalizaci závislosti délky výpočtu na vstupu.
- Často se tak připravujeme o možnost optimalizace kódu (CRT a RSA).
- Některé jiné snahy o obranu přinášejí možnost jiných typů útoků.

Monitorování - výkonové analýzy

- Sledování spotřeby proudu kartou při provádění jednotlivých typů operací. Různé operace mikrokódu používají různé množství tranzistorů a podle provedených operací se mění spotřeba celé karty.
- Útočník může sledovat spotřebu karty při provádění jednotlivých operací.
- Výrazně se liší spotřeba proudu při operacích sčítání a násobení a při zápisu 0 či 1 do paměti.
- Typy výkonových analýz:
 - jednoduchá výkonová analýza (SPA)
 - diferenciální výkonová analýza (DPA)
 - odvozená výkonová analýza (IPA - inferential power analyses)

Indukce chyb během výpočtu

- Cílem útoku je pomocí náhlých změn operačních podmínek vyvolat změnu hodnoty v paměti, registru apod.
- Záměrem je obejít určitou instrukci či změnit data v registrech či na sběrnici.
- Lze takto obejít správnou autentizaci, kontrolu přístupových práv, modifikovat počet cyklů algoritmu.
- Mezi ovlivnitelné prvky okolí patří např.:
 - napájecí napětí
 - hodinový signál, reset signál
 - elektrické pole
 - teplota

Útoky na kartu přes API

- API umožňuje volat rutiny karty jednotným způsobem.
- Chyby návrhu API mohou umožňovat útočnickovi neautorizovaný přístup k datům.
- Žádný kód/návrh není bezchybný
 - rozhraní často bývá složité a rozsáhlé
 - výrobci se snaží maximálně optimalizovat

Autentizační kalkulátory

- Obvykle využívají protokol výzva-odpověď
 - Odpověď je funkcí tajné informace – klíče a výzvy
- Přenos informací (vstup / výstup)
 - Manuální (klávesnice, displej)
 - Automatický (optika, čárový kód, infrared)
- PIN – standardní (někdy i nouzový)



Tokeny založené na hodinách

- Bývají součástí autentizačních kalkulátorů
 - Ale ne vždy – viz nejrozšířenější RSA SecurID
- V daném okamžiku dávají správnou hodnotu
 - Jedinečnou pro daný přístroj
 - Platnou pouze po určitou dobu (časový rámec)
 - Tuto hodnotu umí spočítat i autentizační server
- Je potřeba řešit otázku posunu hodin
 - Otázka platnosti časových rámců před a po
 - Záznam v čítači na serveru



Příklad – bezkontaktní karta

- Autentizace bývá založena pouze na ověření sériového čísla karty (to karta požádání sdělí)
- Bezpečnost staví na obtížnosti výroby karty (zařízení) se stejnou funkčností
- Pozor – zařízení útočnicka nemusí být nutně stejně velké jako původní karta!

Obecné výhody tokenů

- Rychle se zjistí jejich ztráta
- Nejsou jednoduše kopírovatelné
- Tokeny samy o sobě mohou být schopny zpracovávat nebo přenášet další informace

Obecné nevýhody tokenů

- Ke kontrole je potřeba obvykle speciální čtečka, zařízení nebo vycvičená osoba
- Bez tokenu není autorizovaný uživatel rozeznán
- Token musí být dostatečně složitý, aby se zvýšila obtížnost kopírování
- Může se polámat, přestat fungovat, což nemusí být vždy jednoduše detekovatelné uživatelem

Otázky?

Vítány!!!

Příští přednáška 1. 12. 2004 v 18:00

matyas@fi.muni.cz

zriha@fi.muni.cz