Téma #1: Úvod, pojmy

Digitální podpis ověříme pomocí

- Veřejného klíče podepisující osoby
- Soukromého klíče podepisující osoby
- Privátního klíče podepisující osoby
- Certifikátu veřejného klíče podepisující osoby
- Klíče sdíleného s podepisující osobou

Digitální podpis může vytvořit

- Pouze osoba vlastnící sdílený klíč
- Pouze osoba vlastnící soukromý klíč
- Pouze osoba vlastnící veřejný klíč
- Pouze osoba vlastnící certifikovaný klíč

Co je to zaručený elektronický podpis

- Jednoznačně ověřitelný podpis
- Podpis, který má záruky srovnatelné jako elektronický podpis
- Elektronický podpis, za který se dokážeme nějak důvěryhodně zaručit
- Podpis vytvořený pomocí kryptografických prostředků

V dobrých autentizačních protokolech se typicky

- Heslo posílá v hašované podobě
- Heslo neposílá vůbec
- Heslo posílá v otevřené podobě

Pro bezpečné používání digitálního podpisu

- Je nutné zajistit integritu privátního klíče
- Je nutné zajistit integritu veřejného klíče
- Je nutné udržet privátní klíč v tajnosti
- Je nutné udržet veřejný klíč v tajnosti

Při kombinaci šifrování veřejným klíčem a podpisu dokumentu se doporučuje operace provést v následujícím pořadí:

- Podpis, šifrování, podpis
- Šifrování, podpis, šifrování
- Šifrování, podpis
- Na pořadí operací nezáleží
- Podpis, šifrování

Integrita dat znamená

- Data v původní podobě lze obnovit i přesto, že byla modifikována
- Data nebyla neautorizovaně změněna pouze v průběhu přenosu nezabezpečeným kanálem
- Data nebyla neautorizovaně změněna
- Data nebyla autorizovaně předána

Digitálně podepisujeme

- Pouze haš podepisovaného dokumentu
- V případě malých dokumentů celou zprávu, v případě velkých dokumentů jejich haš
- Vždy přímo celý dokument

Při používání digitálního podpisu používáme

- Digitální klíč
- Privátní a veřejný klíč
- Sdílené symetrické klíče mezi všemi komunikujícími partnery
- Digitální pečetě

Jak zajistíme integritu veřejného klíče

- Utajením soukromé části veřejného klíče
- Pomocí klíčované hašovací funkce
- Částečným utajením veřejného klíče
- Pomocí párového privátního klíče
- Pomocí certifikátu veřejného klíče

Zaručený elektronický podpis

- Autorizuje podepisující osobu ve vztahu k datové zprávě
- Umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě
- Je spojen s dostatečnou finanční zárukou
- Umožňuje detekci změn ve zprávě, ke které je připojen
- Je jednoznačně spojen s podepisující osobou
- Je jednoznačně ověřitelný

Které z následujících nejsou hašovací funkce

- RSA
- MD5
- SHA-1
- AES
- MD4
- RC4

Jaká je nevýhoda digitálního podepisování prováděného až po zašifrování dat

- Žádná, naopak výhodou je možnost snadné verifikace podpisu ještě před dešifrováním
- Výrazné urychlení kryptoanalýzy
- Možnost snadného odstranění digitálního podpisu
- Žádná, naopak, výhodou je možnost několikanásobného podepsání zašifrovaných dat

Silná bezkoliznost u hašovacích funkcí znamená

- V rozumném čase nejsme schopni nalézt x, y (x=y) tak, že h(x)!=h(y)
- V rozumném čase nejsme schopni nalézt x, y (x=y) tak, že h(x)=h(y)
- V rozumném čase nejsme schopni nalézt x, y (x!=y) tak, že h(x)=h(y)
- V rozumném čase nejsme schopni nalézt x, y (x!=y) tak, že h(x)!=h(y)

Jednosměrnost u kryptografických hašovacích funkcí znamená

- V rozumném čase nejsme schopni najít x, y tak, aby h(x)=h(y)
- Pro dané y nelze v rozumném čase najít x tak, aby h(x)=y
- Pro dané h(y) nelze v rozumném čase najít x tak, aby h(x)=h(y)
- Pro dané y lze v rozumném čase najít x tak, aby h(x)=y

Co je to hašovací funkce?

- Funkce, která mapuje libovolně velký vstup na výstup s délkou 128, 192, 256 nebo 512 bitů
- Funkce, která mapuje libovolně velký vstup na výstup fixní délky a není prostá
- Funkce, která mapuje libovolně velký vstup na výstup fixní délky a je prostá
- Funkce, která mapuje vstup fixní délky na výstup variabilní délky (podle entropie vstupu)
- Šifrovací funkce se schopností deprese vstupních dat

Protokoly výzva-odpověď mohou být založeny na:

- klíčované hašovací funkci
- symetrickém šifrování
- digitálním podpisu
- MAC kódu, resp. funkci

Co znamená pojem elektronický podpis ve smyslu zákona o elektronickém podpisu?

- Takový pojem zákon neobsahuje
- To stejné, co digitální podpis
- Ručně psaný podpis
- Libovolná identifikující informace připojená ke zprávě

Téma #2: Autentizace uživatelů tajnými informacemi

Pro autentizaci obrazovou informací platí

- Uživatel musí správně vybarvit předložený obrázek
- Uživatel musí do systému nahrát správný obrázek
- Uživatel musí systému slovně popsat obrázek sloužící k autentizaci
- Uživatel musí vybrat správný obrázek nebo jeho část

"Solení" hesel

- Pomůže vyřešit situaci, kdy mají uživatelé stejná hesla
- Zajistí delší efektivní heslo
- Je dodatečná technika při ukládání hesel pro určitou formu identifikace
- Je dnes již jen velmi zřídka používaná technika

Pokud ukládáme hesla šifrovaně

- Musíme věřit administrátorovi
- Musíme znát (jako uživatelé) šifrovací klíč
- Nesmí být použit šifrovací algoritmus DSA
- Šifrovací klíč musí být přístupný autentizační službě

Jak eliminujeme útoky hrubou silou na PINy?:

- Pravidelnou změnou hodnoty PINu
- Omezením počtu pokusů o zadání PINu
- školením uživatelů

U autentizace pomocí hesel

- Musíme řešit aspekt zapamatovatelnosti vs. bezpečnosti
- Musíme řešit aspekt bezpečnosti bez ohledu na zapamatovatelnost
- Musí uživatel prokázat, že si dokáže zapamatovat alespoň 10 náhodně zvolených symbolů

Jaké jsou nevýhody autentizace hašovaným heslem?

- Příliš snadná transformace na zero-knowledge protokoly (protokoly s nulovým rozšířením znalostí)
- Útok přehráním
- Možnost impersonace
- Náchylnost ke slovníkovému útoku

PIN je

- Osobně sdílená informace
- Kombinace čísel a písmen (A-F) pro potřeby autentizace
- Veřejně známá informace
- Kombinace čísel pro potřeby autentizace

Úspěšnost útoku hrubou silou se dá odhadnout podle vzorce

- (velikost abecedy * délka hesla)/(počet odhadů za jednotku času)^(čas platnosti)
- (čas platnosti * počet odhadů za jednotku času)/(velikost abecedy)^(délka hesla)
- (délka hesla * počet odhadů za jednotku času)/(velikost abecedy)^(čas platnosti)
- (počet odhadů za jednotku času * délka hesla)/(čas platnosti)^(velikost abecedy)

Jaká technologie PINmailerů je bezpečnější při útocích prosvícením?

- Laserový tisk
- Průklepový tisk

Při hašování hesel pro autentizaci uživatelů pomocí hesel:

- Ukládáme pouze haš hesla a rekonstrukce otevřené podoby není možná
- Ukládáme pouze haš hesla s možností rekonstrukce hesla v otevřené podobě
- Při ukládání můžeme využít techniky "solení"

Útok na hesla může být

- Slovníkový
- Pomocí sociálního inženýrství
- Matrixovou metodou
- Hrubou silou
- Na základě určitých znalostí o uživateli

Vhodná tajná informace pro autentizaci je

- Rodné příjmení matky
- Tel. číslo, pokud není uvedeno ve Zlatých stránkách
- Heslo
- PIN
- Fráze (passphrase)

Přístupová hesla můžeme rozlišit na

- Jednorázová
- Veřejná
- Původně neveřejná
- Skupinová
- Unikátní pro danou osobu
- Jednocestná

Co je to heslo založené na frázi?

- Heslo, které obsahuje pouze malá písmena
- Heslo založené na veřejně známé frázi, aby si jej všichni snadno zapamatovali
- Heslo, které lze jednoduše přečíst
- Pomůcka pro zapamatování složitého hesla

Ukládání hesel lze realizovat

- Hašovaně
- Impulzně
- V otevřené podobě
- Šifrovaně
- Hlasovaně

Při autentizaci tajnou informací je nutné dodržet

- Tajnou informaci musí vědět jen oprávněný uživatel
- Tajnou informaci musíme sdělit administrátorovi pro případně admin. zásahy v našem systému
- Z tajné informace se musí nejprve vytvořit inicializační vektor
- Prostor, ze kterého vybíráme hodnotu tajné informace musí být rozsáhlý

Z hlediska lidské paměti je vhodné volit

- Složitá, ale snadno zapamatovatelná hesla
- Jednoduchá a jednoduše zapamatovatelná hesla
- Obtížně zapamatovatelná hesla a každý měsíc nutit uživatele ke změně
- Hesla založená na frázích

Co je vyžadováno pro autentizaci transakce při offline verifikaci se šifrováním PINu?

- Originální PIN nutný pro verifikaci, který musí být bezpečně uložen v čipu
- Fyzicky i prostředím dobře zabezpečený PINpad
- Úspěšné proběhnutí automatické správy rizik
- Nový RSA pár klíčů pro šifrování PINů

Soubor /etc/passwd může obsahovat

- Datum a čas posledního úspěšného přihlášení do systému
- Počet zbývajících neúspěšných pokusů o zadání hesla
- Haše hesel uživatelů
- Informaci o délce hesla
- Informaci o tom, že haše hesel jsou v souboru /etc/shadow

Soubor /etc/shadow obsahuje

- Informaci o délce hesla
- Datum a čas posledního úspěšného přihlášení do systému
- Počet neúspěšných pokusů o zadání hesla
- Haše hesel uživatelů
- Informaci o tom, že haše hesel jsou v souboru /etc/passwd

Téma #3: Autentizace uživatelů tokeny

Jaká je správná sekvence operací při ověřování PINu odolná proti přerušení napájení?

- Zvýšení čítače, test čítače pokusů větší než 0, ověření korektnosti PINu, zvýšení čítače při dobrém PINu.
- Test čítače pokusů větší než 0, snížení čítače, ověření korektnosti PINu, zvýšení čítače při dobrém PINu.
- Test čítače pokusů větší než 0, zvýšení čítače, ověření korektnosti PINu, zvýšení čítače při dobrém PINu.
- Test čítače pokusů větší než 0, ověření korektnosti PINu, snížení čítače při špatném PINu.

Pro urychlení počítačových systémů využívajících digitální podpis

- u čipových karet bývají použity kryptografické koprocesory
- používají obě strany identický privátní klíč
- se často používá podchlazování ochranných komponent čipových karet
- obvykle využíváme hašovací funkce pro reprezentaci podepisovaných dat
- lze využít prokazatelnou odpovědnost metodou Monte Carlo

Jaký typ pamětí je typicky používán u současných čipových karet?

- DRAM
- SRAM
- GRAM
- EEPROM

Útok na čipové karty pomocí časové analýzy využívá:

- Délka operace v závislosti na vykonané větvi kódu.
- Délka operace v závislosti na zpracovávaných datech.
- Závislost průběhu odběru proudu na prováděné instrukci.
- Závislost průběhu odběru proudu na zpracovávaných datech.

Jaká technologie přihlašování do systému e-bankovnictví (a autorizace transakcí) je nejbezpečnější (z nabízených možností)?

- Použití autentizačního kalkulátoru s PINem
- Použití hesla zadaného částečně na klávesnici a částečně na virtuální klávesnici
- Použití šifrované autentizační SMS (tj. s využitím SIM Toolkitu)
- Použití klientského certifikátu, který je uložen na čipové kartě s přístupem chráněným PINem

Která z uvedených tvrzení o uživatelově PINu jsou pravdivá (při standardním nastavení karty)?

- Při změně nezablokovaného PINu je třeba zadat starý i nový uživatelský PIN.
- Při změně nezablokovaného PINu stačí zadat nový uživatelský PIN.
- Při změně zablokovaného PINu je třeba zadat starý i nový uživatelský PIN.
- Při změně zablokovaného PINu je třeba zadat odblokovací PIN a nový uživatelský PIN.

Detekcí narušení se u čipových karet myslí:

- Po narušení jsou stopy narušení obtížně odstranitelné.
- Odolnost proti pokusům o zjištění robustnosti vůči fyzickým útokům.
- Vlastnost části systému umožňující detekovat fyzický útok.
- Při zjištění narušení je automaticky provedena chráněnou části obranná akce.

Odpovědí na narušení se u čipových karet myslí:

- Automatická akce provedená chráněnou částí při detekci pokusu o narušení.
- Po úspěšném provedení narušení jsou stopy narušení odstraněny.
- Vlastnost části systému umožňující detekovat fyzický útok.
- Akce provedená bezpečnostním administrátorem po zjištění pokusu o narušení.

Které z uvedených kategorií čipových karet podle technologie komunikace rozlišujeme?

- Hybridní karty.
- Bezkontaktní karty.
- Kontaktní karty.
- Polymorfní karty.

Které z uvedených kategorií čipových karet podle technologie uchování a práce s daty rozlišujeme?

- Paměťové karty se speciální logikou.
- Karty s magnetickým proužkem.
- Paměťové karty.
- Procesorové karty.

Jaké jsou možnosti prevence padělání tokenů?

- Modifikace dostupného vybavení (modifikace vybraných barev u kopírky, vkládání identifikátoru).
- Utajení všech informací nutných ke konstrukci tokenu.
- Utajení některých informací nutných ke konstrukci tokenu.
- Čestné prohlášení všech uživatelů systému.
- Kontrola a licence souvisejících živností.
- Omezení dostupnosti potřebného vybavení.

Které z uvedených útoků na čipové karty nepatří mezi fyzické útoky?

- Preparace čipu
- Odběrová analýza
- Ozařování čipu
- Časová analýza

Jaké typy záznamů lze používat na čipové kartě?

- Nestrukturovaná data.
- Exponenciální záznam s pevnou délkou.
- Lineární záznamy s pevnou nebo variabilní délkou.
- Cyklické záznamy.

Jaké jsou obecné nevýhody tokenů?

- Cena tokenů je příliš vysoká pro komerční využití.
- Bez tokenu není autorizovaný uživatel rozpoznán.
- Ztráta tokenu vede většinou ke kompromitaci celého systému.
- Ke kontrole je obvykle třeba speciální čtečka nebo vycvičená osoba.

Jaké jsou obecné výhody tokenů?

- Rychlé zjištění ztráty.
- Mohou zpracovávat a přenášet další informace.
- Nikdy je nelze zneužít po náhodném nálezu.
- Většinou nejsou jednoduše kopírovatelné.

Co je to semi-invazivní časová analýza?

- Druh semi-invazivního útoku zneužívající u mnohých čipových karet možnost ovlivnění vstupního hodinového cyklu.
- Speciální semi-invazivní útok na autentizační kalkulátor s hodinami.
- Žádná z výše uvedených odpovědí.
- Metrika sloužící k určení a vyhodnocení efektivnosti semi-invazivních útoků.

Útok na čipové karty pomocí indukce chyb je založen na:

- Využití chybného běhu algoritmu po prudkém ovlivnění vnějších podmínek k získání tajných dat.
- Využití indukce chyb po prudkém ovlivnění vnějších podmínek k testování změny chování algoritmu.
- Jako první krok útoku je provedeno fyzického poškození.
- Využití opravných kódů pro automatické odstranění chyby po prudkém ovlivnění vnějších podmínek.

Co patří mezi bezpečnostní problémy používání bankovních karet s čipem?

- Možnost odpozorování PINu na frekventovaných místech.
- Špatná průkaznost nelegitimní autorizace platby pomocí PINu.
- Velká obtížnost kopírování karty.
- Výpočetní výkon nepostačuje pro kryptografické zabezpečení transakcí.

Jaké jsou typické velikosti pamětí u současných čipových karet?

- < 100KB RAM, < 100KB ROM, > 1MB EEPROM
- > 256KB RAM, ~100KB ROM, < 100KB EEPROM
- ~128KB RAM, ~512KB ROM, ~512KB EEPROM
- < 10KB RAM, ~100KB ROM, < 100KB EEPROM

Která z uvedených tvrzení o autentizačních kalkulátorech jsou pravdivá?

- Přístup k využití kalkulátoru může být chráněn PINem.
- Pracují na principu protokolu výzva/odpověď s využitím tajné informace.
- Kalkulátor nelze zneužít i při znalosti PINu.
- Výzva je zadávána manuálně nebo automaticky načtena z vhodného média.

Odolností vůči narušení se u čipových karet myslí:

- Automatická akce provedená chráněnou částí při zjištění pokusu o narušení.
- Vlastnost části systému umožňující detekovat fyzický útok.
- Vlastnost části systému chráněné proti neautorizované modifikaci podstatně lépe než zbylá část systému.
- Ochrana proti útoku rušením radiového signálu (RFID).

Proč je u tokenů založených na hodinách potřeba řešit otázku posuvu hodin?

- Pravým důvodem je přechod na letní/zimní čas a přestupné roky.
- Žádná z výše uvedených odpovědí.
- Nutnost synchronizace drobných odchylek mezi serverem a tokenem.

Které z uvedených útoků na čipové karty nepatří mezi logické útoky?

- Časová analýza
- Útok přes aplikační rozhraní
- Ozařování čipu
- Preparace čipu

Útok na čipové karty pomocí odběrové analýzy využívá:

- Závislost průběhu odběru proudu na ukládaných datech do paměti EEPROM.
- Data získaná odběrem vzorku paměti EEPROM.
- Závislost průběhu odběru proudu na zpracovávaných datech.
- Závislost průběhu odběru proudu na prováděné instrukci.

Která z uvedených tvrzení o tokenech založených na hodinách jsou pravdivá:

- Token s hodinami nelze použít bez přítomnosti klávesnice.
- Autentizační hodnota je vygenerována na základě aktuálního času a tajné informace.
- Přístup k využití tokenu s hodinami musí být vždy chráněn PINem.
- Je potřeba řešit otázku synchronizace hodin mezi serverem a tokenem.

Mezi obecné výhody tokenů nepatří:

- Obtížná kopírovatelnost.
- Snadné zjištění ztráty.
- Snadná detekce a odpověď na narušení.
- Možnost zpracovávání informací.

Které z uvedených typů karet se používají v IT bezpečnosti?

- Kontaktní karty s čipem.
- Karty s bezkontaktním magnetickým proužkem.
- Bezkontaktní karty s čipem.
- SIM karty v mobilních telefonech.

Zjistitelností narušení se u čipových karet myslí:

- Po narušení jsou stopy narušení obtížně odstranitelné.
- Při zjištění narušení je automaticky provedena chráněnou částí obranná akce.
- Odolnost proti pokusům o zjištění robustnosti vůči fyzickým útokům.
- Vlastnost části systému umožňující reagovat na fyzický útok.

Jaký je vztah mezi chybovou analýzou a útoky na a přes API?

- Chybová analýza s útoky na a přes API nijak nesouvisí.
- API mnohdy obsahuje četné chyby hodné důkladné analýzy.
- Chybová analýza je nezbytná součást každého útoku na a přes API.
- Každý útok na a přes API je nezbytnou součástí chybové analýzy.

Co patří mezi bezpečnostní problémy používání bankovních karet pouze s magnetickým proužkem?

- Autentizační podpis je součástí karty.
- Malá odolnost proti chybové analýze.
- Relativně jednoduše se kopírují.
- Přítomný hologram se obtížně automatizovaně kontroluje.

Které z uvedených odpovědí jsou pravdivé?

- Cena výroby jednoho kusu tokenu klesá při výrobě mnohakusové série.
- Cena padělání typicky nezávisí na počtu padělaných kusů.
- Cena padělání jednoho kusu klesá při uplatnitelnosti mnohakusové série padělku.
- Relativní cena padělání se zvyšuje s každým dalším padělkem.

Současné čipové karty:

- Umožňují pouze provádění kryptografických operací asymetrické kryptografie.
- Neumožňují provádění kryptografických operací.
- Umožňují provádění kryptografických operací symetrické a asymetrické kryptografie s využitím koprocesoru.
- Umožňují pouze provádění kryptografických operací symetrické kryptografie.

Fyzickou bezpečností se u čipových karet myslí:

- Ochrana proti hloubkové odběrové analýze na úrovni procesoru.
- Ochrana proti fyzickému zkoušení PINu hrubou silou.
- Fyzická překážka kolem čipu karty ztěžující neautorizovaný přístup.
- Odolnost proti útokům vyžadujícím fyzický přístup ke kartě.

Útok na čipové karty přes aplikační rozhraní (API) je založen na:

- Využití chyby v návrhu rozhraní.
- Nezamýšleném dopadu zpracování útočníkem zaslaných specifických vstupních dat.
- Nedostupnosti aplikačního rozhraní vnitřnímu prostředí karty.
- Využití indukce chyb do zpracování dat zaslaných přes aplikační rozhraní.

Která z uvedených tvrzení o řízení přístupu k datům na čipových kartách jsou pravdivá?

- Data jsou uchována na magnetickém proužku a před použitím v čipu kontrolována.
- Každý soubor má přiřazenu hlavičku s přístupovými právy.
- Data na kartě nemohou být po zápisu nikdy čtena ani měněna.
- Založeno především na řízení přístupu k souborům.

Co je to odpověď na narušení?

- Žádná z výše uvedených odpovědí.
- Služba internetového bankovnictví umožňující automaticky detekovat a upozornit na aktivní nebezpečný software v počítači.
- Reakce nechráněné části systému na potencionální útok.
- Reakce chráněné části systému na probíhající pokus o útok.

Jaké vlastnosti mají magneto-optické čipové karty?

- Umožňují snímání čárových kódů zobrazovaných na monitoru při vstupu do internetového bankovnictví a jejich okamžité zpracování v čipu.
- Žádná z výše uvedených odpovědí.
- Poskytují magneto-optické rozhraní pro vysokorychlostní a prokazatelně bezpečný přenos dat.
- Neumožňují provádění kryptografických operací i přesto, že obsahují sofistikovanější magneto-optický proužek. Každá z dvou komunikujících stran má svůj symetrický klíč.

Které z uvedených typů autentizačních kalkulátorů se používají v IT bezpečnosti?

- Kalkulátor s hodinami.
- Kalkulátor s tajnou informací.
- Kalkulátor bez vstupní klávesnice.
- Kalkulátor s vestavěným budíkem (z angl. embedded alarm).

Téma #4: Biometrické autentizační metody

Komerční biometrická řešení oproti forenzním nabízí

- plně automatizované systémy.
- možnost opakovaného vytvoření nedostatečně kvalitních registračních vzorků.
- vyšší přesnost.
- uchování zpracovaných charakteristik včetně biometrických vzorků.

Biometriky jsou

- automatizované metody identifikace nebo ověření identity.
- založeny na opakovatelně měřitelných fyziologických nebo behaviorálních vlastnostech člověka.
- založeny na neopakovatelně měřitelných fyziologických nebo behaviorálních vlastnostech člověka.
- i metody identifikace pomocí čipové karty obsahující vzorky člověka.

Snímače otisků prstů jsou

- inkoustové (tryskové)
- kapacitní
- polyadické
- optické

Praktické problémy biometrik jsou

- uživatelé s poškozenými či chybějícími orgány.
- legislativa a správa charakteristik.
- nízké FRR (nespokojení uživatelé z důvodu častého odmítnutí).
- nízké FAR (aplikace s nízkou úrovní bezpečnosti).

Běžné komerční biometrické zařízení

- je vybaveno detekcí průniku nebo má zvýšenou odolnost proti průniku.
- typicky dobře šifruje přenášená data pomocí kvalitních algoritmů.
- se neautentizuje vůči dalším komunikujícím.

Který z výroků o autentizaci na základě dynamiky psaní na klávesnici je pravdivý?

- Měří se čas stlačení klávesy a čas mezi stisky kláves.
- Uživatele je možno autentizovat kontinuálně.
- K autentizaci stačí běžná klávesnice.
- Algoritmy pracují na principu srovnávání vzorů (pattern matching) nebo neuronových sítí (neural networks).

Biometrické charakteristiky se dělí na

- geotypické
- genotypické
- biomatické
- fenotypické

Oční duhovka je snímána pomocí

- ultrafialového paprsku.
- černobílé kamery.
- kvalitní barevné kamery.
- laserového paprsku s třídou bezpečnosti 1.

Mezi chyby biometrických systémů patří

- ARR (Acceptance Rejection Rate)
- EDR (Error Disqualification Rate)
- FAR (False Acceptance Rate)
- FRR (False Rejection Rate)

Které biometrické charakteristiky bývají nazývány také dynamickými?

- fyziologické
- genotypické
- behaviorální
- fenotypické

Biometrické technologie mohou být založeny na některém z těchto typů charakteristik:

- fyziologický
- morální
- environmentální
- behaviorální
- chemoterapický

Proces použití biometrik pro autentizaci zahrnuje

- registraci
- verifikaci
- degustaci
- demonstraci

Jaké jsou hlavní výhody biometrik

- rychlé a (relativně) přesné výsledky.
- nemůžeme je ztratit, zapomenout nebo předat jiné osobě.
- jsou tajné.
- jednoduchá správa vzorků.

Na co není výhodné použít biometriky

- na autentizaci dat.
- na ochranu přístupu k tajnému klíči.
- na doplňkovou formu autentizace.

Forenzní řešení biometrik popisují tyto výroky

- výsledek identifikace je získán obvykle za 1s či rychleji.
- miniaturizace zařízení je jedním z hlavním cílů.
- pro používání je nutná odborná znalost systému.
- cena je vysoká, ale s tím se počítá.

Biometrická data při opakovaném měření kvalitním zařízením

- jsou vždy shodná na 99 % a víc.
- nejsou nikdy shodná na 100 %.
- nejsou nikdy shodná na 100 % až na otisky prstů.
- jsou typicky shodná na 100 %.

Autentizace pomocí verifikace hlasu probíhá typicky

- pomocí běžného mikrofonu.
- pomocí soustavy mikrofonů rozmístěných ve vzdálenosti cca 0,5 m ve 4 směrech.
- v samostatné odhlučněné komoře, pro odstranění okolního šumu.
- využitím telefonu.

Které z výroků o autentizaci na základě rozpoznání obličeje nejsou pravdivé?

- Autentizaci komplikuje osvětlení a pozadí.
- Přesnost se v posledních 5 letech příliš nezlepšila.
- Jedná se o velice výpočetně náročnou metodu autentizace.
- Autentizaci komplikuje změna účesu, náušnice a brýle.

U dynamiky podpisu je důležitý

- aretačně-dynamický tablet.
- čas potřebný pro provedení podpisu.
- pořadí jednotlivých tahů pera.
- výsledný podpis.

Základní fakta o biometrických systémech jsou:

- kopírování biometrik nemusí být triviální, ale není obtížné.
- biometrická data mohou být velmi citlivé informace.
- biometrická data jsou tajná.

Které biometrické charakteristiky bývají nazývány také statickými?

- fenotypické
- behaviorální
- fyziologické
- genotypické

Mezi nejslibnější technologie v oblasti identifikace v počítačových systémech pomocí biometrik nepatří

- otisk prstu.
- tvar ruky.
- ověření mluvčího.
- snímání oční duhovky.
- DNA.

Markanta v oblasti biometrik znamená:

- Významný bod v otisku prstu.
- Výrazné poškození dané biometriky u konkrétního uživatele.
- Zpracovaný obraz oční duhovky se zvýrazněnými přechody.
- Biometrická technologie s významně vysokou hodnotou EER.

Která z následujících tvrzení snímání geometrie ruky jsou pravdivá?

- Snímače snímají 2D snímky ruky shora, zespodu a ze stran (dohromady 4 snímky, u špičkových zařízení i 5-6).
- Snímače snímají 2D snímky ruky mikrokamerami ve fixačních kolících.
- Snímače snímají zjednodušený 3D náhled ruky.
- Tvar ruky je jedinečný (ve skupinách o tisících uživatelů).
- Tvar ruky není jedinečný (ve skupinách o tisících uživatelů).

Proč musíme povolit určitou variabilitu mezi registračním vzorkem a později získanými biometrickými daty?

- Z důvodu možné transplantace orgánu, aby i po ní bylo snímání možné.
- Protože buňky mají přirozenou tendenci obnovovat se a tudíž mohou vznikat malé odlišnosti.
- Protože biometrická data nejsou nikdy 100 % shodná.
- Pokud je registrační vzorek nasnímám opravdu kvalitně, tak variabilita nemusí být povolena.

Chybovost biometrických systémů závisí na:

- Schopnosti a motivaci uživatelů.
- Nastavení systému.
- Typu snímače.
- Okolním prostředí.

Mezi reálně používané biometrické technologie patří

- dynamika pohybu hlavy
- otisk prstu
- srovnání obličeje
- geometrie (tvaru) nohy
- vzor oční panenky

Mezi základní nedostatky při snímání obličeje nepatří

- nasazené kontaktní čočky.
- pestré a barevné pozadí.
- nasazená čepice.
- zavřené oči.

Testování živosti obvykle nemá následující dopady

- nepříjemné pocity brnění v oblasti testovaného vzorku.
- zvýšený počet nesprávných odmítnutí.
- zvýšení ceny zařízení.
- vyšší náklady na vývoj a výrobu.

Téma #5: idk

Tato přednáška byla krátká a divná, nevím co k tomu zařadit tak aby odpovědi na to se daly najít v tom tématu. Přišlo mi že tam moc věcí na zkoušku ani nebylo.

Téma #6: Autentizační protokoly

V tiketu používaném v systému Kerberos se objevuje:

- Identifikátor alespoň jedné ze stran
- Soukromý klíč
- Náhodná výzva
- Časové razítko

Protokol Kerberos zajišťuje

- Autentizaci
- Aprobaci
- Autokracii
- Akumulaci

Čeho lze dosáhnout zopakováním zero-knowledge protokolu (protokol s nulovým rozšíření znalostí)?

- Zvýšení bezpečnosti - zvýší se záruka, že nedojde k rozšíření žádných znalostí
- Zvýšení bezpečnosti - sníží se pravděpodobnost, že nepoctivý útočník se může úspěšně vydávat za jinou stranu
- Ničeho - ke spolehlivé autentizaci stačí 1 kolo protokolu
- Ničeho - nezvýší se záruka, že nedojde k rozšíření žádných znalostí

Které časově proměnné parametry se používají v kryptografických protokolech?

- Monoliticky rostoucí sekvence
- Náhodná komplexní čísla
- Náhodné sekvence
- Náhodná časová razítka
- Náhodná čísla
- Časová razítka

Která z následujících tvrzení jsou platná pro protokol SSL/TLS?

- Implicitně je autentizace serveru i klienta vypnuta.
- SSL/TLS protokol neprovádí elektronické podepisování dat.
- Implicitně je autentizace serveru a klienta povinná.
- Implicitně je autentizace serveru povinná, autentizace klienta je volitelná.

Které z uvedených režimů nepodporuje IPsec:

- Transportní režim.
- Dynamický virtuální režim.
- Tunelovací režim.
- Překladový režim.

Na jakém druhu kryptografie je založena základní verze Kerbera?

- Hybridní
- Symetrická
- Asymetrická

Aktualizace klíče se vzájemnou autentizací protokolem AKEP2 (Authenticated Key Exchange Protocol 2)je založena na:

- Generátorech passcode
- Algoritmu MAC (Message Authentication Code)
- Digitálních podpisech
- Bez klíčových kryptografických hašovacích funkcích

Které protokoly umožňují vytvoření sdíleného tajemství?

- Protokoly pro ustavení klíče
- Protokoly implementované v Kerberu
- Zero-knowledge protokoly (protokoly s nulovým rozšířením znalostí)
- Silné autentizační protokoly

Jaký mechanismus je použit pro zajištění bezpečnosti v autentizační hlavičce IPsec?

- Message Authentication Code se sekvenčním číslem.
- Diffie-Hellman autentizace bez klíčů.
- Message Authentication Code s náhodným číslem.
- Digitální podpis využívající RSA nebo DSA.

Na jaké vrstvě funguje protokol SSL/TLS?

- mez aplikační a datovou vrstvou
- na linkové vrstvě
- na síťové vrstvě
- na datové vrstvě

Která z následujících tvrzení jsou platná pro protokol SSL/TLS? !!!

- Autentizace komunikujících stran je založena na symetrické kryptografii.
- Po průběhu Handshake protokolu je komunikace šifrována symetrickým klíčem.
- SSL/TLS protokol zajišťuje integritu a autenticitu dat.
- Po úvodní Handshake protokolu je komunikace šifrována veřejným klíčem příjemce.

Které z protokolů se v současnosti v běžných aplikacích využívají více?

- Challenge-response protokoly (protokoly výzva-odpověď)
- Zero-knowledge protokoly (protokoly s nulovým rozšířením znalostí)

Zero-knowledge protokoly (protokoly s nulovým rozšířením znalostí) umožňují, poctivým stranám vždy dosáhnout úspěšného výsledku. Tato vlastnost se nazývá:

- Částečné uspokojení (partial satisfaction)
- Úplnost (completeness)
- Korektnost (soundness)
- Úplné uspokojení (complete satisfaction)

Které z uvedených možností nezajišťuje protokol IPsec?

- Ochranu proti analýze šifrovaného provozu na síťové vrstvě.
- Integrita a autentizace původu dat.
- Nepopiratelnost přijetí dat.
- Důvěrnost dat, ochrana proti přehrání.

Pravděpodobnost, že se nepoctivý útočník může úspěšně vydávat za jinou stranu je u zero-knowledge protokolů (protokoly s nulovým rozšířením znalostí) mizivá. Tato vlastnost se nazývá:

- Částečné uspokojení (partial satisfaction)
- Korektnost (soundness)
- Úplné uspokojení (complete satisfaction)
- Úplnost (completeness)

Které z níže uvedených typů protokolů existují?

- Autentizační protokoly bez ustavení klíče
- Zero-knowledge protokoly (protokoly s nulovým rozšířením znalostí) pro ustavení klíče.
- Autentizované protokoly pro ustavení klíče
- Protokoly pro ustavení klíče
- Neautentizované protokoly pro ustavení klíče

Která z následujících tvrzení jsou platná pro protokol SSL/TLS? !!!

- SSL/TLS protokol nezajišťuje důvěrnost dat.
- Implicitně je autentizace serveru a klienta je povinná.
- Autentizace komunikujících stran je založena na asymetrické kryptografii.
- SSL/TLS protokol umožňuje vzájemnou autentizaci serveru a klienta.

Které z uvedených režimů podporuje IPsec:

- Překladový režim.
- Transportní režim.
- Tunelovací režim.
- Dynamický virtuální režim.

Který z následujících protokolů je součásti SSL/TLS protokolu?

- Kerberos protokol.
- Record Layer protokol.
- IPSec protokol.
- Handshake protokol.

Které protokoly zaručují určitou míru jistoty o identitě jiné strany?

- Protokoly pro ustavení klíče
- Autentizační protokoly
- Zero-knowledge protokoly (protokoly s nulovým rozšířením znalostí)
- Protokoly implementované v Kerberu

Které časově konstantní parametry se používají v kryptografických protokolech?

- Žádné z uvedených
- V omezeném čase monoliticky rostoucí sekvence (zabraňují tzv. borcení časové osy)
- XOR hodnotou "-1" pro modifikaci náhodné výzvy (tzv. keksík)
- Komplexní čísla s fixní imaginární i reálnou složkou
- Sekvenční číslo (jeho hodnota závisí na implementaci)
- Náhodná časová razítka (platná po určitou dobu - typicky několik desítek hodin)

Která z uvedených tvrzení pro Encapsulated Security Payload (ESP) nejsou pravdivá?

- ESP nemá zajištěnu integritu a autenticitu dat, zajišťuje pouze důvěrnost dat.
- ESP zajišťuje integritu, autenticitu a důvěrnost dat.
- ESP zajišťuje obranu proti analýze šifrovaného provozu na úrovni síťové vrstvy.
- ESP zajišťuje integritu, autenticitu a důvěrnost dat, nezajišťuje však obranu proti útoku přehráním.

Protokoly výzva-odpověď mohou být založeny na:

- klíčované hašovací funkci
- symetrickém šifrování
- digitálním podpisu
- MAC kódu, resp. funkci

Jaké vlastnosti má Shamirův protokol bez klíčů (Shamir's no-key protocol)

- Nevyžaduje žádné ustavení sdílených klíčů
- Vyžaduje komutativní šifrovací algoritmus
- Funguje obzvláště dobře (a prokazatelně bezpečně) jen při použití One-Time Pad
- Prokazuje, že P!=NP
- Umožňuje vzájemnou autentizaci

Kolik zpráv se vymění ve Shamirově protokolu bez klíčů, aby obě strany sdílely stejný klíč?

- 2
- 4
- 3
- žádná z těchto odpovědi není správná

Které z uvedených možností zajišťuje protokol IPsec?

- Nepopiratelnost přijetí dat.
- Důvěrnost dat, ochrana proti útoku přehráním.
- Autentizace a integrita původu dat.
- Podporu správy klíčů.

Co zajišťujeme použitím náhodných čísel?

- Odolnost proti uváznutí a stárnutí
- Aktuálnost
- Nezvratnost
- Stálost a stabilitu
- Čerstvost
- Jedinečnost

Téma #7: Autentizace počítače

K čemu slouží autentizační agent u ssh?

- K autentizaci dat přenášených mezi serverem a uživatelem.
- Opakované požadavky vyžadující heslo řeší agent po prvním zadání automaticky.
- Automaticky autentizuje server vůči uživateli bez nutnosti zadávat opakovaně heslo.
- Autentizační agent se u ssh nepoužívá, neboť je použita asymetrická kryptografie.

Která z uvedených tvrzení jsou pravdivá:

- Autentizace pomocí IP adresy může být použita pouze v kombinaci s MAC adresou.
- Autentizace pomocí IP adresy je výrazně bezpečnější než autentizace pomocí MAC adresy.
- Autentizace pomocí IP adresy je výrazně méně bezpečná než autentizace pomocí MAC adresy.
- Autentizace pomocí IP adresy není spolehlivá, protože IP může být změněna.

IP spoofing označuje:

- Podvržení IP adresy příjemce.
- Zachycení IP adresy odesílatele i příjemce.
- Zachycení IP odesílatele.
- Podvržení IP adresy odesílatele.

Co nezajišťuje protokol ssh?

- Autentizaci uživatele.
- Ochranu proti analýze provozu.
- Ochranu proti distribuovanému odmítnutí služby.
- Autentizaci serveru.

Které z uvedených možností autentizace klienta vůči serveru podporuje protokol ssh?

- RSA autentizaci klienta.
- Využitím protokolu pro nulové rozšíření znalosti.
- Stroje uvedené v souborech .rhosts nebo hosts.equiv.
- Heslem uživatele bez autentizace serveru.

Proti jakým útokům brání protokol ssh?

- Odposlech hesla a pozdější přehrání (na uživatelově PC)
- Analýza šifrovaného provozu na síťové vrstvě
- Odposlech hesla a pozdější přehrání (na síťové vrstvě)
- DNS/IP/Routing spoofing

Chybové hlášení o změně integritního součtu veřejného klíče serveru u SSH může být způsobeno

- Změnou dlouhodobého klíče serveru jeho administrátorem
- Chybějícím záznamem veřejného klíče v souboru známých serverů
- Podvržením serveru útočníkovým strojem
? Změnou souboru s veřejným klíčem serveru na uživatelově PC

K čemu slouží soubor .rhosts?

- K nastavení adres počítačů s povoleným přihlášením bez další autentizace .
- Uchování informací o adresách autentizovaných počítačů připojených k serveru.
- K uchování uživatelů s právem číst (read).
- K uchování RSA klíče(ů) serveru.

Které z uvedených možností jsou proveditelnými útoky při provedení autentizace prostřednictvím .rhosts

- Vrácení podvržené IP adresy po dotazu na DNS server.
- Útok hrubou silou.
- Uvedení nepředpokládaného loginu uživatele.
- IP spoofing.

Jaký je u ssh rozdíl mezi Server key a Host key?

- Server key je krátkodobý klíč použitý pro odvození Host key.
- Host key je dlouhodobý klíč.
- Server key je krátkodobý klíč použitý pro vlastní autentizaci serveru.
- Host key je krátkodobý klíč použitý pro vlastní autentizaci serveru.

Nezařazené, možná sem patří, možná ne a bude se to brát až později

Autentizace dat znamená

- Totéž co integrita
- Potvrzení, že data nebyla neautorizovaně změněna od doby vytvoření
- Potvrzení, že data pochází od určitého subjektu
- Data nemohl odeslat nikdo jiný než jejich původce

Jaké bezpečnostní problémy lze identifikovat v soudobém bankovnictví?

- Použití pouze asymetrické kryptografie v kombinaci s hašovacími funkcemi (pouze pro podpisy)
- Dodatečné autorizační SMS zprávy jen u některých operací e-bankovnictví
- Nedostatečné zabezpečení platebních terminálů
- Použití autentizačních kalkulátorů
- Social engineering např. při telefonním hovoru
- Zasílání embosované karty poštou a nedostatečně zabezpečené doručování PINu a hesla

Autentizace v soudobých systémech e-bankovnictví je výhradně

- Třífaktorová
- Žádná z dalších odpovědí není správně
- Dvoufaktorová
- Jednofaktorová

Co nepatří mezi mechanizmy zabraňující jednodušším útokům na e-bankovnictví s autentizací pouze na základě hesla?

- Anonymizovaný login
- testy délky a kvality hesla
- Virtuální klávesnice pro zadávání hesla
- SSH certifikáty
- Personalizovaný login
- SSL certifikáty

Úspěšné odposlechnutí citlivých dat ze sběrnice platebního terminálu může vést:

- K přečtení citlivých informací banky (sdílené tajné klíče uložené v terminálu)
- K modifikaci nepodepsaného seznamu podporovaných verifikačních metod (CVM)
- K získání přesné kopie dat na magnetickém proužku
- K získání PINu
- K narušení anonymity jednotlivých komunikujících stran
- K modifikaci podepsaného seznamu podporovaných verifikačních metod (CVM)

Generátory passcode slouží pro

- Urychlení generování sekvenčních čísel
- Bezpečné uložení dlouhodobých klíčů
- Realizaci challenge-response (výzva-odpověď) protokolu
- Personalizaci elektronických pasů

Pro statickou autentizaci dat (SDA) platí, že:

- Potvrzuje pravost pouze statických dat uložených v čipové kartě.
- Je prováděna pouze platebním terminálem (čip pouze zasílá data)
- Řeší problém padělání/duplikace karet
- Potvrzuje pravost statických dat uložených v čipové kartě, ale i dynamických dat zaslaných terminálem

- Je prováděna pouze čipovou kartou (terminál pouze zasílá data)
- Potvrzuje pravost statických uložených v čipové kartě, ale i dynamických dat zaslaných čipem

Co je to Chaffing and winnowing

- Pro každý bit zprávy vytvoříme dvě zprávy (správný, chybný MAC), příjemce si ponechá zprávu se správným MAC
- Zprávu rozdělíme na jednotlivé bity a ty šifrujeme z využitím MAC každý zvlášť
- Každý bit zprávy zkopírujeme několikrát za sebe, aby se předešlo chybám v důsledku chybovosti MAC komunikačního kanálu
- "Oddělení zrna od plev"

Slabá bezkoliznost u hašovacích funkcí znamená

- Pro dané x nejsme schopni v rozumném čase najít y!=x tak, že h(x)=h(y)
- Pro dané x nejsme schopni v rozumném čase najít y!=x tak, že h(x)=y
- Pro dané x nejsme schopni v rozumném čase najít y!=x tak, že x=h(y)
- V rozumném čase nejsme schopni nalézt x, y (x=y) tak, že h(x)!=h(y)

Z jakých šifrovacích algoritmů se obvykle tvoří hašovací funkce?

- Asymetrická šifra
- Hašovací funkci nelze vytvořit z žádného šifrovacího algoritmu
- Proudová symetrická šifra
- Bloková symetrická šifra

K čemu slouží MAC (Message authentication code)

- K zajištění důvěrnosti
- K zajištění integrity
- K ověření zprávy síťové karty
- K detekci chyb při přenosu dat
- K transformaci hašovací funkce

Zajistit autentizaci digitálních dat a zpráv lze

- Pomocí klasického (ručního) podpisu
- Pomocí zaručeného elektronického podpisu
- Pomocí MAC
- Pomocí klíčované hašovací funkce
- Pomocí parciálně zaručeného elektronického podpisu

Pro pojem výpočetní bezpečnost platí následující tvrzení.

- Výsledek náročného výstupu je podepsaný, z důvodu zaručení integrity
- Časová náročnost prolomení určitého algoritmu mnohonásobně převyšuje dostupný výpočetní výkon
- Algoritmus jako takový nemusí být považován za neprolomitelný, dosud pouze nebyl nalezen efektivní způsob řešení/výpočtu
- Ani jedno z uvedených tvrzení neplatí

Jaké jsou používané algoritmy při digitálním podepisování

- CBC
- AES
- DSA
- RSA

- El-Gamal

Na jakém problému je založena bezpečnost RSA

- Obchodní cestující
- Eliptické křivky
- Faktorizace čísel
- Diskrétní logaritmus