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

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 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.

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

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 neutorizovaný přístup.

\* Odolnost proti útokům vyžadujícím fyzický přístup ke kartě.

Aktualizace klíče se vzájemnou autentizací protokolem AKEP2 (Authenticated Key Exchange

- Protocol 2) je založena na:

- Generátorech passcode

\* Algoritmu MAC (Message Authentication Code)

- Digitálních podpisech

- Bezklíčových kryptografických hašovacích funkcích

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 kategorií čipových karet podle technologie komunikace rozlišujeme?

- Hybridní karty.

\* Bezkontaktní karty.

\* Konktaktní karty.

- Polymorfní karty.

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

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

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.

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 neplat

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.

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.

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

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.

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

Generátory passcode slouží pro

- Urychlení generování sekvenčních čísel

\* Bezpečné uložení dlouhodobých klíčů

\* Realizaci challenge-response (výzva-odpověď) protokolu

- Personalizaci elektronických pasů

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

- Časová analýza

- Útok přes aplikační rozhraní

\* Ozařování čipu

\* Preparace čipu

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"

Jaké jsou používané algoritmy při digitálním podepisování

- CBC

- AES

\* DSA

\* RSA

\* El-Gamal

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.

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.

Protokol Kerberos zajišťuje

\* Autentizaci

- Aprobaci

- Autokracii

- Akumulaci

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

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.

K čemu slouží CRC (Cyclic redundancy check)

- K ověření autenticity dat

- Ke kompresi dat

- K zašifrování dat

\* K detekci chyb při přenosu dat

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.

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.

Co je to narozeninový paradox?

\* Lze jej ilustrovat faktem, že v sále s 23 lidmi je pravděpodobnost stejného data narození dvou lidí větší než 50 %

- Situace, kdy se začátkem roků rodí víc mužů než žen

- Pravděpodobnost nalezení stejného data narození k pevně zvolenému datu je při 23 lidech větší než 50 %

\* Statisticky podložená vysoká úspěšnost nalezení kolize

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.

Na jakém problému je založena bezpečnost RSA

- Obchodní cestující

- Eliptické křivky

\* Faktorizace čísel

- Diskrétní logaritmus

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

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.

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.

Jak eliminujeme útoky hrubou silou na PINy?:

- Pravidelnou změnou hodnoty PINu

\* Omezením počtu pokusů o zadání PINu

- kolením uživatelů

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

V tiketu používaném v systému Kerberos se objevuje:

\* Identifikátor alespoň jedné ze stran

- Soukromý klíč

- Náhodná výzva

\* Časové razítko

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

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.

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

Na jakém druhu kryptografie je založena základní verze Kerbera?

- Hybridní

\* Symetrická

- Asymetrická

Které z uvedených možností zajišťuje protokol IPsec?

- Nepopiratelnost přijetí dat.

\* Důvěrnost dat, ochrana proti útoku přehráním.

\* Autentizace a integrita původu dat.

\* Podporu správy klíčů.

Který z následujících protokolů je součásti SSL/TLS protokolu?

- Kerberos protokol.

\* Record Layer protokol.

- IPSec protokol.

\* Handshake protokol.

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

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.

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.

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

- Podpis, šifrování, podpis

- Šifrování, podpis, šifrování

- Šifrování, podpis

- Napořadí operací nezáleží

\* Podpis, šifrování

V dobrých autentizačních protokolech se typicky

\* Heslo posílá v hašované podobě

\* Heslo neposílá vůbec

K čemu se používá CAPTCHA

\* K odlišení uživatelů od robotů

- K odlišení chytrých robotů od robotů první generace

- K testu uživatelů, zda chtějí luštit text v obrázku a opisovat jej

- Je to dynamicky se měnící designový prvek www stránek

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.

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.

Které časově proměnné parametry se používají v kryptografických protokolech?

- Monoliticky rostoucí sekvence

- Náhodná komplexní čísla

- Náhodné sekvence

\* Náhodná časová razítka

\* Náhodná čísla

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)

Ukládání hesel lze realizovat

\* Hašovaně

- Impulzně

\* V otevřené podobě

\* Šifrovaně

- Hlasovaně

Digitálně podepisujeme

\* Pouze haš podepisovaného dokumentu

- Vždy přímo celý dokument

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

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)

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

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

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.

Jaké typy záznamů lze používat na čipové kartě?

\* Nestrukturovaná data.

- Exponenciální záznam s pevnou délkou.

\* Lineární záznamy s pevnou nebo variabilní délkou.

\* Cyklické záznamy.

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

\* Chybová analýza s útoky na a přes API nijak nesouvisí.

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

Digitální podpis může vytvořit

- Pouze osoba vlastnící sdílený klíč

\* Pouze osoba vlastnící soukromý klíč

Protokoly výzva-odpověď mohou být založeny na:

\* klíčované hašovací funkci

\* symetrickém šifrování

\* digitálním podpisu

\* MAC kódu, resp. funkci

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 vytořený pomocí kryptografických prostředků

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.

Na jaké vrstvě funguje protokol SSL/TLS?

\* mez aplikační a datovou vrstvou

- na linkové vrstvě

- na síťové vrstvě

- na datové vrstvě

Které z uvedených režimů podporuje IPsec:

- Překladový režim.

\* Transportní režim.

\* Tunelovací režim.

- Dynamický virtuální režim.

Zajistit autentizaci digitálních dat a zpráv lze

- Pomocí klasického (ručního) podpisu

\* Pomocí zaručeného elektronického podpisu

- Pomocí MAC

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

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)

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

- 2

- 4

\* 3

- žádná z těchto odpovědi není správná

Která tvrzení platí pro elektronickou značku

\* Elektronické značky jsou jednoznačně spojené s označující osobou a umožňují její identifikaci prostřednictvím kvalifikovaného systémového certifikátu

\* Technologicky jde o totéž co zaručený elektronický podpis

- Ověření elektronické značky je obtížnější než ověření elektronického podpisu

\* Elektronická značka je ke zprávě připojena tak, že je možné detekovat následné změny ve zprávě

Co zajišťujeme použitím náhodných čísel?

- Odolnost proti uváznutí a stárnutí

\* Aktuálnost

- Nezvratnost

- Stálost a stabilitu

\* Čerstvost

\* Jedinečnost

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

Vhodná tajná informace pro autentizaci je

- Rodné příjmení matky

- Tel. číslo, pokud není uvedeno ve Zlatých stránkách

\* Heslo

\* PIN

\* Fráze (passphrase)

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 patří mezi bezpečnostní problémy používání bankovních karet s čipem?

\* Možnost odpozorování PINu na frekventovaných místech.

- Špatná průkaznost nelegitimní autorizace platby pomocí PINu.

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.