1) Právní předpisy, trestné činy, základní pojmy

Kybernalita je jakýkoli čin, směřující k narušení, nebo zneužití počítače, nebo počítačového systému a informací v něm obsažených (definice OSN).

Právní předpisy:

Bezpečnostní problematika má podporu v zákonech ČR a při veškerých činnostech týkajících se práce s daty a užívání výpočetní techniky je nutné na to pamatovat:
Zákon č. **40/2009 Sb.**, trestní zákoník
§ 230 *Neoprávněný přístup k počítačovému systému a nosiči informací*
(neoprávněný přístup, ukradení dat – flash disk, zůstal přihlášený na PC – to je ale sporné, musí tam být definováno, že se dále jedná o neoprávněný přístup)
§ 231 *Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat*
uchovávám např. ISIC, prodám číslo karty a PIN, karty do automatu udělané tak, že se nemusí nabíjet, kódovací karta pro sdílení na síti před démona, kdo toto poskytuje nebo někomu řekne, jak na to, půjde sedět, trestné je i poskytování hesel
§ 232 *Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti*
§ 182 *Porušení tajemství dopravovaných zpráv*
přečtení cizího emailu, odposlech na sítě

Občanský zákoník (40/1964)
Obchodní zákoník (513/1991)
Telekomunikační zákon (513/1991)

Doplňující legislativa:

Autorský zákon (121/2000)
Zákony na ochranu průmyslového vlastnictví (14/1993)
Zákon o ochraně osobních údajů (101/2000)
Zákon o regulaci reklamy (40/1995)
Zákon o elektronickém podpisu (227/2000)
Zákon o svobodném přístupu k informacím (106/1999)
Zákon o informačních systémech veřejné správy (365/2000)

Úmluva o počítačové kriminalitě (Úmluva o počítačové kriminalitě)

– rada Evropy, USA, Kanada, Japonsko a další.

Počítačový systém:
– jakékoli zařízení nebo skupina vzájemně propojených nebo souvisejících zařízení, z nichž jedno nebo více provádí na základě programu automatické zpracování dat
Počítačová data:
– jakékoli vyjádření skutečností, informací, nebo pojmů ve formě vhodné pro zpracování v počítačovém systému, včetně programu vhodného k zajištění, aby počítačový systém vykonával určitou funkci
Poskytovatel služeb:
– jakýkoli veřejný, nebo soukromý subjekt, který poskytuje uživatelům služby možnost komunikovat prostřednictvím počítačového systému
– jakýkoli jiný subjekt, který zpracovává, nebo ukládá počítačová data pro tuto komunikační službu, nebo uživatele této služby
Provozní data:
– jakákoli pc data související s přenosem dat prostřednictvím pc systému, generovaná pc systémem, který tvořil součást komunikačního řetězce, jež vyjadřují původ, cíl, trasu, dobu, objem, dobu trvání přenosu dat, nebo druh použité služby
– slouží k provozu technologií, které provozujeme
– např.: IP adresa, hlavička e-mailu, druh použité služby – protokol, jaký požil, kolik dat přenesl z té služby, jak dlouho tam byl…
  - **paket** – data o provozu
    - blok dat přenášený v počítačových sítích založených na přepojování paketů, kde je možné přenášet data i při výpadcích některých spojů

Trestné činy

- Trestné činy proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů
  - Neoprávněný přístup
  - Neoprávněné zachycení informací
  - Zásah do dat
  - Zásah do systému
  - Zneužití zařízení
- Trestné činy související s počítači
  - Falšování údajů související s počítači (např.: změna data: vojna – někdo měl u jména 1 – půjde na vojnu, 5 – je na vojně, 4 – v zahraničí, 2 – na cvičení… Když to přepíšu u někoho či u sebe, tak se jedná o trestný čin)
  - Podvod související s počítači
- Trestné činy související s obsahem (zveřejnění třeba rasismu, dětská pornografie…)
  - Trestné činy související s dětskou pornografií
- Trestné činy související s porušením autorského práva a práv příbuzných autorskému právu
  - Trestné činy související s porušením autorského práva a práv příbuzných autorskému právu

Závazky v oblasti mezinárodní spolupráce:

Evropská Úmluva o vydávání osob
Evropská Úmluva o vzájemné pomoci v trestních věcech
Dodatkový protokol k Evropské Úmluvě o vzájemné pomoci v trestních věcech

2) Počítačová kriminalita: Osoby, typy trestné činnosti, metody

Osoby:

- **Script Kiddies**: jsou označováni převážně mladí hackeři s průměrnými znalostmi programování a počítačů
  - k útokům používají předpřipravené nástroje (skripty), do kterých stačí zadat adresu vzdáleného počítače
  - po proniknutí do systému většinou data vymažou a nechají vzkaz typu "Byl jsem tu. Fantomas"
  - žádné techniky pro maskování útoku a zahlazení stop většinou nepoužívají
- **H4H**: Hackers for Hire
  - najmutí hackeři
  - hackeři, kteří nabízejí své služby jiným kriminálním, teroristickým nebo extremistickým skupinám
- Specialisté
- **Armáda**: státní celky

Amatérská činnost

Průmyslová špionáž

- obor lidské činnosti provozovaný státními organizacemi, komerčními subjekty či jednotlivými osobami za účelem získání utajovaných informací z oblasti průmyslových technologií, finančnictví a dalších oborů a jejich následného využití pro vlastní prospěch
- krádeže laptopů a externích disků (taxi, letiště, vlak, hotely, auta)
- útoky po síti
- sabotáže
- **malware (MALicious softWARE)**: pc infiltrace (jakýkoliv neoprávněný vstup do počítačového systému)
  - sbírka škodlivých kódů (havěti, která by měla být pro jakýkoliv antivirus velkou neznámou)
- **DDoS (Distributed Denial of Service – distribuované odmítnutí služby)**: technika útoku na internetové služby nebo stránky, při níž dochází k přehlcení požadavky a pádu nebo minimálně nefunkčnosti a nedostupnosti pro ostatní uživatele
  - cíle útoku jsou většinou:
    - nucení opakovaného resetu cílového počítače
    - narušení komunikace mezi serverem a obětí tak, aby jejich komunikace byla buď zcela nemožná, nebo alespoň velmi pomalá

Příklady:

- **GhostNet (odhalen březen 2009)**: síť duchů (napadeno 1295 důležitých počítačů po celém světě)
- **Operation Aurora**: kybernetický útok; prosinec 2009-1010
  - útok vedený na několik soukromých organizací včetně společnosti Google, která následně hrozila svým odchodem z Čínského trhu
- **CyberSitter a 'Green Dam'**: obsahově řídící software pro Windows vyvinutý v lidové republice Čína

Kyberterorizmus

- termín kyberterorismus byl poprvé požit v 90. letech Barrym Collinem
- je konvergencí terorismu a kyberprostoru
- obvykle je chápán jako nezákonný útok nebo nebezpečí útoku proti počítačům, pc sítím a informacím v nich skladovaným v případě, že útok je konán za účelem zastrašit nebo donutit vládu nebo obyvatele k podporování sociálních nebo politických cílů

Šíření, prodej nelegálního obsahu

- díla chráněná autorským právem
- nelegálně získaná data (Dumpy kreditních karet, Porušování autorských práv)
- šíření závadného obsahu (Porno)
- **botnety**: značení pro SW agenty nebo pro internetové roboty, kteří fungují autonomně nebo automaticky
  - v současné době je termín nejvíce spojován s malware, kdy botnet označuje síť počítačů infikovaných speciálním softwarem, který je centrálně řízen z jednoho centra → botnet pak provádí nežádoucí činnost, jako je rozesílání spamu, DDoS útoky a podobně

Vydírání

- **elektronické výpalné**: zaplať nebo ti hacknem počítač

Kybersquatting

- registrování domén s názvy cizích obchodních značek
- registrace, obchodování nebo užívání doménové jméno se zlým úmyslem - úmyslem těžit z dobrého jména ochranné známky patřící někomu jinému
- s úmyslem těžit z dobrého jména ochranné známky patřící někomu jiného
- nabízí k prodeji domény, osobu nebo společnost, která vlastní ochranné známky obsažené v názvu za nadsazené ceny

Šikana, pomluvy a obtěžování

- fotomontáže (foto na serveru s erotickými službami) (právně pomluva)
- pomluvy (tj, když někomu zveřejníme číslo třeba na nějaké erotické služby, či zveřejním cizí číslo v inzerátu)

Krádeže

Sledování politických cílů

- **StuxNet Worm**: počítačový červ, který se objevil v září 2010
  - k šíření není nezbytně nutné připojení k internetu nebo k jiné počítačové síti – umí se přenášet na paměťových mediích (disky, externí paměti)¨
  - umí přebírat řízení napadených systémů
- **Íranská atomová elektrárna Bushehr**: stavba dokončena v roce 2010, po napadení počítačovým virem však začala vyrábět elektrickou energii až v roce 2011
- zneužití chyby v řídících systémech

Infoware

- termín Tima O´Reillyho
- označuje weby jako Amazon.com používající server a software jako je LAMP, umožňující sdílet na webu data (book comments a ratings) - vlastně určitou formu zpětné vazby

Metody:

Zneužití WEB serverů

SPAM

- krádež e-mail adresy
- krádež identity

Odposlechy dat

- síť
- bezdrátové technologie
- **RFID**: identifikace na rádiové frekvenci je další generace identifikátorů navržených (nejen) k identifikaci zboží, navazující na systém čárových kódů. Stejně jako čárové kódy slouží k bezkontaktní komunikaci na krátkou vzdálenost

DoS, DDoS

- technika útoku na internetové služby nebo stránky, při níž dochází k přehlcení požadavky a pádu nebo minimálně nefunkčnosti a nedostupnosti pro ostatní uživatele

Ovládnutí klienta

- data, cykly, botnety, chyby v klientech

Ovládnutí serveru

- chyby ve službách

Zametání stop

- logy
- **rootkity**: sada pc programů a technologií, pomocí kých lze maskovat přítomnost zákeřného software v počítači (například přítomnost virů, trojských koňů, spyware a podobně)
    - maskuje přítomnost zákeřných programů skrýváním adresářů, v nichž jsou instalovány…

Anonymita

- Pseudoanonymita vs. pravá anonymita
    - **pseudoanonymita**: značí jakousi zdánlivou, nepravou anonymitu
        - i když v komunikaci vystupuje osoba pod přezdívkou a má změněné pohlaví, tak IP adresu počítače, z kého se hlásí a název domény, při které má zřízený účet obvykle nemění → v mnoha případech snadno umožní k anonymně vystupujícímu uživateli nalézt jeho skutečnou identitu
    - **pravá anonymita**: značí skutečnou anonymitu, kdy k vystopování uživatele nevedou žádné viditelné indicie
        - skutečnou anonymitu z většiny případů užívají např. hackeři, crackeři, tedy lidé technicky na výši, jejichž dopadení by pro ně mohlo mít i soudní dohru
        - anonymitu může uživatel získat například tak, že se do komunikačních prostředí hlásí jako host tj. nijak neregistrovaný uživatel
    - real time protokoly (TOR, FreeNet atd.): protokol standardizující paketové doručování zvukových a obrazových (video) dat po internetu
    - email

Šifrování

- šifrování e-malu
- šifrování přenosu
- šifrování dat na disku

Výměna informací

– **IRC** (jednou z prvních možností komunikace v reálném čase po internetu), chaty, fóra, konference, **USENET NEWS** (systém elektronických diskusních skupin, distribuovaný prostřednictvím internetu po celém světě)
– vyhledávání informací

3) Útoky na WEB servery: Základní zdroje, metody získávání inf.

Základní zdroje informací:

– **OWASP(Open Web Application Security Project)**: sdružení, které se zabývá bezpečností webu
  - projekt a komunita zabývající se bezpečností webových aplikací zahrnujíce v to rozměry lidské, procesní a technologické
  - zahájili dne 9. září 2001 Mark Curphey a Dennis Groves
  - je především o sdílení znalostí v oblasti bezpečnosti webových aplikací
– **OWASP Live CD**: cd, které si můžeme stáhnout a vypálit a pak z něj nabootovat nástroje
  - Web goat: server, (stránky opravdu chyby obsahujou)
– OWASP Testing Guide

Získávání informací o systému

robots.txt

– textový soubor, který umožňuje správci webu zakázat nebo povolit přístup některých robotů – tento soubor se musí nacházet v kořenovém adresáři daného webu
– (např.: www.jcu.cz/robots.txt)
– formát souboru:

```
User-agent: * (jakého robota se věc týká – pro který vyhledávač to platí)
Allow: /searchhistory/ (co může proledávat)
Disallow: /admin (co nemůže prohledávat)
```

– získání souboru: wget (slouží k vyrování celých webů)
– více informací o struktuře a funkci:
– útočník získá informace o webu, ale pro zatím nedělá nic nelegálního

Google

– co můžeme Gogolem získat: vyhledávání informací souvisejících se zabezpečením serveru: “Password”, “Heslo”, “Login”, “Index of ...”
  - najít všechny přihlašovací formuláře na www.jcu.cz
    - zadám do Gogole např.: jmeno heslo site: jcu.cz
– operátory:
  - **site**: např. jmeno heslo site: jcu.cz – na daných stránkách hledám to, co by mě jako útočníka mohlo zajímat a také se tak redukuje počet nalezených stránek (ve vyhledávači zadám jcu.cz a mám více výsledků. než site: jcu.cz)
  - **cache**: i s historií, jak stránka vypadala
  - **inurl**: hledá odkazy na stránkách
  - **filetype**: např. hledám excel tabulky s hesly

Identifikace serveru

– pole “Server:” hlavičky HTTP protokolu
  - Využití programu NetCat k získání hlavičky HTTP protokolu:
    - nc IP_adresa_serveru port
    - HEAD / HTTP/1.0
– pořadí polí hlavičky
– nekorektní dotaz

```
nc IP_adresa_serveru port
GET / HTTP/3.0
```

– neexistující protokol:

```
nc IP_adresa_serveru port
GET / BLBOST/1.0
```

Automatizované nástroje:

- **httprint**:

Online:

- **netcraft**:

Aplikace

- detekce aplikace:
  - aplikace se mohou skrývat pod různými adresáři:
    - www.tuzkarny.cz/
    - www.tuzkarny.cz/apl1
    - www.tuzkarny.cz/apl2
  - Jak tyto adresáře nalézt?
    - procházení indexovaných adresářů
    - odkazy z jiných stránek
    - site:www.tuzkarny.cz
    - hrubá síla
  - aplikace se mohou skrývat na jiných (nestandardních) portech:
    - nmap -PN -sT -sV -p0-65535
  - a v různých doménách na virtuálních webserverech:
    - www.tuzkarny.cz
    - apl1.tuzkarny.cz
    - apl2.tuzkarny.cz
  - položka "Host:" HTTP 1.1 hlavičky:
  - DNS zone transfer
  - reverzní DNS dotazy
  - hledání jmen pomocí WEB rozhraní
  - NetCraft

Detekce parametrů aplikace

- lokální Proxy server (Burp proxy, WEB Scarab)

Analýza chybových hlášení

- neexistující stránky
- chybné/žádné parametry
- špatné/žádné jméno heslo

4) Nedostatky konfigurace WEB serveru a aplikace

SSL/TLS

- **SSL (Secure Sockets Layer)**: protokol, resp. vrstva vložená mezi vrstvu transportní (např. TCP/IP) a aplikační (např. HTTP), která poskytuje zabezpečení komunikace šifrováním a autentizaci komunikujících stran
  - využívá se pro bezpečnou komunikaci s internetovými servery pomocí HTTPS (zabezpečená verze protokolu http)
  - po vytvoření SSL spojení je komunikace mezi serverem a klientem šifrovaná
- **TLS (Transport Layer Security)**: kryptografické protokoly, poskytující možnost zabezpečené komunikace na Internetu pro služby jako WWW, elektronická pošta, internetový fax a další datové přenosy
  - umožňují aplikacím komunikovat po síti způsobem, který zabraňuje odposlouchávání či falšování zpráv
  - typicky je autentizován pouze server (jeho totožnost je zaručena), zatímco klient zůstává neautentizován – koncový uživatel (člověk, aplikace, webový prohlížeč) si je jist, s kým komunikuje
  - zahrnuje tři základní fáze:
    - dohodu účastníků na podporovaných algoritmech
    - výměnu klíčů založenou na šifrování s veřejným klíčem a autentizaci vycházející z certifikátů
    - šifrování provozu symetrickou šifrou

- detekce podporovaných slabých šifer
- např. příkazem openssl: openssl s_client -no_tls1 -no_ssl3 -connect IP:443
- validita certifikátu
- kvalita algoritmu, kterým je certifikát podepsán

Management serveru

- identifikace architektury:
  - **ldap (Lightweight Directory Access Protocol)**: definovaný protokol pro ukládání a přístup k datům na adresářovém serveru
    - podle tohoto protokolu jsou jednotlivé položky na serveru ukládány formou záznamů a uspořádány do stromové struktury (jako ve skutečné adresářové architektuře)
    - vhodný pro udržování adresářů a práci s informacemi o uživatelích (např. pro vyhledávání adres konkrétních uživatelů v příslušných adresářích, resp. databázích)
  - firewall: síťové zařízení, které slouží k řízení a zabezpečování síťového provozu mezi sítěmi s různou úrovní důvěryhodnosti a zabezpečení
    - slouží jako kontrolní bod, ký definuje pravidla pro komunikaci mezi sítěmi, ké od sebe odděluje
  - aplikační proxy:
  - DMZ:
- známé chyby serveru
- administrativní rozhraní (web, ftp, WebDAV, NFS)
  - odkud je dostupné? (vnitřní síť, Internet, je filtrované?)
  - autentizační mechanizmus
  - implicitní hesla

Management aplikace

- známé adresáře a soubory (program Wikto)
- příklady, manuály
- directory traversal: kanonizace může být důležitá pro počítačovou bezpečnost
  - např. webový server může mít dovoleno poskytovat jen dokumenty z adresáře /veřejné/web
  - co se ale stane, když ho někdo požádá o soubor /veřejné/web/../../tajné/účetnictví?
    - pokud server nejprve převede požadovanou cestu na kanonický tvar, zjistí, že je ve skutečnosti žádán o soubor /tajné/účetnictví, který pod dovolenou cestu nespadá, takže požadavek odmítne
    - pokud by to však neudělal, chybně by zveřejňoval i tajné dokumenty
    - taková chyba se označuje jako directory traversal
- komentáře

Soubory

- jak server nakládá s různými typy souborů (zobrazí obsah atd.)
  - nejprve vyhledat soubory (Google, spider, analýza kódu)
  - http://filext.com: vyhledávač různých programů - hledání názvu programu, který používá konkrétní příponu souboru
- staré soubory (zálohy, konfigurace, programy) – .old, .bak, .zip, .tar, .tgz, zaloha, backup
- nápovědy: viewuser.cgi: adduser.cgi, deluser.cgi, ...
  - /app/user: /app/admin, /app/manager, ...
  - robots.txt
- • hrubá síla (Wikto)

Administrátorská rozhraní

- detekce URL s rozhraním (viz. nahoře Soubory)
- nápovědy ve zdrojových souborech
- dokumentace
- odhalení alternativních portů s rozhraním
- manipulace s parametry (např menu=admin, menu=1,2,3,...,495

5) Útoky na autentizační mechanizmy WEB aplikací

Jsou autentizační údaje přenášené šifrovaně?

- **POST**: odesílá uživatelská data na server
  - používá se například při odesílání formuláře na webu
  - s předaným objektem se pak zachází podobně jako při metodě GET
  - data může odesílat i metoda GET, metoda POST se ale používá pro příliš velká data (víc než 512 bajtů, což je velikost požadavku GET) nebo pokud není vhodné přenášená data zobrazit jako součást URL (data předávaná metodou POST jsou obsažena v HTTP požadavku)
  - **nešifrovaný přenos (HTTP):**

    POST http://www.tuzkarny.cz/cgi-bin/login.cgi HTTP/1.1
    Host: www.tuzkarny.cz
    ...
    Content-Type: application/x-www-form-urlencoded
    Content-length: 64

    Command=Login&User=franta&Pass=Kotva45
  - **šifrovaný přenos (HTTPS):**

    POST https://www.tuzkarny.cz:443/cgi-bin/login.cgi HTTP/1.1
    Host: www.tuzkarny.cz
    ...
    Content-Type: application/x-www-form-urlencoded
    Content-length: 64

    Command=Login&User=franta&Pass=Kotva45
- **GET**: požadavek na uvedený objekt se zasláním případných dat (proměnné prohlížeče, session id, …)
  - výchozí metoda při požadavku na zobrazení hypertextových stránek, RSS feedů aj.
  - celkově nejpoužívanější
  - šifrovaný přenos (HTTPS):

    GET https://www.tuzkarny.cz/login.html?user=franta&pass=Kotva45 HTTP/1.1
    Host: www.tuzkarny.cz
  - Pozor! URL je uchováváno v historii prohlížeče a v logu proxy serveru
  - nástroje:
    - WEB proxy (Burp, WebScarab)

Identifikace uivatele

- **testování kombinací**:
  - správné jméno/správné heslo
  - správné jméno/chybné heslo
  - neexistující jméno/chybné heslo
- **prostřednictvím**:
  - chybových hlášení
  - návratových kódů
  - URL
- **testování domovských adresářů a specifických souborů (URI)**:
  - *403 Forbidden*: požadavek byl legální, ale server odmítl odpovědět
    - na rozdíl od 401 Unauthorized response zde nehraje žádnou roli autentifikace
  - *404 file Not Found*: požadovaný dokument nebyl nalezen, ale v budoucnosti může být dostupný
- **zneužití schémat obnovy zapomenutých hesel**: uživatel neexistuje/existuje
- **odhadnutí jména uživatele**: jméno uživatele je tvořeno pomocí známého schématu.
- **nástroje**: prohlížeč, WEB proxy

Implicitní, nebo snadno odhadnutelná hesla

- **implicitní hesla**: hesla nastavená po instalaci dané technologie/aplikace: *www.phenoelit-us.org/dpl/dpl.html*
- **snadno odhadnutelná hesla**: admin, root, super, password123, pass123,
- **hesla tvořená podle jména aplikace, firmy, nebo uživatele**: ucto, ucto123, tuzkarny, tuzk789, Janicka6

- hesla získaná ze zdrojových kódů stránek
- **generovaná implicitní hesla**: u001, u002, ...
- **nástroje**: DPL (default password list); slovníky

Hrubá síla

- **před použitím hrubé síly je nutné identifikovat mechanizmus autentizace**:
  - HTTP autentizace (Basic, Digest)
    - **basic**: base64 kódování
      - *Basic access authentication (jednoduché ověření přístupu)*: označení pro jednoduchou autentizaci při přístupu na webové stránky
        - webový server vyzve pomocí protokolu HTTP přistupujícího klienta (typicky webový prohlížeč), aby poslal v rámci požadavku na stránku také autentizační informace (tj. jméno a heslo)
    - **digest**: MD5 a pro spojení unikátní "nonce"
      - Algoritmus MD5 se prosadil do mnoha aplikací (např. pro kontrolu integrity souborů nebo ukládání hesel)
      - MD5 je popsán v internetovém standardu RFC 1321 a vytváří otisk o velikosti 128 bitů
      - vytvořen v roce 1991 Ronaldem Rivestem, aby nahradil dřívější hašovací funkci MD4
  - HTML Form autentizace

Obejití autentizačního schématu

- **přímý přístup ke stránce (forced browsing)**: zadat přímo nechráněné URL *(http://www.tuzkarny.cz/admin/adduser)*
- **modifikace parametrů**: aplikace kontroluje, zda je uživatel autentizován pouze na základě konstantních parametrů
- předpovězení Session ID:
- SQL Injection

Zapamatování hesla v prohlížeči

- kešování v prohlížeči <INPUT TYPE="password" AUTOCOMPLETE="off">
- uložení hesla v trvalém (permanent) Cookie

Zapomenutá hesla

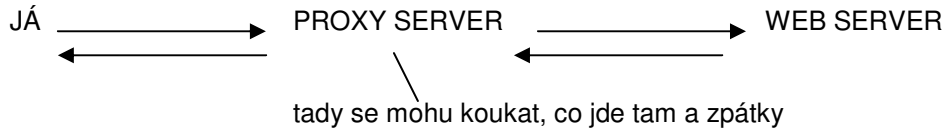
- zaslání e-mailem
- bezpečnostní otázky

Odhlášení (Logout)

- zrušení identifikátoru relace:
  - existuje tlačitko logout?
  - po odhlášení se vrátit o stránku zpět
  - resetovat Cookie na původní hodnotu (proxy, Cookie editor)
- timeout relace

6) Session management

- zajištění, aby útočník nemohl získat ID řetězec, když už ho získá, tak aby ho nemohl použít
- **Co je to relace (session)**? Je to trvající spojení v nějaké počítačové síti.
- **Proč se používá**? Aby web server věděl, s kým komunikuje.
- **Jak se dělá relace**? dotaz se pořád posílá ID řetězec
- **nedostatky relace**: útočníkovi se podaří získat ID řetězec
  - podaří se mu to pomocí nezašifrovaného ID, je schopen předpovědi, ID je platné po určitou dobu, když se špatně napadený odhlásí
- základní nástroj k testování webu: lokální proxy server např. Burp, Web Scarab (OWASP), Paros



- je nutné se vyhnout autentizaci při přístupu ke každé stránce
  - musí tedy existovat mechanizmus k ukládání autentizačního údaje po určitý časový interval (login - logout, timeout)
  - po úspěšné autentizaci uživatele je vygenerován token (Cookie, SessionID), který je následně používán k autorizaci automaticky prohlížečem
- ID=vygenerovaný řetězec
- ID=jméno a heslo
- pokud zavřu email křížkem, tak pachatel může najít moje ID a přihlásit se na můj email
- když ale dám odhlásit se, ID se ruší – ID by nemělo být přenášeno URL, ale POSTEM

Cookie

- v protokolu http se tak označuje malé množství dat, ká WWW server pošle prohlížeči, ký je uloží na pc uživatele. Při každé další návštěvě téhož serveru pak prohlížeč tato data posílá zpět serveru. Cookies běžně slouží k rozlišování jednotlivých uživatelů, např. ukládá se do nich obsah „nákupního košíku“ v elektronických obchodech, uživatelské předvolby apod.
- přestože většina prohlížečů cookies podporuje, jiné jednodušší prohlížeče (např. na mobilních zařízeních) je podporovat nemusejí; navíc cookies lze ve většině prohlížečů zakázat
- ukládají se na straně klienta (uživatele) jako krátké textové soubory a to pro každé webové místo (website)
- **bezpečnost a ochrana soukromí**: neznamenají žádné nebezpečí pro počítač jako takový, ale přesto mohou být nebezpečné pro ochranu soukromí
  - navštívený web si totiž může ukládat do cookies jakékoliv informace, ké o návštěvníkovi zjistí a může tak postupně zjišťovat zájmy konkrétního návštěvníka – jaké stránky navštěvuje, jaké informace vyhledává, jak často daný web navštěvuje apod.
  - lze zneužít zejména tehdy, pokud získá útočník přístup k počítači uživatele, neboť cookies na počítači nejsou nijak chráněny – pak lze předstírat např. cizí identitu
- **útoky na Cookie**: shromažďování dostatečného počtu cookies k následné analýze
  - *reverzní analýza* – reverzní inženýrství (zpětná analýza) je proces, jehož cílem je odkrýt princip fungování zkoumaného předmětu
  - manipulace s cookie
  - přeplnění paměti pomocí Cookie
- **analýza implementace Cookies**:
  - kolik různých Cookie aplikace používá?
  - která část aplikace generuje, nebo modifikuje cookie?
  - které časti aplikace vyžadují Cookie k autentizaci?
    - pokuste se přistoupit ke všem stránkám bez Cookie, nebo s modifikovaným Cookie
  - obsahují všechny direktivy Set-Cookie parametr Secure?
    - cookie přenášeno jen HTTPs
  - jsou některé operace s Cookie prováděny prostřednictvím nešifrovaného protokolu?
  - mohu systém donutit, aby poslal Cookie nešifrovaně?, Pokud ano, jak je apliakcí zajištěna jeho bezpečnost?
  - jsou Cookie nastaveny jako trvalé (persistent = pořád uložený na disku)?
  - jaké jsou nastaveny časy vypršení (Expires=)
  - jsou krátkodobá Cookies konfigurována odpovídajícím způsobem?
  - jaké parametry Cache-Control jsou nastaveny (HTTP/1.0, HTTP/1.1)

Analýza struktury Cookies (tokenů)

- tokeny (Cookie, SessionID, Skrytá pole) musí být dostatečně náhodné, unikátní, odolné proti statistické a krypto analýze a proti únikům informací
- Cookie nesmí obsahovat pouze specifická data: *jmeno:IP:heslo*, která jsou následně pouze zakódovaná (Hex,Base64,MD5)
- **hybridní tokeny**: část dat statická, část dynamická (proměnná)
- **analýza proměnných částí tokenu**:
  - jsou tokeny opravdu náhodné?
  - vygenerují stejné vstupní podmínky stejný token? na základě jakého vstupu se token mění?

  - je token odolný statistické a kryptoanalýze?
  - které elementy tokenu jsou vázané na čas?
  - které části tokenu jsou předvídatelné?
  - je možné vydedukovat následný token na základě znalosti algoritmu, kterým byl vygenerován předcházející?
- **reverzní analýza**:
  - shromáždění dostatečného počtu (způsob generování může být jiný před přihlášením a po přihlášení: může záviset na stavu ve kterém se aplikace nachází)
  - matematická analýza (chi-squares, atraktory)
  - závislost na čase (kdy je generován)
  - co všechno má vliv na tvar výsledného tokenu?
  - jaká znaková sada je v tokenu použita? co se stane, když vložíme znak z jiné znakové sady?
  - skládá se token z více nezávislých částí?

Hrubá síla

- délka trvání útoku X doba životnosti tokenu
- útok hrubou silou je většinou pokus o rozluštění šifry bez znalosti jejího klíče k dešifrování
  - v praxi se jedná o systematické testování všech možných kombinací nebo omezené podmnožiny všech kombinací
  - např. mám hodinu na to, abych hádala hesla

Manipulace

- závisí na předchozí analýze
- změna informací, které jsou v tokenu uvedeny v otevřené formě (jméno, tel.číslo, id uživatele)
- odhadnutelné tokeny
- hrubá síla (Foundstone Cookie Digger)
- overflow

Příklady útoků

- **session fixation**: útočník na internetu uloží stránku s odkazem na zamýšlenou aplikaci a svou oběť/i – např. přes ICQ, e-mail, … – aby na tento odkaz klikly a přihlásily se do aplikace
  - daný odkaz v cílové URL adrese již obsahuje (konstantní) HTTP cookie, která se (pokud aplikace není zabezpečena proti tomuto útoku) použije
  - útočník poté použije stejný odkaz a získá stejná oprávnění jako před tím přihlášený uživatel
  - podmínky:
    - aplikace nezmění SessionID po přihlášení uživatele (nezruší SessionID vygenerované před přihlášením)
    - útočník je schopen podstrčit již vygenerované SessionID uživateli, který se právě přihlašuje
    - ještě snažší, pokud je SessionID přenášeno pomocí HTTP a teprve při přihlášení se přepíná na HTTPS
- **CSRF (Cross-site request forgery)**: jedna z metod útoku do internetových aplikací pracující na bázi nezamýšleného požadavku pro vykonání určité akce v této aplikaci, který ovšem pochází z nelegitimního zdroje
  - většinou se nejedná o útok směřující k získání přístupu do aplikace; spíše využívá akce uživatelů, kteří jsou k ní již v okamžiku útoku přihlášeni
  - *opatření proti CRFS*: pro akce, které mažou určité záznamy nebo je jiným způsobem mění, se doporučuje zásadně používat HTTP metodu POST - to útok CSRF znesnadňuje, ale ještě zcela nevylučuje
    - používat autorizační token – tedy náhodně vygenerovaný řetězec pro tuto akci, platící jen pro aktuálního uživatele
    - implementace autorizačním tokenem je sama o sobě považována za dostatečné opatření proti CSRF útokům

7) Problematika kontrloly vstupů WEB aplikací

Kontrola vstupů

- nedostatečná kontrola vstupů je nejběžnějším nedostatkem WEB aplikací - vede téměř ke všem hlavním útokům jako je například:
  - **Cross site scripting (XSS)**: metoda narušení WWW stránek využitím bezpečnostních chyb ve skriptech (především neošetřené vstupy)
    - manipulace se vstupními parametry takovým způsobem, aby aplikace generovala škodlivé výstupy – pomocí této techniky je možné získat citlivé informace (Cookie s SessionID) z prohlížeče oběti, nebo převzetí kontroly nad prohlížečem
    - reflected XSS: jiný název pro XSS, které není trvalého rázu – tj. škodlivá data se předávají do cizího prohlížeče pomocí URI; škodlivá data většinou tvoří JavaScript, nebo jiný typ skriptovacího jazyka
      - skript pak může být použit k:
        - instalaci keyloggeru
          - SW, který snímá stisky jednotlivých kláves
          - neohrožuje přímo počítač, ale slouží ke zjišťování hesel jiných lidí
        - krádeži Cookies
        - krádeži obsahu clipboardu (schránka)
          - zvláštní oblast operační paměti spravovaná operačním systémem, určená k přechodnému ukládání rozličných dat
        - změně obsahu stránky (např. odkazu na stahovaný soubor)
      - 3 fáze útoků:
        - detekce vstupů
        - vkládání testovacích dat do nalezených vstupů
        - zneužití nalezených nedostatků v reálném útoku
    - stored XSS: data zadávaná uživateli jsou serverem bez dostatečné kontroly lokálně ukládána a následně zobrazována serverem jako součást stránek
      - to může vést k následujícím útokům:
        - uvládnutí cizího prohlížeče
        - získání citlivých informací
        - defacement aplikace
        - sken portů "interních" serverů
        - implementace exploitů prohlížečů
    -
    - *ukázka útoku*:
      - typ 1: označuje se jako *lokální* nebo *DOM based*
        - lze ji využít i na statických stránkách a jde o neošetřené přenesení proměnné z URL adresy do javascriptu
      - typ 2: označuje se jako *non-persistent* nebo *reflected*
        - postaven na úpravě části URL, ká se interpretuje do stránky jako její součást, například jako nadpis
        - pokud do URL přidáme svůj kód, který není před interpretací upraven, tak se stránka v prohlížeči zachová, jako by námi vložený kód byl její součástí
      - typ 3: označován jako *persistent*, *stored* nebo *second-order*
        - nejnebezpečnější možnost, protože na takto napadené stránky nemusíte vstoupit přes upravený link
        - vzniká pokud je obsah stránky generován z databáze
  - **SQL injection**: technika napadení databázové vrstvy programu vsunutím (odtud „injection") kódu přes neošetřený vstup a vykonání vlastního, samozřejmě pozměněného, SQL dotazuInterpreter injection
    - vložení SQL dotazu do vstupních dat WEB aplikace
    - úspěšný útok může:
      - číst data z databáze
      - modifikovat data v databázi
      - zadávat administrátorské příkazy (shutdown)
      - vykonávat příkazy operačního systému
    - *3 typy útoků*:
      - inband: oblast telekomunikací – zasílání metadat a řízení informací ve stejném pásmu
      - out-of-band: má různé využití v komunikaci a telekomunikaci = ovládání signalizace
      - inferetial

- **SQL Injection versus Blind SQL Injection**:
  - blind SQL injection: používá se, pokud je webová aplikace náchylná k SQL injection útoku, ale výsledek útoku se útočníkovi nezobrazí
    - tento typ útoku může být časově náročný, protože každý nový výraz musí být vytvořen pro každý odhalený bit
    - existuje několik nástrojů, které pomohou automatizovat tyto útoky jakmile byla zjištěna lokace zranitelnosti a cílová informace byla zjištěna
    - v první řadě je nutné identifikovat situace, kdy dochází k připojování aplikace do databáze:
      - autentizace
      - vyhledávače informací
      - elektronický obchod
    - a pak identifikovat vstupy pro dotazy:
      - pole formuláře
      - skrytá pole POST příkazů
      - parametry
- Locale/Unicode útoky
- Útoky na souborový systém
- Přeplnění bufferu

XML Injection, SSI Injection, LDAP Injection, IMAP/SMTP Injection atd.

- **XML injection**: útočník se snaží aplikovat různé druhy XML tagů v SOAP zprávě zaměřené na modifikaci XML struktury
- **SSI injection**: hackování pomocí SSI
  - zaměřen na WWW stránky (typu shtml), které zobrazují uživatelem zadaná data (např. boardy)
- **LDAP injection**: protokol pro ukládání a přístup k datům na adresářovém serveru
  - podle tohoto protokolu jsou jednotlivé položky na serveru ukládány formou záznamů a uspořádány do stromové struktury
- IMAP / SMTP injection

8) XSS (Cross-site scripting)

- Viz předchozí otázka

9) SQL Injection

- Viz otázka číslo 7

10) Google hacking

- Johnny Long – průkopník v oblasti Google Hackingu, autor stejnojmenné knihy

Google Hacking

- termín vytvářející komplexní požadavky pro vyhledávač s cílem filtrovat velké množství výsledku pro informace, které souvisí s pc bezpečností – ty potom slouží k nalezení zranitelných stránek, např. stránky s čísly kreditních karet, s hesly
- lze praktikovat v současné době pomocí kteréhokoli vyhledávače (Seznam, Yahoo, Bing), ale primárně je používán pomocí Google
- **Google cache a proxy**:
  - nedostupné stránky
  - jakás takás anonymita (proxy)
  - další proxy servery je možné najít například pomocí: *inurl: "nph-proxy.cgi" "Start browsing"* -google
- **výpisy adresářů**: útočníkovi přinese informace o hierarchii serveru a přístupu k souborům, které mu pomůžou při dalším útoku (také se využívá při hledání hudby a videa)
  - *intitle: „Index.of.nic“.TXT site:cz* (bude hledat na .cz doméně a jen .txt sobory)
  - *intitle:index.of “Apache/1.2.4 server at”* (získáme informaci o verzi serveru)
  - **klíčová slova**: name, parent directory, admin

- **konkrétní adresáře a soubory**:
  - *intitle:index.of inurl:admin*
  - *intitle:index.of inurl:"/admin/*"*
  - *intitle:index.of apache.log*
  - *intitle:index.of index.php.bak*
- **verze serveru**:
  - intitle:index.of "Apache/1.2.4 server at"
- **sbírání informací**:
  - *site:tuzkarny.cz*
  - *intitle:intranet*
  - *intitle:intranet inurl:intranet +intext:"human resources"* (může zobrazit kontaktní informace)
  - **další zajímavé řetězce**: help desk, how to
- **adresy, poštovní schránky, registry, kamarádi**:
  - *filetype:mbx mbx intext:Subject*
  - *filetype:pst pst (contacts | address | inbox)*
  - *filetype:eml eml +intext:"Subject" +intext:"From"*
  - *filetype:reg reg +intext:"internet account manager"*
  - *inurl:buddylist.blt*
- **domény a subdomény**:
  - *site:tuzkarny.cz -site:www.tuzkarny.cz*
  - *link:www.tuzkarny.cz*
- **přihlašovací stránky**:
  - *"login" "password" "heslo" "jméno"*
  - *allinurl:"exchange/logon.asp" (anonymní přístup)*
  - *intitle:"Tomcat Server Administration"*
  - *inurl:citrix/metaframexp/default/login.asp*
- **jména a hesla**:
  - *filetype:xls username password*
  - *filetype:reg reg +intext:"internet account manager"*
  - *filetype:reg reg HKEY_CURRENT_USER username*
  - *filetype:rdp rdp*
  - *filetype:htpasswd htpasswd*
  - *filetype:pwd service (frontpage)*
  - *intitle:"Index of..etc" passwd*

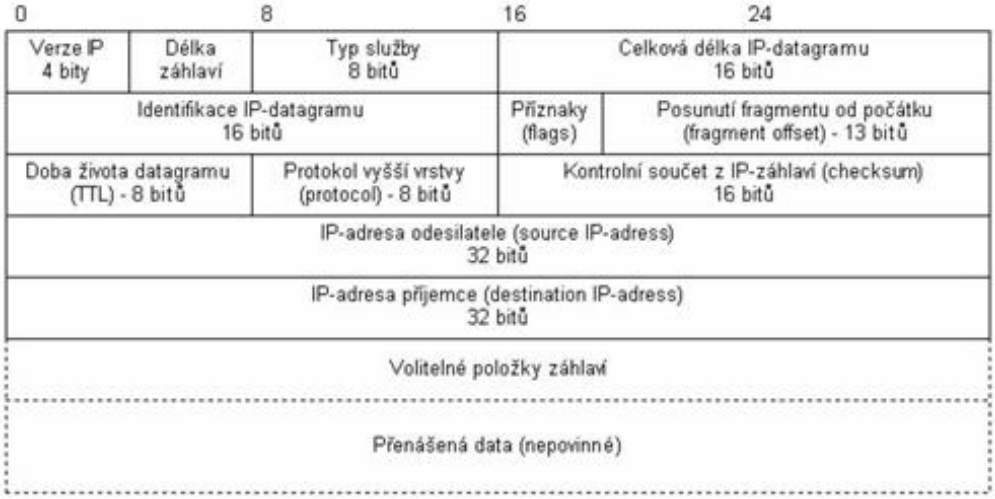
11) Odposlech dat: ethernet, hub, přepínač

- co všechno lze odposlechnout v IP síti? – protokoly HTTP, FTP, TELNET, ICQ apod

struktura IP datagramu

- skládá ze záhlaví a přenášených dat
  - záhlaví má zpravidla 20 bajtů a může obsahovat i volitelné položky – v takovém případě je záhlaví o ně delší
- **IP vrstva**: zabezpečuje přenos dat mezi vzdálenými počítači v internetu
  - základní jednotkou přenosu je IP datagram, který se balí do linkového rámce linkové vrstvy
- **verze IP protokolu (Version)**: obsahuje číslo verze protokolu
  - délka 4 bity
- **délka záhlaví (Header Length)**: max. délka záhlaví IP datagramu, je tedy omezena tím, že položka délka záhlaví má k dispozici pouze 4 bity
- **typ služby (ToS)**: položka, která v praxi nenašla svého naplnění
  - záměr spočíval v jistém nedostatku IP protokolu, jehož podstatou je skutečnost, že v Internetu není zaručena šíře přenosového pásma mezi účastníky
  - délka 8 bitů
- **celková délka IP diagramu (Total Lenght)**: obsahuje celkovou délku IP datagramu v bajtech
  - jelikož je tato položka pouze dvojbajtová, tak maximální délka je 65535 bajtů
  - délka 16 bitů
- **identifikace IP diagramu (Identification)**: obsahuje identifikaci, kou do IP datagramu vkládá operační systém odesílatele
  - tato položka se společně s položkami Příznaky a Posunutí fragmentu využívá mechanismem fragmentace datagramu
  - délka 16 bitů

- **doba života diagramu (TTL)**: slouží k zamezení nekonečného toulání IP datagramu Internetem
  - každý směrovač kladnou položku snižuje alespoň o jedničku – není-li už možné hodnotu snížit, IP datagram se zahazuje a odesílateli je tato situace signalizována protokolem ICMP
  - délka 8 bitů
- **protokol vyšší vrstvy (Protocol)**: obsahuje číselnou identifikaci protokolu vyšší vrstvy, který využívá IP datagram ke svému transportu
  - délka 8 bitů
- **kontrolní součet (Header Checksum)**: obsahuje kontrolní součet, avšak pouze z hlavičky a nikoliv z datagramu celého – jeho význam je tedy omezený
  - délka 16 bitů
- **IP adresa odesílatele a IP adresa příjemce (Source and Destination Adress)**: obsahuje čtyřbajtovou IP adresu odesílatele a příjemce IP datagramu
  - délka obou je 16 bitů



– které části jsou šifrovány a které v otevřené formě?
  - **protokol HTTPS**: nadstavba síťového protokolu HTTP, ká umožňuje zabezpečit spojení mezi webovým prohlížečem a webovým serverem před odposloucháváním a podvržením dat
  - **protokol SSL**: vrstva vložená mezi vrstvu transportní a aplikační, která poskytuje zabezpečení komunikace šifrováním a autentizaci komunikujících stran
  - **protokol SSH**: protokol pro bezpečný přenos souborů pomocí počítačové sítě
    - zároveň i aplikace
  - **protokol TSL**: následovníkem SSL
    - obsahuje několik drobných vylepšení, ale obecné principy zůstávají stejné
  - **protokol RLP**: následovníkem SSL
    - s jeho pomocí se realizují jednotlivá spojení
  - **protokol IPsec (Internet Protokol Security)**: bezpečnostní rozšíření IP protokolu pro bezpečnou komunikaci po internetu

Ethernet

– původně vyvinut firmami DEC, Intel a Xerox pod označením Ethernet II → později standardizován jako norma IEEE 802.3
– původní rozvod Ethernetu byl prováděn tzv. tlustým koaxiálním kabelem
– **ethernetový rámec**:

Název pole	Preambule	Cílová MAC adresa	Zdrojová MAC adresa	Typ/Délka	Data (Výplň)	(FCS)
Délka v bajtech	8	6	6	2	46-1500	4

  - celková maximální velikost rámce (bez Preambule) je 6+6+2+1500+4=1518 bajtů
  - **preambule**: slouží k synchronizaci hodin příjemce
  - **cílová MAC adresa**: MAC adresa cílového síťového rozhraní
    - adresa může být individuální (unicast), skupinová (multicast) a všeobecná (broadcast)
  - **zdrojová MAC adresa**: MAC adresa zdrojového síťového rozhraní

- **typ / délka**: pro Ethernet II je to pole určující typ vyššího protokolu, pro IEEE 802.3 udává délku pole dat
- **FCS kontrolní součet**: 32 bitový kontrolní kód, ký se počítá ze všech polí s výjimkou preambule a FCS
  - slouží ke kontrole správnosti dat – příjemce si jej vypočítá z obdrženého rámce, a pokud výsledek nesouhlasí s hodnotou pole, rámec zahodí jako vadný
- rámec Ethernet se sice liší od rámce Ethernet II pouze v jediném poli Délka
- rámec se šíří na LAN a mění se s různými protokoly vyšší vrstvy. Například IPv4, IPv6, ARP)

Rozbočovač (Hub):

- spojuje několik segmentů sítě do segmentu jednoho (provoz v jedné části sítě se přenese i do částí dalších sítí)
- aktivní prvek fyzické vrstvy, který umožňuje větvení sítě
- veškerá data, která přijdou na jeden z portů, zkopíruje na všechny ostatní porty, bez ohledu na to, kterému portu data náleží → všechny pc v síti „odposlechnou“ všechna síťová data a u větších sítí to znamená zbytečné přetěžování těch segmentů, kterým data ve skutečnosti nejsou určena
- nalezneme je jen ve starších rozvodech, kde je postupně nahrazují switche, které nabízejí vyšší bezpečnost přenášených dat

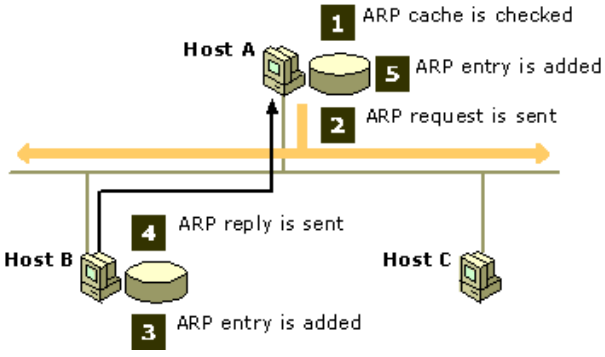
12) Odposlech dat na přepínači

Přepínač (switch):

- typické zařízení druhé (linkové) vrstvy
- částečně ulehčuje práci síťové kartě (a tím pádem i samotnému koncovému zařízení)
- oproti rozbočovači neposílá data na všechny aktivní porty, ale tzv. přepíná
  - implementuje ostatní funkce rozbočovače (především zesílení signálu)
- eliminuje (zmenšuje) kolizní domény
- umožňuje konfigurovat VLAN (resp. umí číst extra velikost rámce s touto informací –viz. standard IEEE 802.11ac)
- pokud se místo rozbočovače umístí jako hlavní aktivní prvek přepínač je každý počítač na síti kolizní doménou jen sám se sebou
- „směruje“ data na příslušné aktivní porty na základě cílové MAC adresy (tzn. data se vysílají jen do rozhraní, jímž je připojen jejich adresát)
- **manipulace se switchem**:
  - **MAC flooding**: útok spočívá v zaplnění CAM tabulky switche a je založen na faktu, že když switch nemá v CAM tabulce cílovou MAC adresu PC, tak paket rozešle na všechny ostatní porty
    - nevýhoda je, že každý switch se zachová na zaplnění CAM tabulky jinak, a podle toho je útok více či méně efektivní
    - útok začíná zaplněním CAM tabulky – to je prováděno posíláním paketů
      - kapacita CAM tabulek se pohybuje od tisíců položek až po statisíce
    - druhou možností je nastavit paketům cílovou MAC adresu příjemce na naší a odchozí generovat náhodně
      - sice přijdeme o možnost zaplnění ostatních switchů, ale náš útok bude téměř nemožné odhalit
  - zaplnění CAM tabulky switche s předpokladem, že při plné tabulce bude switch pakety adresované na neznámou MAC rozesílat na všechny porty

ARP protokol

- jak funguje ARP protokol?
  - překládá adresy IP využívané programovým vybavením založeným na protokolu TCP/IP na adresy řízení přístupu k médiím, se kterými pracuje hardware sítí LAN
  - hostitelům umístěným ve stejné fyzické síti poskytuje následující služby:
    - umožňuje zjistit adresu řízení přístupu k médiím pomocí všesměrově vyslaného



dotazu v podobě otázky: Jaká je adresa řízení přístupu k médiím pro zařízení, u nějž je nastavena přiložená adresa IP?
    - po zodpovězení dotazu ARP uloží odesílatel odpovědi ARP i původce dotazu ARP své adresy IP a adresy řízení přístupu k médiím do místní tabulky nazývané mezipaměť ARP, na kterou se později mohou odkazovat
    - obrázek – postup protokolu ARP při překladu adres řízení přístupu k médiím pro provoz v místní síti
- **ARP Gratuitous Request**: jedná se o dotaz na svou IP adresu
    - tento paket se posílá například při změně IP adresy nebo při spuštění operačního systému
    - slouží ke zjištění, zda není tato IP adresa již obsazena
- **ARP Gratuitous Reply**: zyto pakety se používají pro hromadné otrávení ARP Cache
    - jedná se o normální ARP Reply, kterému nepředcházel ARP Request a MAC adresa příjemce je nastavena na FF:FF:FF:FF:FF:FF
    - přijmou ho všechny počítače na síti, a pokud mají u IP adresy oběti už záznam, změní jej na naší MAC adresu

13) Metody přesměrování datových toků, kvůli odposlechu

DHCP (Dynamic Host Configuration Protocol):

- používáme ke konfiguraci klíčových síťových parametrů jednotlivých klientů
- DHCP server přiděluje počítačům pomocí DHCP protokolu zejména IP adresu, masku sítě, bránu a adresu DNS serveru
- platnost přidělených údajů je omezená, proto je na počítači spuštěn DHCP klient, ký jejich platnost prodlužuje
- **DHCP Spoofing**: útok na přepínané sítě, kdy útočník zapojí do sítě svůj falešný DHCP server, který odpovídá na pakety DHCP discovery a přiděluje stanicím kromě IP adres podvrženou adresu brány a DNS serveru
    - potom bude veškerý provoz od klienta směřovaný ven ze sítě procházet přes útočníkův počítač
    - jde o „Man-in-the-Middle“ útok, protože útočník pak může pakety přeposílat na správnou cílovou adresu, ale přitom může prozkoumat každý paket, který takto zachytil

DNS (Domain Name Service)

- služba sloužící pro překlad doménových jmen na IP adresy a naopak
- doménová hierarchie v internetu má stromovou strukturu
    - kořenem je tečka a prvními podstromy jsou domény prvního řádu (com, org, net, cz, sk atd.)
- má stranu serveru a stranu klienta
    - **server:** spravuje záznamy o doménových jménech v rámci své domény a o serverech spravující nadřazené domény
    - **klient:** klade dotazy na IP adresy na základě doménového jména a naopak, server zná buď odpověď, nebo ví, kde se zeptat.
- **DNS Spoofing**: útok spočívá v podvržení IP adresy v paketu, který se vrací jako odpověď na žádost o překlad doménového jména na IP adresu
    - tento útok už nemusí být pouhá „hračka“ pro odposlech lokální sítě, ale může způsobit přesměrování provozu tisíců uživatelů
    - doba uložení záznamu v DNS Cache je stanovena v odpovědi na dotaz o přeložení doménového jména
    - po vypršení této doby je záznam smazán a při potřebě se provede opětovný překlad
- DNS protokol používá k přenosu dat jak protokol TCP, tak i protokol UDP

ICMP (Internet Control Message Protocol)

- jeden z nejdůležitějších protokolů
- používají ho operační systémy počítačů v síti pro odesílání chybových zpráv, například pro oznámení, že požadovaná služba není dostupná nebo že potřebný počítač není dosažitelný
- liší se od TCP a UDP protokolů tím, že se obvykle nepoužívá síťovými aplikacemi přímo
- **ICMP Redirect (ICMP přesměrování)**: používá se, pokud ze sítě vede k cíli lepší cesta než přes defaultní bránu
    - funguje tak, že stanice pošle datagram své, většinou defaultní, bráně, ta jej přepošle správným směrem a zároveň informuje stanici o lepší cestě

RIP (Routing Information Protocol; směrovací protokol)

- umožňuje routerům komunikovat mezi sebou a reagovat na změny topologie počítačové sítě
- ačkoliv tento protokol patří mezi nejstarší doposud používané směrovací protokoly v sítích IP, má stále své uplatnění v menších sítích a to především pro svoji nenáročnou konfiguraci a jednoduchost

14) WIFI, 802.11

WI-FI 802.11

- jedná se o bezdrátovou komunikaci v počítačových sítích
- samotný název Wi-Fi vytvořilo Wireless Ethernet Compatibility Aliance
- využívá bezlicenčního frekvenčního pásma, proto je ideální pro budování levné, ale výkonné sítě bez nutnosti pokládky kabelů
- pomocí parabolické antény lze signál zachytit na desítky kilometrů

AP (Access Point):

- přístupový bod
- vysílá každých 100ms beacon (administrativní signalizace)
- zařízení, ke kterému se klienti připojují
- klienti spolu nekomunikují přímo, ale prostřednictvím přístupového bodu, takže mohou být jednodušší a nemusí být ve vzájemném rádiovém spojení
- **SSID (Service Set Identifier)**: jedinečný identifikátor každé bezdrátové (WiFi) počítačové sítě
  - přístupový bod (AP) vysílá pravidelně každých několik sekund svůj identifikátor v takzvaném majákovém rámci (beacon frame) a klienti si tak mohou snadno vybrat, ke které bezdrátové síti se připojí
- **WAR driving**: vyhledávání bezdrátových sítí Wi-Fi osobou jedoucí ve voze, pomocí přenosného počítače nebo PDA či smartphone
  - SW pro Wardriving je volně přístupný na internetu, jako třeba *NetStumbler* pro Windows, *Kismet* nebo SWScanner pro Linux, FreeBSD, NetBSD, OpenBSD, DragonFly BSD, Solaris a KisMac pro Macintosh
  - SSID není v žádném případě heslo přístupu k síti
  - v případě uzavřených sítí je hodnota SSID prázdná – klient je však zbaven možnosti roamingu mezi AP
  - vypnutí SSID je proprietární volba a není součástí 802.11
  - otevřená síť: odposlech beaconu
  - uzavřená síť: zachycení legitimní asociace jiného klienta; odeslání podvrženého disasociačního požadavku klientovi
  - **WAR chalking**: jedná se o zjišťování dostupných bezdrátových sítí, které nejsou dostatečně zabezpečeny a informování ostatních "zájemců" o jejich existenci

WEP (Wired Equivalent Privacy):

- označení pro zastaralé zabezpečení bezdrátových sítí podle původního standardu IEEE 802.11 z roku 1997
- nedostatky, ale způsob jak říci, že síť je soukromá (právní důsledky: neoprávněný přístup)
- odposlech je možný v případě zachycení určitého počtu paketů
- 802.11 neřeší správu klíčů (sdílené tajné heslo musí být distribuováno všem uživatelům)
- WEP klíč slouží jak k šifrování dat, tak k autentizaci vůči AP
- cílem WEP bylo poskytnout zabezpečení obdobné drátovým počítačovým sítím (např. kroucená dvojlinka), protože rádiový signál je možné snadno odposlouchávat i na delší vzdálenost bez nutnosti fyzického kontaktu s počítačovou sítí
- byl prolomen v srpnu 2001, a proto by jeho nasazení mělo být nahrazeno zabezpečením pomocí WPA2 podle standardu IEEE 802.11i

WPA (WiFi Protected Access):

- WEP2
- chráněný přístup k Wi-Fi
- obchodní označení pro zabezpečení bezdrátových sítí

- dočasné řešení známých bezpečnostních problémů do doby, než bude hotov standard 802.11i (802.1x, TKIP-Temporal Key Integrity protocol, AES, zabezpečená deautentizace a disasociace)
- WPA je podmnožinou 802.11i (802.1x, TKIP)

TKIP (Temporal Key Integrity Protocol):

- mixování klíče pro každý paket
- vylepšená pravidla generování inicializačního vektoru
- zdokonalená funkce kontroly integrity (Michael)
- pro eliminaci slabých míst – dočasně odstranil problém s inicializačními vektory a zavedl dynamickou správu šifrovacích klíčů, které jsou pomocí něj mezi klientem a přístupovým bodem bezpečně přenášeny nejen na začátku komunikace, ale i během ní
- na straně klienta (počítače připojujícího se k bezdrátové síti) je nasazen tzv. suplikant (prosebník), což je univerzální démon běžící v pozadí na hlavním procesoru počítače a zajišťující autentizaci klienta a správu šifrovacích klíčů pomocí TKIP

IEEE 802.1x

- protokol sloužící k autentizace uživatelů počítačových sítí
- jedná se o fyzickou autentizace
  - pokud je do síťového portu (např. switche) připojeno nové zařízení, je port zablokován (neumožňuje přenos dat) dokud nejsou poskytnuty autentizační údaje (např. uživatelské jméno a heslo)
- nastavuje se na přepínači (tzn. zabezpečení je na druhé vrstvě ISO/OSI modelu)
- uplatňuje se i v bezdrátových sítích, v případech kdy volné připojení by mohlo být snadno zneužito
- problém fyzické zabezpečení připojení k síti
- *princip fungování*: pokud se uživatel připojí na síťový port, má blokovanou veškerou komunikaci kromě EAP protokolu, který zajišťuje autentizace
- **EAP**: autentizace na portech přepínače, ale i v bezdrátových sítích
  - jednoznačná autentizace jednotlivých uživatelů
  - podpora libovolného autentizačniho mechanizmu (MD5, LEAP, TLS, TTLS, PEAP)

WPA2

- implementuje všechny povinné prvky IEEE 802.11i
- přidává k TKIP a algoritmu Michael nový algoritmus CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) založený na AES, který je považován za zcela bezpečný

15) Škodlivý kód, terminologie, prostředí šíření, obranné strategie viru, obrana a detekce, botnety

Terminologie

- **Viry**: malé SW programy určené k šíření z jednoho počítače do jiného a narušování fungování počítače
  - mohou poškodit nebo odstranit data v pc, využít vaši e-mailovou aplikaci k vlastnímu rozšíření do jiných pc nebo dokonce vymazat všechna data na pevném disku
  - nejsnadněji se šíří v přílohách e-mailových zpráv nebo rychlých zpráv
    - nikdy neotevírat přílohy e-mailů, pokud neznáte odesílatele a neočekáváte je
  - mohou být zamaskovány jako přílohy v podobě zábavných obrázků, přání či zvukových souborů a videosouborů
  - šíří se také stahováním z Internetu
    - mohou být skryty v nelegálním SW a dalších souborech či programech, které můžete stáhnout
  - schopen sebe-replikace (množení sebe sama, ovšem za přítomnosti vykonatelného hostitele k němuž je připojen)
  - hostitelem mohou být např. spustitelné (executable) soubory, systémové oblasti disku, popřípadě soubory, které nelze vykonat přímo, ale za použití specifických aplikací (dokumenty Microsoft Wordu, skripty Visual Basicu apod.)
  - jakmile je hostitel spuštěn (vykonán), provede se rovněž kód viru, během tohoto okamžiku se obvykle virus pokouší zajistit další sebe-replikaci a to připojením k dalším vhodným vykonatelným hostitelům

- **Červi**: prvně označen tzv. Morrisův červ
  - v roce 1989 dokázal zahltit značnou část tehdejší sítě, ze které později vznikl Internet
  - sám se šíří – má v sobě mechanismy, aby se mohl sám šířit (
  - pracují na nižší síťové úrovni než klasické viry
  - nešíří se ve formě infikovaných souborů, ale síťových paketů
    - pakety jsou směrovány již od úspěšně infikovaného systému na další systémy v síti Internet
  - šíření červa je postaveno na zneužívaní konkrétních bezpečnostních děr OS, úspěšnost pak od rozšířenosti daného SW obsahující zneužitelnou bezpečnostní díru
  - červy nelze detekovat klasickou formou antivirového softwaru
  - např. SQLSlammer, Lovsan / Blaster, Sasser
  - struktura:
    - vyhledávač obětí (chyby, e-mail adresy)
    - modul šíření infekce (síťový exploit, email:přílohy a odkazy, autorun)
    - rozhraní pro vzdálený přístup
    - rozhraní pro aktualizaci (aktivní, pasivní)
    - funkční část (keylogger, skener, DoS, ...)
    - statistiky
    - hodiny životního cyklu
- **Chobotnice**:
- **Králíci**: programy, klonující sebe sama, obsazovaly systémové prostředky a tak klesala výkonnost systému
  - na přelomu 60. a 70. let
  - většinou nekopíroval své tělo ze systému do sytému, to byly hlavně lokální úkazy
  - hlavní příčinou králíků byly chyby nebo žert systémového programátora
- **Logické bomby**: ničivý kód se spouští až se zpožděním (např. v určité datum či po nakažení určitého počtu jiných hostitelů)
- **Trojští koně**: není schopen sebe-replikace a infekce souborů
  - nejčastěji vystupuje pod spustitelným souborem typu EXE, který neobsahuje nic jiného (užitečného), než samotné „tělo“ trojského koně
  - jedinou formou dezinfekce je odmazání dotyčného souboru
  - *password-stealing trojani (PWS)*: sleduje jednotlivé stisky kláves (keyloggers) a tyto ukládá a následně i odesílá na dané e-mailové adresy
    - majitelé (nejčastěji samotní autoři trojského koně) tak mohou získat i velice důležitá hesla
    - tento typ infiltrace lze klasifikovat i jako spyware
  - *destruktivní trojani*: klasická forma, pod kterou je pojem trojských koní obecně chápán
    - pokud je takový trojský kůň spuštěn, pak likviduje soubory na disku, nebo ho rovnou kompletně zformátuje
    - do této kategorie můžeme zařadit i většinu BAT trojanů, tj. škodlivých dávkových souborů s příponou BAT
    - v tomto případě může překvapit snad jen občasné jednoduché kódování obsahu, díky čemuž není na první pohled zřejmé, co takový kód provádí
  - *downloader (TrojanDownloader)*: další škodlivé programy si nenese s sebou, ale snaží se je stáhnout z Internetu z pevně definovaných adres (url)
    - různé skripty na straně serveru mohou způsobit, že tentýž downloader může nakonec stahovat rozdílný software
  - *proxy Trojan (TrojanProxy)*: infikovaný počítač může být zneužit např. pro odesílání spamu – nevyžádané pošty
    - při využití proxy je téměř nulová šance, že bude vypátrán skutečný autor nevyžádané pošty
- **Zadní vrátka (backdoor)**: aplikace typu klient-server
  - vystupují anonymně, uživatel není schopen jejich přítomnost běžným způsobem vypozorovat
  - slouží pro vzdálenou správu PC a sama osobě nemusí být škodlivá
    - záleží pouze na osobě, která tuto vzdálenou správu vykonává
    - pokud půjde o činnost škodlivou – vzdálený útočník
  - klientská část vysílá požadavky útočníka serverové části, ta tyto požadavky plní, popřípadě odesílá zpět klientu požadované informace
    - klientskou část aplikace by měl vlastnit útočník
    - serverová část by měla být umístěna na pc, kde lze očekávat data
  - pokud je serverová část vypouštěna úspěšně, má vzdálený útočník k dispozici tisíce počítačů, ke kterým může vzdáleně přistupovat
- **Zárodky**:
- **Exploity**:
- **Stahovače**:

- **Droppery a Injektory**:
  - *dropper*: škodlivý program, nejčastěji typu EXE, který po spuštění vypustí do PC další škodlivou havěť, kterou si nese s sebou ve vlastních „útrobách“
  - *injektor*: druh trojského koně
- **Hoax**: poplašná zpráva, která obvykle varuje před neexistujícím nebezpečným virem
  - šíření je zcela závislé na uživatelích, kteří takovou zprávu e-mailem obdrží (přeposlání)
- **Adwre a spyware**:
  - *adware*: znepříjemňuje práci s PC reklamou „vyskakující“ pop-up reklamní okna během surfování, společně s vnucováním stránek (např. výchozí stránka Internet Exploreru), o které nemá uživatel zájem
  - *spyware*: využívá Internetu k odesílání dat z počítače bez vědomí jeho uživatele
    - odcizovány jsou „statistická“ data (přehled navštívených stránek či nainstalovaných programů)
    - činnost odůvodňována zjistit potřeby nebo zájmy uživatele a využívat pro cílenou reklamu
    - šíří se společně s řadou sharewarových programů a jejich autoři o této skutečnosti vědí

Prostředí

- architektura počítače
- procesor
- operační systém
- verze operačního systému
- souborový systém (infekce ISO obrazů)
- formátysouborů (com, exe, NE, PE, DLL, ELF, ovladače, LIB)
- překladač (makro viry, REXX, shell, VBS, mIRC scripty, Jscript, Perl, Python, vim, emacs, TCL, PHP, ABAP, F1)
- autorun.inf
- síťové protokoly
- zdrojové kódy
- debugger
- kompilátor
- Stuxnet

Metody infekce

- **boot viry**: napadají systémové oblasti disku
  - je jich méně než souborových virů, ale vyskytují se častěji
  - *šíří se následujícím způsobem*: když restartujete počítač, který má povoleno zavádění systému z disketové mechaniky a v mechanice je disketa s boot virem, vir se spustí a napadne systémové oblasti pevného disku; při dalším spuštění počítače se boot vir inicializuje z pevného disku a napadá diskety, které uživatel použije
- **infekce souborů**: jsou napadnuté především soubory, které obsahují prováděný kód – programy
  - v napadeném programu přepíší část kódu svým vlastním, nebo vlastní kód k programu připojí a tím změní jeho velikost a chování
- “zavěšování”:
- infekce paměti:

Obranné strategie

- tunelování
- použití nedokumentovaných funkcí
- kódování dat (antivir musí mít dekodér)
  - oligomorfní viry
  - polymorfní
- Metamorfní viry (polymorfizmus těla)
- ochrana proti debuggeru (sledování zásobníku,...vypínání klávesnice)
- ochrana proti emulaci
- retroviry

Botnety

- označení pro softwarové agenty nebo pro internetové roboty, kteří fungují autonomně nebo automaticky
- v současné době je termín nejvíce spojován s malware, kdy botnet označuje síť počítačů infikovaných speciálním software, který je centrálně řízen z jednoho centra → Botnet pak provádí nežádoucí činnost, jako je rozesílání spamu, DDoS útoky a podobně

Bezdrátová zařízení

- zákeřný kód šířený pomocí software
- pomocí chyby
- podvodné dialery
- rekonfigurace zařízení (DNS,...)

Obrana a detekce

- antiviry
- aktualizace
- zabazpečení systému
- zabezpečení síťové infrastruktury
- detekce
  - honeypoty (wormradar, mwcollect)
  - detekce (wireshark, snort)

16) Anonymní přístup k Internetu

Jaké stopy zanecháváme a kdo všechno má tyto informace k dispozici

- Nemusí být až tak důležité „co , ale spíše „kdo s kým , neboli kam se zrovna připojujeme, co si prohlížíme a s kým komunikujeme. A tohle „kdo s kým je s rostoucí uživatelskou přívětivostí technologií na první pohled zcela pod kontrolou uživatele. Vždyť adresář je bezpečně uložen v e-mail klientu, nebo WEB prohlížeči. Po d povrchem uživatelského rozhraní je však všechno jinak. Komunikace probíhá ve velké většině případů IP protokolem, do kterého jsou zapouzdřeny TCP segmenty a UDP datagramy.
- Pole:

  IP adresa zdroje, Cílová IP adresa IP datagramu
  Zdrojový port, Cílový port UDP datagramu
  a Zdrojový port, Cílový port TCP segmentu
  jsou z hlediska „kdo s kým kritická

- Je zřejmé, že uvedené pakety poskytují informace o tom jaké zařízení s kterým dalším zařízením komunikuje, a kterou službu používá. Také není příliš obtížné zjistit, komu dané adresy a provozované služby patří. A to buď z veřejných zdrojů (WHOIS, Google, apod.), nebo v databázích telekomunikačních firem.
- Co se týče elektronické pošty, jsou v hlavičkách e-mailů zaznamenávány adresy o desílatele, příjemce i jména serverů, přes které dopis pro cházel:

  Return-Path: <apache@staff.ipex.cz>
  Received: from adriana.gin.cz (mx.ipex.cz [212.71.175.4])
  by icicle.brehovsky.cz (8.12.8/breh) with ESMTP id l0OFtQSx010932
  for <fantomas@brehovsky.cz>; Wed, 24 Jan 2007 16:55:26 +0100
  Received: from staff.ipex.cz (farm1-dg.ipex.cz [212.71.175.26])
  by adriana.gin.cz (Postfix) with ESMTP id 16E4EDC057
  for <fantomas@brehovsky.cz>; Wed, 24 Jan 2007 17:00:26 +0100 (CET)
  Received: by staff.ipex.cz (Postfix, from userid 48)
  id 088CC100C203; Wed, 24 Jan 2007 17:00:23 +0100 (CET)
  To: fantomas@brehovsky.cz
  From: info@ipex.cz

- Tyto informace jsou uchovávány nejen v lozích klientů a serverů, ale některé také na routerech poskytovatelů připojení (ISP, zaměstnavatel) a poskytovatelů infrastruktury, na zařízeních zaměstnavatele a samozřejmě putují po síti, takže k nim má přístup každý, kdo je schopen je odposlechnout.
- Navíc existují metody analýzy datových toků pomocí kterých se lze pokusit na základě paternů nalezených v komunikaci odvodit přenášené informace, nebo alespoň jejich charakter. A to i v případě šifrovaných dat.
- Úvahu o tom, kdo všechno má, nebo může mít tato data k dispozici a k čemu je může použít, nechť provede každý sám.

Běžná opatření

- V první řadě je vhodné analyzovat data, která náš po čítač po připojení do sítě opouštějí i ta, která na něj přicházejí. Kromě dat o kterých víme, to může být například
  - automatické odesílání registrací aplikací
  - automatická kontrola dostupnosti nových aktualizací
  - automatické o desílání popisů chybových stavů (bug report)
  - atd.
- O datech o desílaných addwarem, a podloudně nainstalovanými trojskými koni ani nemluvě.
- Nevyhovuje ani implicitní konfigurace prohlížeče. Pokud si chceme zachovat alespoň minimální soukromí, měli bychom například v prohlížeči Mozilla nastavit následující:
  - Zapnout filtrování popup oken
  - Zakázat Javu
  - Neodesílat skutečnou e-mail adresu ftp serverům
  - Neakceptovat cookies, nebo alespoň zapnout varování a analyzovat je
  - Zakázat animace
  - Neukládat data z formulářů
  - Neukládat hesla
  - Neinstalovat Flash plugin
- Kontrolu nad daty plynoucími z našeho počítače a přicházejícími ze sítě můžeme zvýšit instalací lokálního proxyserveru. Vhodným se zdá například Privoxy (http://www.privoxy.org/), kerý dovoluje:
  - filtrování toků dat
  - manipulaci s cookies
  - řízení přístupu
  - blokování bannerů, adware, popup oken apod.
- Samozřejmostí je firewall, který je nastaven tak, aby blokoval veškeré pokusy o připojení přicházející zvenčí a odchozí data přesměrovával na proxyserver.
- Jako poslední krok nelze nedoporučit kontrolu komunikace síťovým analyzátorem. Rychlý přehled umožňuje například Etherape (http://etherape.sourceforge.net/).

Anonymní remailery

- Popis technologií zvyšujících soukromí začneme remailery, které jsou schopné ho zaručit v maximální míře. Je to možné díky dávkové povaze zpracování e-mailů. Jak uvidíme v dalších kapitolách, je stejný úkol v případě interaktivních protokolů mnohem složitější.
- Základní princip anonymizace elektronické zprávy spočívá v tom, že zprávu odešleme na speciální poštovní server (remailer) ve formě žádosti o doručení na cílovou adresu. Remailer (nebo systém remailerů) naši zprávu přepošle adresátovi s tím, že změní odchozí adresu (naši e-mail adresu) na adresu vygenerovanou a obě adresy uloží do interní databáze. Příjemce zprávy tedy dostane e-mail přicházející z adresy vygenerované remailerem. Pokud na tuto adresu o dpoví, odpověď dojde remaileru, ten nahradí generovanou adresu, skutečnou adresou (na jde ji uloženou v databázi) a dopis přepošle zpět původnímu odesílateli.
- Protože jsou žádosti o přeposlání obvykle šifrovány, ISP neví komu e-mail ve skutečnosti odesíláme, a protože je odchozí adresa generována remailerem, příjemce neví od koho dopis ve skutečnosti pochází.
- Anonymní remailery dělíme na pseudoanonymní (princip popsaný výše) a anonymní (opravdu anonymní).
- Pseudoanonymní remailery (nym servery) jsou založeny na důvěře provozovateli serveru. Tzn. musíme věřit technickým dovednostem a personální integritě provozovatele, který musí zajistit bezpečnost (nedostupnost) logů a záznamů v databázi remaileru. Velmi poučná je z tohoto hlediska historie remaileru
- V případě pseudoanonymního remailerů, musíme také po čítat s tím, že veškeré naše transakce s remailerem budou logovány na zařízeních mezi námi a remailerem, logovány samotným remailerem a linkovány na náš přístupový bod do Internetu (telefonní číslo, port přepínače ISP, port DSLAMu apod.).
- Oproti tomu anonymní remailery realizují anonymitu principiálně, takže nezávisí na lidském faktoru, nebo slabosti jednotlivého prvku architektury. Rozlišujeme remailery tří typů:
  - Typ I – Cypherpunk

  - Typ II – Mixmaster
  - Typ III – Mixminion
- Remailery typu I akceptují zprávy zpravidla šifrované pomocí PGP, nebo GPG, z jejichž hlaviček odstraňují všechny informace, které slouží k identifikaci odesílatele.
- Cílová adresa (adresa příjemce je specifikována uvnitř zašifrované zprávy).
- Zpráva může být odesílatelem směrována přes několik remailerů aby byla snížena pravděpodobnost o dhalení odesílatele, přičemž dochází k dalšímu šifrování zpráv (přidání další vrstvy, tentokrát s cílovou adresou následujícího remaileru v řetězci).
- Na odeslanou zprávu nelze o dpovědět, protože původní adresa odesílatele se nikde neuchovává.
- Remailery typu II odesílají zprávy rozdělené na pakety, které putují v pozměněném pořadí. Je tak ještě ztíženo trasování zprávy.
- Je možné uměle zadržovat zprávy na jednotlivých serverech, takže je velmi složité odhadnout zda uživatel A odeslal zprávu uživateli B i když jsou oba pod kontrolou (analýza časů odeslaných a přijatých e-mailů).
- Oproti typu I však k o deslání zprávy potřebujeme specializovaného poštovního klienta.
- Typ III se skládá z množství serverů (mixes), které přijímají zprávy rozdělené na pakety konstantní velikosti, přehazují jejich pořadí a odesílají je dále směrem k příjemci.
- Každý paket putuje přes síť serverů jinou cestou, a ani jeden ze serverů tak nezná vazbu:

  původní odesílatel – konečný příjemce

- Jednotlivé pakety jsou na každém serveru rozšifrovány, poté je identifikován další server v řetězci a před odesláním znovu šifrovány veřejným klíčem dalšího serveru.
- Mixminion navíc umožňuje o desílat zprávy anonymním příjemcům (odesílatel není schopen identifikovat příjemce zprávy) a je navržena integrace s nym servery.

Proxy servery

- V případě interaktivních protokolů je o chrana soukromí realizována pomocí anonymizujících proxy serverů.
- Myšlenka je podobná jako u nym serveů. Nenapo jujeme se přímo na server poskytující službu, ale na proxy server, který spojení s cílovým serverem zprostředkuje. Cílový server tak nezná IP adresu klienta (vidí pouze že se na něho připojuje proxy server) a poskytovatel připojení vidí, že se uživatel připojuje na proxy server, a není tedy schopen určit cílovou službu (pouze v případě, že nepřečte z datového toku http příkaz CONNECT).
- Existuje řada anonymizujících proxy serverů pro HTTP/HTTPS, (http://www.findproxy.org/).
- Bezpečnost tohoto řešení je však přibližně na stejné úrovni jako pseudoanonymní remailer, řada veřejných proxy serverů podporuje pouze http a použití jiných protokolů je značně problematické, ne-li nemožné.
- Tyto nedostatky o dstraňuje TheOnionRouter – TOR (http://www.torproject.org/)

Tor a další anonymizery služeb s nízkou latencí

- Tor je síť serverů která umožňuje zachovat soukromí během přístupu k WEB serverům, publikování dokumentů, komunikaci pomocí IRC, instant messagingu, ssh a dalších aplikacích komunikujících pomocí TCP protokolu.
- Tok dat je směrován o d klienta k serveru a zpět, skrz síť serverů tak, aby ISP na straně klienta nebyl schopen určit s kterým serverem klient komunikuje a aby server nedovedl tohoto klienta identifikovat.
- Tor je v současné době pravděpo dobně nejdokonalejší síť tohoto typu.
- Požadavek na nízkou latenci přenášených služeb umožňuje určité typy útoků, ale nebezpečí jejich dopadu na běžného uživatele, který chce pouze zvýšit své soukromí při práci s Internetem je minimální.
- Tor navíc dovoluje definovat takzvané skryté služby, které umožňují publikovat informace (například na WEB serveru) aniž by kdokoli mohl určit, kde se daný WEB server ve skutečnosti nachází.
- Dalším příkladem anonymizační sítě může být síť I2P

Darknets, DeepWeb a Dark Internet

- Obecně jsou **darknets** sítě, určené pro sdílení informací mezi účastníky, kteří si přejí zachovat anonymitu.
- Většinou se jedná o sítě, které jsou dostupné pouzepro konkrétní skupinu lidí, tzn. „zbytek světa„ do nich nemá přístup. Jedná se vlastně o Internet uvnitř Internetu. Příkladem implementace takové sítě může být Freenet (http://freenetproject.org/).
- **DeepWeb** jsou v po dstatě WEB servery, na které nevedou linky a jejichž obsah lze jen těžko indexovat vyhledávači.

- Toho lze dosáhnout například vygenerováním obsahu stránek na základě formy dotazu z dat uložených v databázích, zveřejněním pouze netextových dokumentů, zaheslováním přístupu ke stránce apod.
- **Dark Internet** je adresní prostor IP protokolu, který není dostupný z Internetu. Nejedná se o privátní adresní prostor tak jak ho známe z RFC 1918, ale o běžné adresy, které nejsou dostupné z důvodu chybné konfigurace routerů, výpadků technologie, nebo zákeřných záměrů.
- S rostoucí dostupností síťových technologií (např. 802.11) začína jí vznikat sítě, které nevyužívají síťovou infrastrukturu Internetu, ani infrastrukturu telekomunikačních operátorů ale jsou vybudovány na infrastruktuře vlastní.

17) Sociální inženýrství

- způsob manipulace lidí za účelem provedení určité akce nebo získání určité informace
- termín je běžně používán ve významu podvodu nebo podvodného jednání za účelem získání utajených informací organizace nebo přístup do informačního systému firmy
- ve většině případů útočník nepřichází do osobního kontaktu s obětí
- **techniky**:
  - **Pretexting**: je utváření a využívání vymyšleného scénáře s cílem přesvědčit oběť k učinění potřebné akce nebo k získání potřebné informace
    - skloubení lži s kouskem pravdivé informace získané dříve
    - může se jednat například o datum narození, rodné číslo, velikost posledního účtu, jméno nadřízeného atd.
    - cílem je přesvědčit oběť o legitimnosti akce, která je po ní požadována
    - lze použít při vydávání se za kolegu z práce, policejního vyšetřovatele, bankovního úředníka, zaměstnance finančního úřadu či jiného zaměstnance státní správy, který by mohl mít právo na dotazování dané oběti
  - **Phishing**: mámení přístupových hesel
    - způsob, jak se útočník snaží získat citlivé informace (uživatelská jména, hesla a údaje o kreditní kartě) vydáváním se za důvěryhodnou osobu v elektronické komunikaci
    - principem je rozesílání e-mailových zpráv, které se tváří jako oficiální žádost banky či jiné podobné instituce a vyzývají adresáta k zadání jeho údajů na odkazovanou stránku
    - obrana: nepřistupovat bez rozmyslu k jakémukoli WEBu, neotvírat bez rozmyslu přílohy e-mailů
  - **Baiting**: může být považován za trojského koně v reálném světě
    - útočník nechá infikované CD, flashdisk nebo jiné paměťové médium na místě, kde jej oběť s velkou pravděpodobností nalezne, například v koupelně, ve výtahu, na parkovišti → poté již nechá pracovat zvědavost, se kterou oběť dříve či později vloží toto médium do svého počítače → dojde k instalaci viru, za pomoci kterého získá útočník přístup k počítači nebo celé firemní počítačové síti