IP adresa

- Kdokoliv vám umožnil používat IP adresu z jeho rozsahu, ví že to umožnil právě vám
- Rozsahy IP adres jsou přidělovány jednotlivým ISP a toto rozdělení je zaznamenáno – kdo má co přiděleno
- ISP vám potom buď přímo přidělí konkrétní IP adresy
- Anebo vám je jeho DHCP server přidělí podle vaší MAC adresy, která je pro daný segment jedinečná
- Navíc je obvyklou praxí, aby jste používali modem vašeho ISP, takže ISP pak přesně ví, který zákazník měl v dané době kterou IP adresu

- Předpis č. 485/2005 Sb. ze dne 15. 12. 2005
  - http://www.sagit.cz/pages/sbirkatxt.asp?zdroj=sb05485&cd=76&typ=r

§ 2

Rozsah uchovávání provozních a lokalizačních údajů

(1) Právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací (dále jen "provozovatel") poskytuje orgánu oprávněnému k jejich vyžádání (dále jen "oprávněný orgán") touto vyhláškou vymezené provozní a lokalizační údaje (dále jen "údaje").

(2) U sítí elektronických komunikací s přepojováním okruhů a pevným připojením se uchovávají
a) údaje o uskutečněné komunikaci s uvedením typu komunikace, telefonního čísla účastníka volajícího a volaného nebo identifikátoru telefonní karty pro použití ve veřejném telefonním automatu, data a času zahájení komunikace, délky komunikace, případně stavu komunikace,
b) údaje o všech veřejných telefonních automatech s uvedením jejich telefonního čísla, evidenčního čísla, geografické souřadnice a slovního popisu umístění.

(3) U veřejných mobilních telefonních sítí elektronických komunikací se uchovávají
a) údaje o uskutečněné komunikaci s uvedením typu komunikace, telefonního čísla účastníka volajícího a volaného, data a času zahájení komunikace, délky komunikace, čísla IMEI, čísla stanice StartBTS, popřípadě čísla stanice StopBTS, destinace a doplňkové informace,
b) údaje o vzájemných vazbách mezi čísly MSISDN a čísly IMEI společně použitými v síti, identifikace stanice BTS a čísla IMEI, které zprostředkovaly volání bez SIM karty na číslo tísňového volání "112", IP adresy terminálů, kterými bylo zprostředkováno odesílání zpráv SMS sítí Internet, datum a čas dobíjení kreditu u předplacených služeb, čísla dobíjecích

kuponů k určitému telefonnímu číslu účastníka, telefonní číslo účastníka k určitému dobíjecímu kuponu,
c) údaje o všech stanicích BTS s uvedením jejich čísla, geografické souřadnice, azimutu směrování antén a slovního popisu umístění stanice BTS.

(4) U sítí elektronických komunikací s přepojováním paketů se uchovávají údaje o uskutečněné komunikaci
a) u služeb přístupu k síti s uvedením typu připojení, identifikátoru uživatelského účtu, identifikátoru zařízení uživatele služby, data a času zahájení připojení, data a času ukončení připojení, zájmových identifikátorů (například IP adresa, číslo portu), statusu události (například úspěch, neúspěch, řádné nebo mimořádné ukončení připojení), množství přenesených dat (v příchozím směru/v odchozím směru),
b) u služeb přístupu ke schránkám elektronické pošty s uvedením identifikátoru zájmového uživatelského zařízení, uživatelského účtu, identifikátoru zprávy na poštovním serveru, data a času zahájení komunikace, adresy elektronické pošty odesílatele, adres elektronické pošty příjemců, identifikátoru protokolu elektronické pošty, množství přenesených dat, informace o použití zabezpečené komunikace,
c) u služeb přenosu zpráv elektronické pošty s uvedením identifikátoru zájmového uživatelského zařízení, identifikátoru serveru elektronické pošty, data a času zahájení komunikace, adresy elektronické pošty odesílatele, adres elektronické pošty příjemců, identifikátoru protokolu elektronické pošty, množství přenesených dat, informace o použití zabezpečené komunikace,
d) u serverových služeb s uvedením identifikátoru zájmového uživatelského zařízení, identifikátoru uživatelského účtu, data a času požadavku na službu, veškerých identifikátorů serveru (zejména IP adresa, úplné doménové jméno FQDN), požadovaných identifikátorů URI nebo typu služby, dodatečných parametrů identifikátorů URI nebo služby, použité služby, množství přenesených dat, metody a statusu požadavku na službu,
e) u dalších služeb elektronických komunikací (zejména u služeb typu chat, usenet, instant messaging a IP telefonie) s uvedením veškerých identifikátorů komunikujících stran, transportního protokolu, data a času zahájení komunikace, data a času ukončení komunikace, použité služby, množství přenesených dat.

- Jak je možné zjistit, např. kterou e-mailovou schránku používáte, a to bez vašeho vědomí?
- Analýzou odposlechnuté, soukromé komunikace na úrovni aplikačního protokolu
  - U nezašifrované komunikace to není žádný problém
  - A u zašifrované?
    - Viz útok Man in the Middle
    - Je zaznamenáno, zda jste použili zašifrovanou komunikaci
      - Viz důvody vzniku anonymních p2p sítí

- Bez anonymní p2p sítě anonymita ani soukromí na Internetu neexistuje
  - Když ale použijete anonymní p2p síť, popř. jiný anonymizační prostředek
    - Přistupujete na konkrétní IP adresy, kterými se dostanete k anonymizačním službám
    - Používáte pro ně vyhrazené porty
    - Přenášíte zvýšený objem dat
    - Používáte šifrování
    - Jinými slovy, v současné době vyčníváte z davu
  - Otázka zní, jak si uchovat anonymitu vůči někomu, kdo nemá takové možnosti

Stopy

- Odesíláte-li e-mail, poštovní server do jeho hlavičky napíše cestu, kdy e-mail šel
- Píšete-li na webové fórum, u příspěvku po sobě zanecháváte IP adresu
- U většiny počitadel návštěvnosti získáte i cookie, která vás identifikuje i po změně IP adresy
- Navštívíte-li nějaký server, zanecháte v jeho logu IP adresu

```
127.0.0.1 - frank [10/Oct/2000:13:55:36 -0700]
"GET /apache_pb.gif HTTP/1.0" 200 2326
```

http://httpd.apache.org/docs/1.3/logs.html

- Prohlížeč sám od sebe jen tak nemaže historii stránek
  - Kterou pak lze porovnat s logem serverů

- HTTP referer – identifikuje stránku, ze které jste přišli
  - Máte jako výchozí stránku vašeho prohlížeče svou prezentaci?
    - http://home.zcu.cz/~**login**
    - http://profil.lide.cz/profile.fcgi?akce=profile&user=**jmeno**
  - A co třeba pošta?
    - http://mail.centrum.cz/~~cook~**uživatel**/?js=1&nlogout=0&hp=1

- Vlastníte doménu druhého řádu?
  - Registr WHOIS na vás prozradí např. vaše jméno

- Používáte veřejnou IP?
  - Registr RIPE prozradí vašeho ISP

- Např. ftp server po vás může chtít jako heslo vaši e-mailovou adresu
  - Proč mu ho dávat, když si lze vymyslet neexistující FQDN a to použít?

- ICQ, Skype, p2p, etc.
  - Máte-li povolenou přímou komunikaci, pak v rámci přenosu sdělujete veřejnou IP adresu, kterou používáte

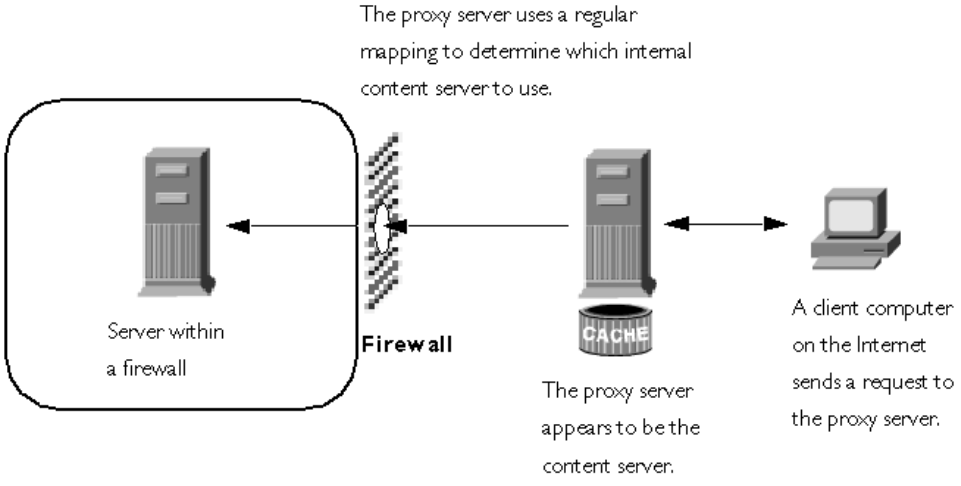
- Lze zanechat i další stopy jako e-mail, OpenID, telefon, nebo dokonce poštovní adresu
  - Ale to už je o zdravém rozumu uživatele

Proxy servery

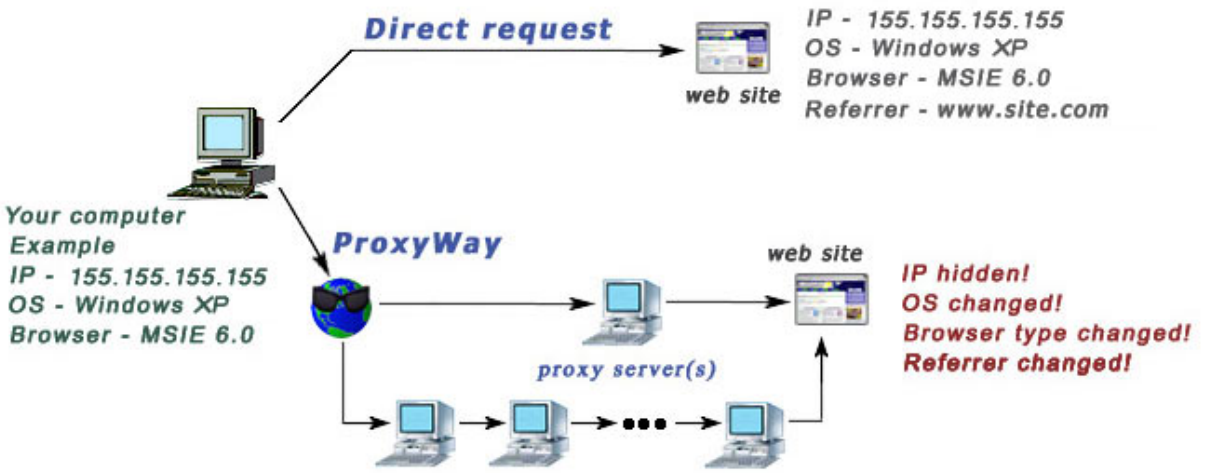
- Prostředník mezi klientem a cílový serverem
- Klient nekomunikuje s cílovým serverem, ale s proxy serverem
- Cílový server nekomunikuje s klientem, ale s proxy serverem, kterého považuje za klienta
- A tak nevidí IP adresu klienta, dokonce o něm ani neví
  - Pokud se pochopitelně uživatel neprozradí jinak
- Proxy serverů může být několik v řadě

- Další možností, jak skrýt svou IP adresu je zfalšování hlavičky IP paketu
  - Stejně jako lze zfalšovat odesílatele e-mailu
  - Je to pouze otázka použitého sw nástroje
  - Má to však zásadní problém a sice, že když podvrhneme IP adresu, na které neposloucháme, tak nedostaneme odpověď

  - HTTP používá TCP a TCP používá tzv. handshake, tj. výměna několika IP paketů, k navázání spojení
    - Když nedostaneme odpověď, nemůžeme ho navázat



http://docsrv.sco.com/INT_Proxy/revpxy.htm



http://www.proxyway.com/www/hide-my-IP/hide-my-IP.html

- Na nějakém „obskurním“ webu se vám může stát, že vás zablokují za psaní názorů, které se neshodují s vedením webu
  - Pokud vás blokují podle IP adresy, přes proxy server se tam stejně dostanete
    - Jejich server uvidí jinou IP adresu

- Každý prohlížeč navíc posílá svůj identifikační řetězec a info o vašem systému
  - Mozilla (compatible: IE 6)
  - Proxy server pošle svoje, ne vaše
    - Tohle lze ovšem podvrhnout i bez proxy

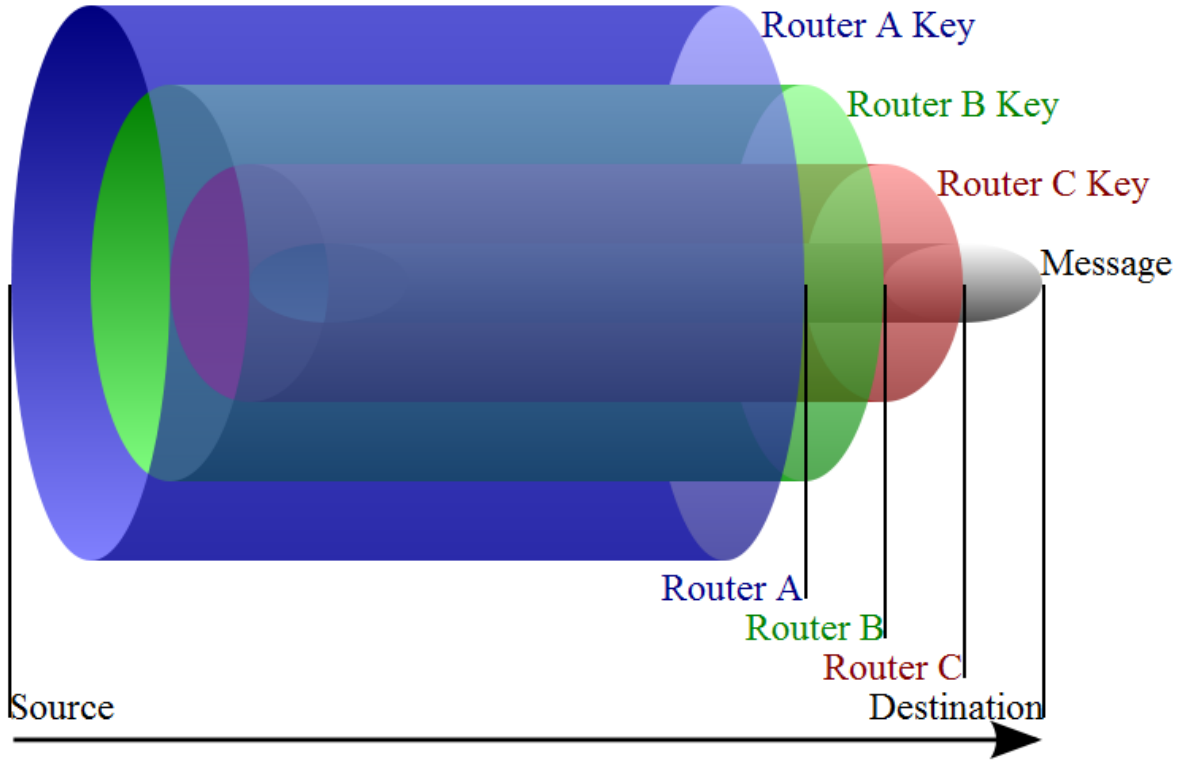
- Ovšem, kdo vlastně provozuje takový server?

Anonymní mailer

- Je třeba splnit dvě věci:
  - Použít proxy server, aby poštovní server neviděl IP adresu klienta
  - Použít takový poštovní server, aby se uživatel nikde nemusel prokázat svým jménem a heslem

Onion Routing

- TOR, JAR, FreeHaven
- Ačkoliv je méně odolný proti útoku než anonymní p2p sítě, zdá se být rozšířenější



http://en.wikipedia.org/wiki/Onion_routing

- Zpráva se zašifruje do několika vrstev
- Každá vrstva je zašifrována jiným heslem
- Jednotlivé vrstvy jsou určeny pro konkrétní routery
- Router přijme zprávu, dešifruje svou vrstvu a z ní se dozví, kterému dalšímu routeru předat zprávu dál

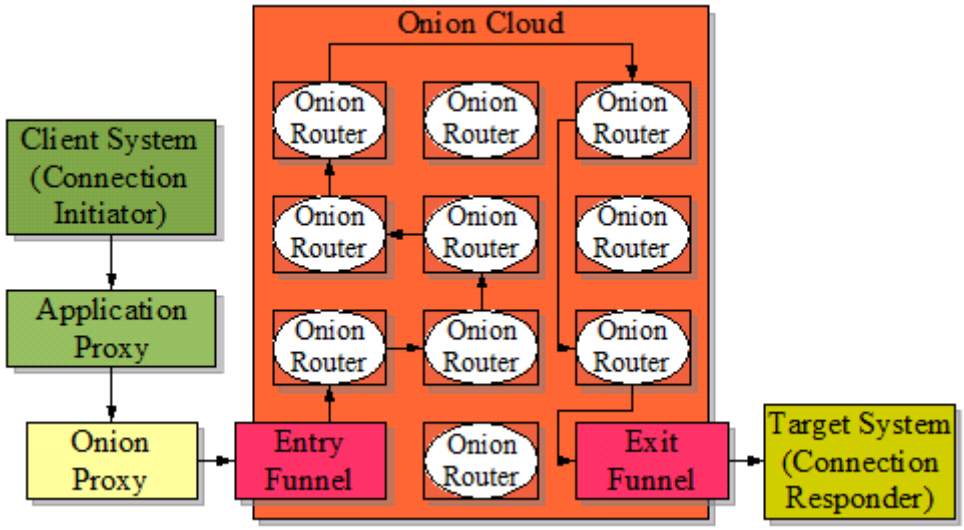
- Výchozí uzel stanoví cestu sítí a zašifruje jednotlivé vrstvy veřejnými klíči, zatímco routery k nim mají privátní klíče
    - A tak jsou jediní, kdo mohou vrstvu dešifrovat

http://www.iusmentis.com/society/privacy/remailers/onionrouting/

- Síť má vstupní a výstupní body
  - Entry Funnel
  - Exit Funnel

- Je-li uživatel mimo síť, musí navázat spojení se vstupním bodem, který už pak jeho zprávu pošle sítí

- Běžný uživatel mimo síť je nejméně odolný proti útoku, protože vždy komunikuje s jedním, konkrétním uzlem
- Chová-li se uživatel jako router, pak přes něj prochází řada zpráv je obtížnější určit, která byla pro něj

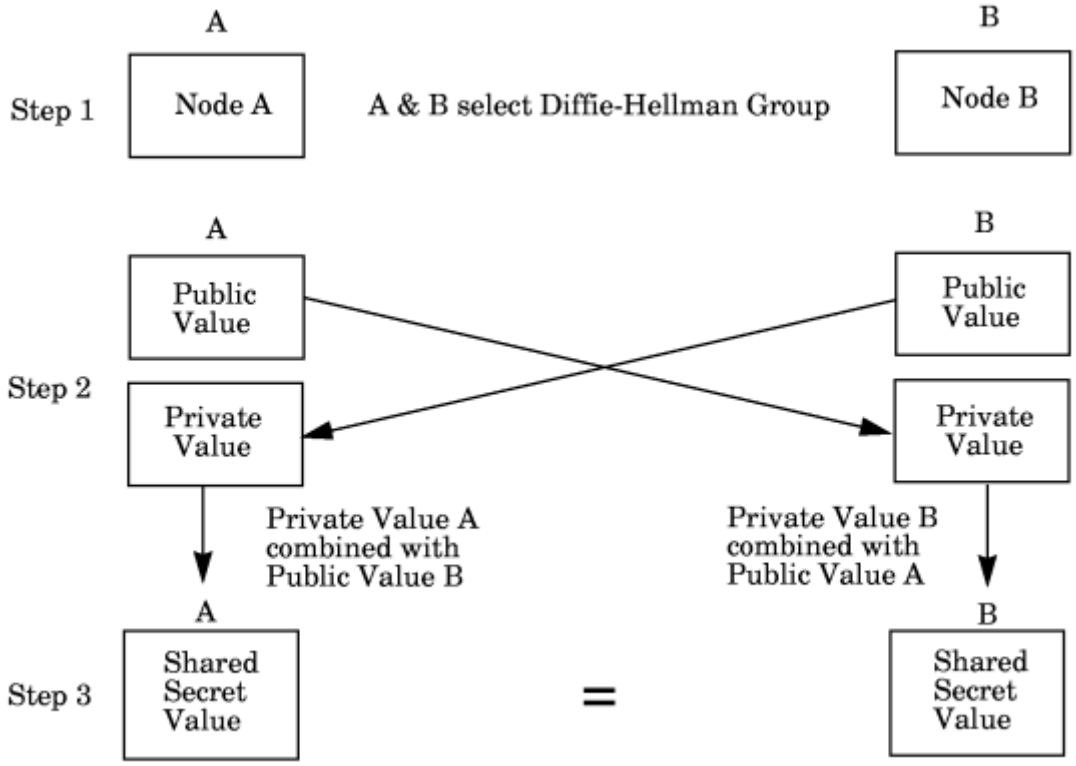


http://ntrg.cs.tcd.ie/undergrad/4ba2.05/group10/index.html

- Je-li však routek cílem zprávy, zpráva u něj končí
  - => Stopa
  - Anonymní p2p síť je odolnější, protože její uzel zprávu vždy přepošle dál, i když byl jejím cílem

Dva nezávislé komunikační kanály

- Máme-li k dispozici veřejný komunikační kanál, např. obyčejné připojení od ISP, můžeme sice pomocí Diffie-Hellman dohodnout tajné heslo pro šifrovaný přenos mezi dvěma stranami, ale
- Nikdy to nebude odolné proti útoku Man in the Middle



http://docs.hp.com/en/J4255-90011/ch04s04.html

- Viz přednáška o bezpečnosti
  - Je možné, aby se útočník vydával za uzel C, který pak naváže dvě zabezpečená spojení s uzly A a B
    - A – C – B
    - Zatímco A a B si budou myslet, že komunikují přímo spolu

- Uzly A a B sice mohou nasadit autentizaci, aby ověřily své identity, ale čeho dosáhnou?
- Pouze toho, že zjistili narušitele, ale nedokážou s tím nic udělat
    - => tj. nedokážou vytvořit bezpečný kanál

- Řešením je použití nezávislého komunikačního kanálu
    - Který sice může být pomalý, pro další použití nevhodný,
    - Ale který umožní přenést první informace zabezpečenou cestou

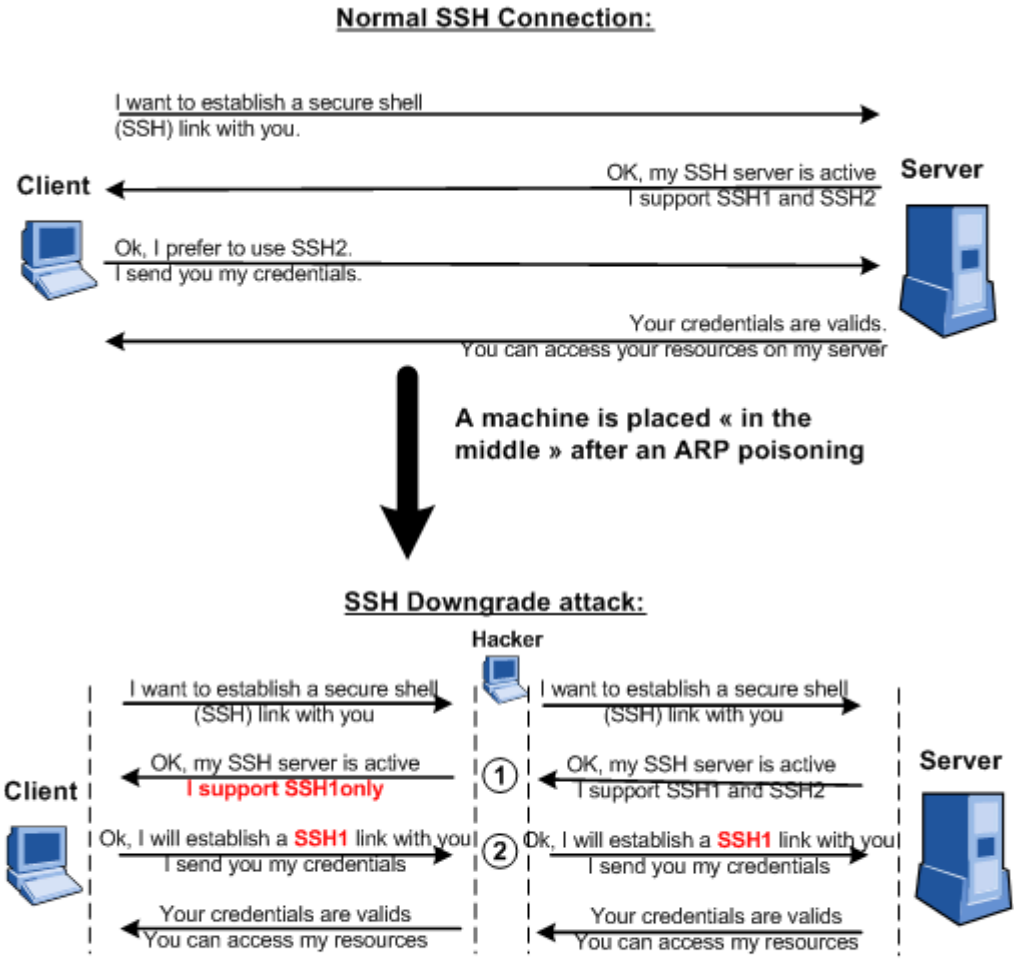
- Např. administrátor SSH2 serveru fyzicky přijde k serveru, který konfiguruje, a nahraje tam, např. z USB disku, svůj veřejný klíč

- V okamžiku, kdy se k serveru připojí, data zašifruje svým privátním klíčem a nikdo po cestě není schopen je dešifrovat, až na cílový server, kterému byl doručen veřejný klíč bezpečnou cestou

- Při zakládání konta dalším uživatelům se už použije tento zabezpečený kanál, k nahrání klíčů jednotlivých uživatelů
    - Tj. druhý kanál stačilo použít pouze jednou

- Používání klíčů se říká i „přihlašování se certifikátem“
- Ke klíči existuje i passphrase
    - Heslo, které je třeba zadat, aby s ním bylo možné dále pracovat – pojistka na lokálním počítači

- Je však třeba dodržet i další bezpečnostní opatření
- Použití dvou kanálů nemá cenu např. u SSH1
- Je třeba být v zabezpečení důsledný



1. The hacker changes the server response from 1.99 to 1.51
2. The credentials are captured by the hacker because ot the ssh1 weak password authentication mechanism.

http://www.openmaniak.com/ettercap_filter.php

- Dalším příkladem může být bankovní spojení
  - Zde už nejde o uchování si anonymity, ale naopak o jednoznačné prokázání identity
    - Tj. aby někdo anonymně nemohl provádět platby z našeho účtu

- Nezávislý kanál může být např. ověřovací kód zaslaný sms zprávou
  - Vzhledem k realizaci zasílání sms ho ale stěží lze považovat za bezpečný – je-li potřebný hw…

- Navíc, sms se pošle na sms bránu po IP
  - A co když banka použije tu samou bránu pro sms i HTTPS komunikaci?

- Daleko bezpečnější forma autentizace je sada kódů, které si osobně odnesete z banky

Spyware

- Jakýkoliv sw, který se snaží zjistit cokoliv o vás, či vaší činnosti
  - Samozřejmě i bez vašeho vědomí

  - Např. keylogger monitorující které klávesy jste kdy stiskli
    - Tj. i když použijete bezpečný kanál, nějak jste tu zprávu do počítače dostat museli

- Spyware nemusí dělat něco na první pohled nebezpečného
  - Jako prohledávat disk v honbě za soubory, které obsahují hesla a jiné přístupové kódy

- Může také jenom sledovat vaše zvyky a obliby
- A pak vám za využití sociálního inženýrství nabídnout něco ke koupi, tak aby byla co největší pravděpodobnost, že něco nakoupíte
  - Nedělá se to individuálně, ale pro skupinu lidí, která má něco společného

- Distribuuje se některými programy, např. p2p
- Anebo se využívá cookies a monitoruje vás přímo web
- Shromážděná data, posílá svému „Lord of the Spywares“

Lidský faktor

- Lidé, kteří tráví spoustu svého času na Internetu mají tendence si časem založit vlastní profil, web, či blog, kde se o nich dá něco zjistit
- Tyto prezentace bývají nejčastěji svázány s e-mailem

- Chce-li si někdo uchovat anonymitu např. při psaní do diskuzí, pak
  - By měl používat alespoň kaskádu proxy serverů, které bude měnit
  - Měl by si vypracovat několik různých postav, lišících se v názorech, věku, prezentovanou historií, pohlaví a přezdívce
    - Pro větší efekt jim může přiřadit i různé fotky, či e-mailové adresy někoho jiného
  - Také by každý z nich měl používat jiný sloh, příp. specifické pravopisné chyby

  - Ale všechny tyto postavy jsou ve skutečnosti jeden člověk, s jedním názorem
    - Kvůli kterému bude muset napsat mnoho textu
    - Sice by se mohl spokojit s většinovým názorem, ale proč by to potom dělal?

- Nikdo není perfektní a tak na sobe po čase vyzradí něco specifického, či udělá jinou chybu
- Je možné si sestavit profil osob a na jeho základě vyhodnotit, s kým si to vlastně píšete
  - Na tohle ani nepotřebujete přístupy k logům serverů
  - Je zde však možnost snadného omylu, např. díky subjektivním názorům na podezřelou osobu
- Teoreticky je možné se uhlídat, ale v praxi…