5. BLOK

Prostředky ochrany dat pro běžné uživatele

5.1 Výsledek jednoduchého odhadu rizik

Pod pojmem *riziko* rozumíme nejčastěji (existují různé definice) vyjádření pravděpodobnosti výskytu specifické škody (realizaci bezpečnostní hrozby).

Analýza rizik je činnost, jejíž výsledkem je výpočet pravděpodobnosti výskytu škod. *Odhad rizik* je pak povrchnější, předběžná činnost, jejíž výsledkem je přibližný odhad pravděpodobnosti výskytu škod. Cílem analýzy rizik je určit optimální poměr mezi možnými hrozbami (či spíše jimi způsobenými ztrátami) a náklady vynaloženými na bezpečnostní opatření, která by tyto ztráty měla omezit. Analýza rizik se vlastně nezabývá jen vlastní analýzou, ale zahrnuje určení, případně odhad rizik a poté vlastní analýzu rizik. S analýzou je pak úzce spojeno řízení a kontrola rizik.

Určení či odhad rizika závisí na možných hrozbách a zranitelnostech systému. Zjištění všech potenciálních hrozeb a určení typu a účinnosti protiopatření není snadný úkol. Jiné hrozby jsou důležité pro armádu, jiné pro školy nebo pro redakce časopisů.

Představme si nejmenovaný rešeršní časopis (a online službu) umožňující odběrateli získat dokonalý přehled o trendech a vývoji v oblasti bezpečnosti elektronického obchodování a souvisejících oblastí (počítačová a komunikační bezpečnost, kryptografie, techniky ochrany duševního vlastnictví atd.). Tento časopis monitoruje významné časopisy, knihy a konference v daných oborech po celém světě.

Při tvorbě časopisu formou teleworkingu se jedná (minimálně) o tyto druhy použití Internetu:

- Komunikace s vydavateli monitorovaných publikací probíhá z cca 80-90 % po Internetu.
- Mnohdy (cca 10-20 %, s rostoucí tendencí) jsou vlastní publikace v elektronické formě a rešeršní pracovníci nebo šéfredaktor je získávají po Internetu.
- Rešerše jsou zaslány do redakce prostřednictvím emailu.
- Veškerá komunikace mezi editory a korektory také probíhá prostřednictvím emailu.

- Finalizované rešerše jsou ukládány do databáze, jejíž jedna kopie se používá přímo pro podporu webové verze časopisu.
- Uživatelé/čtenáři přistupují k online verzi časopisu přes jeho webové stránky. (V budoucnu budou např. také dostávat informace o nových rešerších emailem v případech, že rešerše obsahují zvolená klíčová slova nebo patří do vybraných kategorií.)

Po zvážení bezpečnostních rizik a jejich možného dopadu na průběh projektu a chod firmy vyplynuly následující priority ochrany proti:

1. **Nedostupnosti online verze.** Tento aspekt je hodnocen jako nejkritičtější, protože by přímo ovlivnil spokojenost zákazníků. Nedostupnost může nastat jednak neúmyslým poškozením některé komponenty systému nebo cíleným útokem.
2. **Ztrátě rešerše před naplněním databáze.** Zde by se jednalo nejspíše o ztrátu části rešerší (rešerše jsou zpracovávány po částech tak, jak přicházejí k editorům), ke které ovšem může dojít během kterékoliv ze 5-8 emailových transakcí, kterými každá rešerše před zařazením do databáze projde. Opět může nastat jak cíleným útokem, tak i nezaviněným systémovým selháním.
3. **Ztrátě nebo poničení rešerše v databázi.** Ztráta celé databáze, jedná-li se o zdrojovou databázi pro webový server, bude mít samozřejmě za následek nedostupnost online verze. Zde máme na mysli především ztrátu nebo poničení obsahu části rešerší.
4. **Nedostupnosti firemních dat.** Zde není kritická nedostupnost firemních dat po dobu několika hodin ani dnů (k čemuž již mimochodem v minulosti došlo), ale spíše nedostupnost „trvalá“, kdy by nebylo možno data obnovit ze záloh a muselo by se přistoupit k pracné rekonstrukci dat z papírových archivů, poznámek a zdrojů všech členů týmu.

Další hrozby jako např. zjištění obsahu (ztráta důvěrnosti) rešerše před jejím oficiálním publikováním nebo monitorování komunikace mezi členy týmu nemají v běžných případech zásadní dopad na průběh projektu. Ale i tak jsou mezi členy týmu dnes k dispozici prostředky, kterými lze v případě potřeby některé tyto hrozby eliminovat.

Zálohování dat – jak vnitrofiremních, tak i databáze rešerší a souborů s rozpracovanými rešeršemi – je podle výše uvedeného seznamu nejvyšší prioritou pro zajištění ochrany dat. Dalším významným prostředkem ochrany dat je zajištění integrity dat – k tomuto účelu jsou dnes již běžně dostupné stovky aplikací. Toto jsou dvě zásadní položky pro technické zajištění bezpečnosti. Dalším faktorem, který do velké míry ovlivní úroveň bezpečnosti zpracování dat, je ale i dobrá organizace práce. Tato na první pohled „trivialita“ je velmi důležitým faktorem – šéfredaktor bez dobré organizace práce může lehce přicházet každý měsíc o několik desítek rešerší, pokud nemá kontrolu nad tím, kdo a jaké rešerše má dodat. Při našem projektu by právě takovéto ztráty dat byly jistou cestou k

pozvolnému krachu projektu. K těmto ztrátám ale může docházet nejen při emailových transakcích, ale i třeba nepozorností nebo působením Trojského koně v lokální síti „kamenné redakce“.

Když se nad seznamem možných bezpečnostních problémů zamyslíme z pozice toho, kdo má rozhodnout o tom, zda použít nebo nepoužít teleworking řešení, tak zjistíme zásadní poznatek – pro tento projekt nemá s ohledem na bezpečnost téměř žádný význam, jestli je prováděn výše popsaným teleworking přístupem nebo by byl případně prováděn v kancelářích jedné budovy.

Proč tomu tak je? To ještě nemáme do detailů ověřeno, za podstatné ale považujeme faktory:

1. Firma a její první projekt jsou od počátku budovány na principech teleworking řešení.
2. Jedná se o relativně malý projekt s jasným cílem, produkty a možnostmi řešení.
3. Většina členů firmy jsou profesionálové v oboru bezpečnosti a umí rozlišit která data, proti čemu a jak chránit (neboli hlavně provést primitivní klasifikaci dat).
4. Nepracuje se většinou vyloženě „na cestách“, kde přicházejí v úvahu mnohé další bezpečnostní problémy.

5.2 Použití certifikátů – bezpečnost internetové komunikace

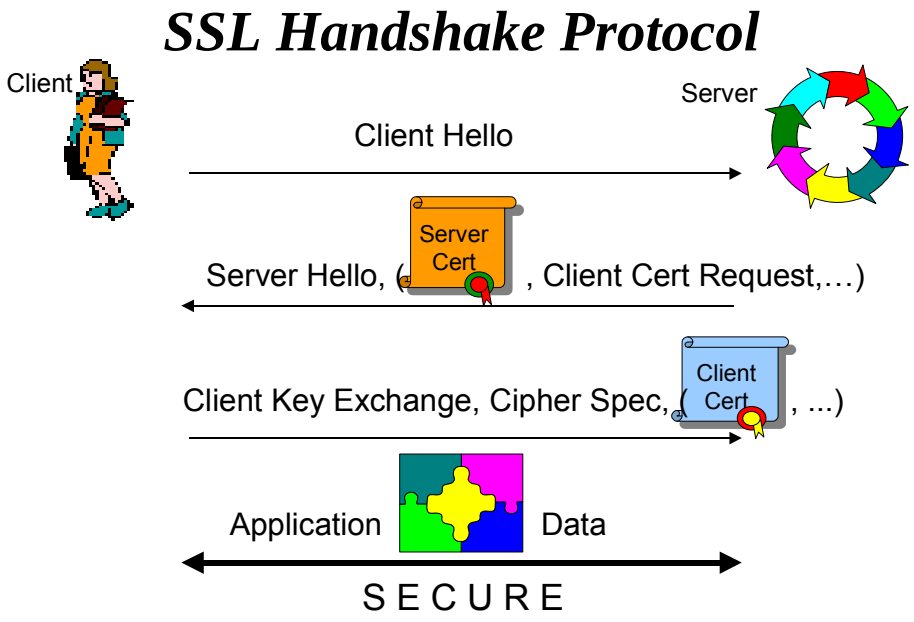
Asi nejznámější internetovou aplikací certifikátů je jejich využití v protokolu SSL (Secure Socket Layer), která pro téměř všechny aplikační protokoly (HTTP, telnet, FTP atd.) může poskytnout:

- **Služby autentizace** - server se vždy musí prokázat předložením certifikátu, který klient může a nemusí akceptovat; autentizace klienta není povinná a záleží na serveru, zda ji vyžaduje.

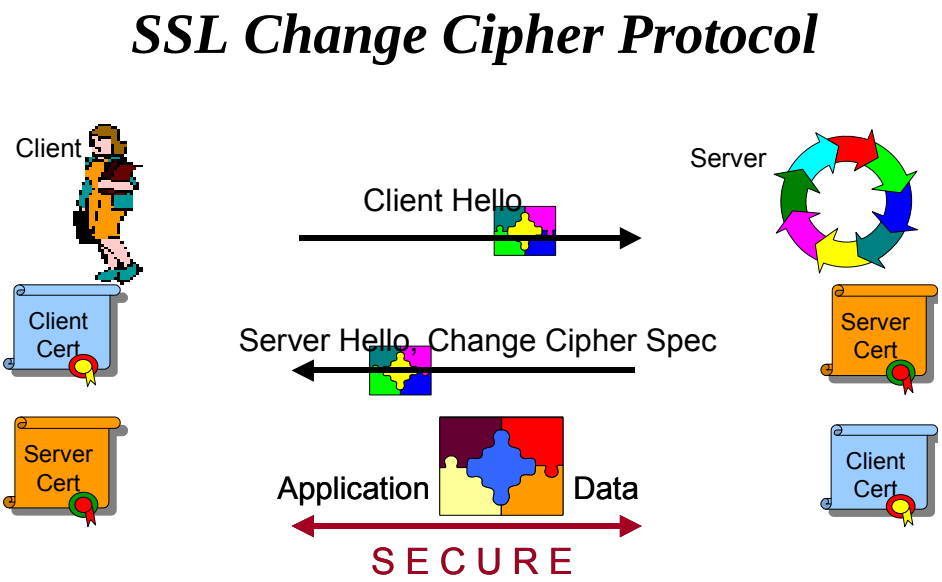
- **Zajištění důvěrnosti obsahu komunikace** - šifrováním dat přenášených kanálem, kdy je po autentizaci ustaven šifrovací klíč pro symetrické šifrování (k dispozici jsou algoritmy RC4 se 40b a 128b klíči, RC2 se 128b klíčem, IDEA se 128b klíčem, DES s 56b klíčem a trojitý-DES se 168b klíčem - ten ale odpovídá jen 112b „úrovni bezpečnosti").

- **Podporu integrity** - data jsou vždy doprovázena autentizačním kódem zprávy (MAC - Message Authentication Code), kterým je 128b MD5.

SSL je bezpečnostní protokol, či spíše soustava protokolů, které navrhla (bývalá) firma Netscape. Je možno je provozovat nad libovolnou spolehlivou spojovanou službou (např. TCP). Na začátku komunikace klienta (např. WWW prohlížeče) a serveru (např. WWW serveru) je potřeba dohodnout kryptografické a další parametry pro následující komunikaci, verzi protokolu, způsob dohody a předání šifrovacích (symetrických) klíčů pomocí šifrovacího algoritmu s veřejným klíčem. Tato fáze se nazývá *SSL Handshake Protokol*.



Poté již probíhá mezi oběma stranami bezpečná komunikace. Protokol dále umožňuje změnu způsobu šifrování a dalších parametrů komunikace kdykoliv v jejím průběhu.



Další informace k používání SSL protokolu a certifikátů lze dnes získat na mnoha místech, např. u bank, které jej využívají k zabezpečení komunikace s klientem při tzv. internetovém bankovnictví.

5.3 PGP

Asi jen stěží najdete někoho, kdo se ochomýtá okolo oboru počítačové bezpečnosti a nikdy neslyšel o PGP (*Pretty Good Privacy* – Zatraceně dobré soukromí). PGP se stalo bezesporu fenoménem pro mnohé uživatele služeb Internetu, především pak e-mailu. Co všechno PGP umožňuje? Nejnovější verze umožňují spoustu vylepšení a dodatků jako např. certifikační server (umožňující aplikaci hierarchického modelu certifikace/důvěry), spolehlivé mazání souborů, šifrování dat na pevném disku, aplikace pro správu bezpečnostní politiky pro SMTP, má přibalen i personální firewall atd. Důležitá informace ovšem je, že verze pro nekomerční použití jsou stále zdarma!

V kostce - PGP umožňuje jednoduché šifrování souborů symetrickou šifrou vámi zvoleným klíčem, digitální podpis souborů (vytvoří se haš souboru a ten se podepíše vaším soukromým klíčem) a zašifrování souborů "asymetrickou šifrou" (uvozovky uvedeny proto, že ve skutečnosti se používá se bloková symetrická šifra s náhodně vygenerovaným klíčem, který je po zašifrování vlastního souboru teprve zašifrován zvoleným veřejným klíčem). V zájmu rychlosti přenosu je při šifrování využita komprese a pro aplikace jako je třeba e-mail se využívá kódování dat přes Radix-64. V podstatě tedy vše co potřebujete pro bezpečnou

komunikaci e-mailem, distribuci zašifrovaných souborů přes FTP a WWW či digitální podpis jakýchkoliv dat.

To je tedy ono pověstné PGP? Ano a ne - výše uvedený výčet funkcí není vyčerpávající a je také třeba zvážit fakt, že dnes se nejedná jen o samotné PGP, ale o tisíce programů umožňujících např. šifrované telefonování po Internetu, propojení PGP a programů pro e-mail atd. Více o funkcích PGP a jeho nástaveb se můžete dočíst např. na *www.pgp.cz*, *www.pgp.net* nebo *www.pgpi.com*, podívejme se nyní ve zkratce na zásadní věci, o kterých je dobré při používání PGP něco vědět.

5.3.1 Klíče

Prvním zásadním krokem, na který při instalaci PGP narazíte, je vygenerování páru klíčů. Stejné klíče lze samozřejmě používat na různých platformách - klíč vytvořený na laptopu Mac nebo Wintel lze bez problémů používat pod Unixem.

Nejprve si řádně zvažte, kolik párů klíčů budete chtít používat. Tedy hlavně se jedná o ochranu soukromých klíčů těchto párů. Můžete stejný klíč používat na všech strojích a systémech, které používáte; můžete zvolit různé klíče pro různé úrovně bezpečnosti (jiné pro vaše osobní stroje pod vaší výhradní kontrolou a jiné pro firemní počítače, kde používáte internetové spojení).

Podle způsobu očekávaného zvolených klíčů zvolte vhodnou délku klíčů a také jejich popisné údaje. Stávající hranice bezpečnosti RSA klíčů je něco pod 600 bitů, takže doporučuji pro klíče, které budete běžně používat v blízké budoucnosti, volit standardních 1024 bitů, příp. délku nad 700 bitů. Větší délka má smysl v případech, kdy váš klíč má být vazbou pro budoucí aplikace nebo klíče a také kdy rychlost kryptooperací nehraje velkou roli (pamatujte - čím delší klíč, tím pomalejší operace s ním). Pro popisné údaje je samozřejmě vhodné jméno a dále je silně doporučován e-mail, lze ale volit jakékoliv jiné údaje (poštovní adresa ap.). Pokud budete používat stejný klíč pro e-mailovou komunikaci prostřednictvím více adres (ať již skutečné e-mailové schránky nebo jen přesměrování pošty), uveďte všechny adresy v dodatečných popisných údajích a pro dokonalé zajištění vazby těchto adres tyto vždy podepište.

Rozšíření vašich veřejných klíčů je dalším stěžejním krokem.

- Nejspolehlivější mechanismus samozřejmě je, když svým partnerům předáte osobně (např. na disketě) nebo osobně předáte alespoň jeho vytištěnou ASCII podobu nebo otisk (haš) a poté zašlete klíč i elektronickou cestou - partner pak může podle vytištěné informace zkontrolovat, zda dostal skutečně ten pravý klíč. Pro tyto účely je např. vhodné uvádět otisk klíče na vizitkách atd.

- O něco méně spolehlivou metodou je klíč poslat elektronickou cestou a haš sdělit telefonicky - pokud druhá strana zná váš hlas, případně je schopna vás

"prověřit" otázkami, na které můžete okamžitě správně odpovědět jen vy. Méně důvěryhodnout alternativou této metody je čistě elektronická cesta, kdy tyto otázky přijdou zašifrovány vámi dodaným veřejným klíčem, vy je musíte dešifrovat (čili být schnopni použít soukromý klíč) a zodpovědět během krátkého časového intervalu (s mírnou nadsázkou pak lze předpokládat, že jste na ně skutečně odpověděli vy).

- Klíče může podepsat a tak "akreditovat" někdo z vašich přátel, kteří mají svoje PGP klíče již dostatečně rozšířeny. Podle toho jakou důvěru ve vás a vaše klíče mají a jakou důvěru ve vaše přátele mají jejich partneři, tak dalece se bude důvěřovat vašim klíčům. PGP je z tohoto hlediska velmi propracovaný mechanismus - tranzitivní důvěru lze pomocí PGP spravovat velmi šikovně.

- Klíče lze pak také rozšířit na servery PGP klíčů (viz např. www.pgp.cz), kam ale může poslat falešné klíče každý (zkuste si najít např. klíče z *whitehouse.gov*), zpřístupnit přes vaše WWW stránky atd. Ve všech těchto případech je ale vhodné mít klíče podepsány jinými akreditory, příp. rozšířeny spolehlivými způsoby - tyto metody jsou vhodné pro širokou veřejnost, vaši důvěrní přátelé by měli získat vaše klíče spolehlivější cestou.

Analogicky pak získejte veřejné klíče všech stran, se kterými chcete do budoucna bezpečně komunikovat. Případně si také zjistěte, zda existuje nadstavba nad PGP pro e-mailové klienty, se kterými pracujete.

Velmi důležitým rysem PGP je to, že většina verzí je dostupná nejen jako zkompilované balíky, ale také jako zdrojový program. Je tím umožněna nezávislá kontrola, které se mnozí kutilové a hackeři (v kladném slova smyslu) rádi oddávají a případné nedostatky pak mohou prezentovat na veřejnosti. Princip je zde v podstatě stejný jako u kryptografických algoritmů - rozsáhlá a neomezená kontrola odbornou veřejností odhalí více chyb než jednorázové (ať už jakkoliv dlouhé) otestování sebelepšími odborníky.

PGP je nástroj, který umožnil internetové komunitě bezpečnou výměnu informací. Je ideálním zhmotněním myšlenky části tohoto kurzu - bezpečnostní nástroj, který nám umožňuje zatraceně dobrou ochranu informačního soukromí.

6. BLOK

Systémy pro poskytování anonymity

Pro zabezpečení komunikace na Internetu se v současné době aktivně využívá šifrovacích mechanizmů. Tyto technologie ale zabezpečí pouze vlastní obsah přenášených dat, takže útočník není schopen získat otevřenou podobu informací, které jsou předmětem komunikace. Je ale schopen zjistit od koho tato zpráva pochází a komu byla adresována. Znalost takové informace může být v různých prostředích značně nežádoucí, protože může útočníkovi poskytnou jistou znalost o pravděpodobném obsahu přenášených dat. V důsledcích potom může různým způsobem poškodit komunikující strany.

Naproti tomu lze vyžadovat existenci takového prostředí, kdy nemusí být zabezpečen vlastní obsah dat, ale útočník se nemá možnost dozvědět, kdo tato data odeslal a kdo byl jejich příjemcem. Pokud např. zachytí zprávu „Sejdeme se v 10 hodin na náměstí“, ale nebude mít informaci o tom, kdo komu tuto zprávu poslal, tak je pro něj prakticky bezcenná. Ideální je tyto dva přístupy skloubit dohromady a vytvořit takové prostředí, kde je zajištěna jak anonymita komunikujících partnerů, tak i důvěrnost a integrita přenášených dat.

Terminologie, která se v této oblasti používá, je popsána v bloku 1, ale v souvislosti se systémy pro poskytování anonymity se můžeme setkat s alternativní definicí anonymity. (Pozn.: další části textu vycházejí z článku *Anonymita a ochrana informačního soukromí,* Kumpošt, Matyáš, *VII. ročník konference Internet a konkurenceschopnost podniku*. Univerzita Tomáše Bati ve Zlíně, 2005,. 5 s. ISBN 80-7318-269-6.)

6.1 Anonymita

Anonymita je stav, kdy není možné identifikovat subjekt v rámci množiny všech uvažovaných subjektů (anonymitní množina). Jedná se o úplné odstranění všech identifikačních informací daného subjektu. Dále lze uvažovat anonymitu odesílatele (tj. množinu všech možných odesílatelů dané zprávy) nebo anonymitu příjemce (tj. množiny všech možných příjemců dané zprávy).

6.2 Mixy

Autorem prvotního návrhu mix systému byl Chaum v roce 1981. Navrhovaný systém měl sloužit k anonymnímu posílání elektronických zpráv.

Celý proces mixování v tomto prvotním návrhu je poměrně jednoduchý. Mix přijme několik zpráv od uživatelů, kteří chtějí anonymně poslat email. Následně z těchto zpráv odstraní veškeré informace, které by mohly vést k identifikaci uživatelů (a další informace, především časové, využitelné k různým útokům) a takto zpracované zprávy odešle. Základním problémem při zajištění anonymity (a

částečně i ostatních aspektů ochrany soukromí) je totiž možnost odlišení jedné pozorované entity (např. emailu) od ostatních – tento problém spadá do otázek tzv. analýzy provozu (traffic analysis). Analýza provozu je útok, kdy se útočník snaží získat nějaké identifikační informace pouhým sledováním provozu na síti.

Příchozí zprávy do mixu jsou zašifrovány veřejným klíčem mixu, aby byl utajen i vlastní obsah zprávy. Mix, jakožto vlastník odpovídajícího privátního klíče, je schopen takto zašifrované zprávy dešifrovat a poté provést příslušné operace vedoucí k odstranění veškerých identifikačních informací o odesílateli zprávy. Takto upravené zprávy jsou dále zpracovány (typicky odeslány na další mix nebo přímo příjemci) v okamžiku, kdy je splněna určitá „prahová“ podmínka. Podmínka, která ovlivní odeslání zpráv z mixu má značný vliv na celkovou míru anonymity poskytovanou daným systémem a také chrání uživatele před různými typy útoků na mixovací systémy nebo celé mixovací sítě.

Obr. 6.1: Schéma mixovacího uzlu.

Vzhledem k procesu, kterým systém zpracovává data a zajišťuje tak určitou míru anonymity, dochází k velkým prodlevám při zpracování zpráv. Zpracování zprávy přes síť mixů může trvat řádově až hodiny. Tato latence je akceptovatelná v případě zasílání elektronické pošty a obecně zpráv. V případě systémů pracujících v reálném čase (ssh připojení, prohlížení www stránek, ftp apod.) je tento přístup nepoužitelný, protože je vyžadována okamžitá reakce na požadavky uživatelů. V těchto situacích se používá systémů založených na Onion routingu.

6.3 Onion routing (cibulové směrování)

Návrh systému Onion Routing byl poprvé představen v roce 1996 jako metoda pro skrytí směrovacích informací v aplikacích, které vyžadují síťové propojení bez přílišných prodlev. Přístup použitý v tomto systému spočívá ve vytvoření speciální šifrované vrstvené datové struktuře (odtud název cibule), která je v síti zpracována při průchodu přes zvolené směrovače. Každá „slupka“ takové struktury je zašifrována klíčem daného směrovače, a tedy pouze tento uzel je schopen provést úspěšné „sloupnutí“ vnější vrstvy. Dešifrováním získá informaci o adrese dalšího uzlu v síti, na který mají být data odeslána. Aplikováním stejného postupu dojde na konci datové cesty k tomu, že poslední uzel získá po dešifrování již ta data, která jsou určena pro příjemce zprávy.

Vlastnímu přenosu dat předchází tzv. ustavení komunikační cesty – inicializační fáze, kdy dojde k vytvoření sdílených symetrických klíčů mezi odesílatelem dat a každým uzlem po cestě k příjemci. Odesílatel potom použije tyto symetrické klíče k vytvoření jednotlivých zašifrovaných vrstev. Každý uzel v síti zná pouze množinu svých předchůdců a následníků a dále do sítě „nevidí“. Výhoda je v tom, že pokud útočník úspěšně zaútočí na konkrétní uzel, získá pouze informaci o dalším skoku, ale následně již nebude schopen zprávu dále sledovat. Pro úspěšný útok je nutné mít pod kontrolou všechny uzly v síti a schopnost poslouchat datový provoz na všech koncích sítě. Nicméně návrh tohoto systému si neklade za cíl být odolný proti takto silnému typu útočníka.

Aby při průchodu sítí nedocházelo ke „zmenšování“ datové struktury vlivem „odšifrovávání“ vnějších vrstev, přidává každý uzel určité množství náhodných dat tak, aby byla celková velikost cibule vždy konstantní. Tento přístup snižuje riziko útoku na systém Onion Routing pouhým odposlechem provozu.

Zástupcem tohoto typu systému pro poskytování anonymity je systém TOR – The Onion Routing (*http://www.torproject.org*). Jedná se o druhou generaci Onion Routing systému, která se od původního návrhu liší řadou nově přidaných funkcí vlastností a vylepšení.

Mezi hlavní novinky systému TOR můžeme zařadit např. zajištění tzv. dopředné bezpečnosti (forward secrecy) kdy není možné zpětně dešifrovat odposlechnutou komunikaci. Novinkou je též testování integrity přenášených dat a spolehlivější budování komunikačního okruhu (telescopic circuit building). Je zde řešena i anonymita serverů, ke kterým se uživatelé připojují. Tato technologie se jmenuje Rendezvous point a Hidden services (místa setkání a skryté služby). Server má možnost své služby poskytovat prostřednictvím uzlů sítě TOR, takže klienti nevidí skutečnou adresu. Velikou výhodou tohoto přístupu je kontrola připojených klientů na straně serveru a tím pádem i účinná ochrana proti případným útokům typu DoS.

6.4 Anonymní proxy

Další možností pro zajištění „jisté“ míry anonymní komunikace je použití nějaké anonymní proxy. Seznam takových serverů lze snadno vyhledat pomocí Google. Pokud pak v prohlížeči nastavíte tuto proxy, tak bude vaše skutečná IP adresa skryta za adresou proxy serveru. Službám na internetu se bude zobrazovat IP adresa proxy serveru, která se zpravidla ještě s určitou frekvencí mění. Tento způsob je poměrně snadný, nicméně z pohledu uživatele nemusí být příliš bezpečný. Tím, že veškerý provoz směrujeme přes něčí server, tak dáváme svá data k dispozici neznámým lidem. Jakékoliv přihlašovací údaje odeslané z formuláře budou dostupné provozovateli proxy serveru. Je tedy vhodné použít takovou proxy, která podporuje i SSL provoz a poté používat výhradně šifrovaný protokol https.