PROJEKT DO PŘEDMĚTU BZSG

2017/18

TOMÁŠ DVONČ, 173974

Počet stran mimo titulku, obsah a literaturu: 6

Generováno: 14. novembra 2017

OBSAH

1 Zabezpečenie komunikácie **3**
1.1 História vývoja SSL/TLS protokolov 3
1.2 Kryptografické protokoly 4
1.2.1 SSL protokol 4
1.2.2 TLS protokol 5
1.3 Architektúra zabezpečenia (SSL/TLS) 6
1.3.1 Výmena kľúčov 6

2 Realizácia a výsledky analýzy **8**
2.1 Spracovanie výsledkov analýzy 8

Literatúra **9**

ZOZNAM OBRÁZKOV

1.1 Štruktúra TLS protokolu 5
1.2 Efektívna ochrana pomocou hybridného kryptosystému 7
2.1 Výsledky analýzy zabezpečenia webových serverov 8

ZOZNAM TABULIEK

1.1 Prehľad symetrických šifrovacích algoritmov 6

1 ZABEZPEČENIE KOMUNIKÁCIE

1.1 História vývoja SSL/TLS protokolov

SSL prvýkrát predstavila spoločnosť *Netscape* v rokoch 1993-1994. Rast počtu ľudí používajúcich internet rýchlo stúpal a rovnako aj potreba bezpečnosti komunikácie. Dnes SSL/TLS používa takmer každá online služba.

Prvá verzia **SSL 1.0** nebola nikdy uvedená na trh, pretože mala obrovské bezpečnostné medze. Prvé oficiálne vydanie **SSL 2.0** prišlo o rok neskôr v roku 1995. Posledná verzia SSL protokolu vyšla v novembri 1996. S odstupom času už ani táto verzia sa nedala považovať za dostatočné zabezpečenú. V roku 2011 bol protokol SSL 2.0 stiahnutý z trhu pretože mal tieto nedostatky:

1. Komunikácia používala slabý hashovací algoritmus, ktorý sa už dal v tú dobu prelomiť. Táto forma kryptografického algoritmu sa viac nepovažovala za bezpečnú.
2. Pri nadviazaní komunikácie útočník získal odosielanú správu a bol schopný prinútiť klienta zameniť hashovací algoritmus za zraniteľnejší ako si normálne vybral.
3. Integrita a šifrovanie správ používali rovnaký kľúč. V prípade ak klient a server používali slabý šifrovací algoritmus dochádzalo k prelomeniu zabezpečenia.

V roku 1999 bola uvedená na trh prvá verzia protokolu **TLS 1.0** Neskôr bola vyvinutá novšia verzia **SSL 3.0** ale v roku 2015 bola opäť zastarala a podľa oficiálneho vyhlásenia *IEFT* bola akákoľvek verzia TLS považovaná za bezpečnejšiu ako SSL 3.0 a to z nasledujúcich dôvodov:

1. Výmena kľúčov medzi klientom a serverom sa považovala naďalej za nezabezpečenú.
2. Všetky certifikáty boli postavené na princípe slabých hashovacích algoritmov, ktorých použitie už nebolo ideálne.
3. SSL 3.0 malo obmedzene možnosti a nebolo schopné využiť mnohé funkcie, ktoré boli pridané do novších verzii TLS.

TLS 1.1 bolo vydané v roku 2006, oproti staršej verzií bola pridaná ochrana proti CBC (*cipher-block chaining*) útokom. Implicitný inicializačný vektor bol nahradený explicitným.

TLS 1.2 bolo uvedené na trh v roku 2008. Bolo to pokračovanie protokolu TLS 1.1 s novými zmenami. Niektoré hashovacie algoritmy boli nahradené za novšie kryptografické funkcie.

TLS 1.3 je v štádiu vývoja a podrobnejšie detaily sú zatiaľ nejasné. Niektoré z hlavných zmien oproti verzii TLS 1.2 sú nasledovné:

1. Ukončenie podpory slabších kryptografických hashovacích funkcií.
2. Bude zavedené vyžadovanie digitálneho podpisu aj v prípade použitia predchádzajúcej konfigurácie.
3. Podpora znižovania počtu nezabezpečených alebo zastaraných funkcií, vrátane kompresie a ďalšie iné. [1]

1.2 Kryptografické protokoly

Šifrovanie je proces, v ktorom sa čitateľná správa (text) konvertuje na šifrovaný formát, ktorý nie je čitateľný človekom. Hlavným účelom šifrovania je zabezpečiť, aby iba autorizovaná strana mohla dešifrovať a čítať pôvodnú správu. Keď sa nezašifrované dáta vymieňajú medzi dvoma účastníkmi, s použitím akéhokoľvek média, tretia strana môže zachytiť a prečítať vymieňanú komunikáciu.

Ak výmena obsahuje citlivé informácie a tretia strana môže takúto komunikáciu zachytiť, mohla by tiež manipulovať s údajmi a zmeniť informácie, ktoré sa vymieňajú, čím ohrozí integritu správy.

Jeden zo spôsobov ako zmierniť potenciálny útok a zabezpečiť komunikáciu je použitie kryptografického protokolu SSL alebo TLS, ktoré si v tejto sekcií detailnejšie popíšeme.

1.2.1 SSL protokol

SSL (*Secure Sockets Layer*) je kryptografický komunikačný protokol, ktorý na prenos informácií využíva protokol transportnej vrstvy TCP.

Základnou podstatou protokolu SSL je poskytnúť súkromie a spoľahlivosť medzi dvomi komunikujúcimi aplikáciami.

SSL používa kombináciu verejného kľúča a symetrického šifrovania kľúčov na zabezpečenie spojenia medzi dvoma zariadeniami. Zvyčajne sa jedná o webový alebo poštový server komunikujúci prostredníctvom internetu alebo inej siete, napríklad TCP/IP.

SSL poskytuje mechanizmus na šifrovanie a overovanie údajov pri prenose informácie medzi klientom a serverom. SSL pracuje medzi transportnou a sieťovou vrstvou, ktoré sú zodpovedné za prenos a smerovanie dát pod protokolmi aplikačnej vrstvy, ako je HTTP a SMTP (*Simple Mail Transport Protocol*).

Okrem podpory prenosu informacií medzi webovým serverom a klientom je tento protokol implementovaný aj pre aplikácie vrátane e-mailu, prenosu súborov, správ a VoIP (Voice over IP).

Protokol SSL obsahuje dva pod protokoly (viac obr. 1.1):

1. ***Record* protokol** definuje spôsob akým si komunikujúce zariadenia vymieňajú dáta pomocou protokolu SSL. Ďalej špecifikuje ako majú byť odosielané údaje pripravené na prenos a ako majú byť overené alebo dešifrované pri prijatí.
2. ***Handshake* protokol** definuje ako klient a server vytvoria spojenie SSL vrátane dohody o tom, ktoré kryptografické systémy budú použité.

Z dôvodu početných nedostatkov a zraniteľností protokolu a implementácie bol protokol SSL v roku 2015 považovaný organizáciou *IETF* (*Internet Engineering Task Force*) za zastaraný a bol nahradený protokolom TLS, ktorý je spätne kompatibilný s protokolom SSL 3.0.

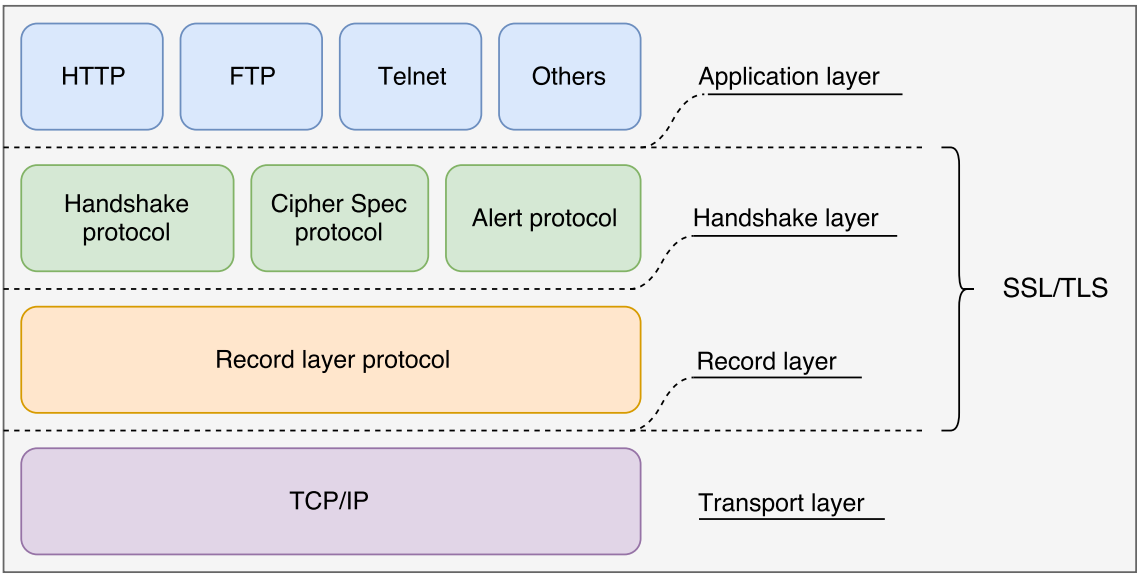
1.2.2 TLS protokol

S cieľom poskytnúť nový internetový štandard SSL, vydal *IETF* v januári 1999 protokol TLS (*Transport Layer Security*). Protokol TLS je navrhnutý, aby aplikáciám umožňoval komunikovať bezpečným spôsobom: autentifikáciou, predchádzaním odposluchu a odolnosťou proti modifikácii správ. V praxi zabezpečená webová aplikácia využíva všetky tri služby.

1. **Šifrovanie**: je mechanizmus na utajenie toho, čo sa posiela z jedného hostiteľa do druhého
2. **Autentifikácia**: je mechanizmus na overenia pravosti poskytnutého identifikačného materiálu.
3. **Integrita**: je mechanizmus na detekciu neoprávnenej správy a falšovaniu správ

Za účelom vytvorenia kryptograficky zabezpečeného dátového kanálu sa musia účastníci dohodnúť, ktoré šifry a kľúče budu používať na šifrovanie dát. Súčasťou nadviazania komunikácie je umožnenie obidvom stranám overiť svoju totožnosť. Pri používaní v prehliadači tento mechanizmus autentifikácie umožňuje klientovi overiť, či server (napr. banka) je ten, kto tvrdí že je a nie niekto iný. Tým sa overí totožnosť organizácie.

Nakoniec pri šifrovaní a autentifikácii protokol TLS poskytuje aj svoj vlastný mechanizmus šifrovania správ a každú správu podpíše autentifikačným kódom správy MAC (*Message Authentication Code*). MAC algoritmus je jednosmerná kryptografická hashovacia funkcia, ktorej kľúče sú predurčené oboma partnermi. Pri každom odoslaní záznamu TLS sa pre danú správu vygeneruje a pripojí hodnota MAC a prijímač potom dokáže vypočítať a overiť odoslanú hodnotu MAC na zabezpečenie integrity a pravosti správ. [2]



Obr. 1.1: Štruktúra TLS protokolu

1.3 Architektúra zabezpečenia (SSL/TLS)

Kryptografia je nevyhnutný nástroj na ochranu informácií v počítačových systémoch. Používa ju denne milión ľudí na celom svete. Kryptografické systémy sú najdôležitejšou súčasťou štandardných protokolov ako je napríklad **TLS**, čo pomerne ľahko začleňuje silné šifrovanie do širokej škály aplikácií.

1.3.1 Výmena kľúčov

Dôležitá vlastnosť, ktorá určuje účinnosť šifry, je veľkosť tajného kľúča. Čím je kľúč väčší, tým zložitejšie je prelomenie kódu. Pre pochopenie zvážime algoritmus s extrémne malou veľkosťou kľúča: 2 bity. V tomto príklade samotný typ algoritmu naozaj nezohráva dôležitú úlohu. Koniec koncov, s 2 bitmi sú len štyri možné kombinácie kľúčov. Útočník, ktorý získal šifrované údaje jednoducho môže vyskúšať všetky štyri možnosti.

Existujú dve základné techniky šifrovania informácií: **symetrické** šifrovanie (tiež nazývané šifrovanie tajného kľúča) a **asymetrické** šifrovanie (tiež nazývané šifrovanie verejným kľúčom).

1. **Symetrické šifrovanie** je najstaršou a najznámejšou používanou technikou. V texte správy sa použije **tajný kľúč** aby sa zmenil obsah určitým spôsobom. Použije sa napríklad číslo, slovo alebo len reťazec náhodných písmen. Môže to byť aj jednoduché posunutie každého písmena o niekoľko miest v abecede. Pokiaľ odosielateľ aj príjemca poznajú tajný kľúč, môžu šifrovať a dešifrovať všetky správy, ktoré tento kľúč využívajú. Kryptografovia tiež charakterizujú symetrické šifrovacie algoritmy podľa toho, ako spracovávajú vstupné dáta. Môžeme ich rozdeliť do dvoch skupín:
   (a) **Prúdové šifry** spracovávajú vstupne dáta (bajty) v čase, a môžu prijať akúkoľvek veľkosť vstupu pre šifrovanie.
   (b) **Blokové šifry** na rozdiel od toho, pracujú iba na blokoch dát s pevnou veľkosťou, typicky 8 bajtov. V porovnaní s prúdovými šiframi vyžadujú menej výpočtov a sú vo všeobecnosti o niečo menej náchylné na útok. Sú však o niečo menej pohodlné na použitie.

   V tabuľke 1.1 sú uvedené symetrické šifry, ktoré sa najčastejšie používajú s protokolom *Secure Sockets Layer* (SSL).

Tab. 1.1: Prehľad symetrických šifrovacích algoritmov

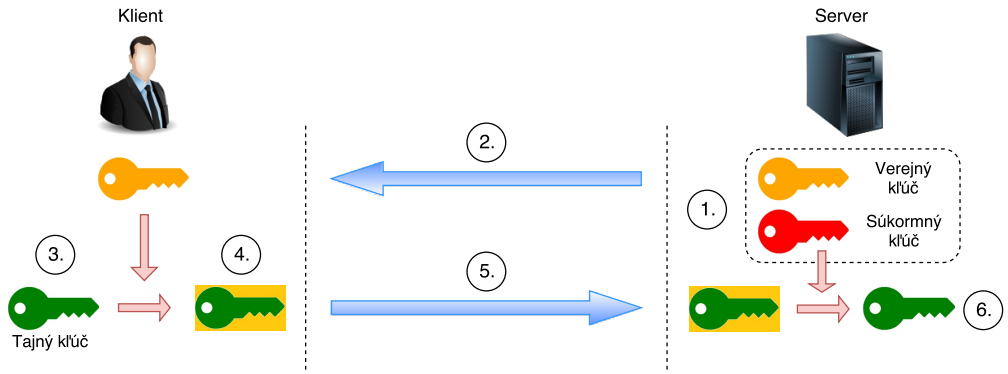
Skratka	Algoritmus	Typ
DES	Data Encryption Standard	Bloková šifra
3DES	Triple-Strength Data Encryption Standard	Bloková šifra
RC2	Rivest Cipher 2	Bloková šifra
RC4	Rivest Cipher 4	Prúdova šifra

2. **Asymetrické šifrovanie** vzniklo ako riešenie problému symetrického šifrovania, ktoré používa jeden kľúč na výmenu informácií cez internet. Každý, kto pozná tento kľúč, môže dešifrovať správu.
   Asymetrické šifrovanie používa pri výmene informácií dva kľúče, **verejný** kľúč a **súkromný** kľúč. Verejný kľúč je k dispozícii každému, kto sa snaží odoslať nejakú správu. Druhý súkromný kľúč je uchovaný v tajnosti.
   Každá správa (text, binárne súbory alebo dokumenty), ktoré sú zašifrované pomocou verejného kľúča sa môžu dešifrovať iba s použitím rovnakého algoritmu, ale s použitím zodpovedajúceho súkromného kľúča.
   Komplexné matematické operácie môžu na niektoré systémy vyvinúť zaťaženie, čo si vyžaduje väčšiu kapacitu. Našťastie existuje pomerne jednoduchý spôsob, ako získať výhody šifrovania verejného kľúča a zároveň sa vyhýbať väčšine nákladov na systém.
   Príklad výpočtu algoritmu RSA:

$$\int_{-\infty}^{x} \frac{(\varphi - 3x)}{x + x^{-\varphi}} \,\mathrm{d}x = \lim_{x \to \infty} \frac{x^3 - \varphi}{(2\varphi + 1)\,(3x - 1)}, \tag{1.1}$$

$$m^{ed} = m^{1+h\varphi(n)} = m(m^{\varphi(n)})^h \equiv m. \tag{1.2}$$

3. **Hybridný kryptosystém** je optimálny spôsob ako zlepšiť výkonnosť a efektivitu výmeny informácií. Je to kombinácia symetrického a asymetrického šifrovania. V podstate sa jedna o to, že pre veľmi dlhé správy je väčšina práce v šifrovaní a dešifrovaní vykonaná efektívnejšou schémou symetrických kľúčov, zatiaľ čo neefektívna schéma asymetrického šifrovania sa používa iba na šifrovanie a dešifrovanie krátkej kľúčovej hodnoty.
   Obrázok 1.2 znázorňuje architektúru hybridnej komunikácie.



Obr. 1.2: Efektívna ochrana pomocou hybridného kryptosystému

2 REALIZÁCIA A VÝSLEDKY ANALÝZY

2.1 Spracovanie výsledkov analýzy

Výsledky analýzy boli sprostredkované za pomocí naprogramovanej aplikácie. Na výstupe boli zhrnuté bezpečnostné mechanizmy serverov využívajúce rôzne typy zabezpečenia.

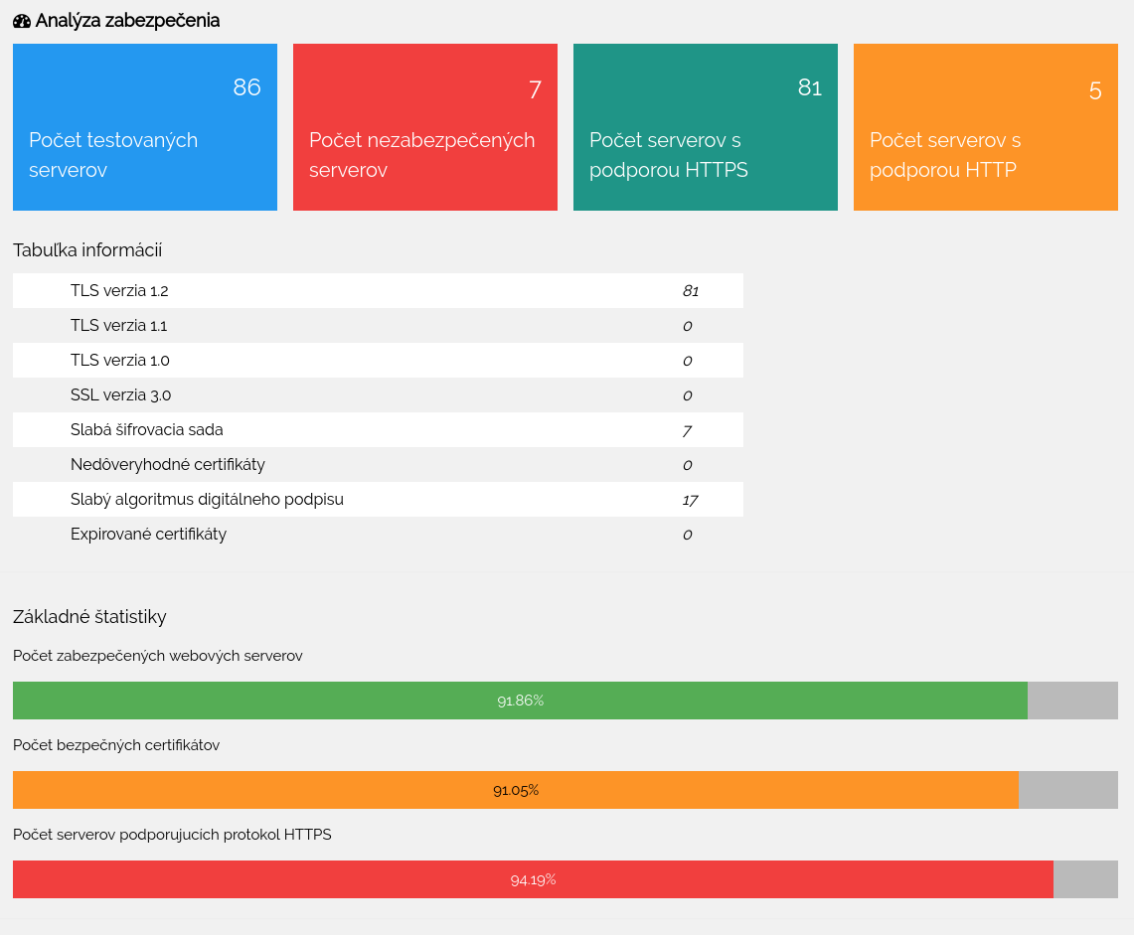
Z celkového počtu testovaných serverov 86, bola väčšina **zabezpečených**.

Keď si viac rozoberieme servery, ktoré používali protokol HTTPS, väčšina z nich komunikovala prostredníctvom najnovšieho kryptografického protokol **TLS 1.2**.

Boli nájdene servery, ktoré nepoužívali bezpečnú šifrovaciu sadu, ktorá je pre takúto komunikáciu veľmi dôležitá.

Nakoniec pri analýze certifikátov vidíme, že niektoré nepatria medzi certifikačnú autoritu, takže sa nedajú považovať za dôveryhodné a je na každom užívateľovi, či sa rozhodne dôverovať príslušnej spoločnosti, ktorá vydala tento certifikát.

Na obrázku 2.1 vidíme výsledky analýzy webových serverov.



Obr. 2.1: Výsledky analýzy zabezpečenia webových serverov

LITERATÚRA

[1] A brief history of TLS/SSL. *Acunetix* [online]. Prodromou, 2017 [cit. 27. 10. 2017]. Dostupné z:
`https://www.acunetix.com/blog/articles/history-of-tls-ssl-part-2`

[2] Transport Layer Security (TLS). *High Performance Browser Networking* [online]. Grigorik, 2013 [cit. 30. 10. 2017]. Dostupné z:
`https://hpbn.co/transport-layer-security-tls`

[3] A Graduate Course in Applied Cryptography. *Tanford University* [online]. Boneh, Shoup, 2015 [cit. 30. 10. 2017]. Dostupné z:
`https://crypto.stanford.edu/~dabo/cryptobook/draft_0_2.pdf`