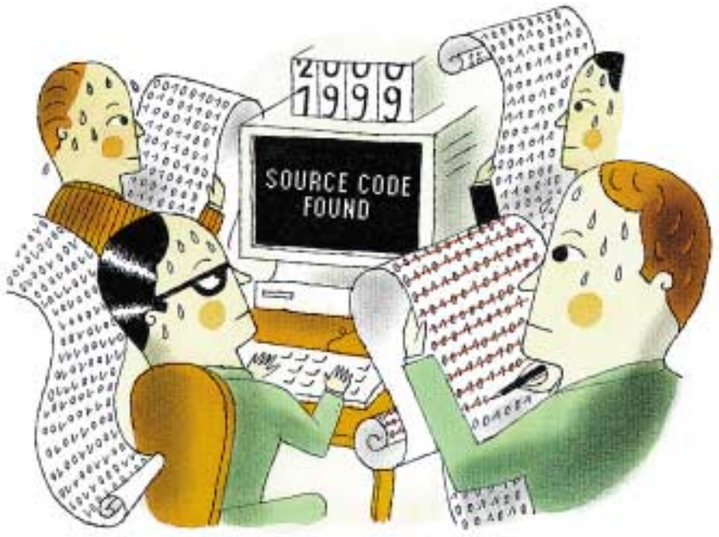
Když se řekne SSL

MILAN PINTE

BEZPEČNÁ KOMUNIKACE NA INTERNETU



Bezpečnost – to je to slovo, které se téměř ve všech médiích pravidelně skloňuje snad ve všech pádech. Stále více nás různá sdělovací média ale upozorňují už i na bezpečnost elektronickou. A tak lze lehce dojít k závěru, že téměř neuplyne týdne, v němž bychom se nedozvěděli, co se právě povedlo různým osobám (označme je jako hackeři) v této, přiznejme si to, mediálně atraktivní oblasti. A proto je logické, že jejich motivem zpravidla bývá pouze upozornění široké internetové komunity na své přednosti a znalosti, a naopak na nedostatečné znalosti, případně „lajdáckou“ práci tvůrců bezpečnostní politiky napadených podnikových systémů či internetových serverů. To ovšem v lepším případě – v tom horším mají tyto osoby zájem poškodit napadený subjekt a to buď finančně (například zneužitím informací o bankovních kontech pro „své vlastní účely“), či jen v očích počítačové veřejnosti (někdy se může jednat i o cílený nekalý konkurenční boj), což má de facto stejný důsledek. Neboť jakmile jednou veřejnost ztratí zájem o služby napadeného subjektu, bývá obtížné získat důvěru zpět. Kdo by přece obchodoval a svěřoval citlivé informace společnosti, která není schopna zajistit jejich adekvátní ochranu?

Naštěstí se lze vůči těmto snahám útočníků poměrně úspěšně bránit, neboť existuje již celá řada osvědčených prostředků, pomocí nichž lze zvýšit nejen bezpečnost elektronické výměny dat na internetu.

Myslí-li to subjekt, ať se jedná o jedince či velkou mezinárodní společnost, s ochranou citlivých údajů v prostředí všeobjímajícího internetu vážně, musí nejprve vyhotovit tzv. bezpečnostní politiku, která (zjednodušeně řečeno) vznikne analýzou toho, které informace jsou citlivé a tudíž by se neměly dostat mimo společnost, a dále analýzou a predikcí možných rizik (způsobu jejich ohrožení) a obrany proti nim. Teprve poté je možné definovat vlastní bezpečnostní politiku, která zpravidla obsahuje kombinaci různých prostředků zajišťujících zvolenou úroveň bezpečnosti.

V tomto článku bude zmíněn bezpečnostní protokol, se kterým se mohou běžní uživatelé setkávat každodenně na internetu, například pokud nakupují v internetových obchodech. Seznámíme vás s protokolem SSL.

SSL – SECURE SOCKET LAYER

Protokol SSL vytvořila firma *Netscape Communications* pro účely bezpečných přenosů v prostředí internetu. A současně ho uvolnila i jako tzv. nekomerční protokol, z čehož vyplývá, že souhlasí s jeho neomezeným využíváním pro účely tvorby internetových aplikací.

Její analytici při návrhu protokolu řešili do té doby „zbytečné“ požadavky na zabezpečení internetové komunikace spolu i s požadavkem, jak vhodně využít existujících, již zaběhnutých standardů internetové komunikace (HTTP, FTP, SMTP a dalších). Výsledkem jejich úsilí bylo začlenění přídavné vrstvy mezi aplikační a transportní vrstvu protokolu TCP/IP.

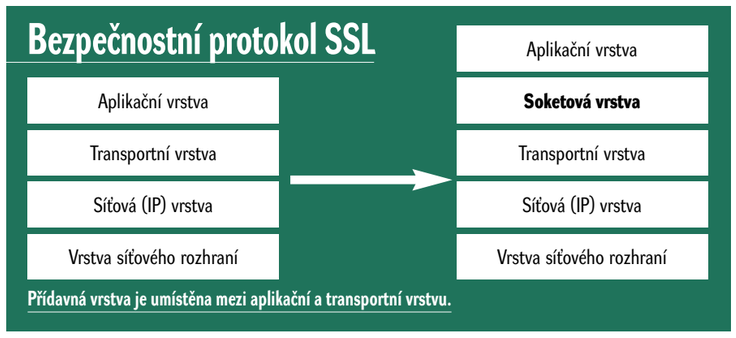
Tak vznikla architektura protokolu SSL, která umožňuje:

- provádět autentizaci serveru na základě jeho certifikátu, a současně poskytnout i možnost autentizace klienta na základě certifikátu klienta
- během procesu autentizace využívat asymetrické kryptografie
- urychlit komunikaci mezi klientem a serverem (po procesu autentizace) použitím symetrického šifrování
- zajistit integritu přenášených dat pomocí tzv. kontrolního součtu.

Vlastní komunikační dialog, mezi prohlížečem klienta na straně jedné a bezpečným serverem na straně druhé, probíhá zjednodušeně podle následujícího postupu:

1. Nejprve klient pošle požadavek na připojení k bezpečnému serveru spolu se svým veřejným klíčem (public key).

2. Poté server zašle svůj certifikát klientskému prohlížeči spolu se svým veřejným klíčem. Tyto informace jsou zašifrovány pomocí veřejného klíče prohlížeče.



Přídavná vrstva je umístěna mezi aplikační a transportní vrstvu.

▲ Tato ikona visacího zámku nás upozorní, že se můžeme cítit „bezpečně“.

3. Klientský prohlížeč prozkoumá, zda je certifikát platný. V případě, že není vystaven certifikační autoritou anebo není již nainstalován na klientském počítači, může prohlížeč postupovat dvěma způsoby: buď pokračovat výzvou uživateli (ovládajícímu klientský počítač), zda si přeje pokračovat v navazovaném spojení, nebo rovnou automaticky sám přerušit spojení se serverem.

4. V dalším kroku prohlížeč porovná informace obsažené v certifikátu se jménem domény serveru a se serverovým veřejným klíčem. V případě shody je server akceptován jako autentický.

5. Poté prohlížeč vytvoří klíč relace (tzv. session key pro potřebu symetrického šifrování) a následně jej zašifruje pomocí veřejného klíče serveru a takto zašifrovaný klíč zašle serveru.

6. Server přijme tento klíč a rozšifruje jej pomocí svého soukromého klíče (secret key).

7. Pak už server a klient využívají dále tento klíč relace k šifrování a dešifrování přenášených dat via internet.

Poznámka: V některých modifikacích může proces tvorby klíče relace probíhat na straně serveru.

OD TEORIE ZPĚT K UŽIVATELI

Jak ale zjistíme, že jsme skutečně připojeni na bezpečný server? Snadno. Stačí se podívat na URL adresu serveru. Pokud totiž začíná *https://* (oproti nezabezpečenému *http://*), jedná se o bezpečné spojení – příkladem je server *https://www.verisign.com/*.

Navíc při příchodu na zabezpečený server jsme ještě informováni naprostou většinou prohlížečů, že následující přenos bude probíhat zabezpečenou formou. Analogicky při odchodu na nezabezpečenou URL adresu budeme pomocí dialogového okna opět informováni, že tentokráte opouštíme zabezpečený server. MS Internet Explorer nás dále informuje o navázaném bezpečném spojení malou ikonkou visacího zámku. Obdobným způsobem jsme o zabezpečeném připojení informováni také v případě, že používáme prohlížeče od jiných společností.

SHRNUTÍ

Protokol SSL nabízí podstatně vyšší úroveň zabezpečení oproti nezabezpečenému protokolu HTTP, se kterým se uživatelé internetu každodenně během svého surfování po celosvětové síti setkávají, a umožňuje jim, aby spojení bylo: **soukromé** (neboť přenášená data jsou zašifrována pomocí symetrického šifrování), **důvěryhodné** (server, případně i klient jsou autentizováni) a **spolehlivé** (integrita přenášených dat je zajištěna hashovacími algoritmy). A právě díky těmto vlastnostem se s tímto protokolem můžeme běžně setkávat v internetovém bankovnictví, internetových obchodech – prostě všude tam, kde je zapotřebí chránit přenášená data na internetu, intranetu či extranetu. Je ovšem nutné si uvědomit, že SSL řeší pouze jednu otázku bezpečnosti, tj. komunikaci po internetu, a proto myslí-li to jednotlivec či společnost s bezpečností privátních informací vážně, musí tento protokol dále kombinovat s dalšími prvky zvyšujícími bezpečnost dat. 3 0068/FEL ❑

Pojem	Info
Autentizace	proces ověření totožnosti uživatele/serveru
Šifrování	transformace dat do nečitelné – utajené formy
Šifrování symetrické	též šifrování s privátním klíčem se vyznačuje existencí jediného klíče, který je využíván jak pro zašifrování zprávy, tak i pro její dešifrování
Šifrování asymetrické	též šifrování s veřejným klíčem používá klíče dva – privátní a veřejný. Cokoli je zašifrováno jedním klíčem, lze dešifrovat pouze druhým klíčem a naopak
SSL	Secure Socket Layer – bezpečná soketová vrstva, slouží ke zvýšení bezpečnosti komunikace dvou účastníků prostřednictvím internetu
Certifikát	slouží k prokázání identity dalším subjektům. Existují tři základní typy digitálních certifikátů: osobní digitální certifikáty, serverové certifikáty (server ID) a object signing certifikáty
Certifikační autorita	podepisuje a vydává certifikáty, odvolává je v případě potřeby a podepisuje a vydává CRL (Certificate Revocation List)
HTTP	Hypertext Transport Protocol – množina pravidel pro výměnu souborů na webu
URL	Uniform Resource Locator – nejpoužívanější schéma specifikace dokumentu (jeho umístění a typ) v internetu
TCP/IP	Transmission Control Protocol / Internet Protocol – základní komunikační jazyk/protokol internetu