Protokol S-HTTP, zabezpečené připojení

Minule jste se mohli seznámit s druhy útoků, které hrozí vašim datům, a s bezpečnostním protokolem Secure Socket Layer (SSL). Další možnou ochranou, kterou vám nyní přiblížíme, je protokol Secure Hypertext Transport Protocol (S-HTTP).

Pozor, útok! (2. díl)

Úvod

Jak již v dnešní době víme, návrháři protokolu HTTP původně nepočítali s ohromným množstvím cenných informací a privátních transakcí, které se budou vyskytovat či realizovat pomocí internetu. Teprve prudký rozmach těchto transakcí a stále rostoucí počet útoků na interní data jednotlivých účastníků komunikačního procesu připojených k internetu si vyžádal rychlou reakci.

Odpovědí na požadavek zvýšení bezpečnosti bylo v roce 1994 navržení protokolu S-HTTP pány E. Rescorlou a A. Schiffmanem ze společnosti EIT (Enterprise Integration Technologies).

Co je S-HTTP?

Odpověď na otázku “Co je protokol S-HTTP?” si objasníme vyjmenováním jeho některých charakteristických vlastností:

🚓 S-HTTP je bezpečnostní protokol navržený pro konjunktní užití se stávajícím protokolem HTTP. Protokol tedy umožňuje snadnou integraci do stávajících HTTP aplikací.

🛌 Poskytuje množství variant bezpečnostních mechanismů jak klientu, tak serveru.

🚘 S-HTTP nevyžaduje žádný veřejný klíč na straně klienta, pokud je podporován mod symetrického klíče.

🖼 Podporuje šifrované přenosy “end-to-end” (bezpečná transakce od jednoho koncového uživatele k druhému).

🛢 Ochrana zpráv je zajištěna pomocí podepisování, autentizace a šifrování, včetně kombinace těchto metod zabezpečení.

💰 Poskytuje pružnou podporu jednotlivým šifrovacím algoritmům, jejich modům a parametrům.

🏷 Používá záhlaví ve stylu HTTP.

💳 Umožňuje stálé spojení klient/proxy a proxy/server užitím speciálních hlaviček.

Příprava zprávy

Komunikace mezi příjemcem zprávy (klientem) a odesílatelem (serverem) začíná přípravou zprávy. Příprava a vlastní tvorba zprávy jsou realizovány během tří kroků.

🚓 Nejprve je vytvořen tzv. otevřený text zprávy (cleartext message). To může být buď HTTP zpráva, nebo nějaký datový objekt (např. grafika).

🛥️ Poté jsou zpracovány kryptografické preference a odpovídající údaje o klíčích příjemce.

🚘 V dalším kroku jsou zpracovány kryptografické preference a odpovídající údaje o klíčích odesílatele.

Podmínkou pro vytvoření S-HTTP zprávy je tedy shoda nějaké vhodné šifrovací metody z výčtu bezpečnostních preferencí odesílatele a příjemce zprávy. Výsledkem tohoto porovnání je seznam aplikovatelných šifrovacích metod (např. PKCS-7, RSA, Diffie-Hellman a další), ze kterého je následně zvolena odpovídající metoda.

Dešifrování zprávy

Z minulého odstavce víte, že vytváření S-HTTP zpráv lze při troše obrazotvornosti přirovnat k funkci, jejímiž vstupy jsou tři parametry (tzv. otevřený text zprávy, kryptografické preference příjemce a odesílatele). Proces dešifrování lze naopak přirovnat k nějaké další funkci se čtyřmi vstupy:

🚓 Prvním vstupem je samotná S-HTTP zpráva.

🛥️ Po obdržení dané zprávy se pokusí příjemce dešifrovat zprávu pomocí kryptografických preferencí a údajích o klíčích (druhý vstup), které byly poskytnuty odesílateli před přenosem.

🚘 Neodpovídá-li šifrovací standard, který byl původně odeslán, je použito současné nastavení kryptografických preferencí a údajů o klíčích příjemce (třetí vstup).

🏞️ Pokud se nepodařilo dešifrovat zprávu ani teď, jsou použity původní volby odesílatele (čtvrtý vstup).

Podmínkou správného dešifrování zprávy je, aby příjemce přečetl hlavičku této zprávy a získal informaci o použité šifrovací transformaci. Poté je odstraněna transformace užitím údaje o klíči, který byl aplikován.

Průběh transakce

Komunikace mezi prohlížečem klienta na straně jedné a bezpečným serverem na straně druhé probíhá zjednodušeně podle následujícího postupu.

Nejprve se klient pokusí připojit na S-HTTP stránku serveru, odešle tedy požadavek na připojení. Server zašle zprávu typu “Spojení úspěšně navázáno”. V okamžiku, kdy klient obdrží tuto zprávu, zašle serveru svůj veřejný klíč (záleží na zvoleném modu: šifrování se symetrickým/asymetrickým klíčem) spolu s informací o systému šifrování. Poté server zašle klientu klíč relace, který zašifroval pomocí

přijatého klientského veřejného klíče (pozn.: Pokud server nepodporuje klientský šifrovací systém, je spojení ukončeno). Poté probíhá následný přenos zpráv pomocí šifrování klíčem relace.

Pozn.: Pokud URL adresa serveru začíná **shttp://,** jedná se o bezpečné připojení.

Závěr

Vhodným rozšířením protokolu HTTP o bezpečnostní mechanismy je umožněno pomocí S-HTTP přijímat a odesílat zprávy přes web bezpečněji. Protokol umožňuje bezpečnějším způsobem provádět finanční transakce, řídit bankovní účty a nakupovat v internetových obchodních domech.

Příště si opět povíme o dalších možnostech zvýšení bezpečnosti na internetu.

Ing. Milan Pinte (pinte@kpv.zcu.cz)

Infotipy

RSA

www.rsa.com

What is

www.whatis.com/ssl.htm

Terisa Systems, Inc.

www.terisa.com/shttp

The World Wide Web Encyclopedia

www.akkib.com/encyclop