Protocoale de securitate pentru sisteme distribuite

Sistemul World Wide Web a apărut la începutul anilor '90 ca fiind un sistem de aplicații. Acesta poate fi instalat pe diferite tipuri de rețele, care nu trebuie să facă parte din Inernet și poate fi folosit chiar pe calculatoare neconectate la retea.

Elementele de baza Web sunt URL (Universal Resource Locators) care permite identificarea resurselor din Internet, HTTP (HyperText Transfer Protocol) care permite comunicarea între serverul si navigatorul Web si HTML (HyperText Markup Language) care permite crearea documentelor hipertext.

URL (Universal Resource Locators) permite identificarea resurselor din Internet. O resursa poate fi un fisier sau un director, o referinta la un obiect mai complicat cum ar fi o interogare la o baza de date sau un motor de cautare.

URL-ul este alcatuit din urmatoarele componente aflate in aceasta formula:

<*Protocol>:// <Host> :<Port> / <Path>*

De exemplu: http://webhost.uoradea.ro:80/cpopescu/curscrypto.html

Protocolul specifica protocolul folosit pentru a accesa resursa. Exemple: http, https (secure http), ftp, ldap, rmi, ...

Host specifica server-ul unde este stocata resursa. Este specificat prin numele hostului (http://webhost.uoradea.ro) sau prin adresa IP a host-ului (xxx.yyy.zzz.ttt).

Port defineste portul de conectare la server. Acesta este determinat de protocol (http utilizeaza portul 80 sau 81, https utilizeaza portul 343, etc.).

Path specifica numele resursei pe host.

World Wide Web este un sistem de comunicare a informaţiilor hipertext folosit în general în reţeaua Internet. Funcţionează prin comunicare de date pe baza unui model client-server. Clienţii, adică navigatoarele Web, au acces la informaţiile hipermedia şi multiprotocol aflate pe un server Web.

Modelul client-server pentru calculatoarele conectate în reţea implică trei componente: clientul, serverul, reţeaua. Clientul este o aplicaţie care de obicei rulează pe calculatorul utilizatorului final. Serverul este o aplicaţie care de obicei rulează pe calculatorul furnizorului de informaţii.

Programul client este adaptat sistemului hardware pe care rulează şi funcţionează ca o interfaţă între sistemul respectiv şi informaţiile furnizate de server. Cererea este transportată prin reţea, de la client la server. Serverul analizează cererea şi execută activităţile corespunzătoare.

Protocolul HTTP (Hyper Text Transfer Protocol) este un protocol simplu, la nivel aplicaţie, în modelul TCP/IP. HTTP descrie cererile de la clienţi şi răspunsurile de la servere. Acesta foloseşte portul TCP 80.

**HTTP** (**H**yper**t**ext **T**ransfer **P**rotocol) este metoda cea mai des utilizată pentru accesarea informaţiilor în Internet care sunt păstrate pe servere World Wide Web (WWW). Protocolul HTTP este un protocol de tip text, fiind protocolul "implicit" al WWW. HTTP presupune că pe calculatoarele dest. rulează un program care înţelege protocolul. Fişierul trimis la destinaţie poate fi un document HTML (abreviaţie de la **H**yper**T**ext **M**arkup **L**anguage).

HTML este un fişier grafic, de sunet, animaţie sau video, de asemenea un program executabil pe server-ul respectiv sau şi un editor de text. După clasificarea după modelul de referinţă OSI, protocolul HTTP este un protocol de nivel aplicaţie. Realizarea şi evoluţia sa este coordonată de către World Wide Web Consortium (W3C). HTTP oferă o tehnică de comunicare prin care paginile web se pot transmite de la un computer aflat la distanţă spre propriul computer. Dacă se apelează un link sau o adresă de web cum ar fi http://www.example.com, atunci se cere calculatorului host să afişeze o pagină web (index.html sau altele). În prima fază numele (adresa) www.example.com este convertit de protocolul DNS într-o adresă IP. Urmează transferul prin protocolul TCP pe portul standard 80 al serverului HTTP, ca răspuns la cerere. Informaţii suplimentare ca de ex. indicaţii pentru browser, limba dorită ş.a. se pot adăuga în header-ul (antetul) pachetului HTTP. În urma cererii urmează din partea serverului răspunsul cu datele cerute, ca de ex.: pagini în (X)HTML, cu fişiere ataşate ca imagini, fişiere de stil (CSS), scripturi (Javascript), dar pot fi şi pagini generate dinamic (SSI, JSP, PHP şi ASP.NET). Dacă dintr-un anumit motiv informaţiile nu pot fi transmise, atunci serverul trimite înapoi un mesaj de eroare.

O modalitate de a furniza securitatea Web este utilizarea securităţii la nivel IP (IPSec). Avantajul utilizării IPSec este acela că este transparent pentru utilizatorii finali şi pentru aplicaţii. Mai mult, securitatea la nivel IP include posibilităţi de filtrare aşa încât numai mesajele selectate circulă în reţea.

O altă soluţie de a furniza securitatea Web este aceea de a implementa o securitate deasupra protocolului TCP.

Cel mai cunoscut exemplu este folosirea protocolului Secure Sockets Layer (SSL) şi a urmaşului lui SSL, numit Transport Layer Security (TLS). Browserele Netscape şi Microsoft Explorer au încorporate protocolul SSL şi cele mai multe servere Web au implementat acest protocol.

A treia soluţie pentru securitatea Web este folosirea unor aplicaţii cum ar fi: Kerberos, S/MIME, PGP, SET (Secure Electronic Transaction).

Netscape a introdus protocolul Secure Sockets Layer (SSL). In 1994 a fost proiectată versiunea SSL 1.0. In 1995 apare implementarea versiunii SSL 2.0 pe browserele Netscape.

In 1995 se publică versiunea 1.0 a PCT (Private Communication Technology) – concepută de Microsoft ca o extensie minoră a SSL 2.0. PCT se bazeaza pe SSL 2.0. Aceste puncte slabe au fost remediate odată cu versiunea SSL 3.0, tot în 1995.

Din 1996, dezvoltarea SSL a trecut în responsabilitatea organizaţiei internaţionale pentru standarde Internet, IETF (Internet Engineering Task Force). IETF a redenumit SSL în TLS (Transport Layer Security). Suportul pentru SSL este implementat în aproape toate browserele. Majoritatea serverelor suportă de asemenea comunicare peste SSL. Conventional URL-urile care implementeaza conexiunile SSL încep cu https:// în loc de http://. Tot din independenţa SSL ca şi protocol decurge şi alt avantaj: anume că SSL poate fi folosit în conjuncţie şi cu alte protocoale, nu doar cu HTTP.

SSL asigură îndeplinirea celor trei deziderate de securitate în comunicaţie, astfel:

* confidenţialitate - prin folosirea unui algoritm de criptare;
* autentificare - prin folosirea certificatelor digitale;
* controlul integrităţii - prin folosirea unor algoritmi pentru integritatea mesajelor.

Stabilirea tuturor elementelor menţionate mai jos:

* algoritmul de criptare (ex. DES – Data Encryption Standard, AES),
* schimbul de chei publice între server şi client,
* algoritmul pentru integritatea mesajelor (ex. MAC – Message Authentication Code),

se negociază la începutul comunicării SSL.

Scenariul de negociere a unui canal sigur de comunicaţie: cerere client catre server, verifică certificatul şi extrage cheia publică a Server-ului-Kpub-S,, certificatul lui S poate fi găsit pe Internet, e necesar să se asigure că nu e folosit de altcineva-verificare, C verifică faptul că mesajul vine de la S, C trimite la S o cheie de sesiune criptata cu cheia publica a lui S-Kpub-S

SSL poate fi divizat pe 2 niveluri: protocolul care asigura securitatea si integritatea datelor (SSL Record Protocol-Protocolul de înregistrare SSL) si Protocolul care stabileste conexiunile SSL ( Protocolul SSL Handshake -Protocolul dialogului de confirmare, Protocolul SSL Change Cipher -Protocolul modificare de cifru SSL, Protocolul SSL Alert -Protocolul de alerta SSL).