# PERTEMUAN 11
# KEAMANAN SISTEM WWW

## A. TUJUAN PEMBELAJARAN

Pada Pertemuan ini akan dijelaskan mengenai keamanan sistem www. Setelah mempelajari materi ini mahasiswa diharapkan mampu untuk:

1. Memahami keamanan sistem www
2. Memahami keamanan client server
3. Meningkatkan keamanan sistem www

## B. URAIAN MATERI

### 1. Memahami Keamanan Sistem WWW

WWW adalah jaringan virtual yang dilapisi di Internet. Ini terdiri dari semua sistem klien dan server yang berkomunikasi satu sama lain menggunakan Hypertext Transfer Protocol (HTTP). HTTP, pada gilirannya, adalah protokol aplikasi klien / server sederhana yang dilapisi di atas layanan transportasi yang andal, seperti yang disediakan oleh Transport Control Protocol (TCP). Protokol menentukan bagaimana sumber daya WWW dapat diminta dan dikirim melalui Internet.

HTTP dan WWW awalnya ditemukan pada akhir 1980-an oleh Tim Berners-Lee dan rekan-rekannya di Laboratorium Eropa untuk Fisika Partikel (CERN) yang berlokasi di Geneva, Swiss. Digambarkan sebagai cara menerbitkan makalah fisika di Internet tanpa mengharuskan fisikawan melalui proses yang melelahkan untuk mengunduh file dan mencetaknya. Dengan demikian, HTTP dan WWW telah digunakan sejak tahun 1989. Namun, perlu diketahui bahwa versi pertama HTTP, disebut sebagai HTTP / 0.9 (yaitu, HTTP versi 0.9), hanyalah protokol sederhana untuk transfer data mentah melintasi Internet. Setelah implementasi pertama HTTP / 0.9, protokol ditingkatkan dengan beberapa fitur baru, seperti meminta header dan metode permintaan tambahan, serta format pesan yang sesuai dengan spesifikasi ekstensi email Internet multiguna (MIME) yang semula diusulkan untuk Internet olahpesan berbasis

elektronik. Spesifikasi HTTP / 1.0 (versi 1.0) yang dihasilkan secara resmi dirilis pada tahun 1996 di RFC 1945.

Awalnya dikembangkan di komputer NeXT, WWW tidak benar-benar lepas landas sampai tim peneliti di National Center for Supercomputer Application (NCSA) dari University of Illinois menulis Mosaic, browser untuk sistem X Window. Pada awal 1990-an, browser ini segera menjadi standar pembanding semua browser lainnya. Marc Andreessen, yang merupakan kepala tim pengembangan Mosaic asli, kemudian menjadi salah satu pendiri perusahaan baru bernama Mosaic Communications. Perusahaan pertama kali membuat browser baru bernama Mozilla. Setelah itu, perusahaan berganti nama menjadi Netscape Communications dan peramban yang sesuai diganti namanya menjadi Netscape Navigator. Setelah Microsoft merilis browsernya sendiri, disebut Internet Explorer, Netscape Communications dan Microsoft memulai persaingan ketat untuk pangsa pasar. Kompetisi tersebut berakhir pada tahun 1998 ketika America On-line (AOL) membeli Netscape Communications. Netscape Navigator masih tersedia dan digunakan sampai sekarang, tetapi telah kehilangan banyak pangsa pasar. Alih-alih Netscape Navigator, browser baru bernama Opera digunakan dan digunakan secara luas di Internet saat ini. Opera telah dikembangkan di Norwegia untuk memenuhi kebutuhan klien dengan daya komputasi terbatas. Dengan demikian, ini adalah browser pilihan bagi banyak pengguna personal digital assistant (PDA) dan perangkat komputer genggam. Saat tulisan ini dibuat, sulit untuk mengatakan apakah Microsoft Internet Explorer akan meningkatkan pangsa pasarnya atau kehilangannya ke pesaing, seperti Opera.

Teknologi HTTP dan Web ada di mana-mana di Internet, dan semakin banyak layanan Internet telah didesain ulang dan diimplementasikan sehingga juga dapat diakses dari browser standar standar (bukan dari satu klien perangkat lunak khusus). Misalnya, sebagian besar browser menerapkan File Transfer Protocol (FTP) selain HTTP, dan dapat digunakan untuk mengunduh file secara elektronik. Oleh karena itu, browser ini dapat berfungsi sebagai alat pengganti untuk klien FTP lama. Selain itu, banyak pengguna email secara rutin mengakses penyimpanan pesan mereka menggunakan HTTP dan browser web, bukan agen pengguna email dan protokol akses penyimpanan pesan seperti POP3 atau IMAP4. Faktanya, webmail telah menjadi sangat populer di masa lalu (terutama di antara pengguna roaming) dan banyak perusahaan telah memasang dan

mengoperasikan antarmuka web yang sesuai untuk infrastruktur email mereka. Dalam kasus Microsoft Exchange, misalnya, Outlook Web Access dapat menyediakan jenis fungsionalitas ini.

Kerentanan, Ancaman, dan Penanggulangannya

Secara umum, kerentanan mengacu pada kelemahan yang dapat dimanfaatkan oleh seseorang (misalnya, seorang penyusup) untuk melanggar sistem atau informasi yang dikandungnya. Dalam jaringan komputer atau sistem terdistribusi, kata sandi yang dikirimkan dalam teks yang jelas seringkali merupakan kerentanan yang signifikan. Kata sandi rentan terhadap penyadapan dan serangan pelacakan yang sesuai. Demikian pula, kemampuan host jaringan untuk melakukan booting dengan alamat jaringan yang awalnya ditetapkan ke host lain mengacu pada kerentanan lain yang dapat digunakan untuk memalsukan host tersebut dan melakukan spoof yang sesuai. Sayangnya, kekuatan teknologi web secara umum dan HTTP pada khususnya juga membuat WWW rentan terhadap sejumlah serangan serius.

Ancaman mengacu pada keadaan, kondisi, atau peristiwa yang dapat melanggar keamanan sistem atau merusak sumber daya sistem. Jaringan komputer dan sistem terdistribusi rentan terhadap berbagai macam ancaman yang dapat dipasang oleh penyusup atau pengguna yang sah. Faktanya, pengguna yang sah adalah musuh yang lebih kuat karena mereka memiliki informasi orang dalam yang biasanya tidak tersedia untuk penyusup. Terakhir, tindakan balasan adalah fitur atau fungsi yang mengurangi atau menghilangkan satu (atau lebih) kerentanan dalam sistem atau terhadap satu (atau lebih) ancaman. Misalnya, penggunaan teknik otentikasi yang kuat mengurangi kerentanan kata sandi yang ditransmisikan dengan jelas dan menggagalkan ancaman perayapan kata sandi dan serangan ulang. Selain itu, penggunaan otentikasi kriptografi pada lapisan jaringan secara efektif menghilangkan serangan berdasarkan spoofing alamat IP mesin lain dan terhadap serangan spoofing IP.

## 2. Memahami Keamanan Client - Server

Pelanggaran Privacy Ketika kita mengunjungi sebuah situs web, browser kita dapat “dititipi” sebuah “cookie” yang fungsinya adalah untuk menandai kita. Ketika kita berkunjung ke server itu kembali, maka server dapat mengetahui

bahwa kita kembali dan server dapat memberikan setup sesuai dengan keinginan (preference) kita. Ini merupakan servis yang baik. Namun data-data yang sama juga dapat digunakan untuk melakukan tracking kemana saja kita pergi.

Ada juga situs web yang mengirimkan script (misal Javascript) yang melakukan interogasi terhadap server kita (melalui browser) dan mengirimkan informasi ini ke server. Bayangkan jika di dalam komputer kita terdapat data-data yang bersifat rahasia dan informasi ini dikirimkan ke server milik orang lain.

a. Penyisipan Trojan Horse

Cara penyerangan terhadap client yang lain adalah dengan menyisipkan virus atau trojan horse. Bayangkan apabila yang anda download adalah virus atau trojan horse yang dapat menghapus isi harddisk anda. Salah satu contoh yang sudah terjadi adalah adanya web yang menyisipkan trojan horse Back Orifice (BO) atau Netbus sehingga komputer anda dapat dikendalikan dari jarak jauh. Orang dari jarak jauh dapat menyadap apa yang anda ketikkan, melihat isi direktori, melakukan reboot, bahkan memformat harddisk. SSH memiliki port default 22, jadi agar tidak semua orang mengetahui port yang Anda gunakan untuk login maka sebaiknya merubah port standart. Dengan merubah port default akan membuat orang lain kesulitan saat mengakses server. Selain itu dengan port SSH sudah tidak standart lagi akan mencegah dari script jahat yang mencoba masuk lewat port standart yang belum diganti.

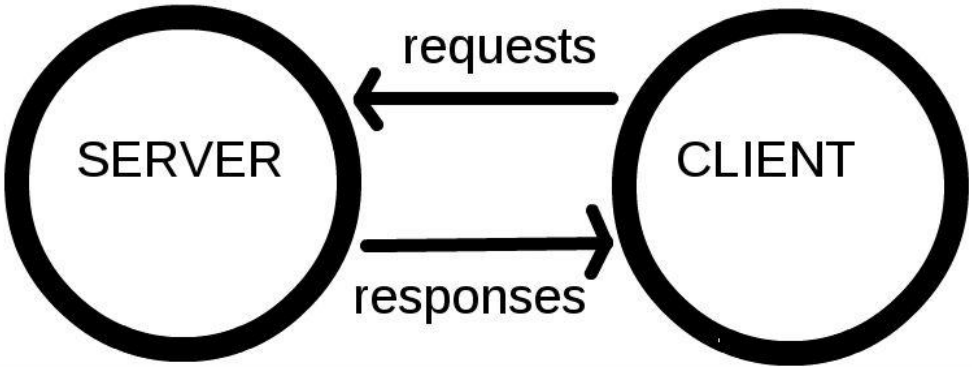
Untuk merubah port SSH standart caranya gampang, Anda tinggal masuk ke bagian file konfigurasi SSH sesuai dengan sistem operasi yang diinstall pada server. Selain itu perlu dicatat juga jangan sampai port yang Anda rubah bertabrakan dengan port aplikasi lain yang bisa menyebabkan error pada server.

Secara default server akan memberikan password hasil generator yang kuat, tetapi memang sulit sekali diingat, solusinya Anda bisa mencatatnya. Password ini menjadi ancaman terbesar dalam keamanan internet, jadi jangan sampai asal membuat password seperti 12345, abcde, ~!@#$%, rahasia dan password lemah lainnya. Untuk proteksi keamanan server tambahan, Anda bisa mengaktifkan two factor authentication, sehingga saat login akan selalu meminta kode verifikasi yang dikirimkan kepada Anda.

Selain menggunakan password yang kuat, ada satu hal penting yaitu menonaktifkan akun root server. Bayangkan jika ada hacker yang bisa mengakses root server, semua file yang ada pada server bisa dikuasainya dengan mudah. Hal ini cukup berbahaya untuk keamanan server website, solusinya bisa dengan menonaktifkan akun root server. Jadi untuk amannya Anda bisa memberikan permission untuk setiap orang yang login sesuai dengan keperluannya saja, tidak perlu memberikan akses full root kepada user.

b. Aplikasi Web

Pada awalnya aplikasi Web dibangun hanya dengan menggunakan bahasa yang disebut HTML (HyperText Markup Language). Pada perkembangan keamanan client WWW Pelanggaran Privacy Adanya penyimpanan data browsing pada “cookie” yang fungsinya adalah untuk menandai kemana user browsing.- Adanya situs web yang mengirimkan script (misal Javascript) yang melakukan interogasi terhadap server client (melalui browser) dan mengirimkan informasi ini ke server.Attack (via active script, javascript, java)- Pengiriman data-data komputer (program apa yang terpasang, dsb.)- DoS attack (buka windows banyak)- Penyusupan virus, trojan horse, spyware. Berikutnya, sejumlah skrip dan objek dikembangkan untuk memperluas kemampuan HTML. • Aplikasi Web itu dapat dibagi menjadi Web statis dan Web dinamis • Dari sisi teknologi yang digunakan untuk membentuk web dinamis terdapat dua pengelompokan, yaitu teknologi pada sisi client dan teknologi pada sisi server.




**Gambar 15 .** *Ilustrasi Client Server*

Aplikasi Web-Client Side Programming • Teknologi Web pada sisi client diimplementasikan dengan mengirimkan kode perluasan HTML atau program tersendiri dan HTML ke client. • Clientlah yang bertanggung jawab dalam melakukan proses terhadap seluruh kode yang diterima. • Kelemahan pendekatan seperi ini adalah terdapat kemungkinan bahwa browser pada client tidak mendukung fitur kode perluasan HTML. • Kelebihan teknologi pada sisi client, yaitu memungkinkan penampilan yang bersifat dinamis. • Contoh teknologi pada sisi client, yaitu Kontrol ActiveX, Java Applet, dan Skrip sisi-client

c. Aplikasi Web-Server Side Programming

Teknologi Web pada sisi server memungkinkan pemrosesan kode di dalam server sehingga kode yang sampai pada pemakai berbeda dengan kode asli pada server. Contoh teknologi yang berjalan di server, yaitu CGI, ASP, JSP, PHP dan lain sebagainya. Keuntungan penggunaan teknologi pada sisi server adalah sebagai berikut:

1) Mengurangi lalu lintas jaringan dengan cara menghindari percakapan bolak-balik antara client dan server.
2) Mengurangi waktu pemuatan kode, mengingat client hanya mengambil kode HTML saja.
3) Mencegah masalah ketidakkompatibelan browser. – Client dapat berinteraksi dengan data yang ada pada server.
4) Mencegah client mengetahui rahasia kode (mengingat kode yang diberikan ke client berbeda dengan kode asli pada server) (Nugroho, 2004).

d. Aplikasi Web-Client Side Programming

Teknologi Web pada sisi client diimplementasikan dengan mengirimkan kode perluasan HTML atau program tersendiri dan HTML ke client. • Clientlah yang bertanggung jawab dalam melakukan proses terhadap seluruh kode yang diterima. • Kelemahan pendekatan seperi ini adalah terdapat kemungkinan bahwa browser pada client tidak mendukung fitur kode perluasan HTML. • Kelebihan teknologi pada sisi client, yaitu memungkinkan penampilan yang bersifat dinamis. • Contoh teknologi pada sisi client, yaitu Kontrol ActiveX, Java Applet, dan Skrip sisi-client.

### 3. Meningkatkan Keamanan Sistem WWW

Keamanan server WWW biasanya merupakan masalah dari seorang administrator. Dengan memasang server WWW di system, berikut cara untuk meningkatkan keamanan sistem www :

a. Proteksi halaman dengan menggunakan password

Salah satu mekanisme mengatur akses adalah dengan menggunakan pasangan userid (user identification) dan password. Untuk server Web yang berbasis Apache, akses ke sebuah halaman (atau sekumpulan berkas yang terletak di sebuah directory di sistem Unix) dapat diatur dengan menggunakan berkas ".htaccess".

b. Membatasi Akses

Penyedia informasi dalam bentuk berkas, sering inginkan pembatasan akses. Contoh, ingin agar orang-orang tertentu saja yang mampu mengakses berkas (informasi) tertentu. Pada prinsipnya ini adalah perkara *access control*. Pembatasan akses dapat dilakukan dengan:

1) Pembatasan domain atau IP yang mengakses;
2) Gunakan userid & password;
3) Mengenkripsi data sehingga dapat didekripsi oleh orang yang memiliki kunci pembuka saja.
4) Menggunakan token.
5) Mekanisme untuk kontrol akses ini bergantung pada program yang digunakan sebagai server.

c. Membatasi htaccess Apache

Berikut ini cara untuk membatasi htaccess di Apache :

1) Isi berkas ".htaccess" AuthUserFile /home/Lias/passme
   AuthGroupFile /dev/null AuthName "Khusus tamu Lias"
   AuthType Basic <Limit GET> require user tamu </Limit>
2) Membatasi akses ke user "tamu" dan password
3) Menggunakan perintah "htpasswd" untuk membuat password yang disimpan di ".passme"

d. Secure Socket Layer (SSL)

Menggunakan enkripsi untuk mengamankan transmisi data Mulanya dikembangkan oleh Netscape Implementasi gratis pun tersedia openSSL. Beberapa masalah dengan SSL ASN.1 compiler yang bermasalah menimbulkan masalah di beberapa implementasi SSL (sehingga server down)

Salah satu cara untuk meningkatkan keamanan server WWW adalah dengan menggunakan enkripsi pada komunikasi pada tingkat socket. Dengan menggunakan enkripsi, orang tidak bisa menyadap data-data (transaksi) yang dikirimkan dari/ke server WWW. Salah satu mekanisme yang cukup populer adalah dengan menggunakan Secure Socket Layer (SSL) yang mulanya dikembangkan oleh Netscape.

Sejauh ini ada tiga versi SSL:

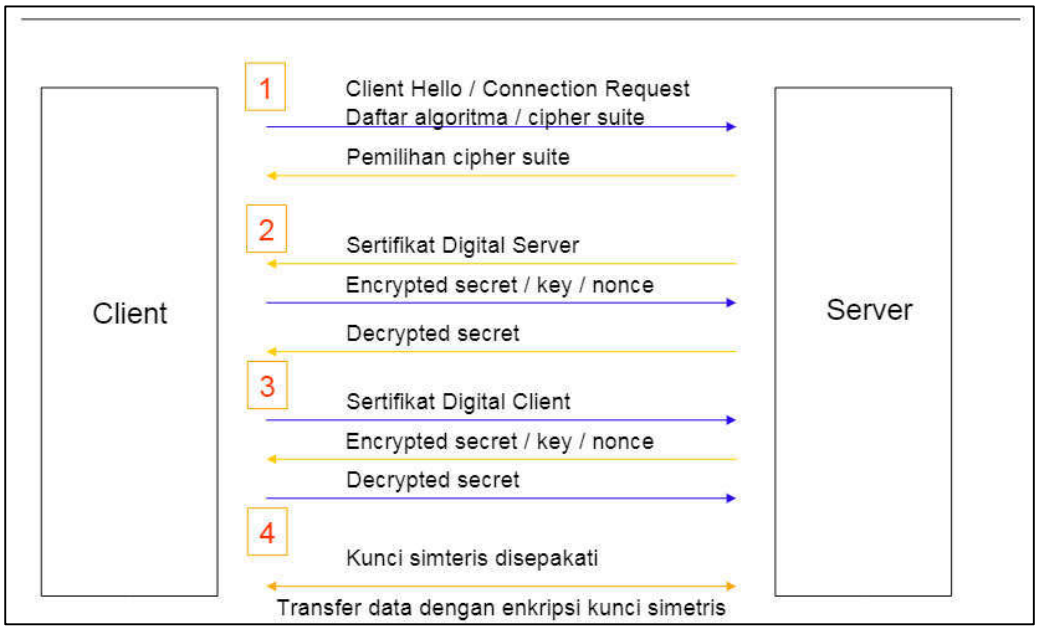
1) SSL versi 1.0 telah digunakan secara internal hanya oleh Netscape Communications. Itu berisi kekurangan yang serius dan tidak pernah dipublikasikan.

2) SSL versi 2.0 telah dimasukkan ke dalam Netscape Navigator versi 1.0 hingga 2.x. Itu memiliki beberapa kelemahan yang berhubungan dengan inkarnasi spesifik dari serangan man-in-the-middle. Dalam upaya mengambil keuntungan dari ketidakpastian publik tentang keamanan SSL, Microsoft juga memperkenalkan protokol Teknologi Komunikasi Pribadi Kompetitif (PCT) dalam versi pertama Internet Explorer pada tahun 1996.

3) Netscape Communications menanggapi tantangan PCT Microsoft dengan memperkenalkan SSL versi 3.0, yang membahas masalah SSL 2.0 dan menambahkan fitur baru. Pada titik ini, Microsoft mundur dan setuju untuk mendukung SSL pada semua versi perangkat lunak berbasis TCP / IP (walaupun perangkat lunaknya sendiri masih sesuai dengan PCT untuk kompatibilitas ke belakang).

Selain server WWW dari Netscape, beberapa server lain juga memiliki fasilitas SSL juga. Server WWW Apache (yang tersedia secara gratis) dapat dikonfigurasi agar memiliki fasilitas SSL dengan menambahkan software tambahan (SSLeay - yaitu implementasi SSL dari Eric Young - atau OpenSSL-yaitu implementasi Open Source dari SSL). Bahkan ada sebuah perusahaan (Stronghold) yang menjual Apache dengan SSL.

Info server Informasi tentang server digunakan sebagai bagian dari casing the joint Dapat dilakukan dengan Memberikan perintah HTTP langsung via telnet Menggunakan program netcat




**Gambar 16**. *Client - Server*

e. Kemanan CGI

Common Gateway Interface (CGI) digunakan untuk menghubungkan sistem WWW dengan software lain di server web. Adanya CGI memungkinkan hubungan interaktif antara user dan server web. CGI seringkali digunakan sebagai mekanisme untuk mendapatkan informasi dari user melalui “fill out form”, mengakses database, atau menghasilkan halaman yang dinamis.

Meskipun secara prinsip mekanisme CGI tidak memiliki lubang keamanan, program atau skrip yang dibuat sebagai CGI dapat memiliki lubang keamanan (baik secara sengaja dibuat lubang keamanannya ataupun tidak sengaja). Pasalnya, program CGI ini dijalankan di server web sehingga menggunakan resources web server tersebut. Pada mulanya CGI digunakan sebagai interface dengan sistem informasi lainnya (gopher, WAIS, ftp). Diimplementasikan dengan berbagai bahasa (perl, C, C++, python, sh, dll.). Skrip CGI dijalankan di server (oleh siapa saja dari jaringan) sehingga membuka potensi lubang keamanan jika skrip tidak dibuat dengan baik.

f. Kemanan Lubang CGI
   1) CGI dipasang oleh orang yang tidak berhak
   2) CGI dijalankan berulang-ulang untuk menghabiskan resources (CPU, disk): DoS Masalah setuid CGI di sistem UNIX, dimana CGI dijalankan oleh userid web server Penyisipan karakter khusus untuk shell expansion
   3) CGI yang lemah sehingga dapat mengambil berkas yang
   4) seharusnya tidak berhak atau mengeksekusi perintah yang seharusnya tidak dilakukan (misal: wget trojanhorse, eksekusi trojanhorse). Contoh kelemahan awstats
   5) Kelemahan ASP di sistem Windows
   6) Guestbook abuse dengan informasi sampah (link ke pornografi atau sekedar info yang berulang)

Web & SQL Banyak aplikasi (transaksi) menggunakan basis web untuk mengakses database Juga dynamic web site Database diakses melalui SQL Sayangnya seringkali implementasi teledor SQL injection attack Memasukkan perintah-perintah SQL yang nakal dengan akibat yang berbeda (server down, database berubah) drop table tanda petik UNION/OR Tidak terdeteksi oleh firewall atau IDS karena pada level aplikasi.

Berhubungan dengan masalah privacy Cookies untuk tracking kemana saja browsing Pengiriman informasi pribadi Attack (via active script, javascript, java) Pengiriman data-data komputer (program apa yang terpasang, dsb.) DoS attack (buka windows banyak) Penyusupan virus, trojan horse, spyware Security hole di JPEG bisa mengeksekusi aplikasi di sisi client. WWW merupakan salah satu aplikasi utama Internet dan Intranet Meskipun memiliki banyak keuntungan, sistem www masih banyak lubang keamanan – baik di sisi server maupun di sisi client.

## C. SOAL LATIHAN/ TUGAS

1. Jelaskan keamanan sistem WWW yang Anda ketahui!
2. Apa yang di maksud dengan Keamanan Client Server?
3. Jelaskan tentang SSL yang anda ketahui!
4. Bagaimana pencegahan keamanan Protokol SSL?

## D. REFERENSI

Bishop, M. (2019). *Computer Security Art and Science*. 2nd Edition. Boston: Pearson Education Inc.

Goodrich, M., & Tamassia, R. (2014). Introduction to Computer Security. Harlow: Pearson Education Ltd.

Panek, C. (2020). Security Fundamental. Canada: Sybex A Wiley Brand.

Pfleeger, P. C., Pfleeger, S. L., & Margulies, J. (2015). Security in Computing. 5th Edition. Westford: Pearson Education Inc.

Salomon, D. (2006). Foundations of Computer Security. Springer Science+Business Media

Nieles, M., Dempsey, K., & Pillitteri, P. Y. Computer Security. National Institute of Standards and Technology [Internet]. Juni 2017. NIST Pubs. Tersedia pada: https://www.nist.gov/publications/introduction-computer-security-nist-handbook

Paulsen, C., & Byers, R. D. *Glossary of Key Information Security Terms* [Internet]. Juli 2019. NIST Pubs. Tersedia pada: https://www.nist.gov/publications/glossary-key-information-security-terms-2, https://csrc.nist.gov/glossary

Shirey, R. (2007). Internet Security Glossary version 2. (diakses 24 Oktober 2020). Tersedia pada: https://www.rfc-editor.org/info/rfc4949

Buku Tim Berners-Lee, “Weaving the Web”