Keamanan Sistem Komputer

Network Encryption, Browser Encryption, IP Sec, VPN, Firewall, IDS

Cryptography in Network Security

- Mengimplementasi kedua metode enkripsi
  - Kunci Simetrik, digunakan untuk enkripsi dengan jumlah data yang besar, cocok untuk menangani data di traffic jaringan computer.
  - Kunci Asimetrik, digunakan untuk autentikasi dan membuktikan kepercayaan antara kedua belah pihak dan hal ini dapat saja terjadi pada situasi jaringan komputer.

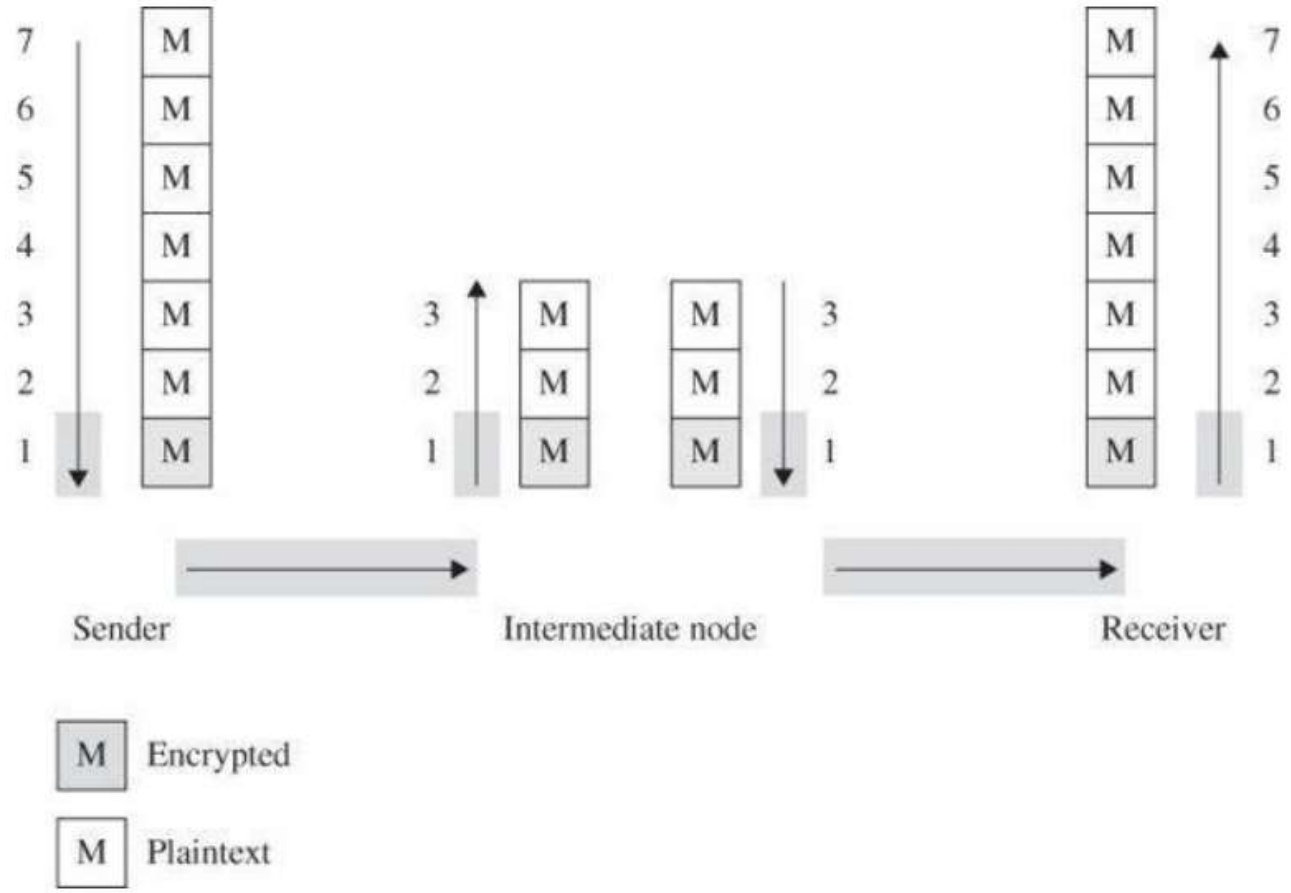
Security Objectives

- Menjaga Kerahasiaan data dari computer lain
- Komunikasi dengan user luar jaringan tidak dinginkan
- Sembunyikan data traffic sebanyak mungkin
- Keamanan lebih penting dari cost

Network Encryption

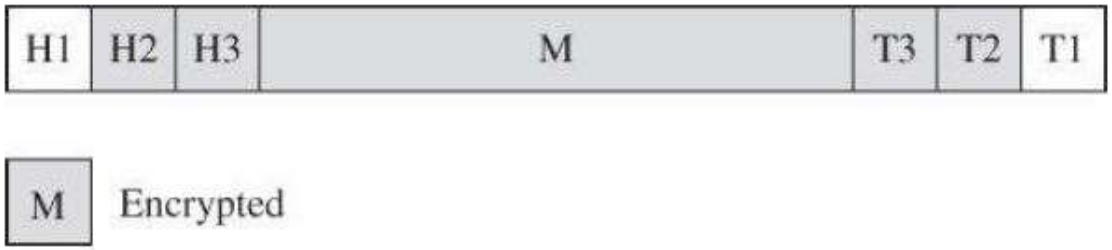
- Enkripsi hanya dapat memproteksi data pada saat TELAH dienkrip, tidak akan pernah dapat bertahan dari pencurian data tepat sesaat sebelum dienkripsi.
- Perancangan sistem enkripsi sebaiknya dilakukan oleh yang sudah ahli, hal ini dikarenakan perubahan kecil pada sistem (enkripsi) dapat memiliki pengaruh yang sangat besar dari sisi keamanan sistem
- Sistem pertukaran dan penggunaan kunci sangat menjadi masalah. Apabila kunci yang digunakan lemah, semua SELESAI (THE END, GAME OVER)
- Sistem keamanan dengan enkripsi, tidak membuat sistem MUTLAK aman. Terutama apabila diterapkan pada sistem yang sudah lemah
- Pada aplikasi jaringan, enkripsi dapat diterapkan diantara 2 host (link encryption) atau berada diantara 2 aplikasi (called end-to-end encryption).

Network Encryption (Link Encryption)



Network Encryption (Link Encryption)

- Data dienkrip sesaat sebelum sistem menempatkannya di layer fisik
- Dekripsi data dilakukan ketika sudah mencapai tujuannya dan dilakukan setelah masuk ke dalam layer fisik penerima
- Di titik tengah, cipher text harus dikembalikan menjadi plain text sehingga switch/router dapat mengetahui tujuan paket ini dikirim.
- Link encryption melindungi komunikasi antara titik yang satu dengan lainnya sampai dengan diterima di tujuannya
- Enkripsi model ini sangat cocok apabila jalur transmisi merupakan celah terbesar dalam komunikasi pada jaringan computer yang ada

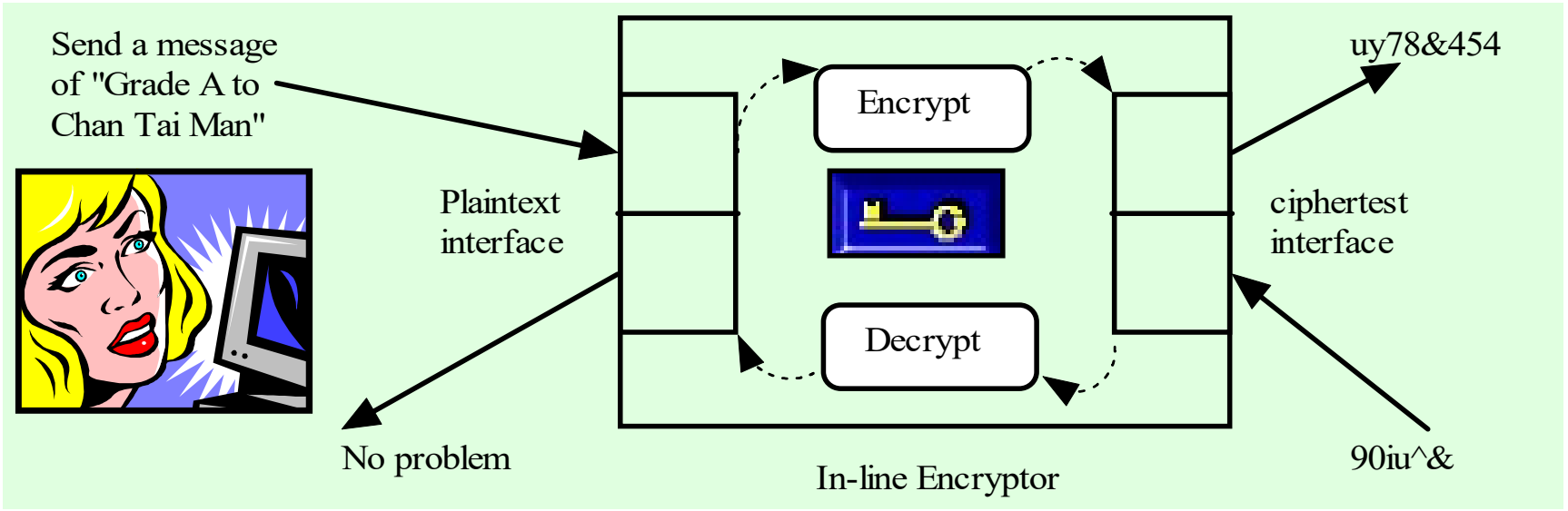


In-line Encryptor Hardware

In-line Network Encryptor

Code Encryptor

Inside In-line Encryptor



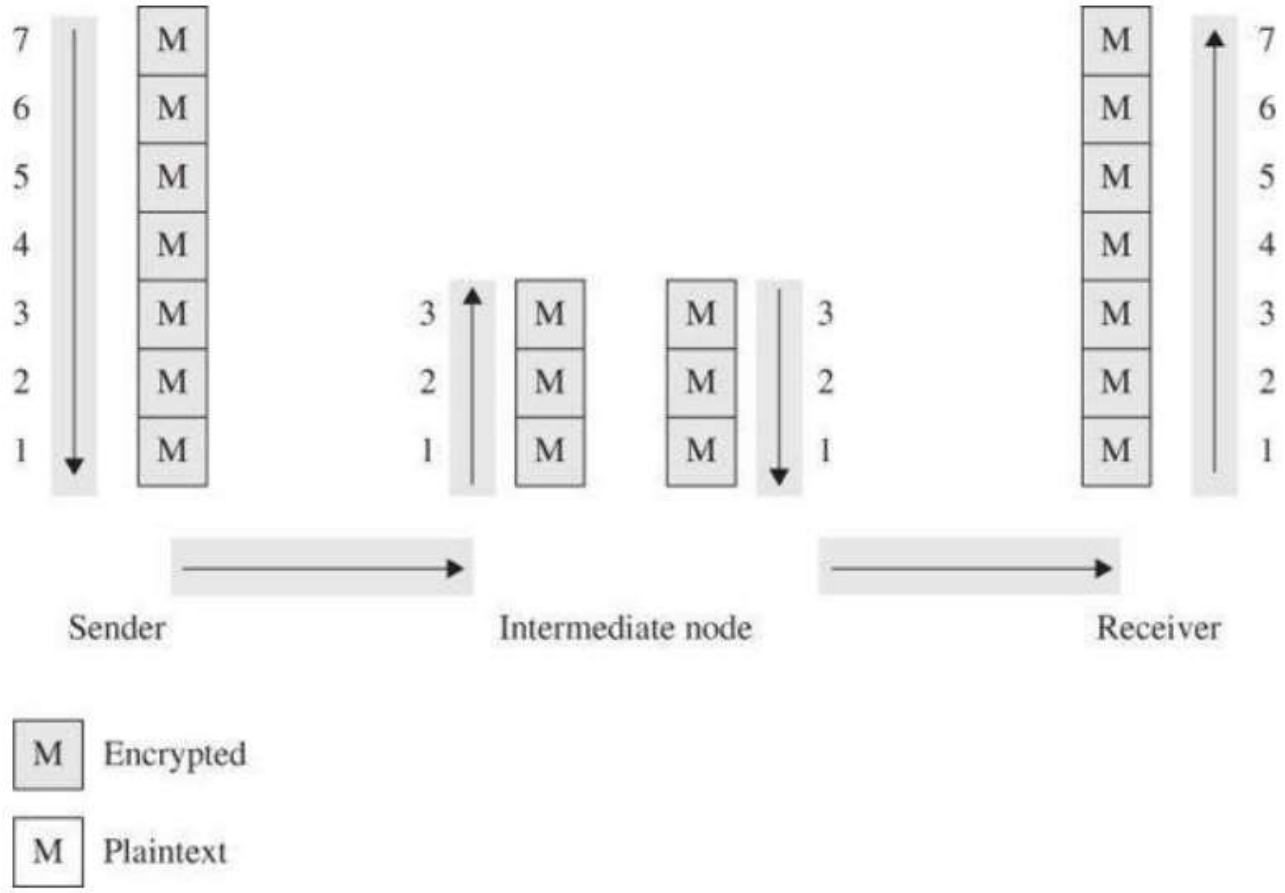
Features of In-line Encryptor

- Plain text dan cipher text terpisah
- Menggunakan Stream/Block Cipher
- Pada prakteknya lebih digunakan RC4 untuk mode komersial

Attacks in Link Encryption

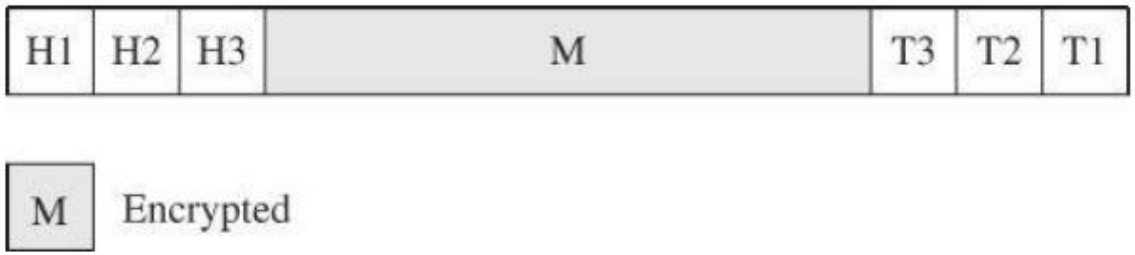
- Replay Attacks
  - Korban akan menerima message yang sama secara berulang
- Rewrite Attacks
  - Attacker dapat menulis ulang/modifikasi cipher text, sehingga plain text memiliki arti yang berbeda
- Convert Signaling Attacks
  - Attacker mendapatkan data penting melalui spyware yang sudah ditanam di korban

Network Encryption (End-to-End Encryption)



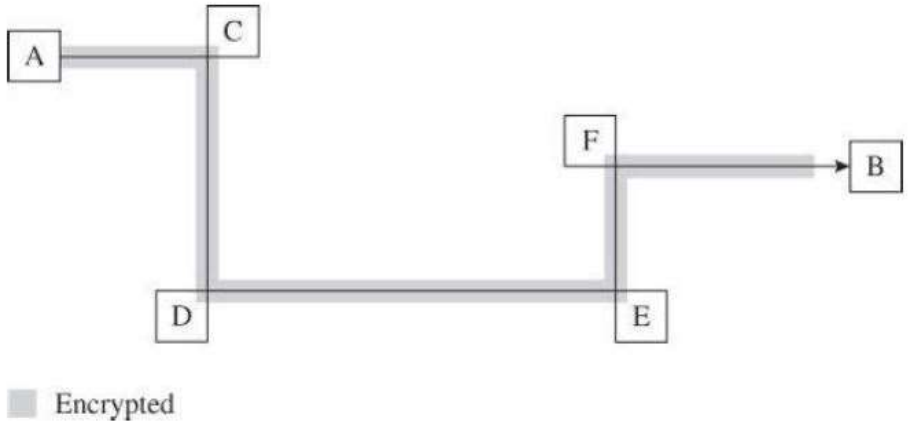
Network Encryption (End-to-End Encryption)

- Menerapkan keamanan pada end-user application (layer 7) pengirim, hingga ke end-user application penerima
- Enkripsi dapat diimplementasi antar user dengan menggunakan perangkat keras atau menggunakan software yang ada di salah satu user (host)
- Atau dengan kata lain proses enkripsi dilakukan pada layer paling atas
- Data yang ditransmisikan, dikirimkan dengan menerapkan enkripsi ke seluruh layer yang dilaluinya
- End-to-end encryption melindungi komunikasi dari pengirim ke penerima secara utuh.



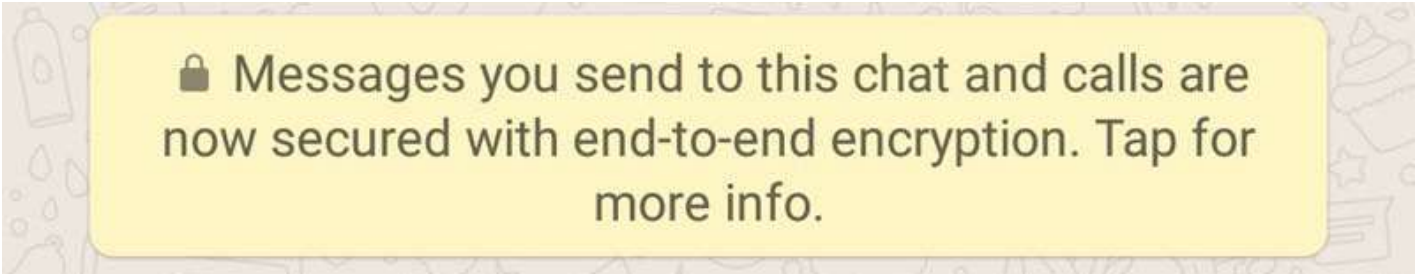
Network Encryption (End-to-End Encryption)

- Pada End-to-End Encryption, data yang dikirimkan yang melalui beberapa node transit, akan tetap terenkripsi
- Hal ini diuntungkan apabila ternyata node yang dilewati ternyata tidak aman.



Implementation

- Trend : Secure chat



- Fyi, walaupunkita sudah men-delete chat yang ada pada akun WA kita, data tersebut masih ada di dalam database, dan tidak didelete, akan tetapi hanya dapat diakses dengan melakukan tindakan forensic fisik

Link Encryption	End-to-End Encryption
Security within hosts	
Data partially exposed in sending host	Data protected in sending host
Data partially exposed in intermediate nodes	Data protected through intermediate nodes
Role of user	
Applied by sending host	Applied by user application
Invisible to user	User application encrypts
Host administrators select encryption	User selects algorithm
One facility for all users	Each user selects
Can be done in software or hardware	Usually software implementation; occasionally performed by user add-on hardware
All or no data encrypted	User can selectively encrypt individual data items
Implementation considerations	
Requires one key per pair of hosts	Requires one key per pair of users
Provides node authentication	Provides user authentication

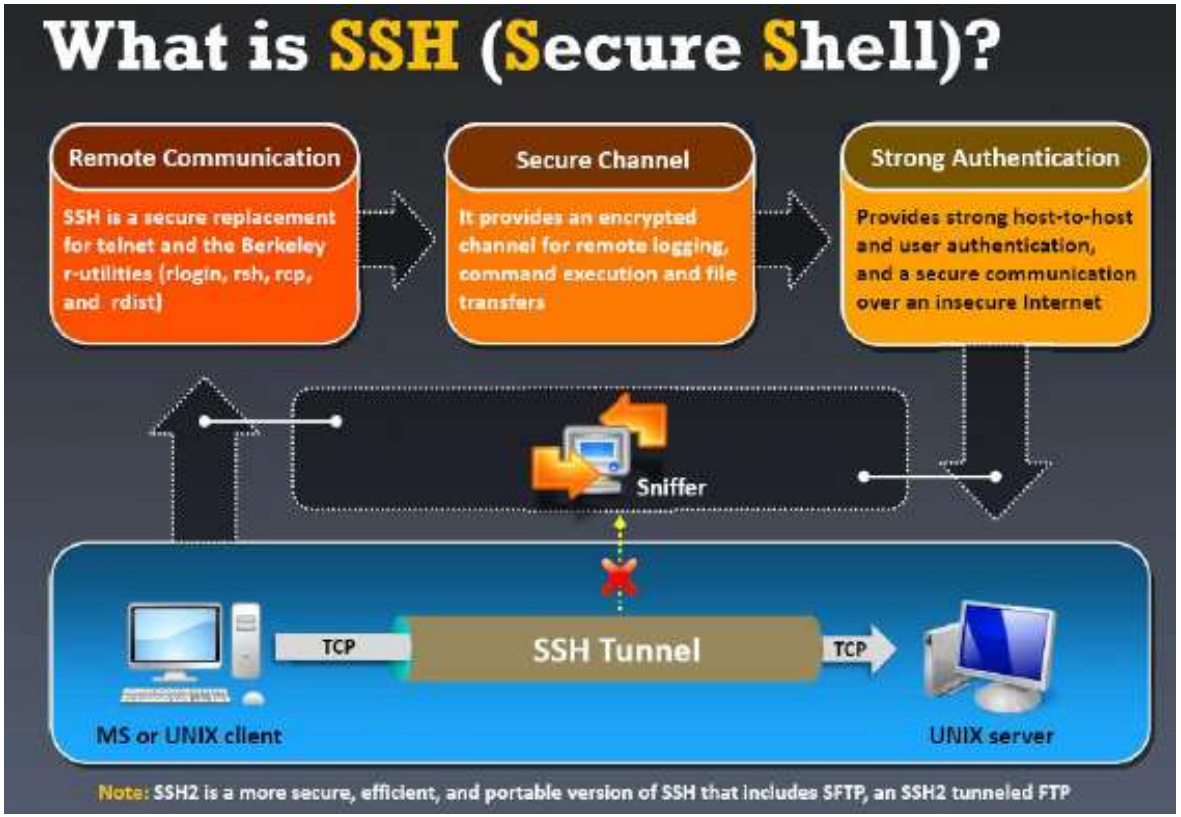
Internet Cryptographic Protocols

Protocol	Purpose
CyberCash (5)	Electronic funds transactions
DNSSEC (5)	Domain Name System
IPSec (layer 3)	Packet-level encryption
PCT	TCP/IP level encryption
PGP (layer 5)	E-mail
S-HTTP (layer 5)	Web browsing
Secure RPC	Remote procedure calls
SET (layer 4)	Electronic funds transactions
SSL (layer 4)	TCP/IP level encryption

Browser Encryption (SSH Encryption)

- Melibatkan negosiasi antara computer yang berada di area lokal dan remote untuk melakukan autentikasi.
- SSH mendukung kanal yang aman ketika komunikasi terjalin pada unsecured network
- Versi Mayor SSH : SSH-1 & SSH-2
- SSH didesain untuk menggantikan Telnet, rlogin, rsh, rexec
- Enkripsi pada SSH mendukung kerahasiaan dan keutuhan data yang ditransmisikan melalui unsecured network
- Menggunakan public-key cryptography

Browser Encryption (SSH Encryption)



Uses of SSH Encryption

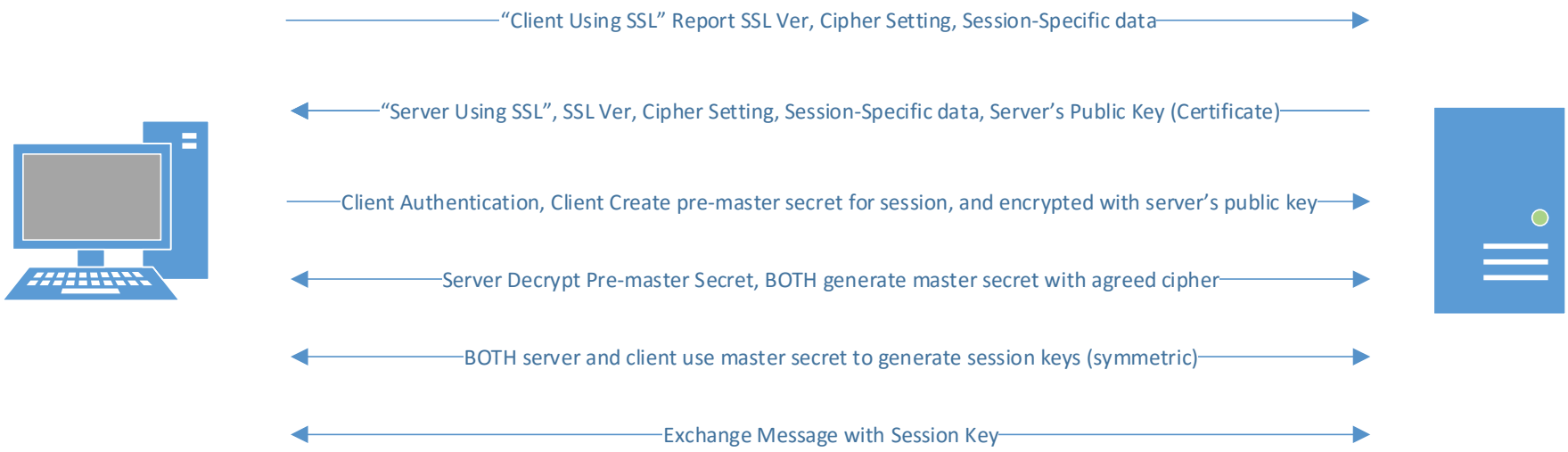
- For login to a shell on a remote host (replacing Telnet and rlogin)
- For executing a single command on a remote host (replacing rsh)
- For setting up automatic (passwordless) login to a remote server (for example, using OpenSSH)
- Secure file transfer
- In combination with rsync to back up, copy and mirror files efficiently and securely
- For forwarding or tunneling a port (not to be confused with a VPN, which routes packets between different networks, or bridges two broadcast domains into one).
- For using as a full-fledged encrypted VPN. Note that only OpenSSH server and client supports this feature.
- For forwarding X from a remote host (possible through multiple intermediate hosts)
- For browsing the web through an encrypted proxy connection with SSH clients that support the SOCKS protocol.
- For securely mounting a directory on a remote server as a filesystem on a local computer using SSHFS.
- For automated remote monitoring and management of servers through one or more of the mechanisms discussed above.
- For development on a mobile or embedded device that supports SSH.

Browser Encryption (SSL/TLS Encryption)

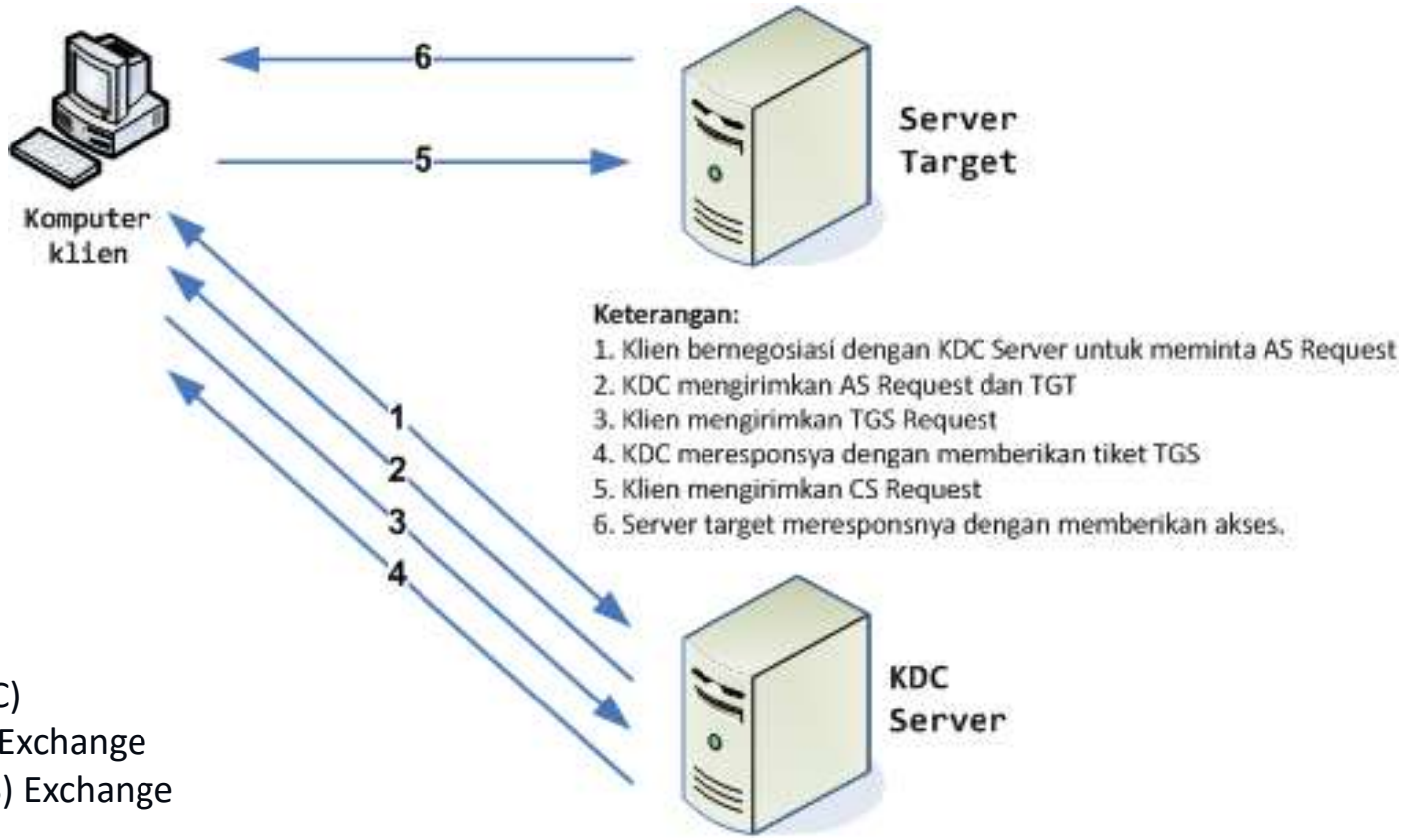
- SSL and TLS Encryption; melindungi komunikasi antara browser dan web host
  - Cipher Suite; proses negosiasi antara client dan server untuk mendapatkan autentikasi, enkripsi, MAC (message authentication code), algoritma pertukaran kunci, yang nantinya akan digunakan pada saat menjalankan SSL/TLS

Browser Encryption (SSL/TLS Encryption)

- SSL and TLS Encryption; melindungi komunikasi antara browser dan web host



Kerberos



Keterangan:

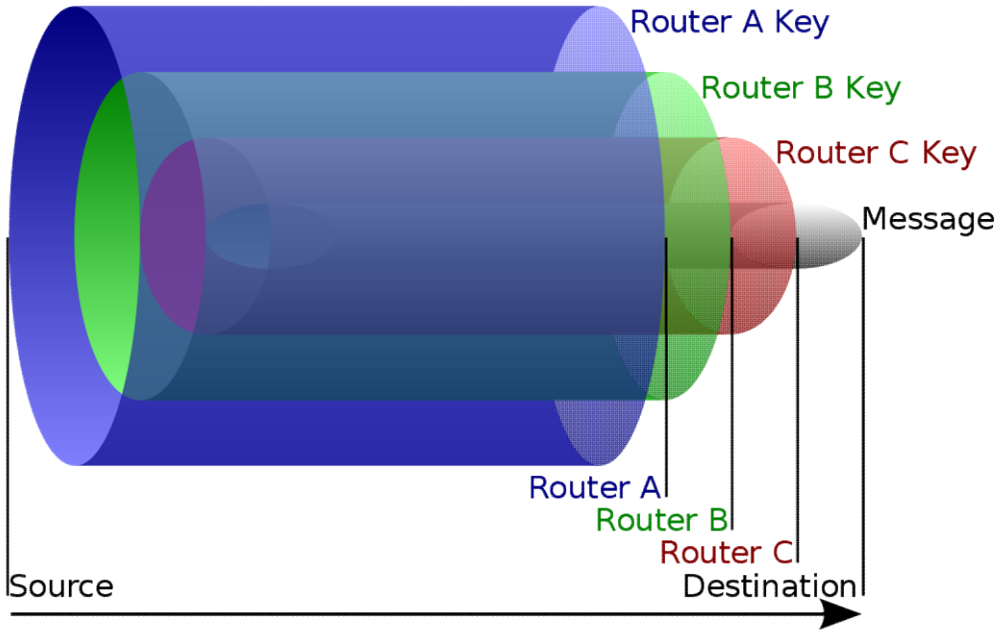
1. Klien bernegosiasi dengan KDC Server untuk meminta AS Request
2. KDC mengirimkan AS Request dan TGT
3. Klien mengirimkan TGS Request
4. KDC meresponsya dengan memberikan tiket TGS
5. Klien mengirimkan CS Request
6. Server target meresponsnya dengan memberikan akses.

Key Distribution Center (KDC)
Authentication Service (AS) Exchange
Ticket-Granting Service (TGS) Exchange
Client/Server (CS) Exchange

TOR (The Onion Router)

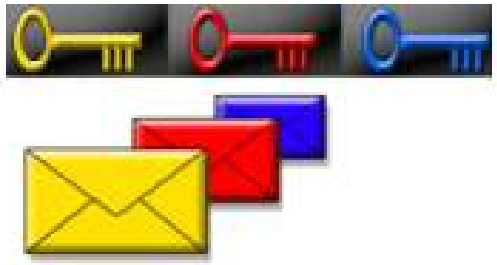
- Merupakan sebuah teknik untuk melakukan komunikasi anonym pada sebuah jaringan computer
- Dianalogikan seperti bawang yang berlapis-lapis
- Data yang telah dienkripsi ditransmisikan melalui serangkaian node pada jaringan yang disebut dengan onion router, dimana akan dikupas setiap melalui setiap router tersebut hingga layer terakhir
- Ketika sudah sampai pada layer terakhir, data didekrip, dan sampai di tujuannya
- Penggunaan paling terkenal ada pada email tersembunyi, dan private web browsing
- Onion routing mencegah seorang eavesdropper dari mempelajari source, destination, atau content dari data yang ditransmisikan di jaringan

TOR (The Onion Router)

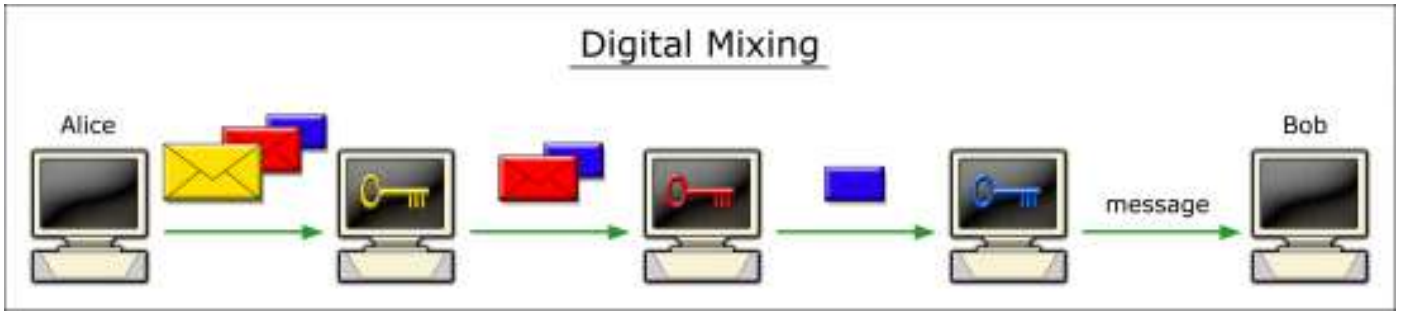


TOR (The Onion Router)

- Digital Mixing



Ciphertext = $E_{PK1}[E_{PK2}[E_{PK3}[message]]]$

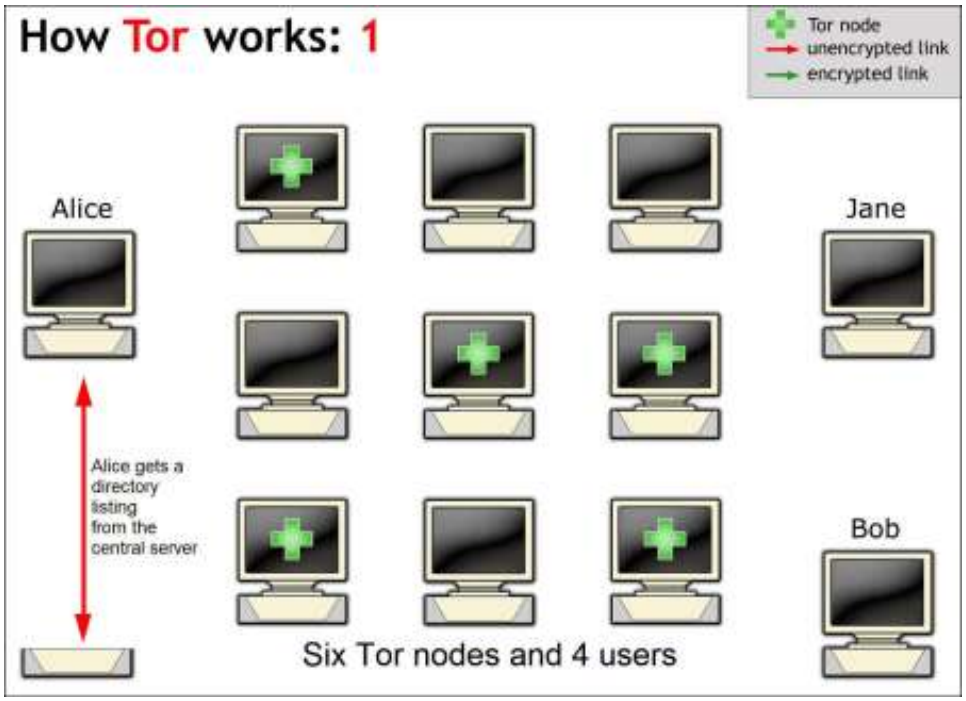


TOR (The Onion Router)

- **Anonymizing proxy server**; merupakan server yang berfungsi sebagai node
- Jika Alice ingin menjalin komunikasi dengan Bob, tanpa sepengetahuan Bob, maka Alice mengisi IP Bob pada Proxy Server, Proxy akan membuat koneksi ke Bob, dan menyampaikan semua informasi dari Bob ke Proxy, dan diteruskan ke Alice
- Proxy Server memiliki banyak keuntungan seperti :
  - Dapat digunakan untuk hal yang static (email) dan dynamic (browsing)
  - Tidak membutuhkan teknik yang mahal (biaya, waktu, dsb) untuk menggunakan public-key encryption
  - Sistem yang mudah
- Anonymizing proxy memiliki 1 fatal flaw, membuat user menjadi kurang terpercaya ketika mereka menggunakan anon communication. Apabila anon proxy digunakan untuk phising, tidak ada lagi garansi untuk secure, anonymous, communication

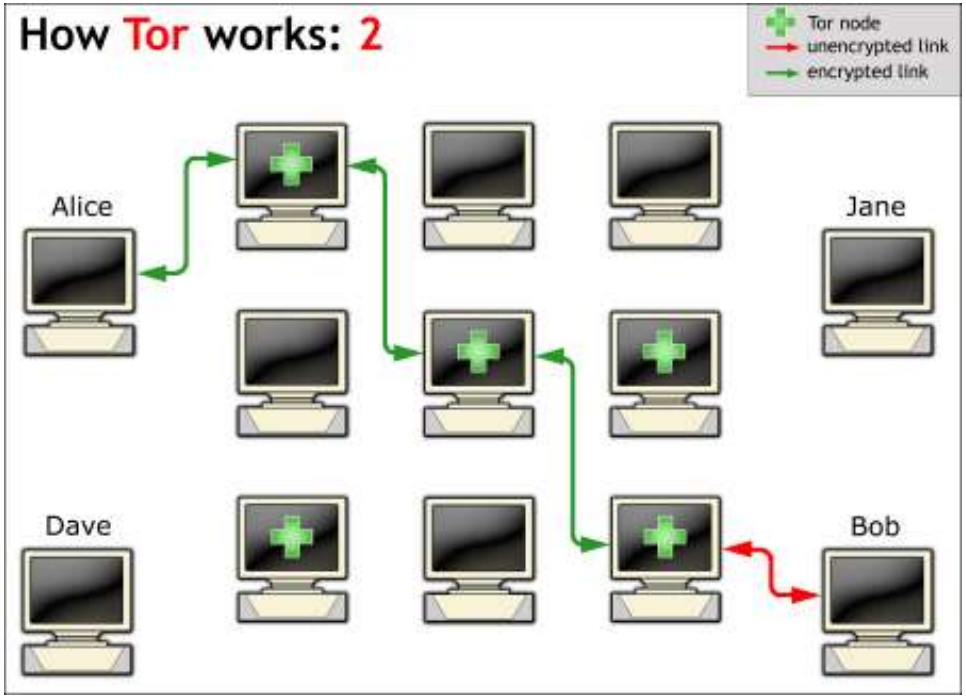
Onion routing with Tor

- Get Tor Nodes Address from Directory Server



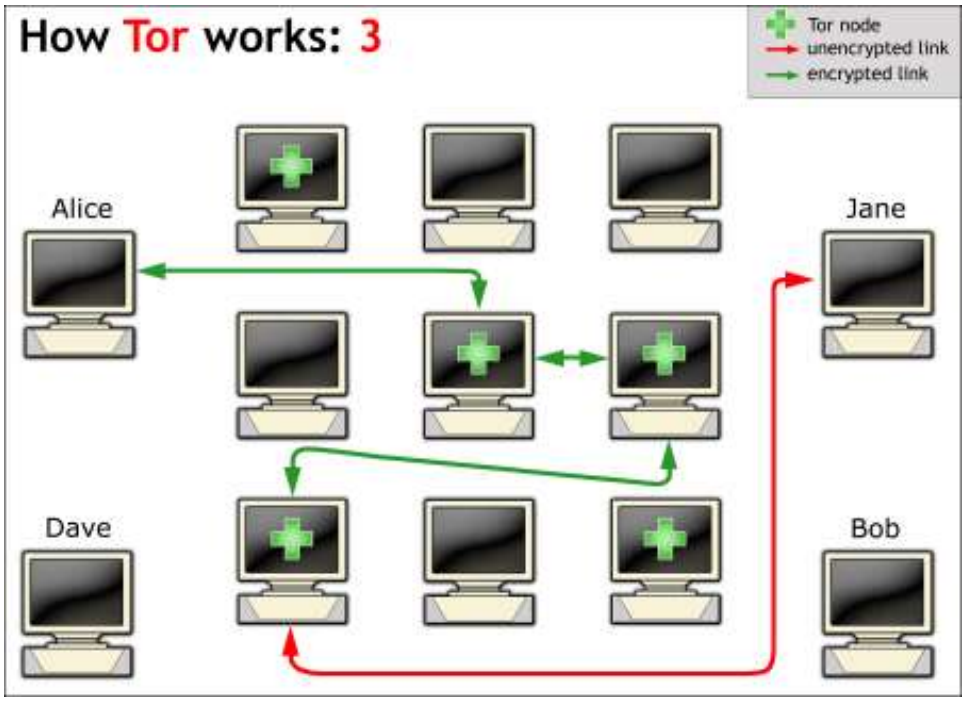
Onion routing with Tor

- After receiving the address list the Tor client software will connect to a random node
- The entry node would make an encrypted connection to a random second node which would in turn do the same to connect to a random third Tor node.
- That third node, the exit node, would then connect to Bob as visualized
- The same node cannot be used twice in one connection and depending on data congestion some nodes will not be used



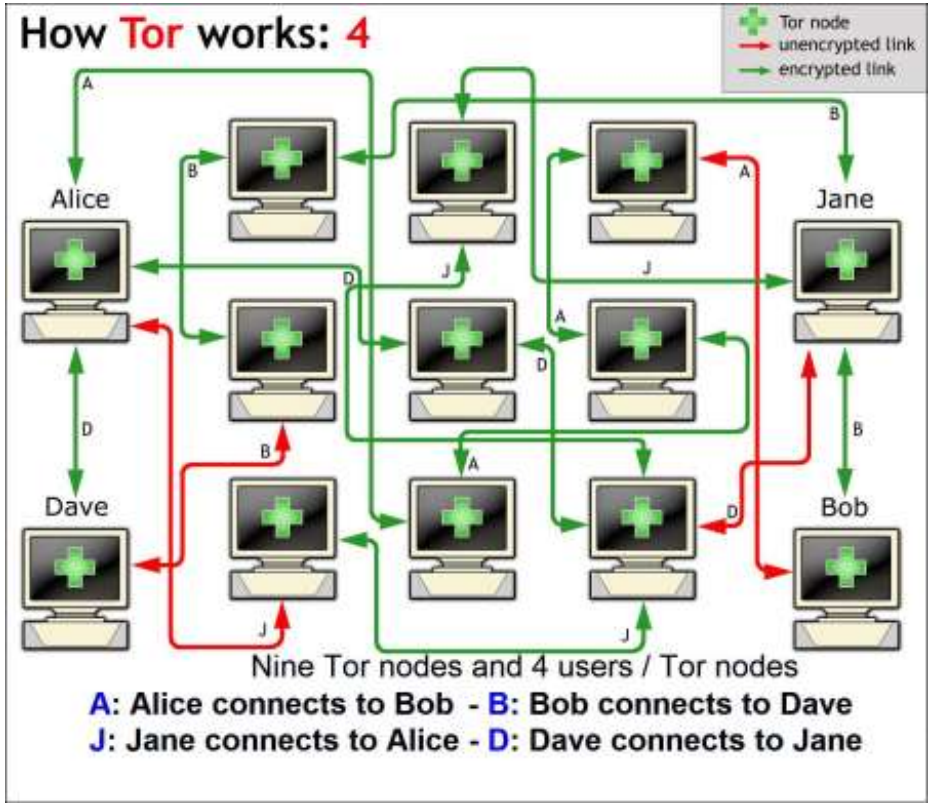
Onion routing with Tor

- If the same connection, the same array of nodes, were to be used for a longer period of time a Tor connection would be vulnerable to statistical analysis, which is why the client software changes the entry node every ten minutes, as illustrated.



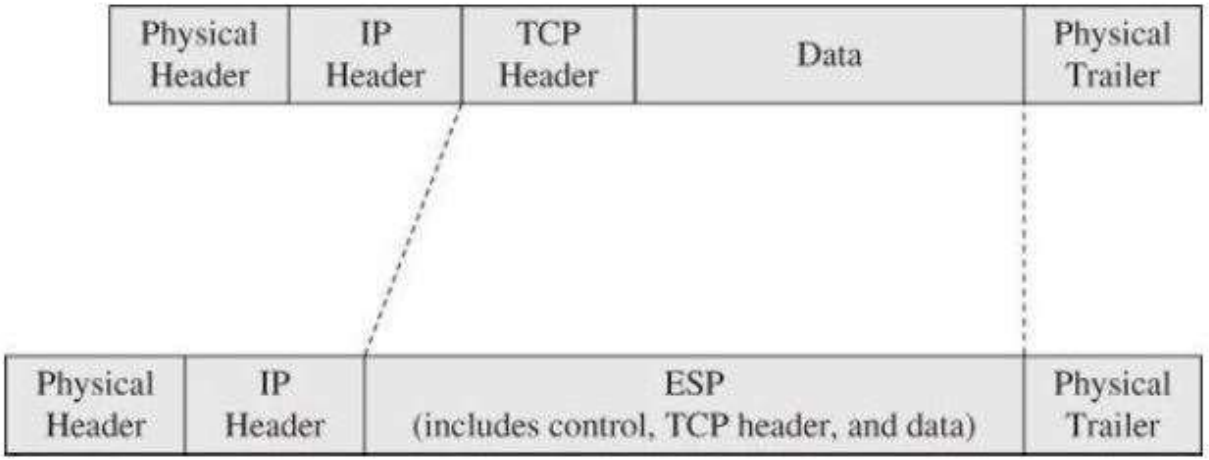
Onion routing with Tor

- To increase anonymity Alice could also opt to run a node herself
- If Alice uses the Tor network to connect to Bob, she does this by connecting to a Tor node, however if she functions as node for Jane she would also connect to a Tor node. This would result in a situation in which a malevolent third party would not be able to know which connection is initiated as a user and which as node.
- Which means this makes data mining significantly more difficult, and in a situation where Alice functions as a node for dozens of users, it makes data mining virtually impossible



IP Security Protocol (IPsec)

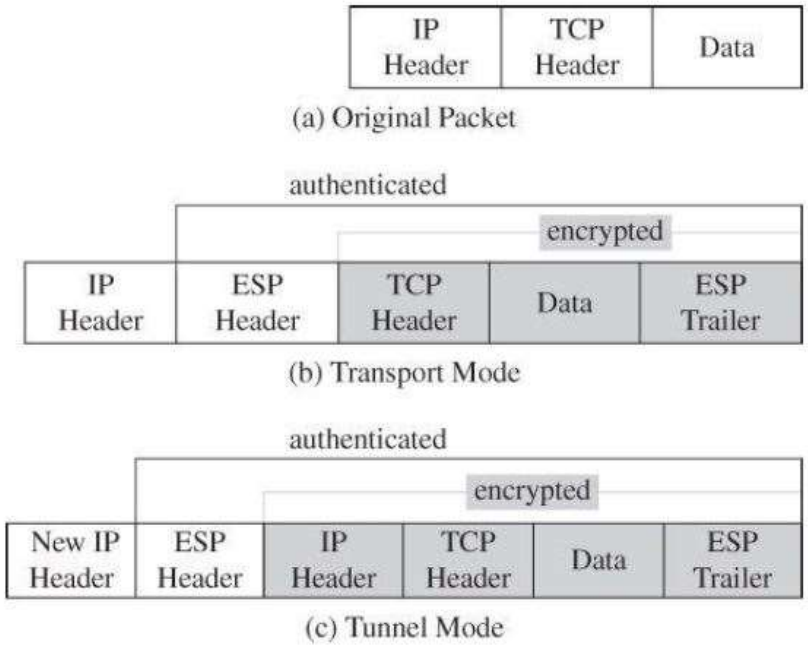
- IPsec adalah sebuah protocol yang mengizinkan untuk kelakukan autentikasi dan enkripsi pada IP Packet untuk setiap sesi komunikasi
- Encapsulated security payload terdiri atas descriptor yang tugasnya adalah memberitahu penerima untuk interpretasi konten yang terenkripsi.
- IPsec dapat melidungi salah satu atau keduanya dari confidentiality dan authenticity.



IPSec Modes of Operation

- In transport mode, only the payload of the IP packet is usually encrypted or authenticated

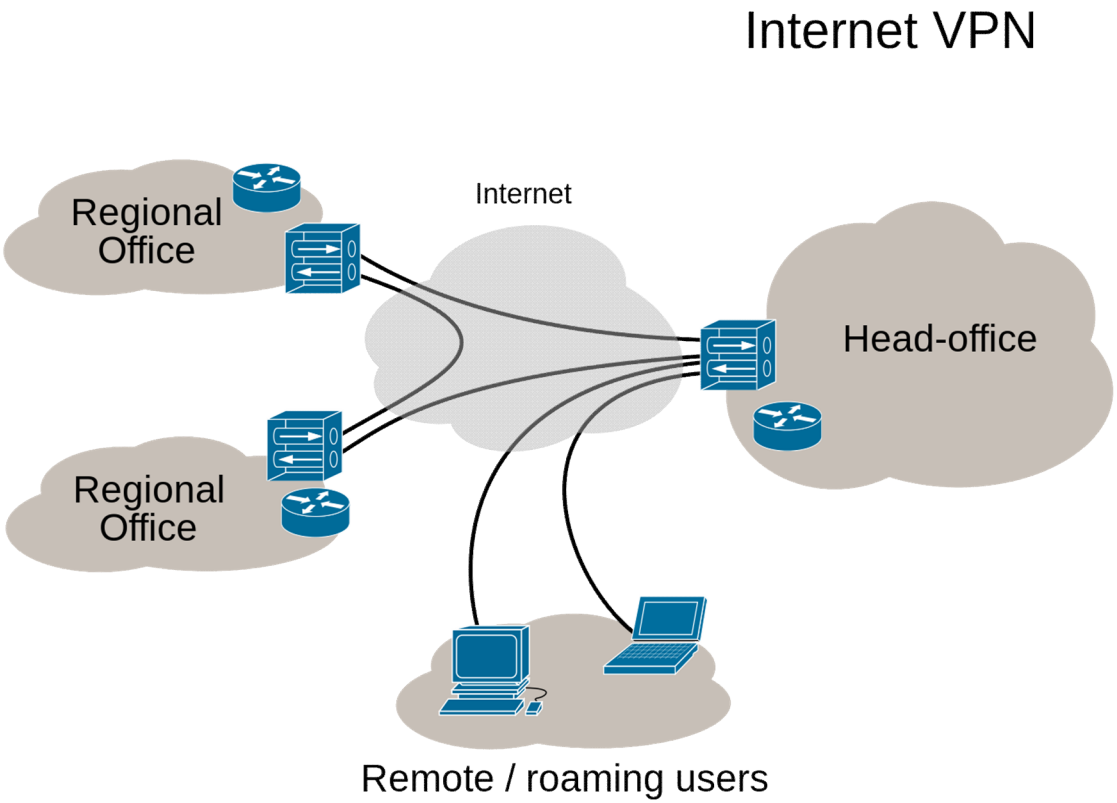
- In tunnel mode, the entire IP packet is encrypted and authenticated. It is then encapsulated into a new IP packet with a new IP header.



Virtual Private Network (VPN)

- Sebuah private network yang meluas dan berjalan diantara public network atau internet
- Mengizinkan user mengirim atau menerima data di public network atau internet layaknya computer user terkoneksi langsung ke jaringan private miliknya
- Tetapi VPN dapat memiliki dampak negative seperti melanggar privasi user dengan cara melakukan logging kegiatan seseorang, dan mempublikasikannya tanpa sepengetahuannya. Atau menjual bandwidth nya kepada orang lain.
- Koneksi VPN, menggunakan IPSec Mode Tunneling

Virtual Private Network (VPN)



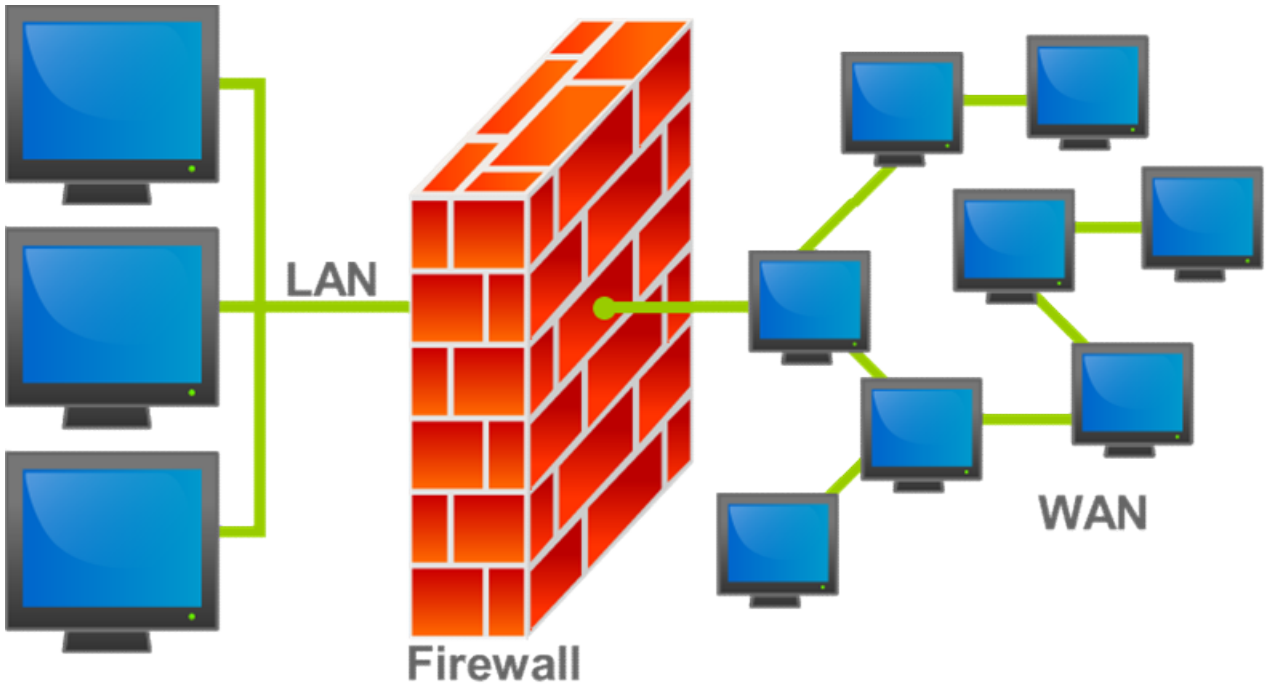
Virtual Private Network (VPN)

- OSI Layer 2 Services
  - Virtual LAN
  - Virtual private LAN service (VPLS)
  - Pseudo wire (PW)
  - Ethernet over IP tunneling
  - IP-only LAN-like service (IPLS)
- OSI Layer 3 PPVPN architectures
  - BGP/MPLS PPVPN
  - Virtual router PPVPN

Firewall

- Sistem pada jaringan computer yang tugasnya untuk memonitoring dan mengatur traffic yang masuk (incoming) dan keluar (outgoing) berdasarkan rule yang sudah ditentukan
- Diasumsikan jaringan internet adalah jaringan yang tidak aman (unsecured network)
- Firewall secara umum dapat dikategorikan sebagai : network firewalls atau host-based firewall
  - Network firewalls melindungi 1 jaringan dengan jaringan lain (dapat berupa software-based ataupun hardware-based firewall
  - Host-based firewalls hanya mengatur traffic yang keluar/masuk dari 1 mesin saja

Firewall



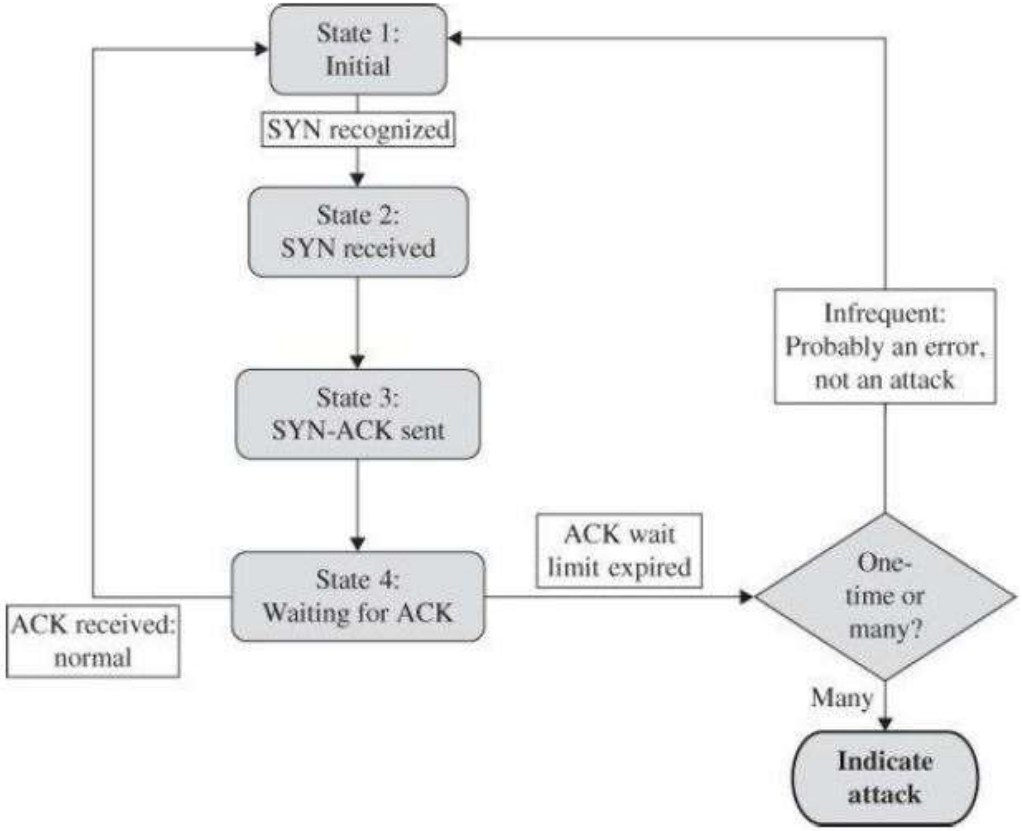
Firewall

- Generation of Firewall :
  - Packet Filters : hanya memfilter packet, drop packet yang tidak sesuai dengan rule dari firewall
  - “Stateful” Filters : Beroperasi di Layer 4 (Transport); sampai menjudge isi dari paket nya.
  - Application Layer : Firewall Toolkit (FWTK), IDS; Pada generasi ini, firewall dapat mengerti rule pada FTP/DNS/HTTP dll.
    - Next-generation Firewall : IPS, User Identity Management Integration, Web Application Firewall (WAF)

Intrusion Detection

- Pencegahan Penyusupan
  - Firewall
    - Membatasi aliran paket
  - Sistem Keamanan
    - Menemukan kelemahan buffer overflow dan menghilangkannya
- Deteksi Penyusupan
  - Menemukan modifikasi sistem
    - Tripwire
  - Mencari serangan yang sedang terjadi
    - Pola trafik jaringan
    - System call, even sistem lainnya

Intrusion Detection



Intrusion Detection - Tripwire

- Gambaran serangan umum
  - Mendapatkan akses user
  - Mendapatkan akses root
  - Mengganti binari sistem untuk membuat backdoor
  - Menggunakan backdoor untuk aksi selanjutnya
- Titik deteksi tripwire: binari sistem
  - Hitung hash dari kunci binari sistem
  - Bandingkan hash hasil hitungan dengan hash tersimpan
  - Laporkan jika berbeda
  - Simpan kode hash referensi di media read-only

Intrusion Detection - Tripwire

- Serangan umum pada server
  - Mendapatkan akses
  - Menginstall backdoor
    - Bisa dilakukan di memori, tidak harus di disk
  - Menggunakan server
- Tripwire
  - Ide bagus
  - Tidak akan menangkap serangan yang tidak mengubah sistem file
  - Mendeteksi sebuah penguasaan yang telah terjadi

Intrusion Detection - SNORT

- Terdapat banyak sistem deteksi penyusupan (misal : snort)
  - Hampir 100 sistem saat ini
  - Berbasis jaringan, berbasis host atau kominasinya
- Dua model dasar
  - Model deteksi salah penggunaan
    - Memelihara data dari serangan yang diketahui
    - Mencari aktifitas dengan tanda tangan yang berhubungan
  - Model deteksi anomali
    - Mencari / menentukan ‘normal’
    - Melaporkan perilaku menyimpang
- Masalah dasar: terlampau banyak alarm palsu

Goals of IDS

- IDS harus FAST, SIMPLE, dan ACCURATE
- Goal akhir dari IDS :
  - Filter on packet headers.
  - Filter on packet content.
  - Maintain connection state.
  - Use complex, multipacket signatures.
  - Use minimal number of signatures with maximum effect.
  - Filter in real time, online.
  - Hide its presence.
  - Use optimal sliding-time window size to match signatures.

Stealth Mode IDS

- IDS (Host-based / Network-based) dapat saja dideteksi (scan) oleh attacker.
- Membuat IDS menjadi tidak aman (dari serangan DOS?)
- Pada IDS, terdapat Stealth Mode, membuat IDS tidak dapat di-scan
- Pada Stealth Mode, ketika attacker menyerang sistem, Attacker tidak mengetahui bahwa alarm IDS telah berbunyi.