

# Konsep IP Spoofing dan Cara Pencegahannya

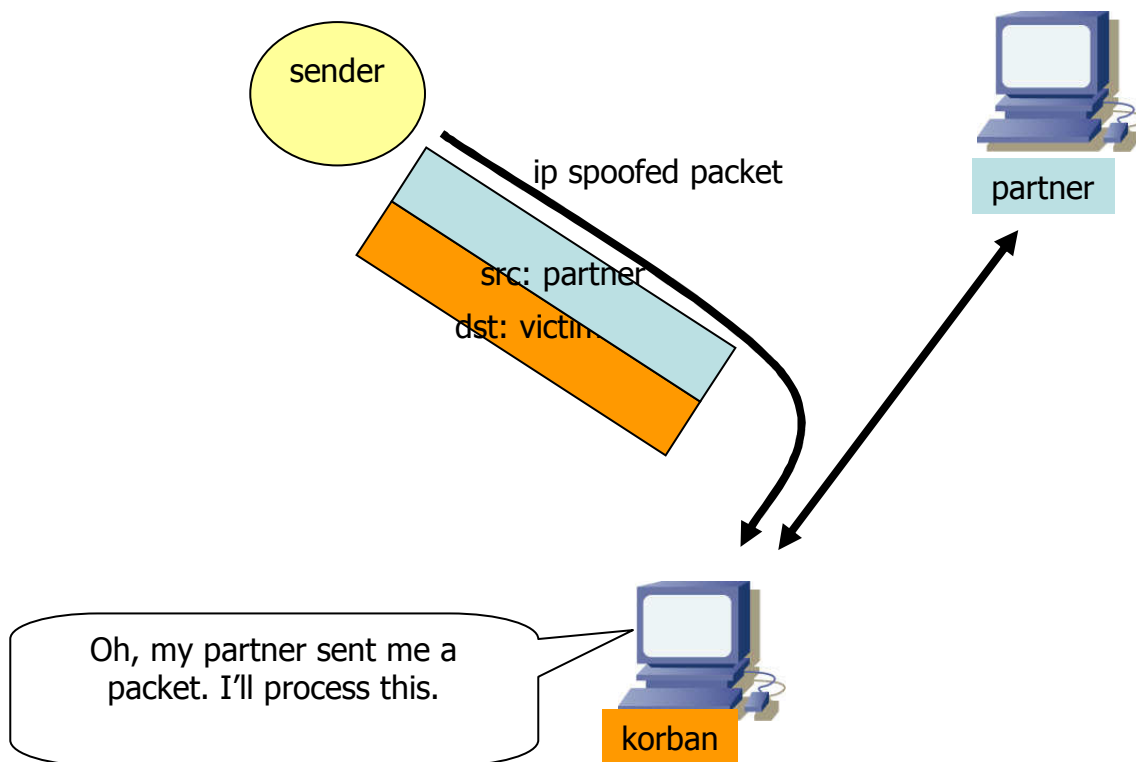


Putra Prima A 0410630078

JURUSAN TEKNIK ELEKTRO FAKULTAS TEKNIK  
UNIVERSITAS BRAWIJAYA  
MALANG  
2007

## Pengertian IP Spoofing

Ip Spoofing adalah sebuah teknik untuk membuat *untrusted host* terlihat seperti *trusted host* dalam sebuah jaringan. Hal ini terjadi karena *crackers* merubah IP *address host* tersebut sehingga menyerupai *trusted host*. Dengan kata lain penyusup menipu *host* dalam jaringan sehingga penyusup tersebut tidak perlu melakukan autentikasi untuk dapat terhubung dengan jaringan lokal.



## Sejarah IP Spoofing

Konsep dari IP spoofing sendiri sudah mengemuka di kalangan akademik sejak tahun 1980 an. Pada awalnya hanya merupakan sebuah teori sampai akhirnya Robert Morris menemukan celah keamanan pada protokol TCP yang di kenal

dengan "sequence prediction". Stephen Bellovin juga mengemukakan permasalahan ini lebih mendalam pada sebuah paper yang berjudul "Security Problems in the TCP/Ip Protocol Suite". Serangan "Cristmas Day" yang dilakukan oleh Kevin Mitnick ke komputer Tsutomu Shimomura juga menggunakan IP Spoofing dan TCP sequence prediction. Teknik spoofing masih merupakan pilihan utama untuk melakukan eksploitasi jaringan dan harus benar benar di perhatikan oleh seorang administrator jaringan.

## **Konsep dan Teknik IP Spoofing**

Protokol yang di gunakan pada pengiriman data di internet dan banyak jaringan komputer adalah Internet Protocol("IP"). Header dari masing masing paket IP terdiri dari data numerik dan alamat tujuan dari paket yang akan di kirimkan. Alamat sumber di gunakan untuk memberi tahu dari mana sebuah paket itu di kirimkan. Dengan mengubah header IP di bagian "source address" nya seorang cracker dapat menipu seakan akan sebuah paket di kirim dari komputer yang lain. Dan komputer tujuan ("destination address") yang menerima paket yang telah di modifikasi tadi akan mengirimkan respon balik ke "source address" palsu yang telah di modifikasi oleh cracker, dengan demikian konsekuensinya teknik ini digunakan jika cracker tersebut tidak menghiraukan respon dari komputer tujuan, atau sudah mempunyai sebuah metode untuk menebak respon apa yang akan terjadi.

Pada beberapa kasus, cracker dapat melihat atau me redirect respon dari komputer tujuan ke komputernya sendiri. Kebanyakan kasus IP spoofing terjadi pada jaringan yang sama baik LAN atau WAN.

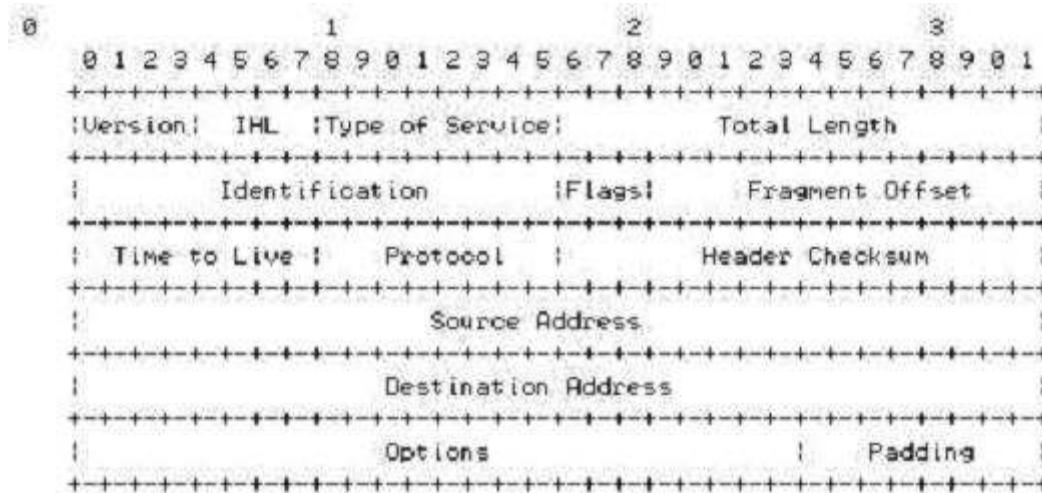
## **Teknik Pelaksanaan IP spoofing**

Untuk memahami secara lengkap bagaimana serangan IP spoofing di laksanakan, kita harus memahami struktur dari protokol TCP/IP. Pemahaman

yang baik mengenai heder dan pertukaran jaringan menjadi bagian penting dalam pelaksanaan IP spoofing.

## Internet Protocol - IP

Internet Protocol (IP) adalah protokol jaringan yang bekerja di layer ke tiga(network) dari model OSI. Menggunakan "connectionless model" artinya tidak ada informasi mengenai state transaksi, yang digunakan untuk mengantarkan paket dalam sebuah jaringan. Juga tidak ada metode yang dapat memastikan bahwa paket yang di kirimkan sampai ke tujuan dengan sempurna.

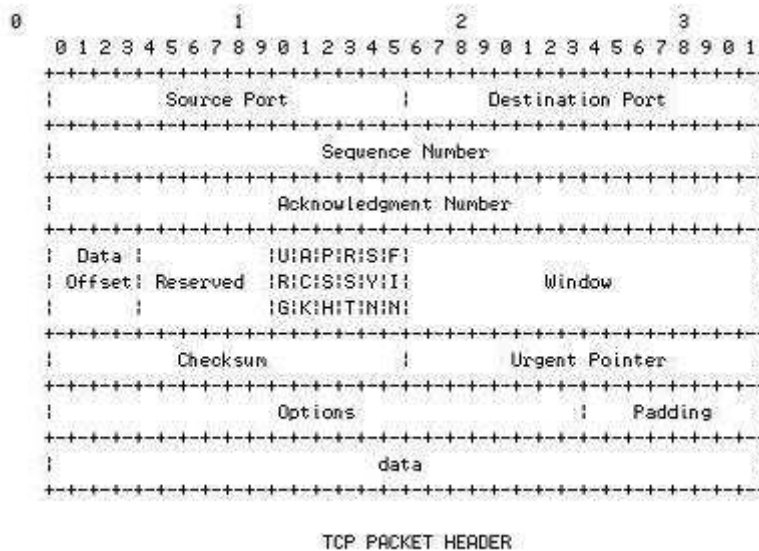


IP PACKET HEADER

Dengan memeriksa header IP di atas, dapat kita lihat bahwa 12 byte pertama ( atau tiga baris pertama dari header ) terdiri dari bermacam macam informasi tentang packet. Delapan byte selanjutnya (2 baris selanjutnya) terdiri dari alamat IP *source* dan *destination*. Dengan menggunakan beberapa tools yang ada kita dapat mengubah alamat IP dari *source* dan *destination* terutama pada alamat *source*. Juga penting di ingat bahwa setiap datagram di kirim satu sama lain secara independent hal ini terjadi karena sifat *stateless* dari IP.

## Transmission Control Protocol – TCP

Tidak seperti IP, TCP menggunakan *connection-oriented design*. Artinya dua komputer yang ingin terhubung dengan TCP harus membuat koneksi terlebih dahulu melalui tiga cara *handshake* (SYN-SYN/ACK-ACK) – lalu mengupdate progress masing masing melalui sederetan *acknowledgements*. Dengan komunikasi yang seperti ini dapat memastikan reliability data, karena pengirim menerima sinyal OK dari penerima untuk setiap paket yang di terima.



Dapat kita lihat pada diagram di atas, header TCP jauh berbeda dengan header IP. Kita akan fokus pada 12 byte pertama dari paket TCP, yang terdiri dari port dan *sequence number*. Sama seperti datagram IP, paket TCP juga dapat di manipulasi dengan menggunakan software. Sumber dan port tujuan biasanya tergantung pada aplikasi network yang di gunakan misalnya HTTP menggunakan port 80. bagian yang paling penting untuk memahami spoofing adalah *sequence* dan *acknowledgement number*. Data yang ada di filed ini memastikan paket di sampaikan ke tujuan dan dapat menentukan apakah paket harus di kirim ulang atau tidak. *Sequence number* adalah angka yang terdapat pada byte pertama pada sebuah paket yang berhubungan dengan stream data. *Acknowledgement*

*number* adalah angka selanjutnya dari *sequence number*. Dengan adanya *sequence number* dan *acknowledgement number* ini dapat di pastikan paket yang diterima adalah paket yang benar dan berurutan.

## **Konsekuensi dari desain TCP/IP**

Setelah kita memahami konsep dari TCP/IP sekarang kita dapat memeriksa kelemahan dari desain ini. Seperti yang kita ketahui untuk mengganti *source address* dengan memanipulasi header IP. Teknik ini digunakan untuk memanipulasi alamat pengirim yang merupakan bagian terpenting dari IP spoofing. Sementara pada TCP kita dapat memprediksikan *sequence number* yang dapat di gunakan untuk melakukan *session hijacking* atau mengeksploitasi host.

## **Jenis Jenis Serangan IP Spoofing**

Ada beberapa variasi dalam serangan yang menggunakan IP spoofing. Walaupun beberapa teknik sudah termasuk teknik lama, beberapa teknik yang lain masih sangat perlu di perhatikan untuk keamanan jaringan saat ini.

### **Non-Blind Spoofing**

Tipe serangan ini biasanya terjadi jika korban berada dalam satu subnet jaringan yang sama. Dengan dalam satu jaringan yang sama kita dapat melakukan sniffing nomor *sequence* dan *acknowledgement*, hal ini menghilangkan kesulitan dalam menghitung nomor *sequence* dan *acknowledgement*. Ancaman terbesar dari teknik Non-Blind Spoofing ini adalah dapat terjadinya *session hijacking*. Hal ini dapat di lakukan dengan mengeksploitasi *datastream* dari koneksi yang ada, kemudian membentuk kembali koneksi tersebut dengan nomor *sequence* dan *acknowledgement* yang sesuai dengan komputer target. Dengan menggunakan teknik ini kita dapat memotong autentikasi yang dilakukan untuk membentuk koneksi ke komputer target.

## Blind Spoofing

Pada Blind Spoofing serangan yang di lakukan akan lebih sulit untuk di laksanakan karena angka *sequence* dan *acknowledgement* tidak dapat di sniffing karena tidak dalam satu subnet. Untuk memperoleh angka *sequence* dan *acknowledgement* beberapa paket di kirimkan ke komputer target untuk melakukan sampling terhadap angka *sequence*. Dulu komputer secara otomatis akan membentuk angka yang berurutan. Dan dengan hanya melakukan sampling pada beberapa paket data kita dapat memperkirakan formula yang di gunakan untuk membentuk angka *sequence* dan *acknowledgement*.

Contoh proses perkiraan *sequence number* :

```
14:18:26.507560 apollo.999 > osiris.514: S 1382726991:1382726991(0)
14:18:26.694691 osiris.514 > apollo.999: S 2021952000:2021952000(0) ack
1382726992
14:18:26.775037 apollo.999 > osiris.514: R 1382726992:1382726992(0)
14:18:27.014050 apollo.998 > osiris.514: S 1382726992:1382726992(0)
14:18:27.174846 osiris.514 > apollo.998: S 2022080000:2022080000(0) ack
1382726993
14:18:27.251840 apollo.998 > osiris.514: R 1382726993:1382726993(0)
14:18:27.544069 apollo.997 > osiris.514: S 1382726993:1382726993(0)
14:18:27.714932 osiris.514 > apollo.997: S 2022208000:2022208000(0) ack
1382726994
14:18:27.794456 apollo.997 > osiris.514: R 1382726994:1382726994(0)
14:18:28.054114 apollo.996 > osiris.514: S 1382726994:1382726994(0)
14:18:28.224935 osiris.514 > apollo.996: S 2022336000:2022336000(0) ack
1382726995
14:18:28.305578 apollo.996 > osiris.514: R 1382726995:1382726995(0)
...
14:18:35.735077 apollo.981 > osiris.514: S 1382727009:1382727009(0)
14:18:35.905684 osiris.514 > apollo.981: S 2024256000:2024256000(0) ack
1382727010
14:18:35.983078 apollo.981 > osiris.514: R 1382727010:1382727010(0)
```

Dari sequence number di atas dapat di tebak pola dari sequence number nya

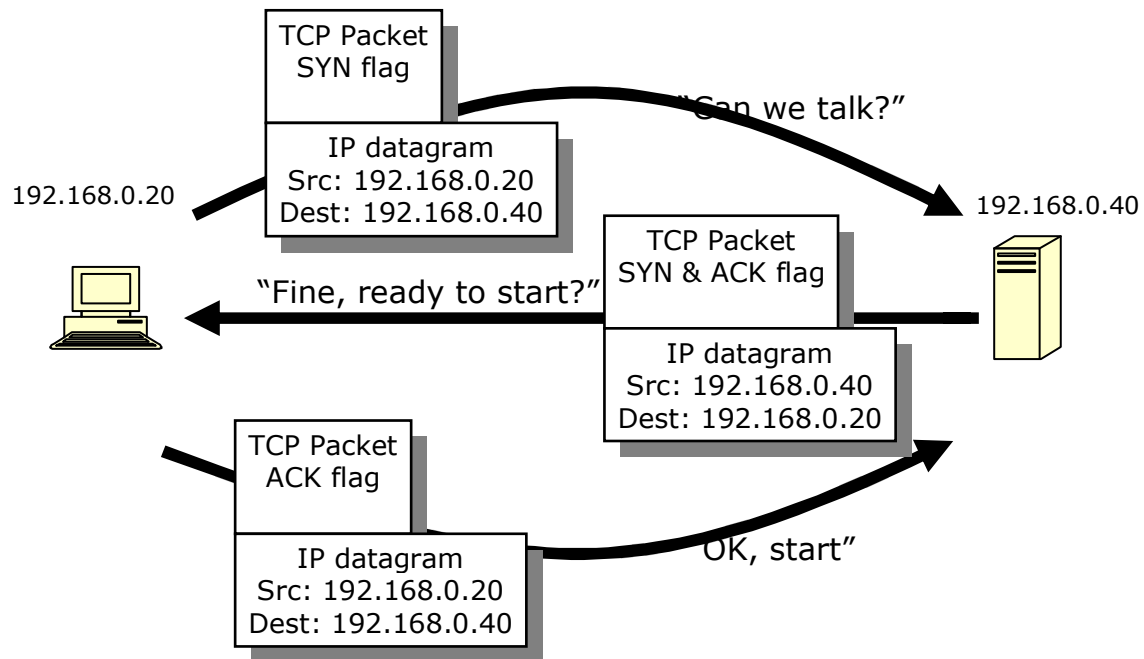
$$\mathbf{ISN_{i+1} = ISN_i + 128000}$$

### **Man In the Middle Attack**

Pada tipe serangan ini sebuah komputer memotong jalur komunikasi dari dua komputer yang terhubung, kemudian mengontrol alur komunikasi dan dapat menghapus dan membuat informasi yang di kirim dari salah satu komputer yang terhubung tadi tanpa diketahui oleh keduanya. Dengan cara ini, kita dapat mengelabui target dengan mengirim informasi yang seolah olah datang dari komputer yang "dipercaya" oleh target.

### **Denial of Service Attack**

IP spoofing sering kali di gunakan untuk melakukan denial of service, atau DoS. Dalam hal ini kita hanya ingin menghabiskan bandwidth dan resource, tidak memikirkan tentang penyelesaian handshakes dan transaksi yang di lakukan. Tujuannya untuk membanjiri korban dengan paket sebanyak banyak nya dalam waktu yang singkat. Proses TCP Handshaking :



Dari Proses Handshaking di atas dapat di simpulkan pada sebuah host untuk melakukan komunikasi dengan host lain harus melakukan hal sebagai berikut :

- merekam mesin mana yang telah dikirim "SYN+ACK"
- menyimpan daftar paket TCP SYN yang telah diberi jawaban SYN+ACK
- ketika ACK diterima, daftar paket dihilangkan karena koneksi sudah dibuka

Bagaimana jika pengirim tidak menjawab dengan ACK?

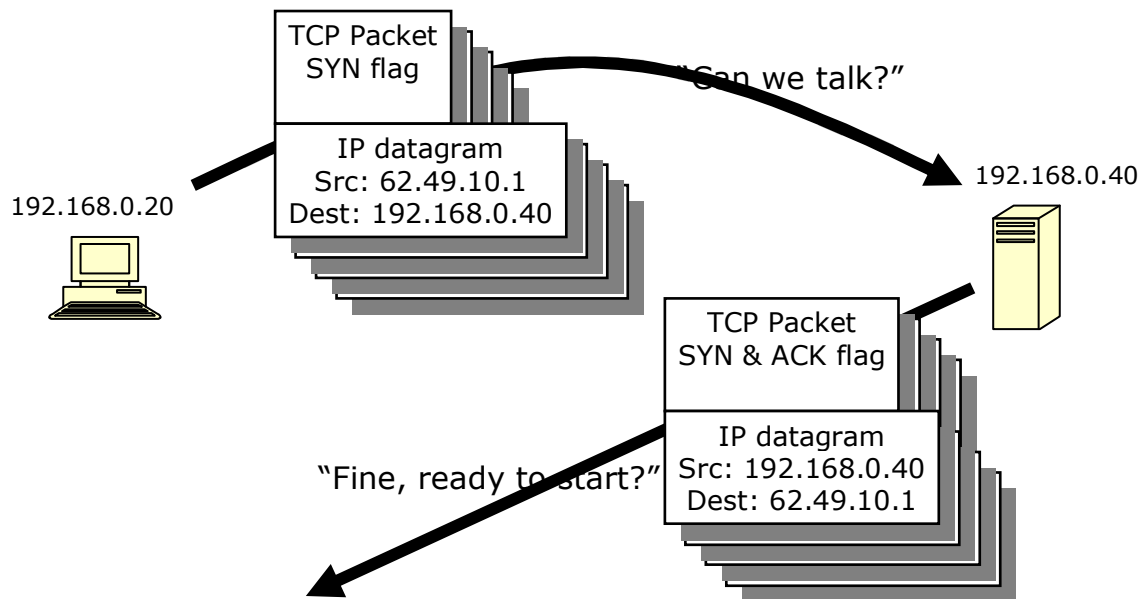
- Sebuah paket SYN dikirimkan dari pengirim ke penerima
  - "Can we talk?"
- Sebuah paket SYN/ACK dikirimkan dari penerima ke pengirim
  - "Fine – ready to start?"
- .....nothing.....

Jika pengirim mengirimkan 100 buah paket SYN per detik

- Akhirnya penerima akan kehabisan memori untuk merekam SYN+ACK.

- Ini adalah *SYN flooding*

Dengan memanipulasi header IP yang ada kita dapat mengganti isi dari *source address* dengan menggunakan *source address* palsu ini kita dapat menyembunyikan identitas asli dari komputer. Jika dalam satu detik kita mengirim 100 paket SYN dengan IP address yang sudah di spoof maka yang terjadi pada host adalah :



Karena terlalu banyak paket SYN yang masuk dan tidak ada Balasan dari tujuan akhirnya host tidak dapat lagi melayani permintaan dari user

## Cara Pencegahan IP Spoofing

Ada beberapa langkah pencegahan yang dapat kita lakukan untuk membatasi resiko dari IP spoofing dalam jaringan, antara lain :

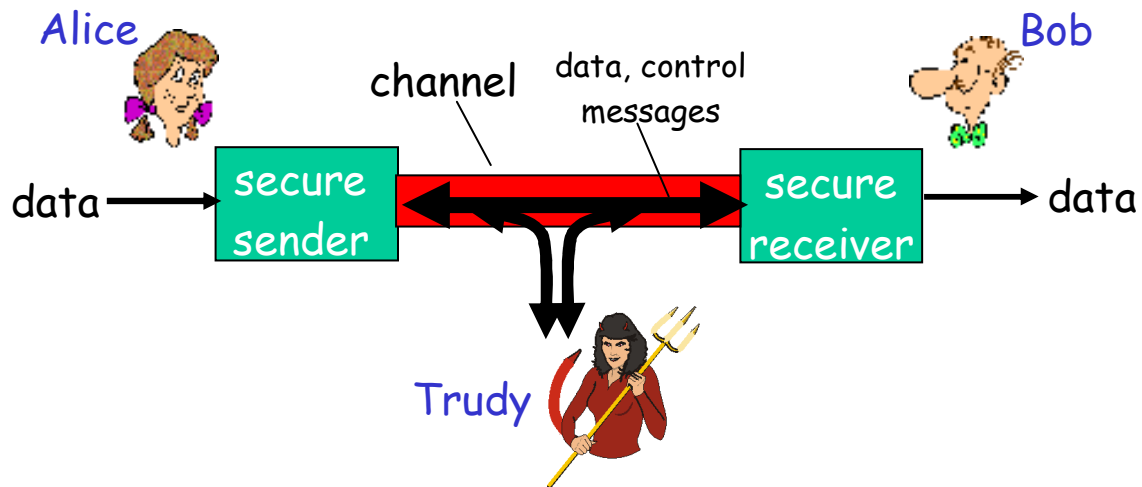
**Memasang Filter di Router** – dengan memanfaatkan “ingress dan engress filtering” pada router merupakan langkah pertama dalam mempertahankan diri dari spoofing. Kita dapat memanfaatkan ACL(access control list) untuk memblok alamat IP privat di dalam jaringan untuk downstream. Dilakukan dengan cara mengkonfigurasi *router-router* agar menahan paket-paket yang datang dengan alamat sumber paket yang tidak legal (*illegitimate*). Teknik semacam ini membutuhkan *router* dengan sumber daya yang cukup untuk memeriksa alamat sumber setiap paket dan memiliki *knowledge* yang cukup besar agar dapat membedakan antara alamat yang legal dan yang tidak.

**Enkripsi dan Autentifikasi** – kita juga dapat mengatasi IP spoofing dengan mengimplementasi kan autentifikasi dan enkripsi data. Kedua fitur ini sudah digunakan pada Ipv6. Selanjutnya kita harus mengeliminasi semua autentikasi berdasarkan host, yang di gunakan pada komputer dengan subnet yang sama. Pastikan autentifikasi di lakukan pada sebuah jalur yang aman dalam hal ini jalur yang sudah di enkripsi.

1. Gunakan autentifikasi berbasis *exchange key* antara komputer dalam jaringan, seperti *IPsec* akan menurunkan resiko jaringan terserang spoofing.
2. Gunakan daftar access control untuk menolak alamat IP privat dalam *downsteram interface*.
3. Gunakan filter pada aliran *inbound* dan *outbound* .

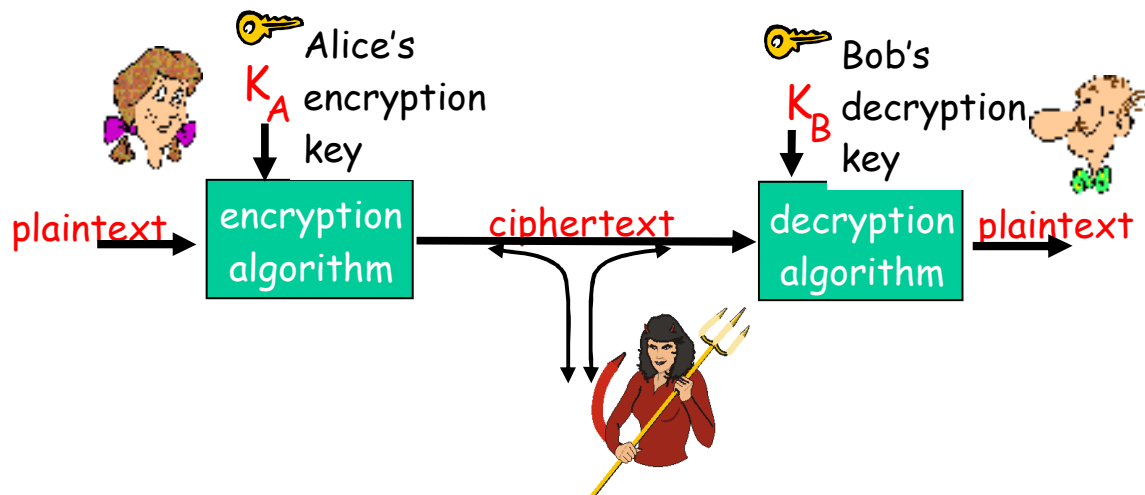
4. Konfigurasi router dan switch dengan sedemikian rupa sehingga dapat menolak paket dari luar network yang mengaku sebagai paket yang berasal dari dalam network.
5. Aktifkan enkripsi session di router sehingga *trusted host* yang berasal dari luar jaringan anda dapat berkomunikasi dengan aman ke *local host* anda.

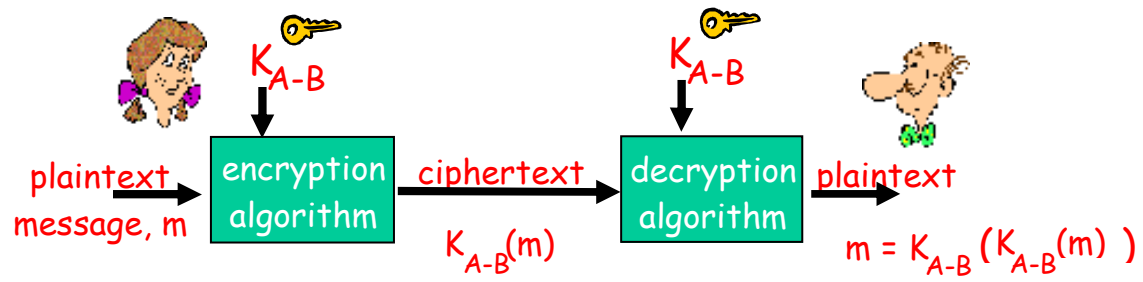
Kondisi sebelum di enkripsi :



Seorang penyerang (Trudy) melakukan spoofing dan dapat berklaku sebagai Man In The Middle antara Alice dan Bob.

Kondisi setelah di lakukan enkripsi :





Jadi walaupun ada Man In The Middle data yang di dapatkannya adalah data yang di enkripsi jadi resiko dari spoofing nya dapat di kurangi.