



MỘT SỐ GIAO THỨC BẢO MẬT THÔNG DỤNG

Nội dung chính

1. Các giao thức bảo mật email
2. Các giao thức bảo mật mạng
3. Các giao thức thanh toán điện tử

1. Các giao thức bảo mật email

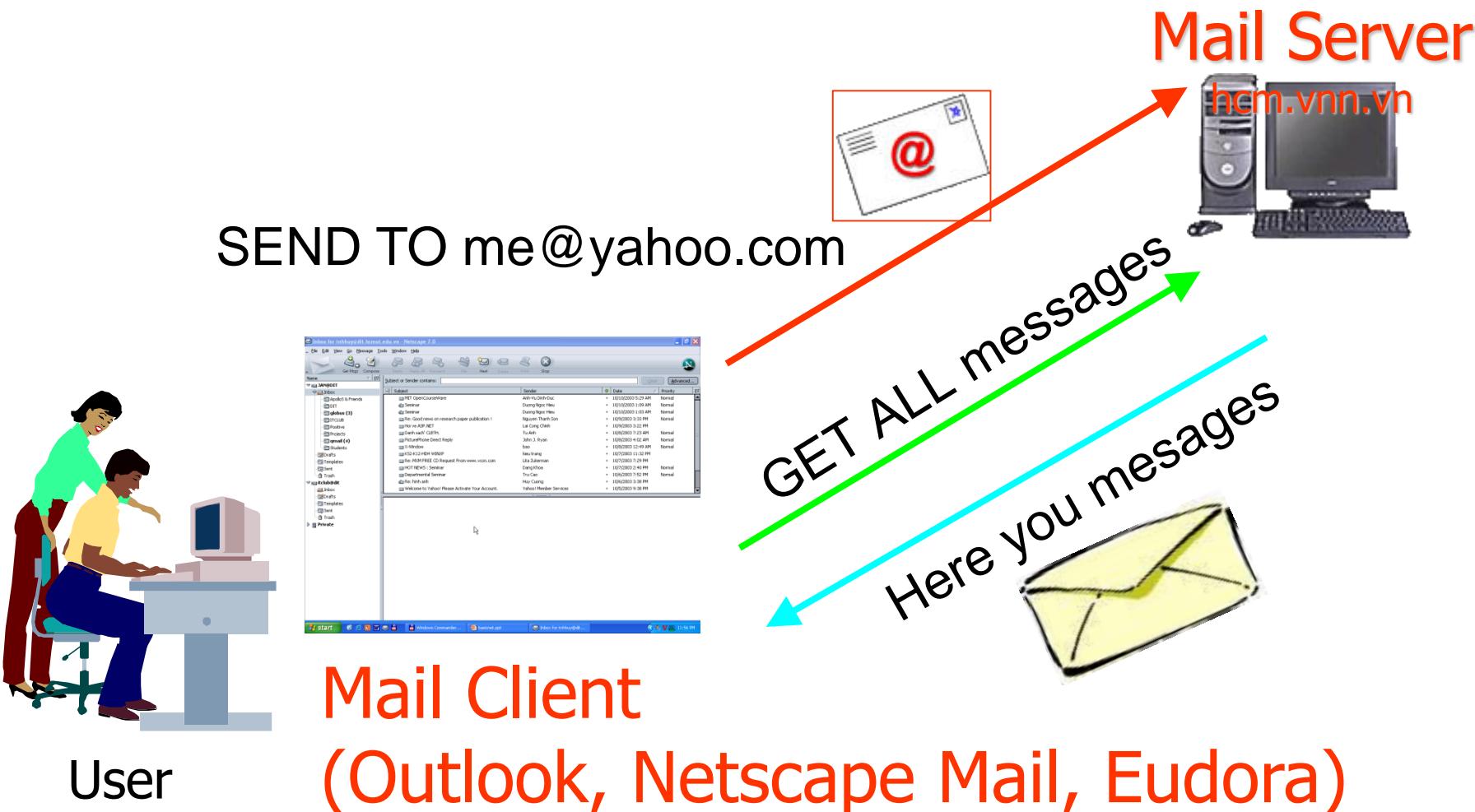
Giới thiệu: E-mail là hình thức liên lạc phổ biến, dễ bị tấn công

- Các hình thức quấy nhiễu e-mail:

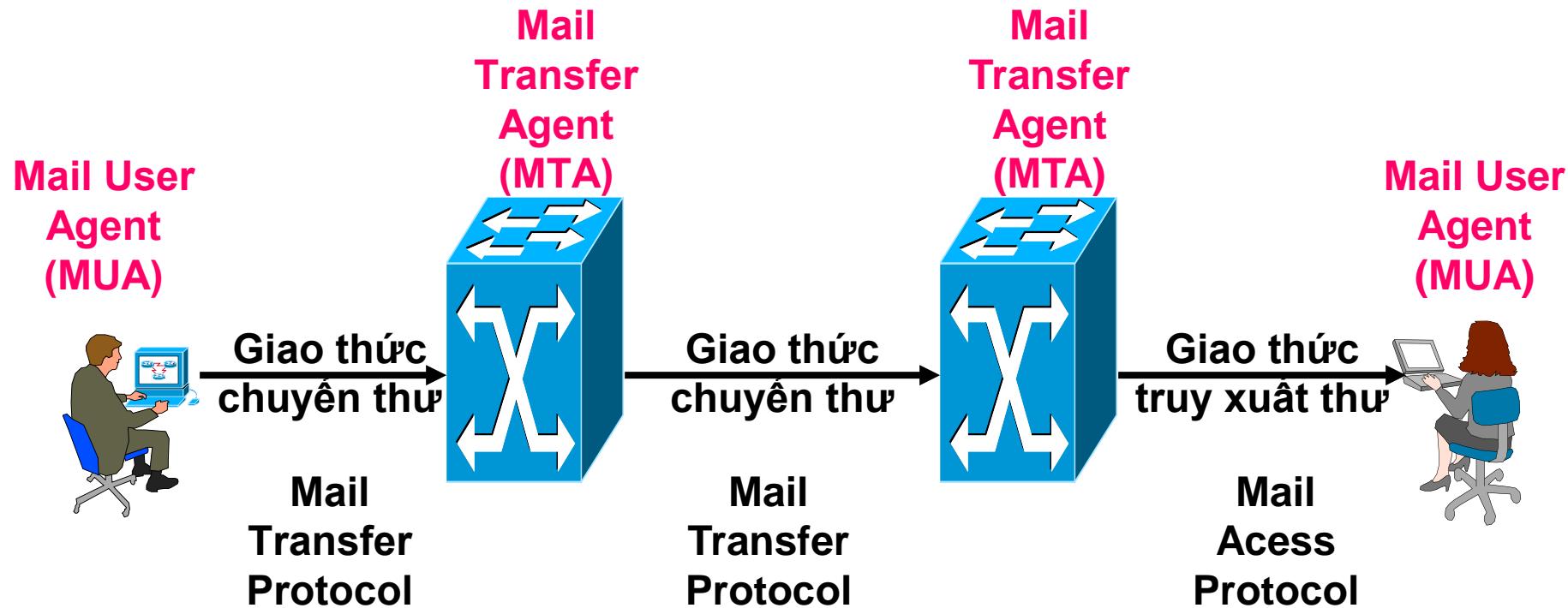
- Chặn nhận, đọc, gửi thư
- Thay đổi, giả mạo nội dung thư
- Thay đổi, giả mạo địa chỉ gửi thư
- Thay đổi, giả mạo nội dung thư (lừa đảo)
- Thay đổi, giả mạo địa chỉ nhận thư
- Nội dung email chứa virus, worm, trojan
- Gửi thư rác, quảng cáo, tuyên truyền
- Tấn công phân phối thư...

1. Các giao thức bảo mật email

Giới thiệu: E-mail là hình thức liên lạc phổ biến, dễ bị tấn công



Tổ chức dịch vụ e-mail



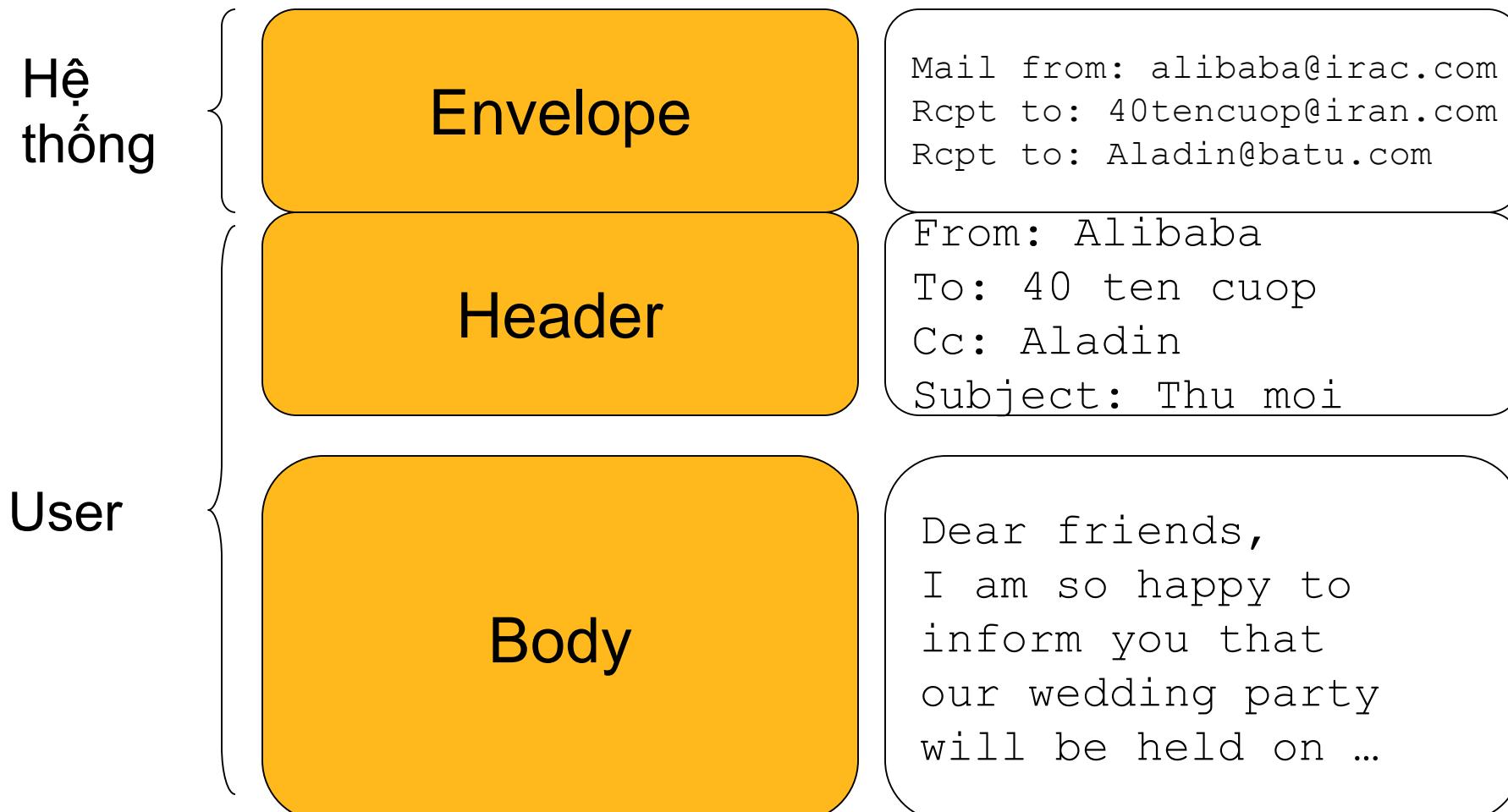
Các chức năng cơ bản của hệ thống e-mail

- Soạn thư (composition)
- Chuyển thư (transfer)
- Hồi báo (reporting)
- Hiển thị nội dung thư (displaying)
- Tổ chức lưu trữ thư (disposition)

Địa chỉ thư

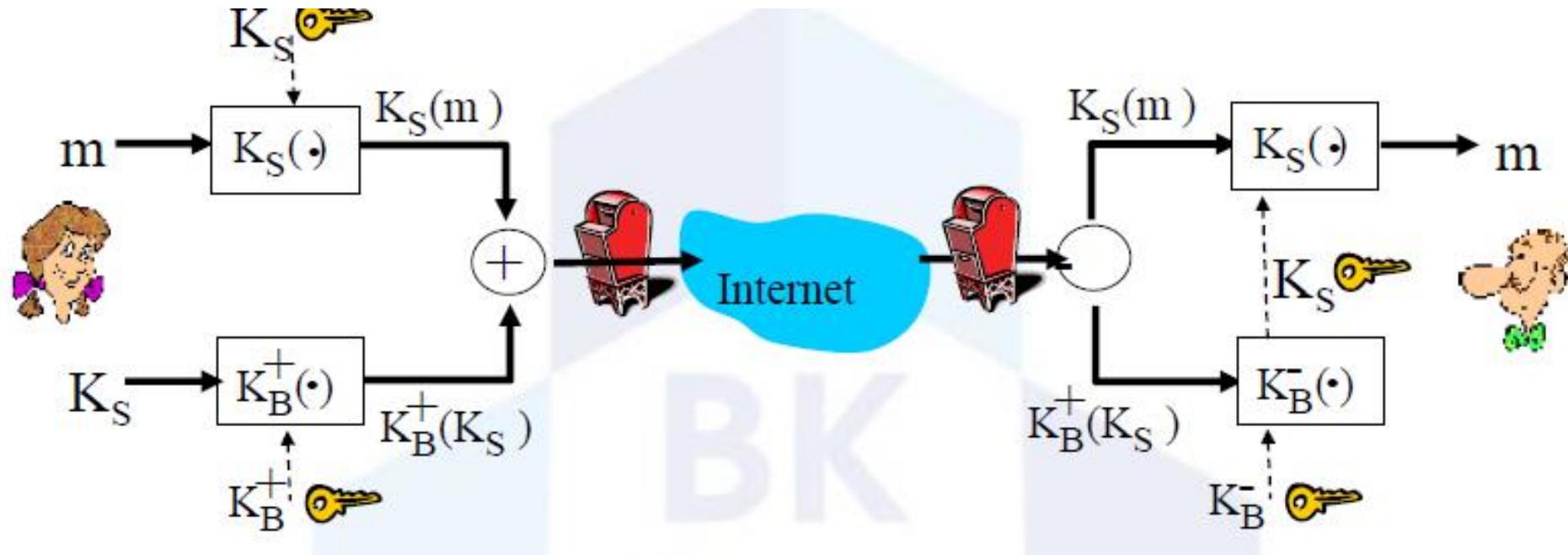
- Địa chỉ thư (e-mail address) có dạng tổng quát: *user-name@domain-name*
- Trong đó:
 - User-name: tên của hộp thư (mail box) trên từng mail server.
 - Domain-name: tên miền đã đăng ký của tổ chức sở hữu mail server. Để biết tên miền đầy đủ (FQDN) của mail server, cần phải truy vấn MX record.

Cấu trúc thư theo chuẩn RFC 822



Bảo mật email

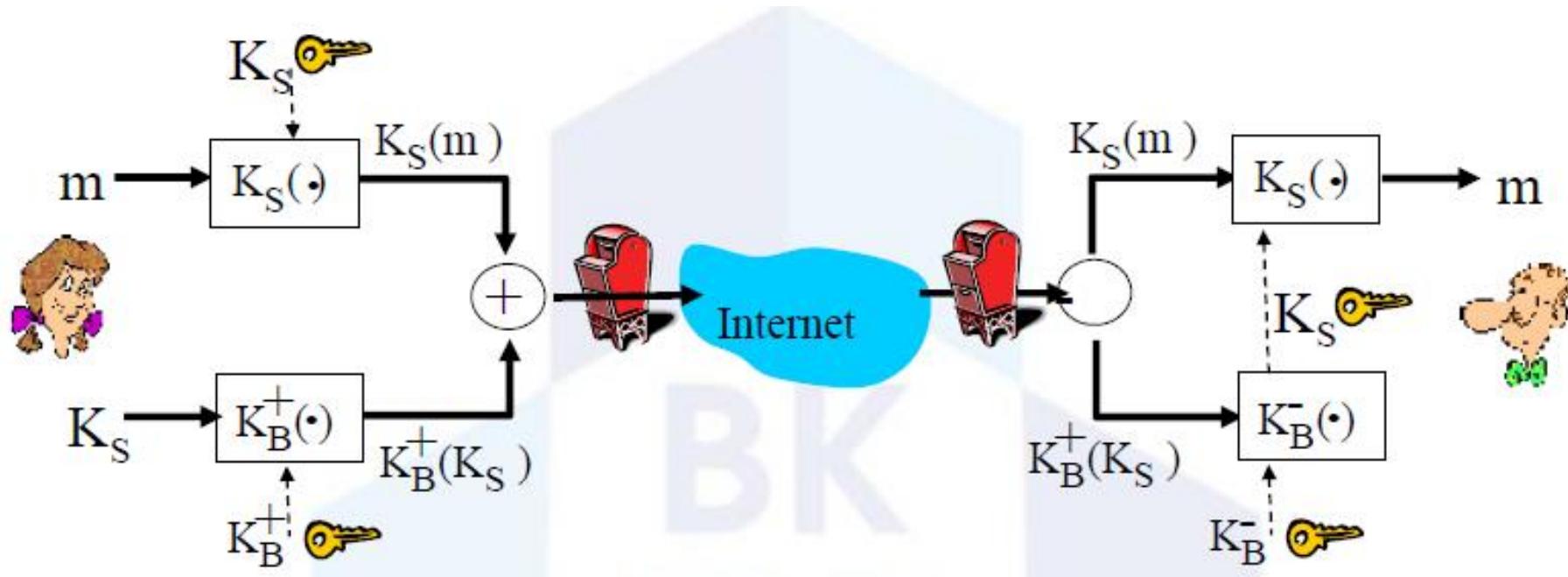
- Alice muốn gửi email bí mật, m , cho Bob.



- Alice:
 - sinh ngẫu nhiên khóa cá nhân đối xứng , K_S .
 - mã hóa t/điệp với K_S (tăng hiệu suất)
 - đồng thời mã hóa K_S với khóa công khai của Bob.
 - gửi cả hai $K_S(m)$ và $K_B(K_S)$ cho Bob.

Bảo mật email

- Alice muốn gửi email bí mật, m , cho Bob.

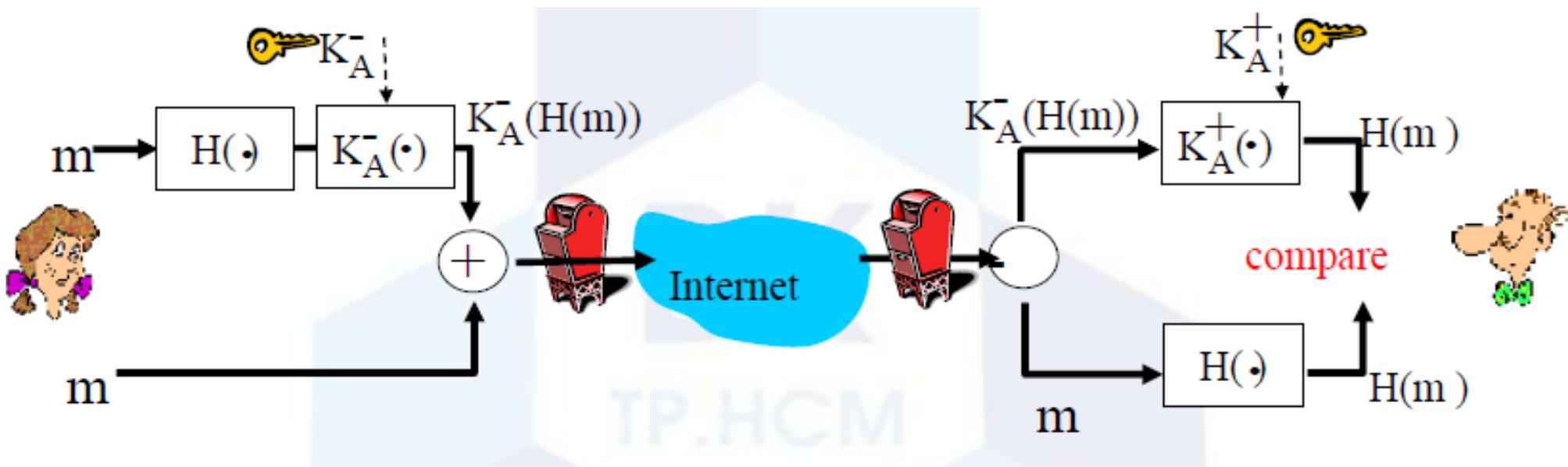


- Bob:

- sử dụng khóa cá nhân của anh để giải mã và lấy được K_S
- sử dụng K_S để giải mã $K_S(m)$ để lấy được m

Bảo mật email

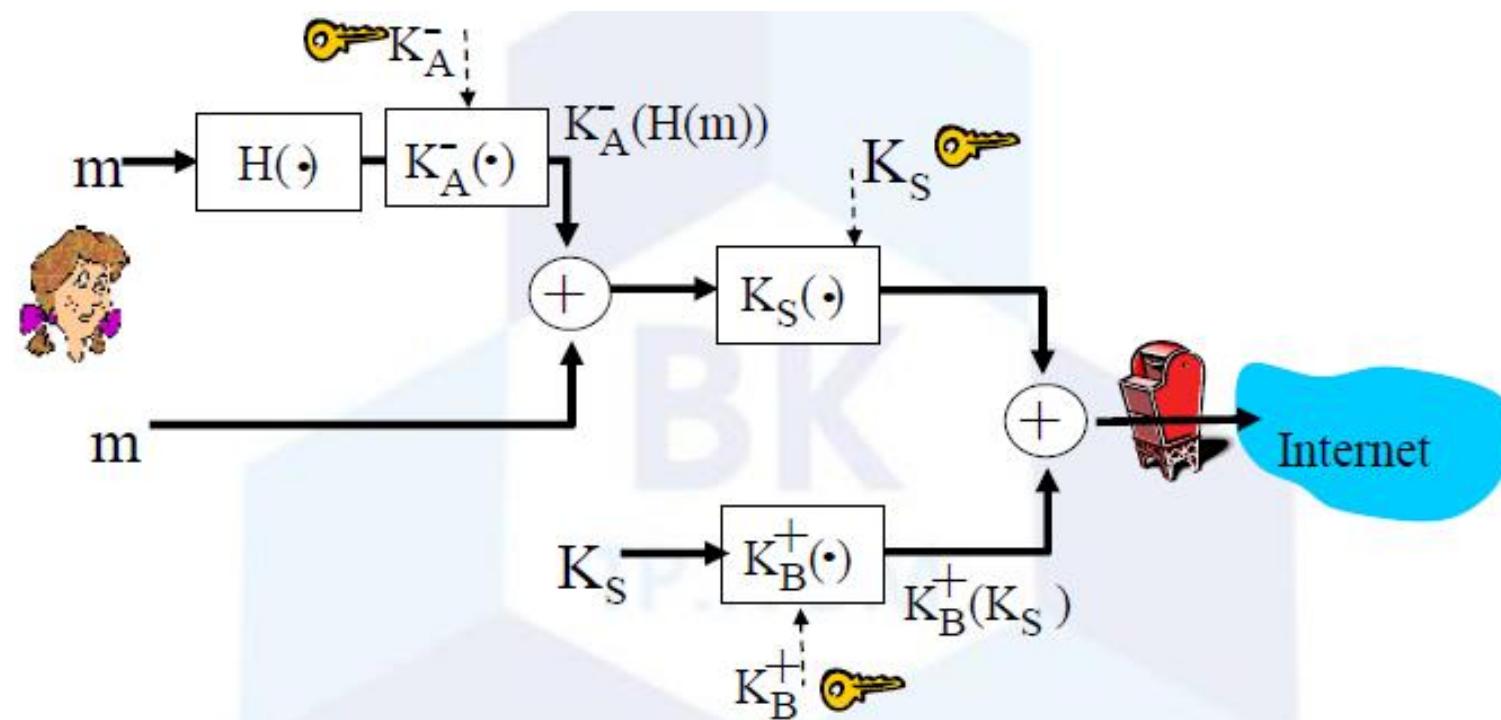
- Alice muốn cung cấp sự xác thực người gửi, tính toàn vẹn thông điệp.



- Alice kí số vào thông điệp.
- gửi cả thông điệp (chưa mã hóa) và chữ kí số.

Bảo mật email

- Alice muốn cung cấp tính bí mật, sự xác thực người gửi, tính toàn vẹn thông điệp.



- Alice sử dụng 3 khóa: khóa cá nhân của cô ta, khóa công khai của Bob, khóa đối xứng vừa tạo ra

MIME

- Cấu trúc thư 822 chỉ chấp nhận thư có nội dung là ký tự.
- MIME (Multi-purpose Internet Mail Extensions) là cấu trúc cho phép tích hợp các loại thông tin khác vào nội dung thư như hình ảnh, âm thanh, video, ký tự có dấu, văn bản định dạng, ...

Các loại thông tin có thể có trong nội dung thư theo cấu trúc MIME

Type	Subtype	Description
Text	Plain	Unformatted text
	Enriched	Text including simple formatting commands
Image	Gif	Still picture in GIF format
	Jpeg	Still picture in JPEG format
Audio	Basic	Audible sound
Video	Mpeg	Movie in MPEG format
Application	Octet-stream	An uninterpreted byte sequence
	Postscript	A printable document in PostScript
Message	Rfc822	A MIME RFC 822 message
	Partial	Message has been split for transmission
	External-body	Message itself must be fetched over the net
Multipart	Mixed	Independent parts in the specified order
	Alternative	Same message in different formats
	Parallel	Parts must be viewed simultaneously
	Digest	Each part is a complete RFC 822 message

Giao thức chuyển thư

- SMTP (Simple Mail Transfer Protocol): sử dụng giao thức vận chuyển TCP, port 25.
- SMTP được sử dụng để chuyển thư từ mail client đến SMTP relay agent (outgoing mail server) và chuyển thư từ mail server này đến mail server khác

Thủ tục gửi thư trong SMTP

- HELO <domain>
- MAIL FROM: <e-mail address>
- RCPT TO: <e-mail address>
- DATA
 - Header
 - Body
 - . <kết thúc thư>
- QUIT

Thủ tục gửi thư trong SMTP

```
S: 220 xyz.com SMTP service ready
C: HELO abcd.com
    S: 250 xyz.com says hello to abcd.com
C: MAIL FROM: <elinor@abcd.com>
    S: 250 sender ok
C: RCPT TO: <carolyn@xyz.com>
    S: 250 recipient ok
C: DATA
    S: 354 Send mail; end with "." on a line by itself
C: From: elinor@abcd.com
C: To: carolyn@xyz.com
C: Subject: Earth orbits sun integral number of times
C:
C: Happy birthday to you
C: Happy birthday to you
C: .
    S: 250 message accepted
C: QUIT
    S: 221 xyz.com closing connection
```

Một số đặc điểm của SMTP

- Giao thức SMTP không yêu cầu xác thực.
- Kích thước tối đa của thư là 64 KB.
- Khi thời gian timeout giữa client và server không đồng bộ thì kết nối có thể bị ngắt giữa chừng.
- Có thể bị lặp thư vô hạn nếu dùng mailing list lồng nhau.

Giao thức truy xuất hộp thư

- POP3 (Post Office Protocol version 3): sử dụng giao thức vận chuyển TCP, port 110
- POP3 là giao thức được mail client sử dụng để truy xuất đến hộp thư trên mail server.
- IMAP (Internet Message Access Protocol) là một giao thức tương tự như POP3 nhưng ít được dùng hơn.

Thủ tục truy xuất hộp thư trong POP3

- USER <user-name>
- PASS <password>
- LIST: liệt kê thư trong hộp thư
- RETR <id>: đọc thư
- DELE <id>: xóa thư
- QUIT: Kết thúc

Thủ tục truy xuất hộp thư trong POP3

```
S: +OK POP3 server ready
C: USER carolyn
    S: +OK
C: PASS vegetables
    S: +OK login successful
C: LIST
    S: 1 2505
    S: 2 14302
    S: 3 8122
    S: .
C: RETR 1
    S: (sends message 1)
C: DELE 1
C: RETR 2
    S: (sends message 2)
C: DELE 2
C: RETR 3
    S: (sends message 3)
C: DELE 3
C: QUIT
    S: +OK POP3 server disconnecting
```

Dịch vụ WEBMAIL



User



WebMail Client = Browser
(Yahoo, Hotmail, FPTNET, VASC,...)

Mail Server
hcm.vnn.vn

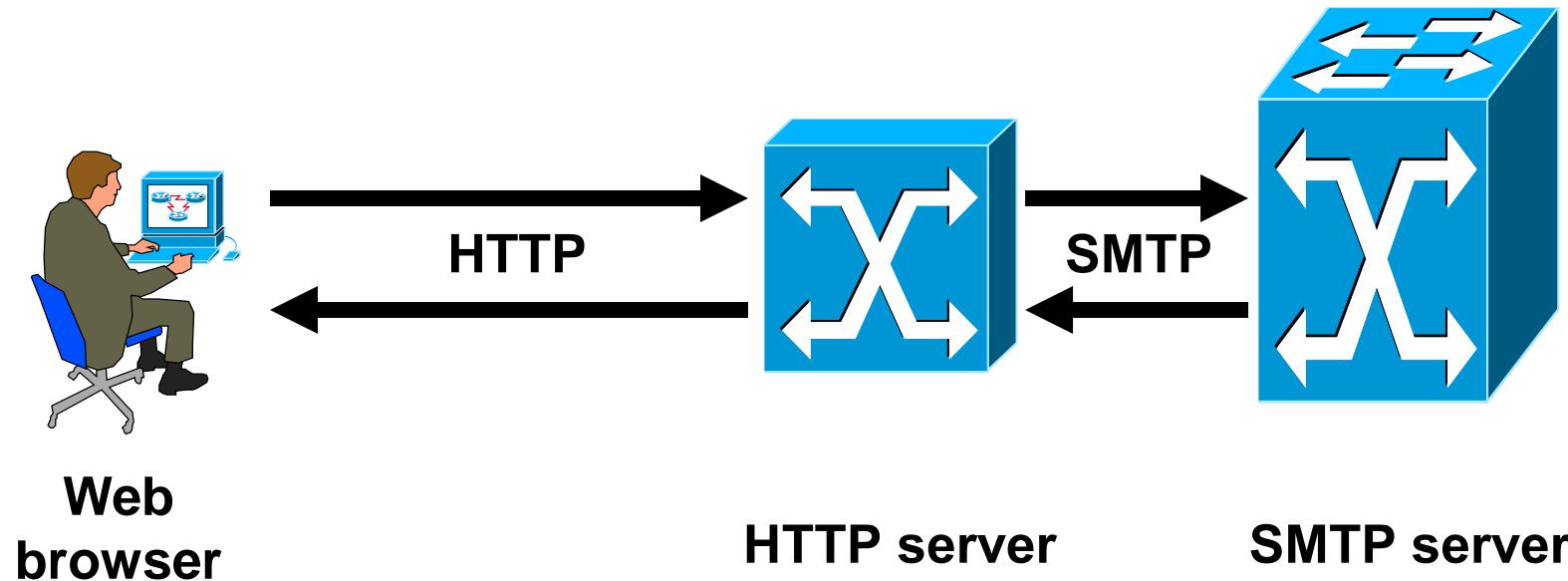


SEND TO me@yahoo.com

GET ALL messages
Here you messages

Web mail

Sử dụng giao diện Web thay cho mail client

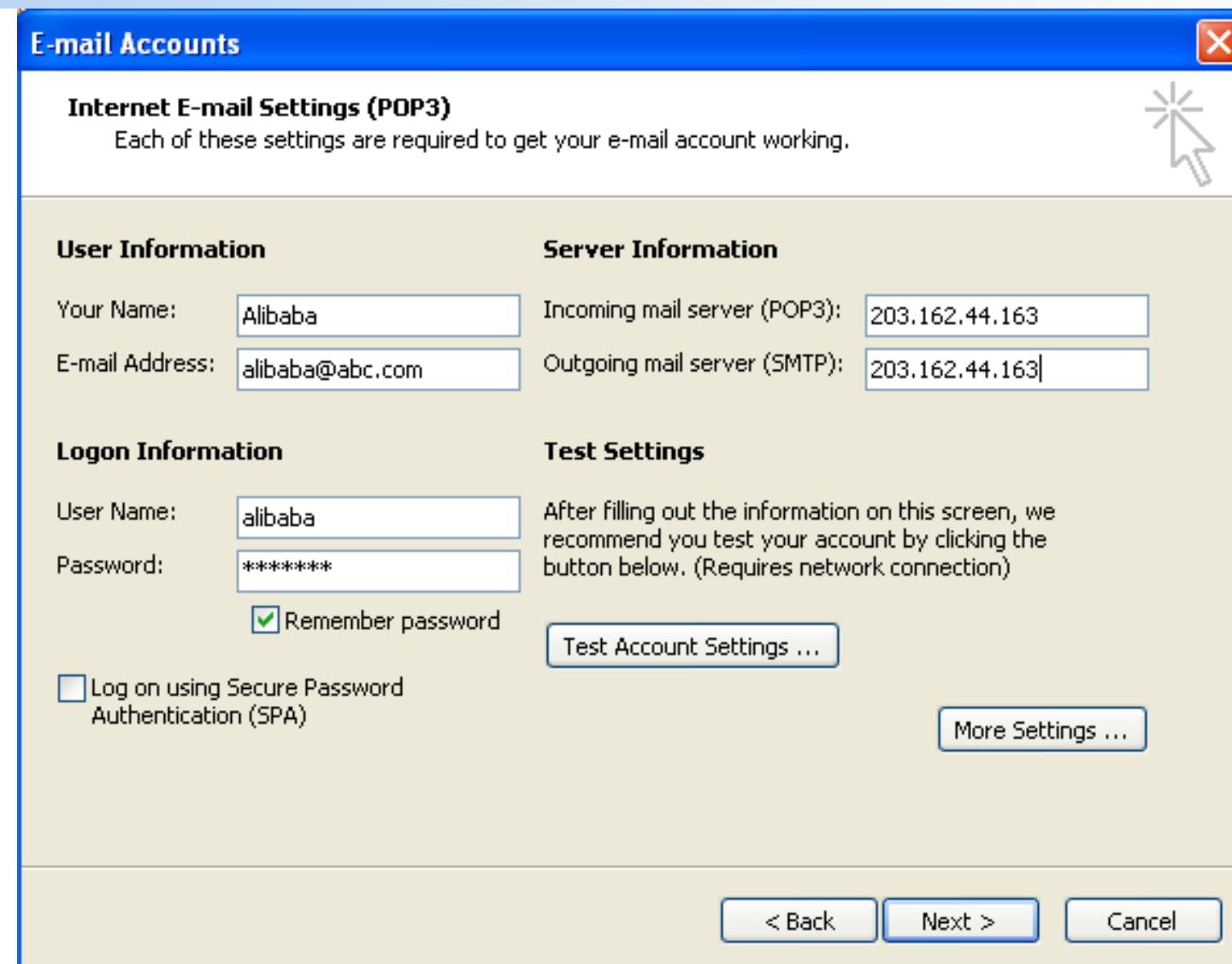


Cấu hình mail client

Các thông số cấu hình mail client:

- Incoming mail server
- Outgoing mail server
- User-name
- Password
- Các tùy chọn nâng cao

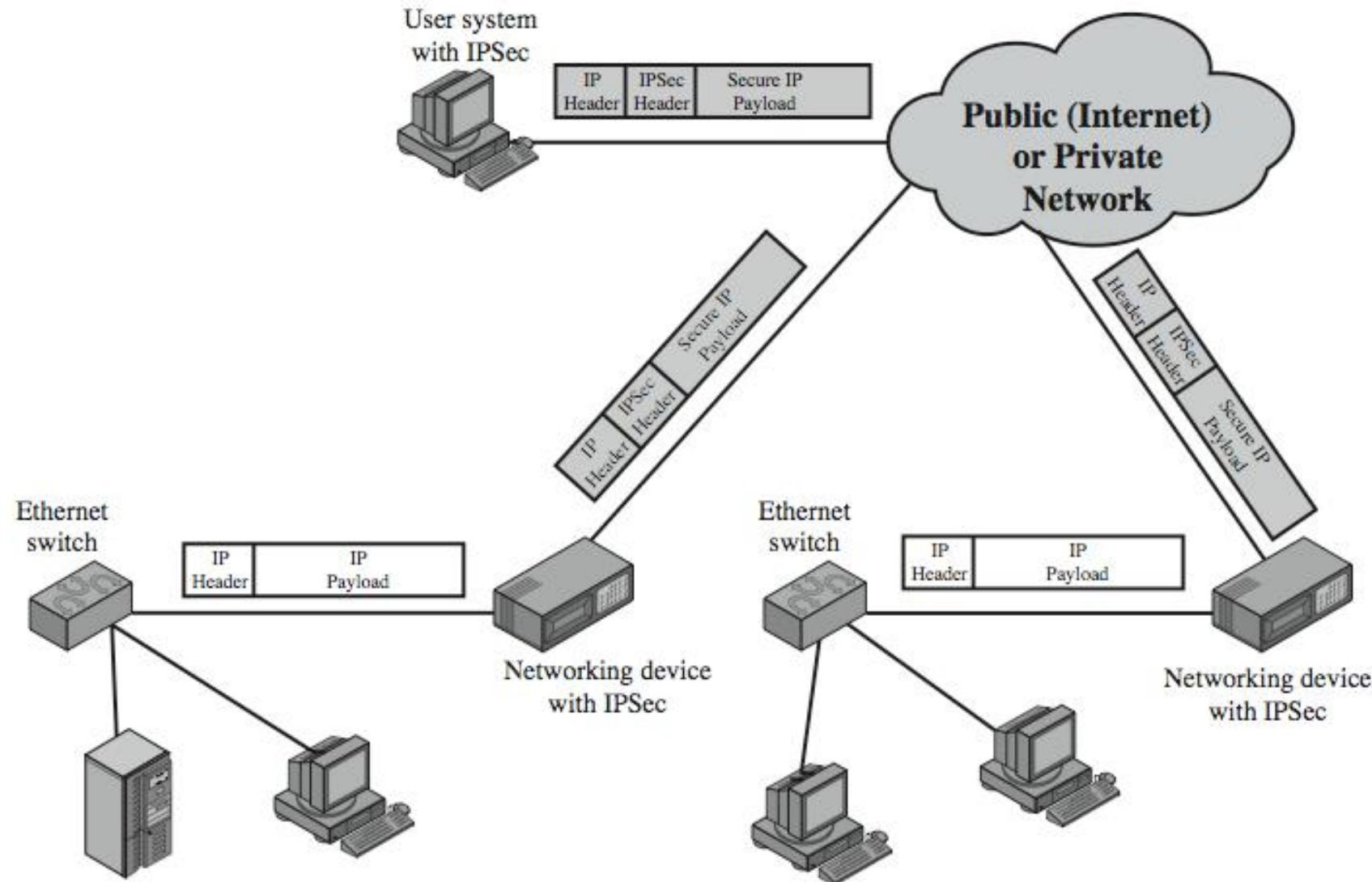
Cấu hình Outlook



Các giao thức bảo mật mạng

- Các cơ chế an toàn Ip cung cấp:
 - Xác thực - Authentication
 - Bảo mật - confidentiality
 - Quản trị khóa - key management
- IP security được dùng trên mạng các mạng LAN, mạng WAN riêng và chung, và cho cả trên Internet
- 1994, Hội đồng kiến trúc internet (Internet Architecture Board - IAB) đưa ra một báo cáo với tiêu đề "Security in the Internet Architecture" (RFC 1636). Cần xác thực, mã hóa trong IPv4 & IPv6

IP Security Uses



Lợi ích của IPSec

- IPSec trên một firewall/router cung cấp an toàn mạnh cho tất cả việc truyền qua vành đai. Nó chống lại việc đi vòng qua firewall/router
- IPSec nằm bên dưới tầng vận chuyển (transport layer) nên trong suốt (transparent) đối với tất cả các ứng dụng.
- Có thể trong suốt với người dùng cuối
- Nó có thể cung cấp an toàn cho tất cả các người dùng cá nhân và bảo vệ kiến trúc rẽ nhánh (routing architecture)

Kiến trúc IP Security

- Đặc tả IPSec rất phức tạp, được định nghĩa qua một số chuẩn (RFCs) với các nhóm sau:
 - Architecture. Bao phủ các khái niệm chung, các yêu cầu an ninh, các định nghĩa, và cơ chế xác định kỹ thuật Ipsec.
 - RFC4301 *Security Architecture for Internet Protocol*
 - Phần đầu xác thực (**Authentication Header**). AH một phần đầu mở rộng cho việc chứng thực thông điệp.
 - RFC4302 *IP Authentication Header*
 - Tải trọng an toàn đóng gói (**Encapsulating Security Payload**). ESP bao gồm một phần đầu đóng gói và phần cuối (trailer) được dùng để cung cấp việc mã hóa hoặc phối hợp mã hóa/xác thực
 - RFC4303 *IP Encapsulating Security Payload*

Kiến trúc IP Security

- Trao đổi khóa Internet (**Internet Key Exchange**). Một tập hợp các tài liệu mô tả các cơ chế quản lý khóa để dùng cho IPsec
 - RFC4306 *Internet Key Exchange (IKEv2) Protocol*
- Thuật toán mật mã (**Cryptographic algorithms**). Một tập lớn các tài liệu mà định nghĩa và mô tả các thuật toán mật mã của việc mã hóa, xác thực thông điệp, hàm phát sinh ngẫu nhiên giả, và việc trao đổi khóa mật mã.
- Khác. Có một số chuẩn RFCs liên quan đến IPSec khác, bao gồm việc xử lý chính sách an toàn và nô dung cơ sở thông tin quản lý (**Management Information Base**)

Các dịch vụ IPSec

- IPSec cung cấp các dịch vụ an toàn ở tầng IP bằng cách cho phép hệ thống chọn lựa các giao thức an toàn cần thiết, định rõ các thuật toán để dùng cho các dịch vụ, và đưa ra các khóa mật mã cần thiết để cung cấp các dịch vụ yêu cầu.
 - Điều khiển truy nhập
 - Toàn vẹn phi kết nối
 - Xác thực nguồn gốc dữ liệu
 - Tùy chối các gói tin phát lại. Đây là một dạng của toàn vẹn liên kết từng phần
 - Bảo mật (mã hóa)
 - Bảo mật luồng thông tin hữu hạn

Các dịch vụ IPSec

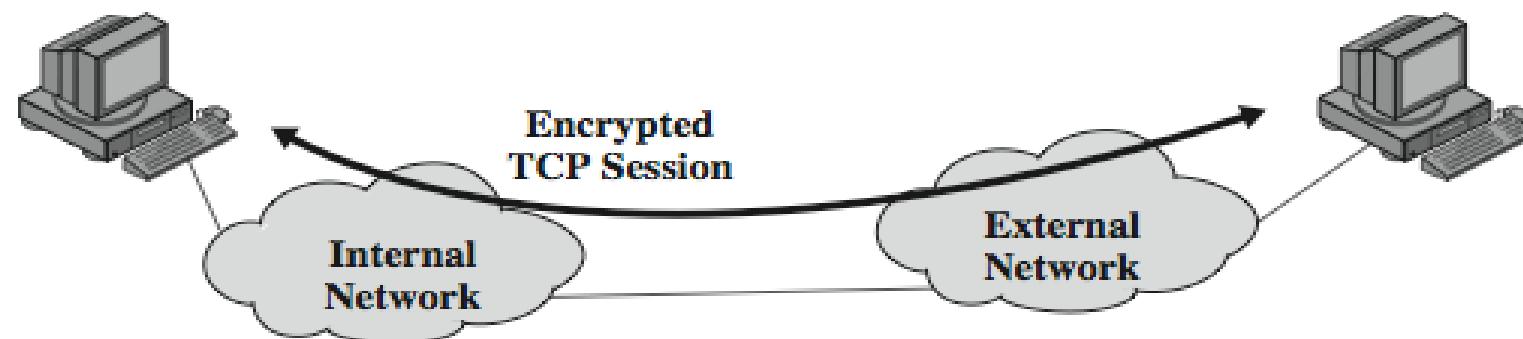
- Sử dụng một trong hai giao thức
 - Giao thức xác thực (ứng với AH)
 - Giao thức xác thực/mã hóa (ứng với ESP)
- Cả AH và ESP hỗ trợ hai chế độ sử dụng:
 - Chế độ vận chuyển (Transport mode)
 - Chế độ ống (tunnel mode)

Transport mode và Tunnel mode

- Chế độ vận chuyển (Transport Mode)
 - Dùng để mã hóa và tùy chọn chứng thực dữ liệu IP
 - Có thể thực hiện phân tích lưu lượng một cách hiệu quả
 - Tốt đối với ESP để máy chủ vận chuyển tới máy chủ
- Chế độ ống (Tunnel Mode)
 - Mã hóa toàn bộ gói IP
 - Thêm phần đầu mới cho bước nhảy kế tiếp
 - Không có bộ định tuyến trên đường có thể kiểm tra phần đầu IP bên trong
 - Tốt cho mạng riêng ảo (VPNs), an toàn cổng đến cổng

Transport mode và Tunnel mode

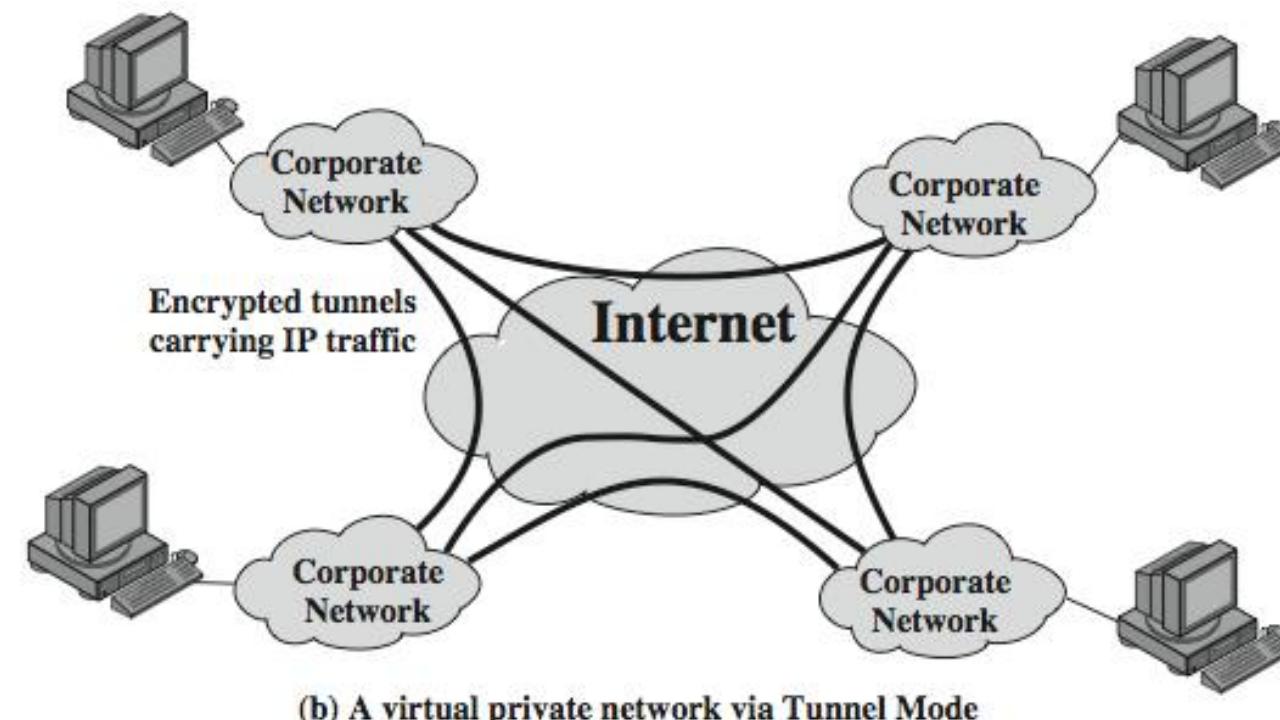
- Việc mã hóa (và chứng thực tùy chọn)được cung cấp trực tiếp giữa hai host



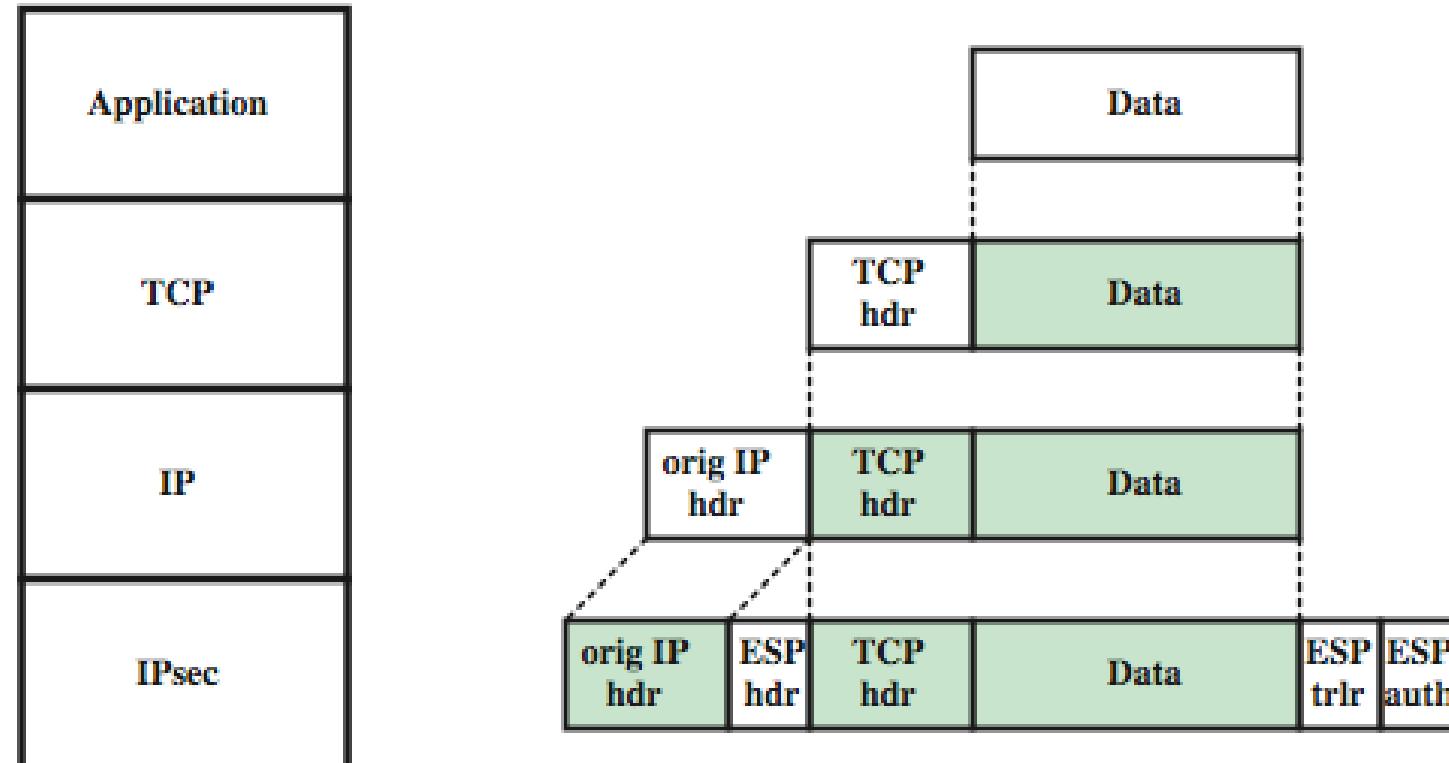
(a) Transport-level security

Transport mode và Tunnel mode

- Vd: 4 mạng riêng kết nối nhau thông qua internet
- Các host của từng mạng nội bộ dùng internet để chuyển tải dữ liệu như không tương tác với các host dựa trên internet.

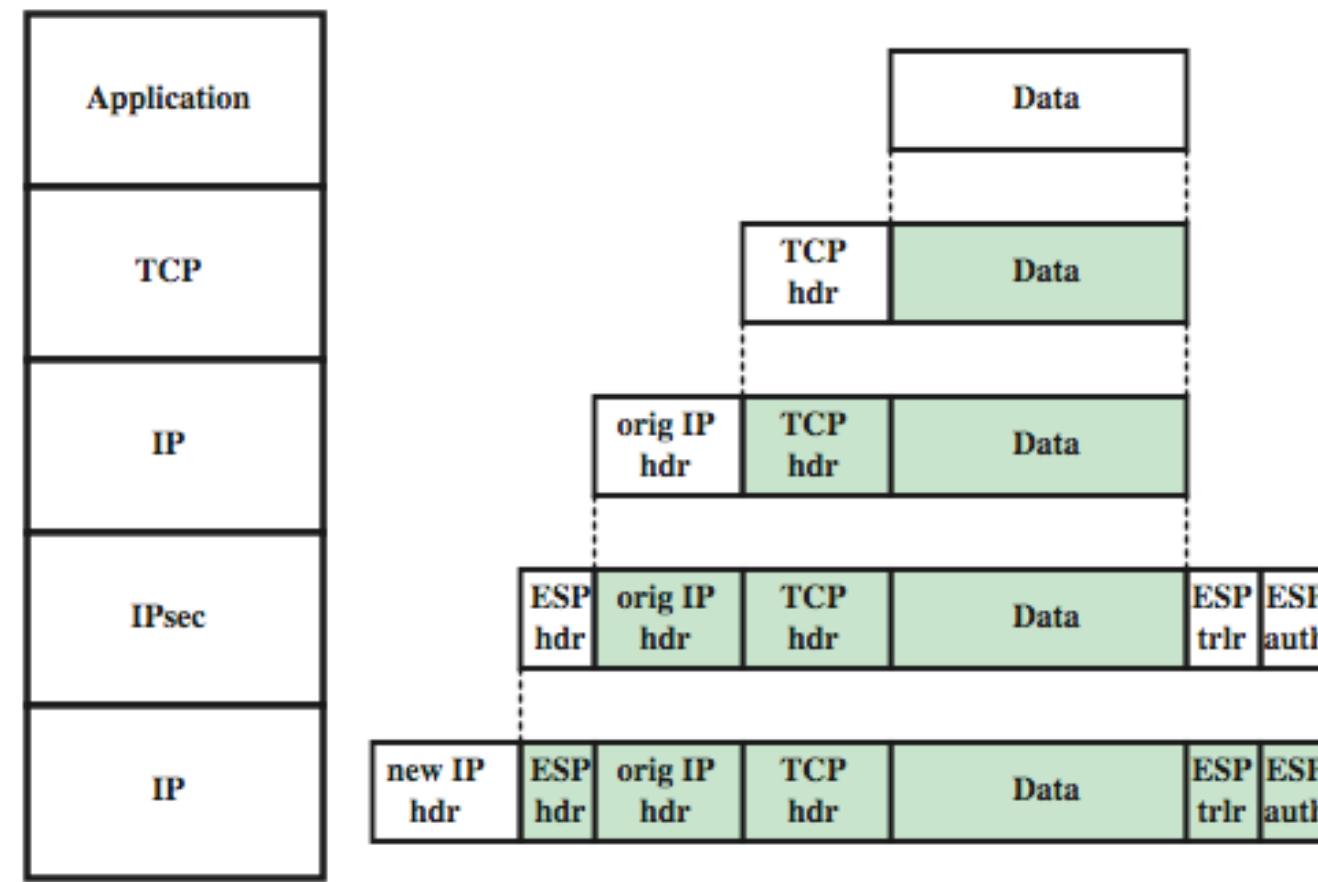


Giao thức Transport và Tunnel Mode



(a) Transport mode

Giao thức Transport và Tunnel Mode



(b) Tunnel mode

2. Chính sách IP Security

- Chính sách Ipsec được xác định chủ yếu bởi sự tương tác của hai CSDL: CSDL liên kết an ninh (**Security Association Database - SAD**) và CSDL chính sách an ninh (**Security Policy Database -SPD**).

Các liên kết an ninh (SA)

- SA là một mối quan hệ một chiều giữa người gửi và người nhận mà cung cấp sự an ninh cho luồng tin lưu chuyển
- SA được định nghĩa bởi 3 tham số:
 - Chỉ mục tham số an ninh (Security Parameters Index - SPI)
 - Địa chỉ IP đích
 - Định danh giao thức an ninh
- Các tham số khác lưu trong CSDL SA
 - Chỉ số dây, thông tin về phần đầu xác thực (AH) và phần đầu mở rộng AH & EH, thời hạn sống, ...
- Có lưu trữ CSDL của các liên kết an toàn

CSDL chính sách an ninh

- Liên quan đến lưu lượng IP với các SA đặc trưng
 - So khớp tập con của lưu lượng IP với SA liên quan
 - Sử dụng bộ chọn lọc để lọc lưu lượng gửi đi
 - Dựa trên: các địa chỉ IP nội bộ và từ xa, giao thức tầng kế tiếp, tên, các công cụ bộ và từ xa

Protocol	Local IP	Port	Remote IP	Port	Action	Comment
UDP	1.2.3.101	500	*	500	BYPASS	IKE
ICMP	1.2.3.101	*	*	*	BYPASS	Error messages
*	1.2.3.101	*	1.2.3.0/24	*	PROTECT: ESP intransport-mode	Encrypt intranet traffic
TCP	1.2.3.101	*	1.2.4.10	80	PROTECT: ESP intransport-mode	Encrypt to server
TCP	1.2.3.101	*	1.2.4.10	443	BYPASS	TLS: avoid double encryption
*	1.2.3.101	*	1.2.4.0/24	*	DISCARD	Others in DMZ
*	1.2.3.101	*	*	*	BYPASS	Internet

Các giao thức bảo mật mạng

- Bảo vệ kết nối TCP: SSL

Giao thức bảo mật được triển khai rộng rãi

- được hỗ trợ bởi hầu hết các trình duyệt và máy chủ web
- https
- hàng chục tỉ \$ được sử dụng hàng năm qua SSL

Thiết kế bởi Netscape vào 1993

Có vài biến đổi:

- TLS: transport layer security, RFC 2246

Cung cấp:

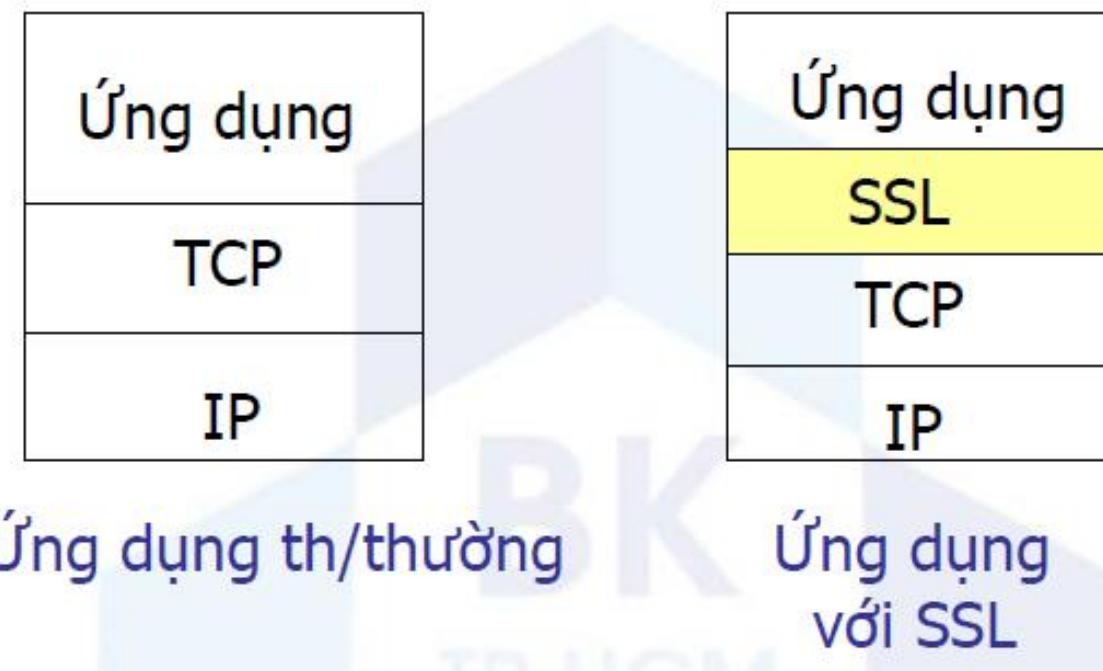
- Bí mật
- Toàn vẹn
- Xác thực

Các mục tiêu ban đầu:

- Có giao dịch thương mại điện tử
- Mã hóa (đặc biệt là số thẻ-tín dụng)
- xác thực máy chủ Web
- xác thực khách (tùy chọn)
- Hạn chế thủ tục khi mua bán với bạn hàng mới
- Có sẵn trong tất cả ứng dụng TCP
- giao diện socket kết nối an toàn (Secure socket interface)

Các giao thức bảo mật mạng

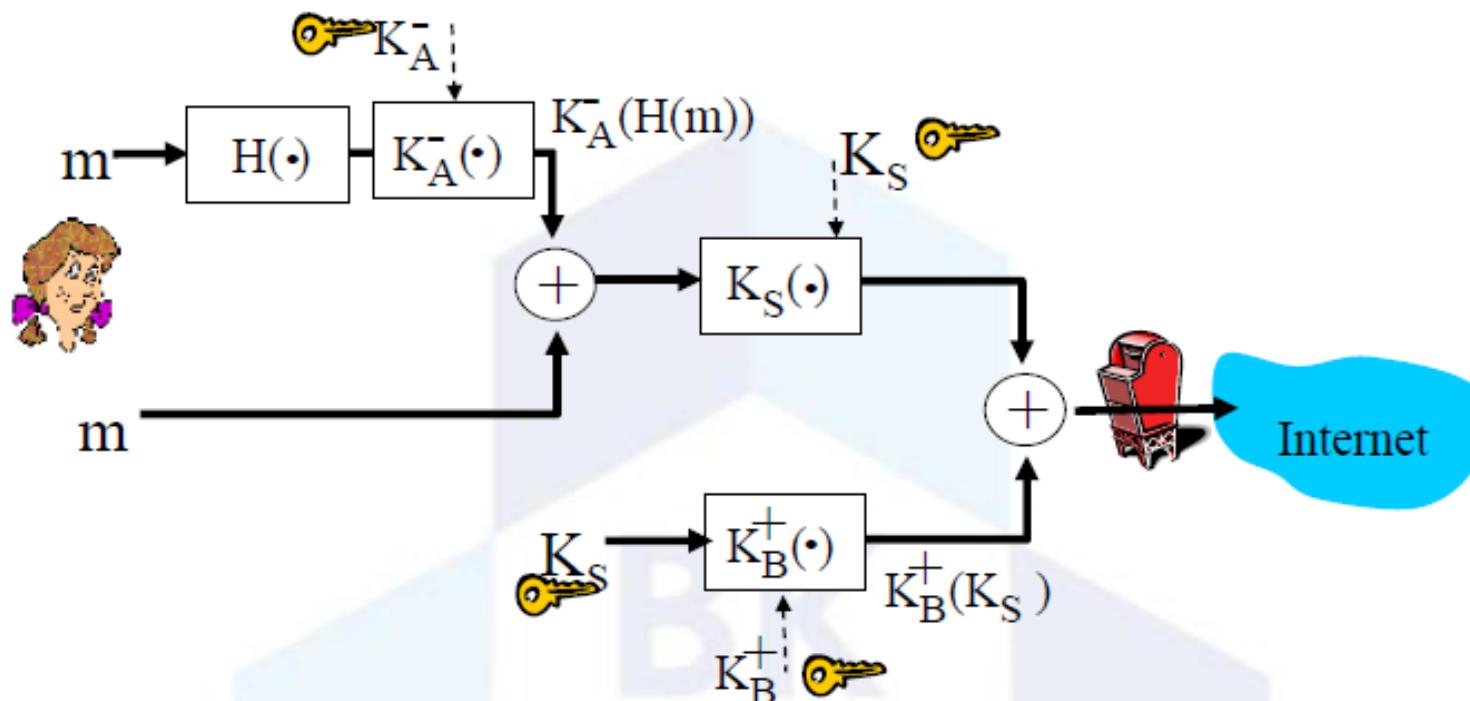
- SSL and TCP/IP



SSL cung cấp giao diện lập trình ứng dụng (API) cho ứng dụng
• các thư viện/lớp SSL trong C và Java đã có sẵn

Các giao thức bảo mật mạng

- Quá trình làm việc:



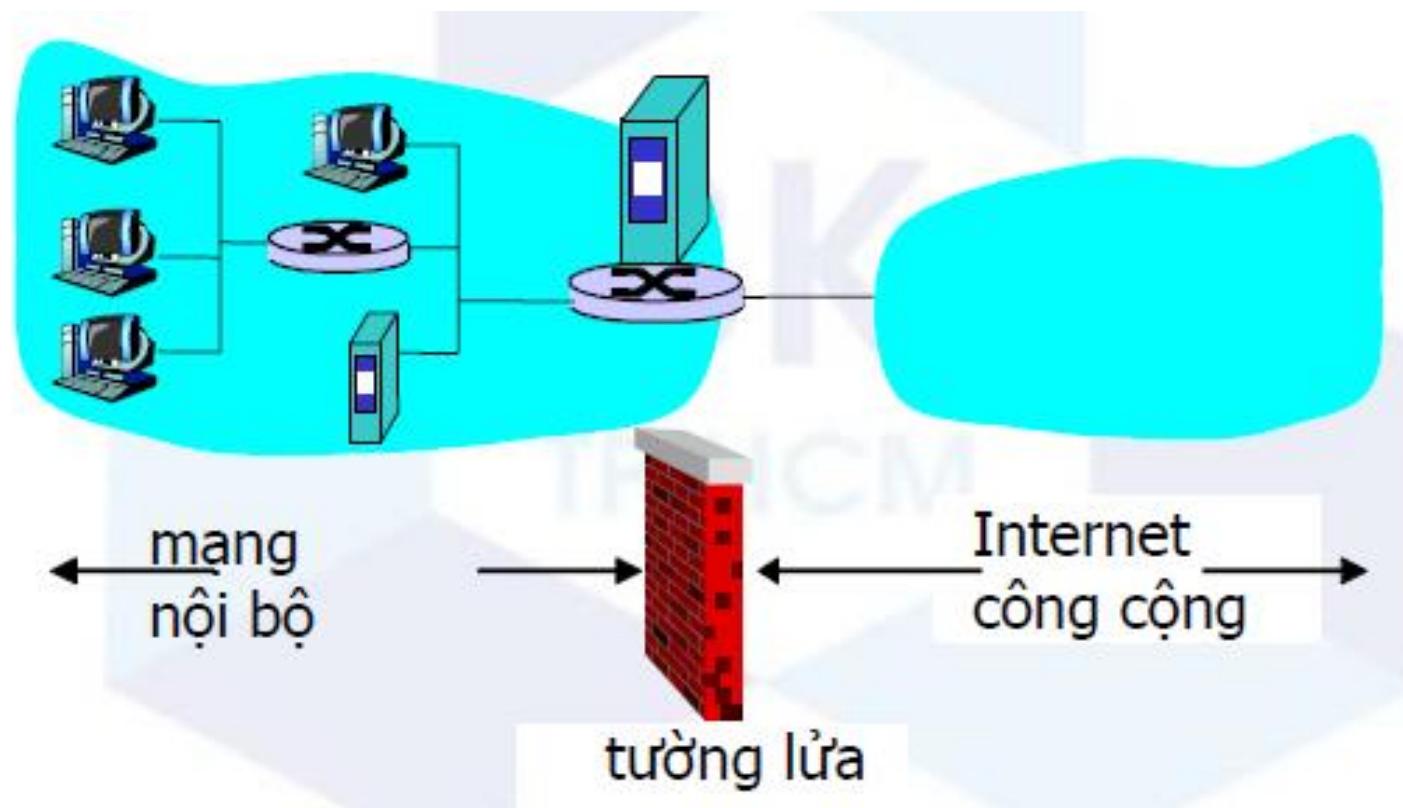
Nhưng cần gửi luồng byte và dữ liệu tương tác

- Cần một bộ các khóa bí mật cho toàn bộ kết nối
- Cần phần trao đổi chứng chỉ của giao thức: pha bắt-tay

Các giao thức bảo mật mạng

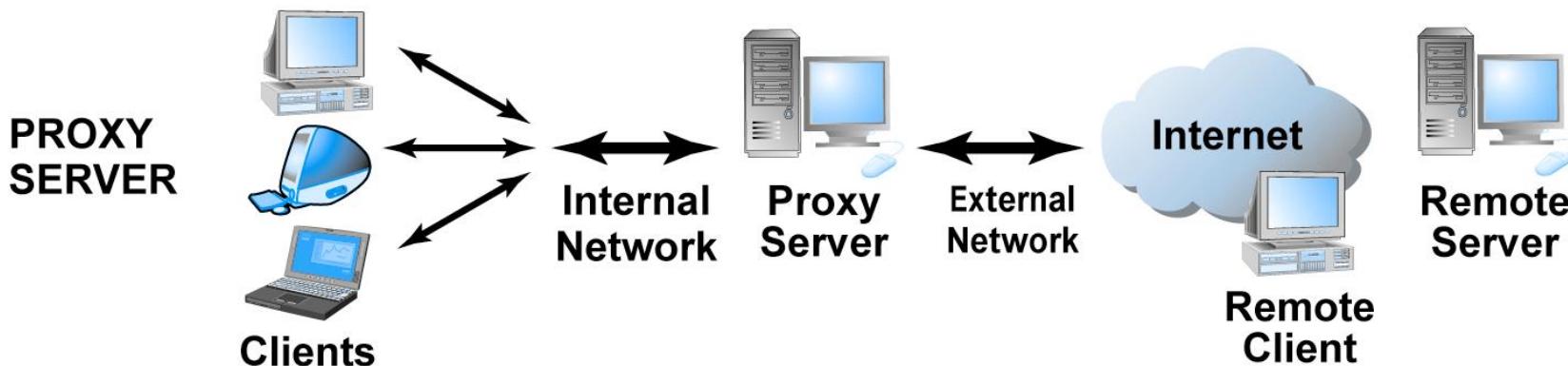
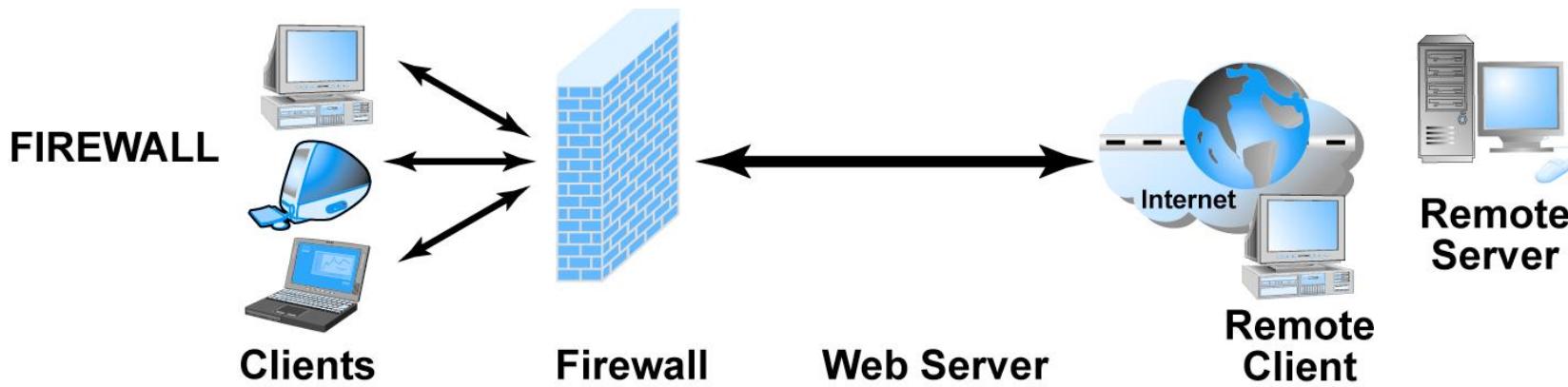
Bảo mật hành vi: tường lửa và IDS

- Tường lửa: cách ly mạng bên trong tổ chức với mạng Internet, cho phép vài gói tin đi qua, chặn những gói khác.



Các giao thức bảo mật mạng

Firewalls and Proxy Servers



Các giao thức bảo mật mạng

Tường lửa: Để làm gì?

- ngăn chặn tấn công từ chối dịch vụ:
 - Sự gửi tràn SYN: kẻ tấn công thiết lập nhiều kết nối TCP giả, không còn tài nguyên cho những kết nối “thật”
- ngăn chặn sự truy cập/thay đổi không hợp pháp vào dữ liệu nội bộ.
 - vd: kẻ tấn công thay đổi trang chủ của công ty
- chỉ cho phép những truy cập được xác thực vào bên trong mạng (nhóm các người dùng, máy đã được xác thực)
 - ba loại tường lửa:
 - bộ lọc gói không trạng thái
 - bộ lọc gói trạng thái
 - cổng kiểm soát ứng dụng

Các giao thức bảo mật mạng

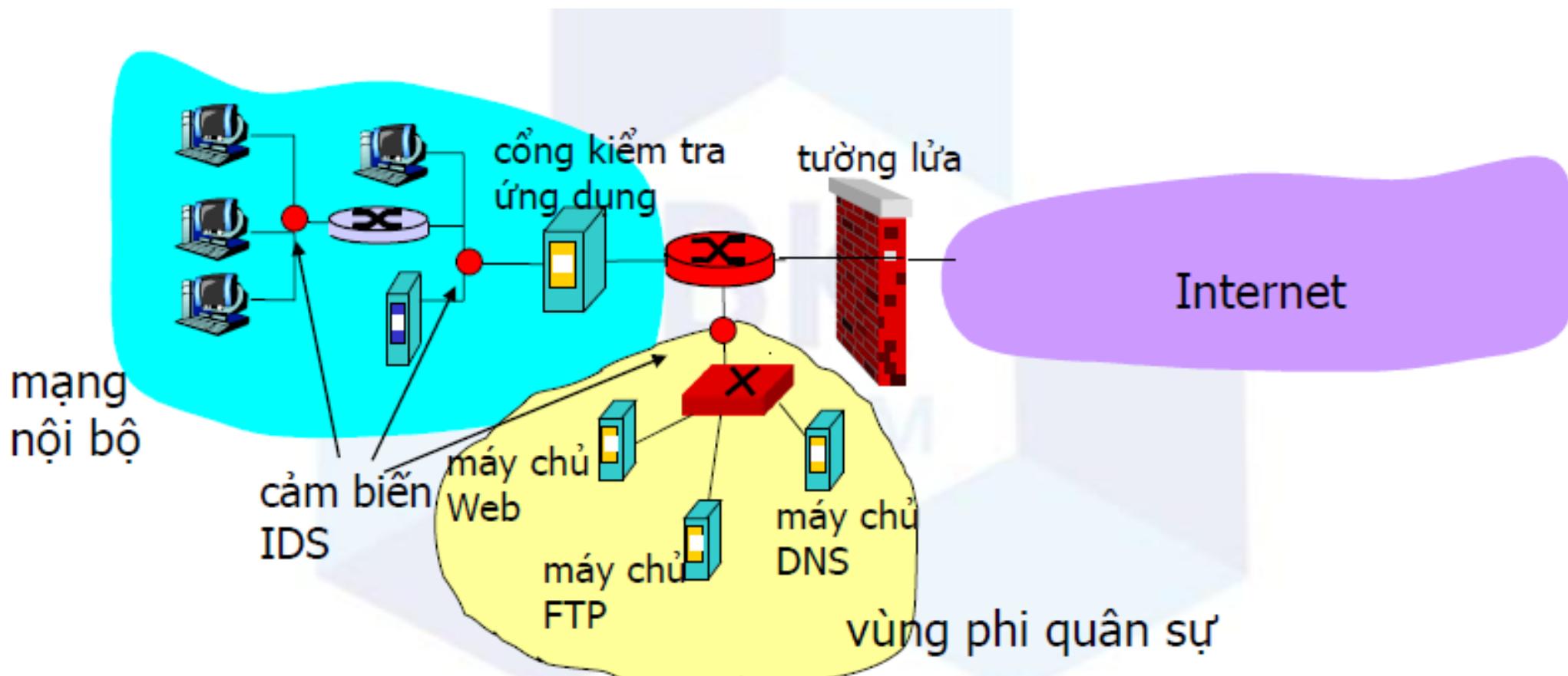
Hệ thống phát hiện xâm nhập

- sự lọc gói:
 - chỉ làm việc với đầu vào TCP/IP
 - không kiểm tra sự tương quan giữa các phiên
 - IDS: hệ thống phát hiện xâm nhập
 - Kiểm tra gói sâu: xem xét nội dung gói tin (vd: kiểm tra chuỗi kí tự trong gói tin, so sánh với cơ sở dữ liệu của vi-rút, chuỗi tấn công)
 - xem xét mối tương quan giữa nhiều gói tin
- sự dò cổng
- ánh xạ mạng
- tấn công DoS

Các giao thức bảo mật mạng

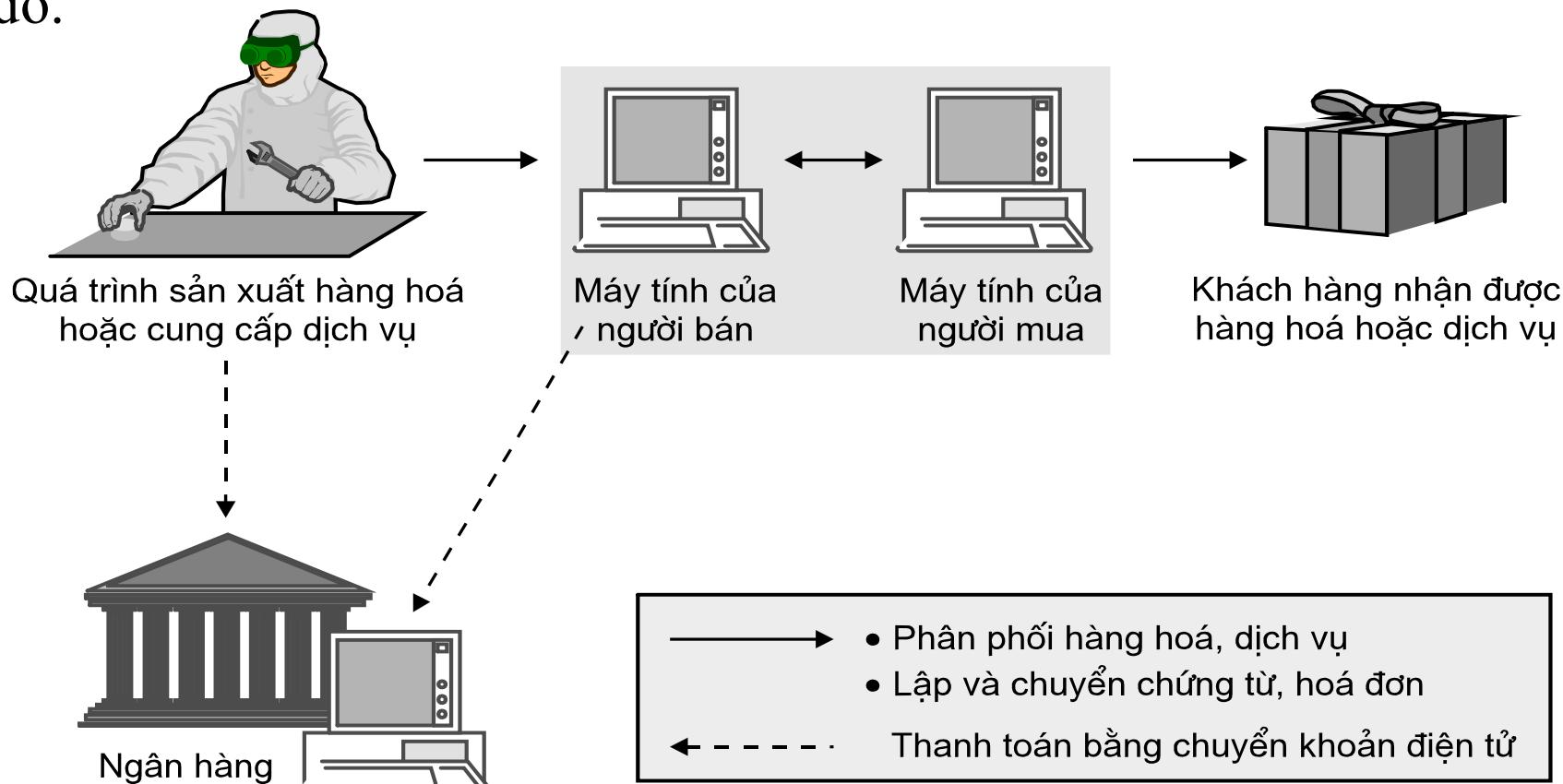
Hệ thống phát hiện xâm nhập

- nhiều IDS: nhiều loại kiểm tra khác nhau tại nhiều vị trí khác nhau



Các giao thức thanh toán điện tử

Khái niệm: **thanh toán trực tuyến** là một hình thức thanh toán trực tuyến cho một sản phẩm nào đó (Hàng hóa, dịch vụ ..) tại các website thương mại điện tử mà sản phẩm đó có thể phát hành thẻ thanh toán, hoặc là thống nhất với một nhà cung cấp dịch vụ cụ thể nào đó (Ngân hàng, thậm chí là mạng di động ...) người mua sản phẩm thanh toán qua các hình thức đó.



CÁC LOẠI HÌNH THANH TOÁN TRỰC TUYẾN

1. *Tiền mặt*
2. *Các loại thẻ tín dụng(Credit card), thẻ trả phí và thẻ ghi nợ (Debit card)*
3. *Các loại séc (check)*
4. *Chuyển khoản điện tử (EFT - Electronic Funds Transfer) và Trung tâm thanh toán bù trừ tự động (ACH - Automated Clearing House)*
5. *Lệnh chi (Money order)*
6. *Thanh toán ngang hàng – Person two person*
7. *Thanh toán qua di động*

Yêu cầu cơ bản của Thanh Toán điện tử

- *Tính tin cậy*
- *Tính toàn vẹn*
- *Tính xác thực*

Tính tin cậy

- Trong một giao dịch, khi khách hàng đưa mã số thẻ tín dụng của mình cho người bán, họ phải được bảo đảm độ ***tin cậy***, nghĩa là mã số thẻ tín dụng của họ sẽ chỉ được tiết lộ cho những người cần biết, như ngân hàng phát hành

Tính toàn vẹn

- Trong mỗi giao dịch, chi tiết, khối lượng, chất lượng bản thân hàng hoá mà khách hàng đã mua đều không bị thay đổi bất hợp pháp, cũng như giá trị thanh toán không thay đổi

Tính xác thực

- Người mua và người bán đều yêu cầu tính **xác thực** của giao dịch, nghĩa là phải đảm bảo rằng, **đối tác** của mình trong giao dịch **là có thực** và **có thể xác nhận được**, các loại hàng hóa, dịch vụ có thể xác nhận được.
- Bản thân người bán hàng cũng cần đến sự xác thực. Nếu khách hàng không sử dụng tiền mặt để thanh toán, người bán sẽ yêu cầu xuất trình những chứng cứ để xác minh như bằng lái xe hoặc bản sao chứng minh nhân dân.

Đk người mua: đăng ký một loại thẻ



- Cách phổ biến nhất hiện nay là sử dụng thẻ tín dụng Credit card của các công ty, tập đoàn uy tín

Các thẻ tín dụng thông dụng (16 chữ số)



Số thẻ (16 chữ số được in trên mặt trước thẻ)

Họ tên chủ sở hữu in trên thẻ

Thời hạn hết hạn của thẻ, cũng in trên mặt trước thẻ

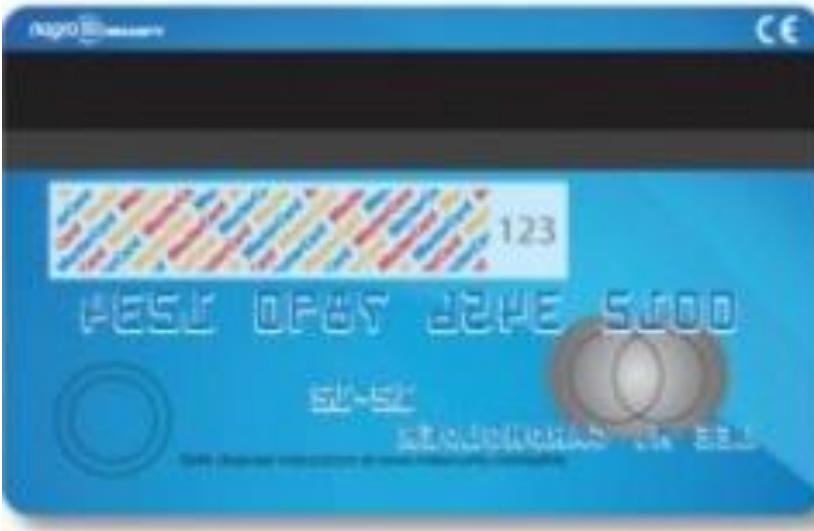
Mã số an toàn (security code) là ba chữ số cuối cùng in trên mặt sau của thẻ.

Thông số này không bắt buộc phải cung cấp, tùy website có yêu cầu hay không.

Địa chỉ nhận hóa đơn thanh toán việc sử dụng thẻ do ngân hàng gửi cho chủ thẻ.

Thông số này cũng không bắt buộc phải cung cấp, tùy website có yêu cầu hay không.

3 số cuối cùng mặt sau =mã an toàn



Mã an toàn là 304



Hai điều kiện người bán:MA và PG

- ❖ Có một Thương khoản(Merchant Account)
- ❖ Một cổng thanh toán(Payment Gateway)

Merchant Account



Payment Gateway



Qui trình giao dịch cơ bản



CÁCH THỨC THANH TOÁN TRỰC TUYẾN

Cổng thanh toán trực tuyến (Payment gateway)
hoạt động như thế nào?



Credit, Debit, or Charge Card Online Payment Processing

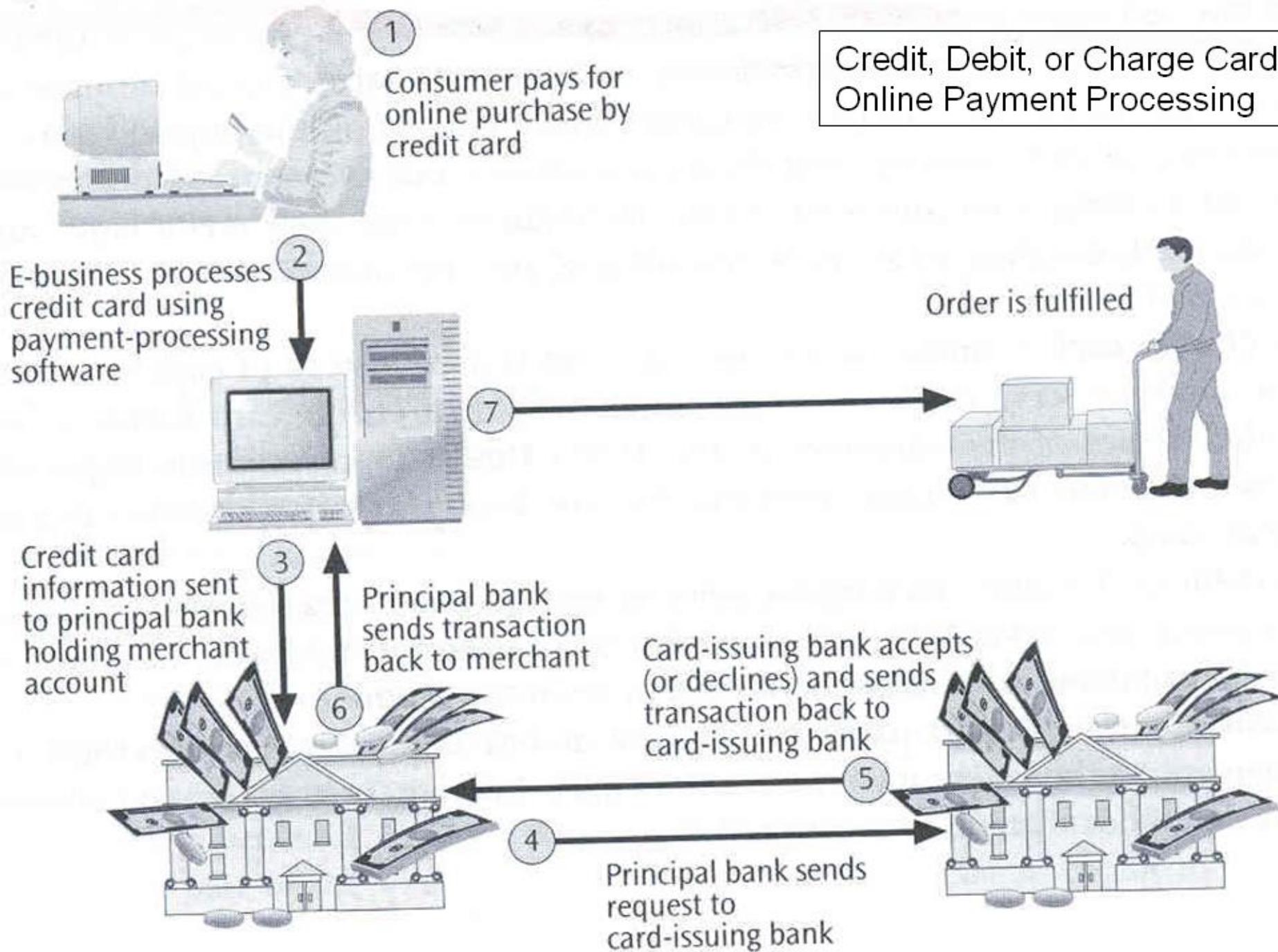
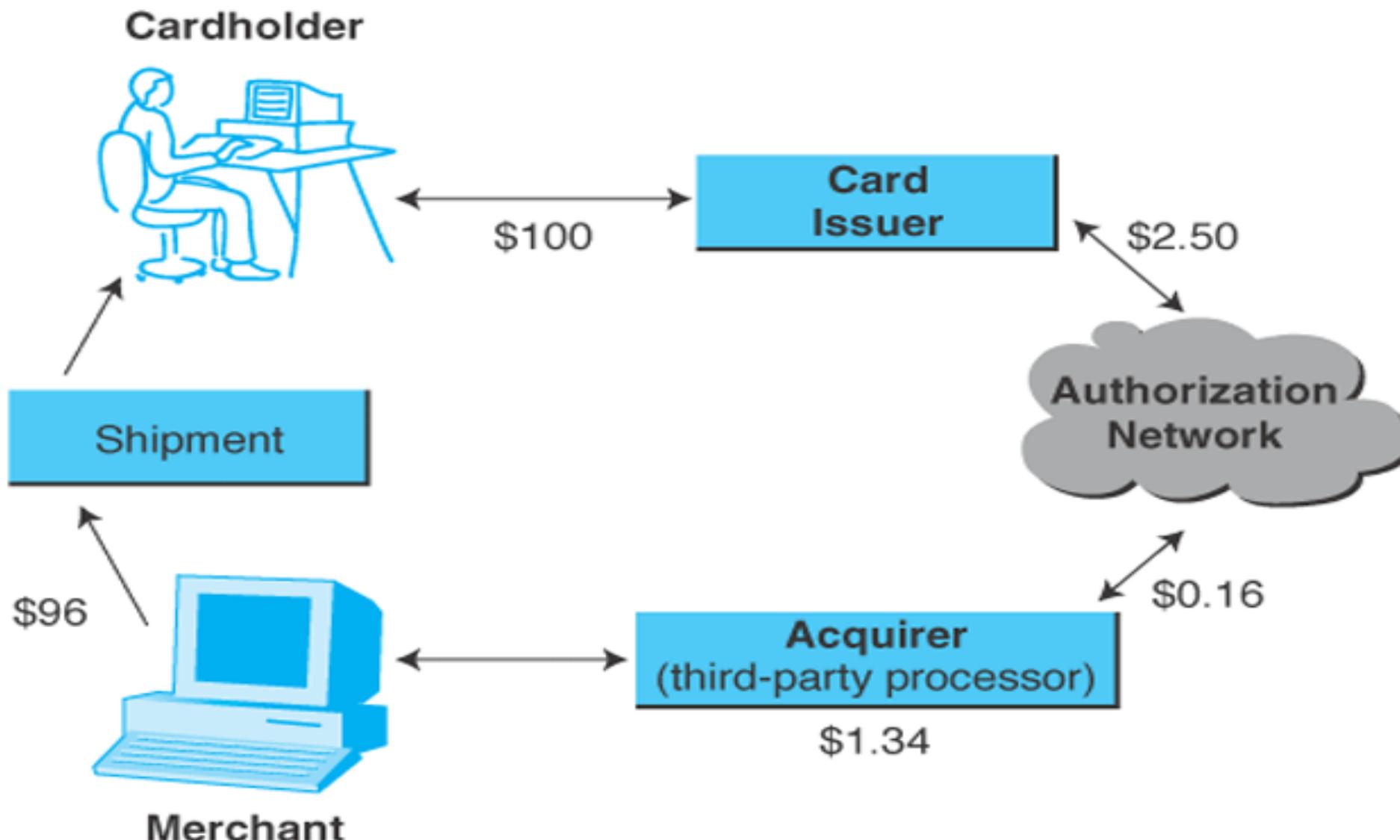
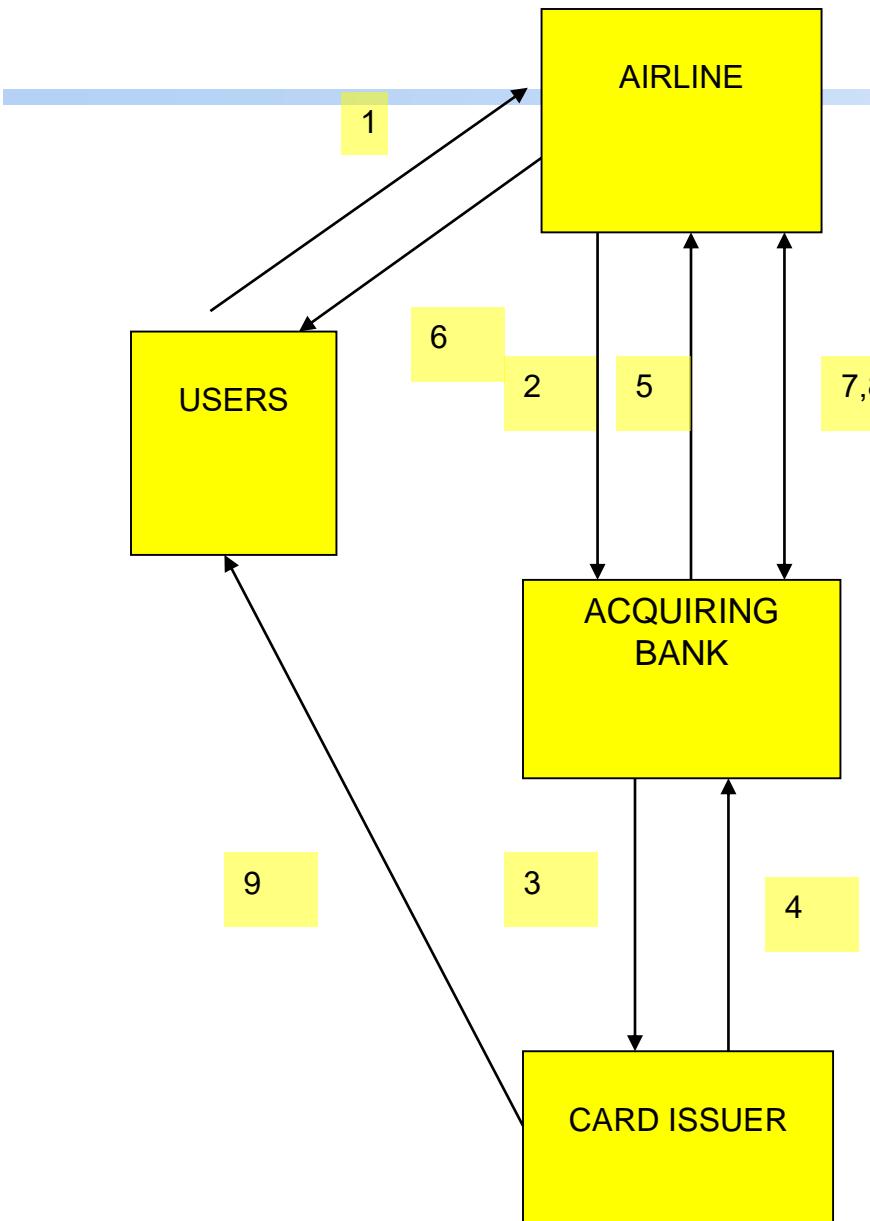


Exhibit 13.1 Online Credit Card Processing



Source: S. Korper and J. Ellis, *The E-Commerce Book: Building the E-Empire*. © 2000 by Academic Press, used with permission from Elsevier.

Mua vé máy bay trực tuyến



1. Người mua thực hiện giao dịch bằng cách gửi thông tin xác nhận mua vé kèm theo số thẻ tín dụng. Tuy nhiên, hãng máy bay không có được số thẻ vì nó đã được mã hóa
2. Hãng máy bay xác nhận gd với ngân hàng.
3. Ngân hàng kiểm tra lại với ngân hàng phát hành thẻ xem thẻ có hợp pháp không
4. Ngân hàng phát hành thẻ xác nhận lại với ngân hàng của hãng máy bay.
5. Ngân hàng của hãng máy bay thông báo cho hãng máy bay xác nhận giao dịch.
6. Người mua vé nhận được vé (eTicket) là một con số
7. Ngân hàng trả tiền
8. Hãng máy bay nhận tiền.
9. Người mua nhận được hóa đơn từ ngân hàng

Các nhà cung cấp dịch vụ thanh toán trực tuyến

Sử dụng VisaCard

Sử dụng thẻ AMERICAN EXPRESS CARD

Sử dụng cổng thanh toán WebMoney

PayPal

MoneyBookers

Alert Pay

CheckOut

WorldPay

Cổng thanh toán PayPal

- Hoạt động trong lĩnh vực tmđt
- Cung cấp dịch vụ thanh toán
- Chuyển tiền qua mạng Internet
- Xử lý thanh toán cho các hằng hoạt động trực tuyến, các trang đấu giá, và các khách hàng doanh



Cổng thanh toán PayPal

Tiểu sử PayPal

Thành lập: Palo Alto, California, USA (1998)

Trụ sở: tòa nhà North First Street, thung lũng
Sillicon, San Jose, California USA

Công ty mẹ: eBay (**10/2002**)

Trang chủ: www.paypal.com

Cổng thanh toán PayPal

Có hơn 153 triệu tài khoản trên toàn cầu, mạng lưới trải rộng khắp 190 thị trường và hỗ trợ 17 đơn vị tiền tệ, thúc đẩy hoạt động thương mại điện tử bằng các giải pháp thanh toán không giới hạn địa lý, tiền tệ và ngôn ngữ.

Tiện ích:

- Cực kỳ bảo mật.
- Hỗ trợ an toàn giao dịch cho cả người mua và người bán.
- Thanh toán qua Paypal rất nhanh chóng, an toàn và tiện lợi
- Khi thanh toán, bạn sẽ không phải nhập số thẻ thanh toán (Visa, Master...) của mình mỗi khi cần

CÁC YÊU CẦU ĐỂ LẬP TÀI KHOẢN PayPal

- Trên 18 tuổi
- Có 1 trong các loại sau:
 - Thẻ ghi nợ (Debit Card)
 - Thẻ tín dụng (Credit Card)
 - 1 tài khoản ngân hàng và địa chỉ e-mail

3 loại tài khoản PayPal

- **PayPal Personal:** dành cho cá nhân
- **Premier PayPal:** dành cho người dùng thanh toán với số tiền nhiều và thường xuyên thực hiện giao dịch.
- **PayPal Business:** dành cho doanh nghiệp

Trạng thái PayPal

- Blance=0: chuyển tiền vào thông qua tài khoản ngân hàng hoặc Credit Card.
- Blance > 0: thực hiện các giao dịch và có thể rút về sử dụng.

Ưu khuyết PayPal

Nhược điểm:

Quá trình thực hiện hợp đồng mất thời gian

Trong quá trình sử dụng Paypal, chúng ta cần phải lưu ý đến những vấn đề sau để bảo đảm tài khoản không bị hạn chế hoặc bị khóa:

- Thường xuyên truy cập tài khoản Paypal.
- Cập nhật thông tin cá nhân.
- Thay đổi mật khẩu định kỳ.

Ưu điểm:

Nhận tiền thanh toán ngay lập tức

An toàn, giảm rủi ro

PayPal thay đổi chính sách ở VN

- TK đăng ký từ Việt nam chỉ có chức năng chi mà không có chức năng nhận tiền.
- 14/10/2009: Chính thức thực hiện chức năng nhận tiền

CÁC DỊCH VỤ THANH TOÁN PHỔ BIẾN QUỐC TẾ

3. Sử dụng cổng thanh toán MoneyBookers

a/ Đặc điểm

- Là dịch vụ thanh toán trực tuyến, giúp gửi và nhận tiền online một cách nhanh chóng thông qua Email.
- Là một trong những nhà cung cấp dịch vụ thanh toán online lớn nhất thế giới
- Có trên 10 triệu tài khoản người dùng, và là một trong những hình thức thanh toán online được chấp nhận rộng rãi nhất.



CÁC DỊCH VỤ THANH TOÁN PHỔ BIẾN QUỐC TẾ

3. Sử dụng cổng thanh toán MoneyBookers

b/ Tính năng

- Thanh toán tại các website/dịch vụ chấp nhận MB
- Nạp tiền và rút tiền từ các website, dịch vụ cá cược thể thao, casino, poker...
- Chuyển và nhận tiền giữa các tài khoản MB
- Chuyển tiền vào tài khoản Moneybookers bằng thẻ tín dụng hoặc thẻ ghi nợ
- Rút tiền từ MB về tài khoản ngân hàng hoặc thẻ Visa.

CÁC DỊCH VỤ THANH TOÁN PHÔ BIÊN Ở VIỆT NAM

1. Các cổng thanh toán trực tuyến ở Việt Nam

a/ Cổng thanh toán Baokim.vn

- Là cổng thanh toán trực tuyến xây dựng theo mô hình hệ thống Paypal, Moneybookers...
- Là cách đơn giản nhất cho phép người mua hàng (trực tuyến), bán hàng (trực tuyến) thực hiện giao dịch tài chính (chuyển tiền, nhận tiền) một cách an toàn và tiện lợi.

CÁC DỊCH VỤ THANH TOÁN PHỔ BIẾN Ở VIỆT NAM

1. Các cổng thanh toán trực tuyến ở Việt Nam

a/ Cổng thanh toán_Baokim.vn

❖ Chức năng của Baokim.vn

- Thanh toán đơn hàng qua hệ thống Bảo Kim
- Chuyển tiền giữa hai người dùng là thành viên của Bảo Kim
- Cung cấp dịch vụ thanh toán trực tiếp và chuyển tiền trực tiếp
- Chức năng hoàn trả lại tiền, chức năng từ chối? hủy bỏ giao dịch chuyển tiền.

BAOKIM.VN

Niềm tin mua sắm



CÁC DỊCH VỤ THANH TOÁN PHÔ BIÊN Ở VIỆT NAM

1. Các cổng thanh toán trực tuyến ở Việt Nam

b/ Cổng thanh toán_Nganluong.vn

Là dịch vụ thanh toán trực tuyến cho TMĐT tiên phong và hàng đầu tại Việt Nam .

Cho phép các cá nhân và doanh nghiệp gửi và nhận tiền thanh toán trên Internet ngay tức thì một cách **AN TOÀN, PHÔ BIÊN, TIỆN LỢI VÀ ĐƯỢC BẢO VỆ**

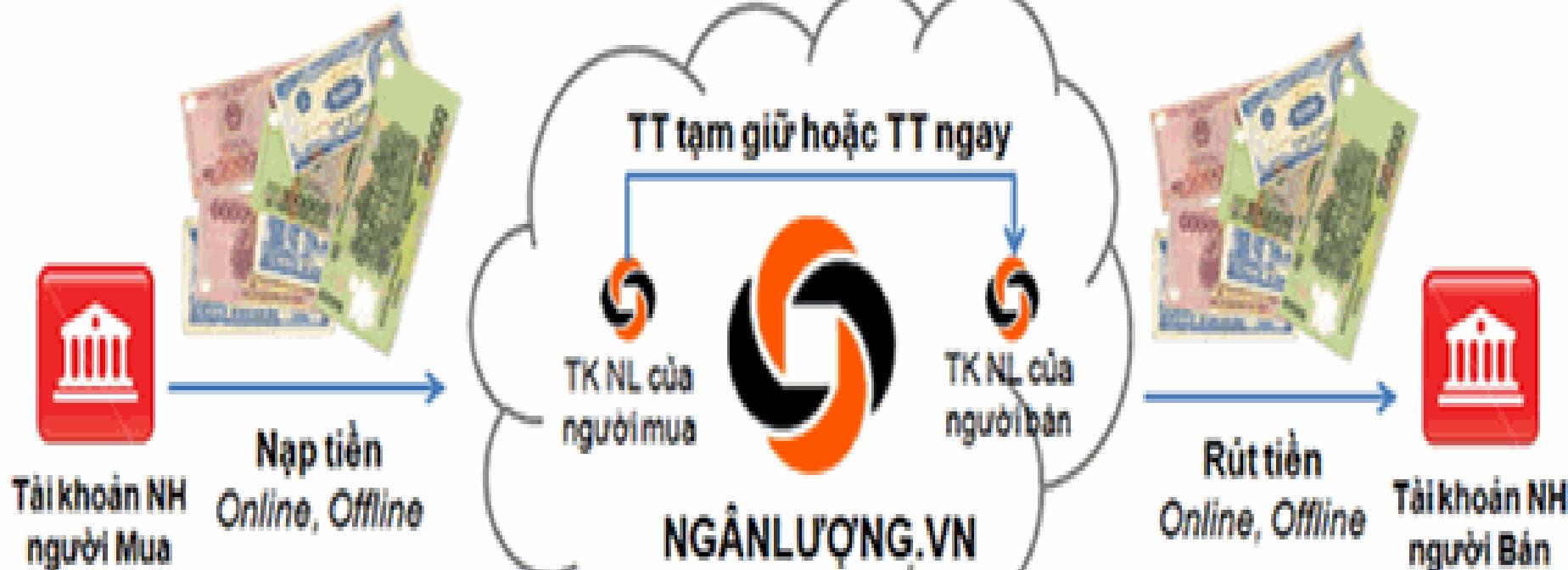
Hiện nay, Ngân lượng có trăm ngàn tài khoản và hơn 2000 website sử dụng dịch vụ của nó.



NgânLượng.vn

Thanh toán trực tuyến - Bảo vệ người mua

Môi trường Internet



IV/ CÁC DỊCH VỤ THANH TOÁN PHÔ BIỂN Ở VIỆT NAM

1. Các cổng thanh toán trực tuyến ở Việt Nam

c/ Cổng thanh toán VNmart.vn

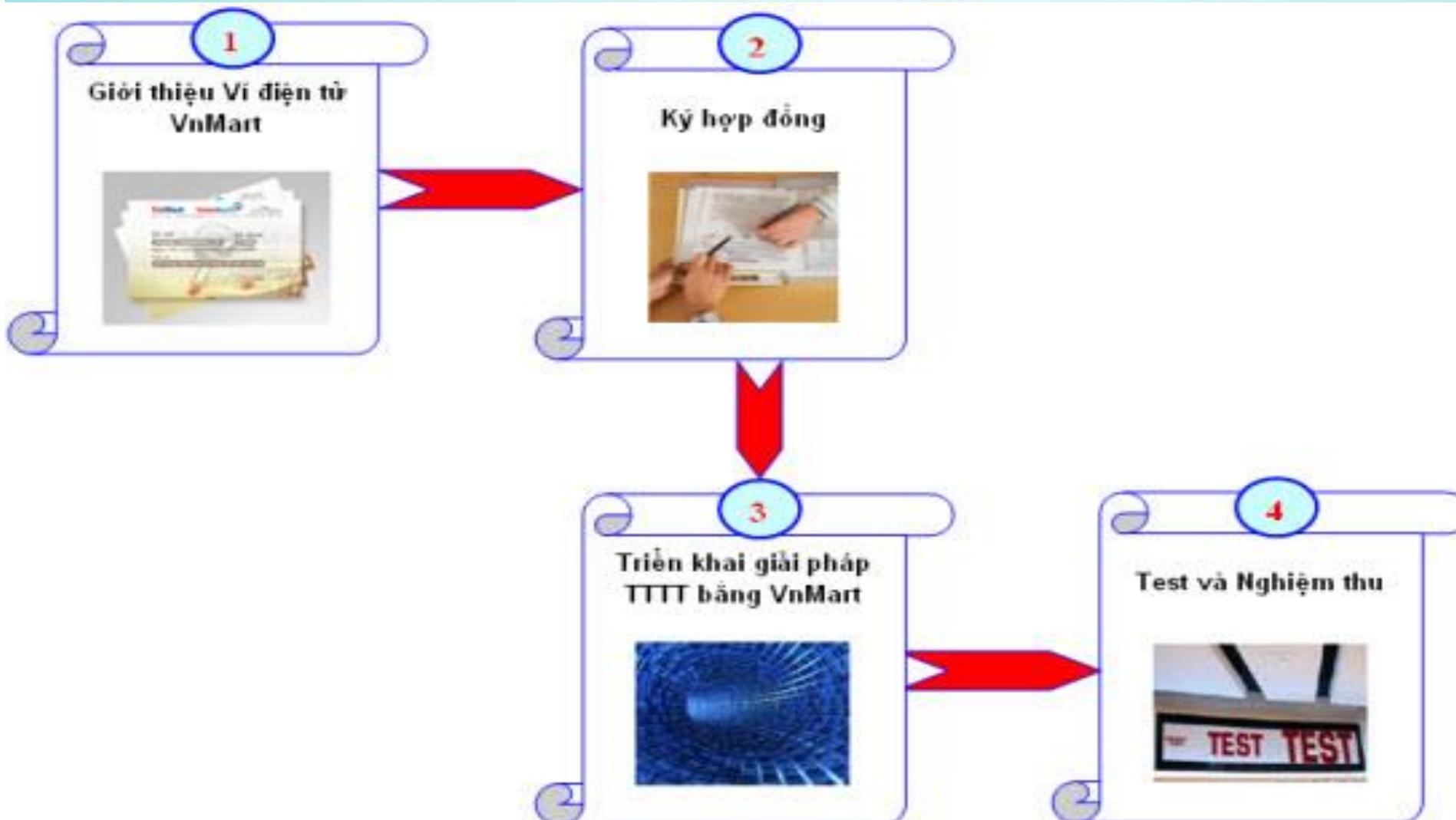
Là sản phẩm của Ngân hàng Công thương Việt Nam (VietinBank) và Công ty cổ phần giải pháp thanh toán Việt Nam (Vnpay) kết hợp, ra đời từ năm 2008

Có 2 loại ví điện tử VnMart:

- Ví điện tử cá nhân
- Ví điện tử doanh nghiệp

VnMart Cổng thanh toán trực tuyến

Giải pháp thanh toán hiện đại cho cuộc sống đơn giản hơn



CÁC DỊCH VỤ THANH TOÁN PHÔ BIỂN Ở VIỆT NAM

1. Các cổng thanh toán trực tuyến ở Việt Nam

d/ Cổng thanh toán OnePay

- Là sản phẩm dành cho các đơn vị kinh doanh thương mại điện tử chuyên nghiệp, cho phép doanh nghiệp thực hiện thanh toán trực tuyến trên website, qua email hoặc Tel/Fax.
- Có hơn 60 website đã ứng dụng thành công giải pháp thanh toán trực tuyến với khách hàng thông qua công thanh toán của OnePay, tiêu biểu như Jestar Pacific Airlines, Saigon Tourist, Vietravle...

CÁC DỊCH VỤ THANH TOÁN PHỐ BIÊN Ở VIỆT NAM

1. Các cổng thanh toán trực tuyến ở Việt Nam

e/ Cổng thanh toán Payoo.vn

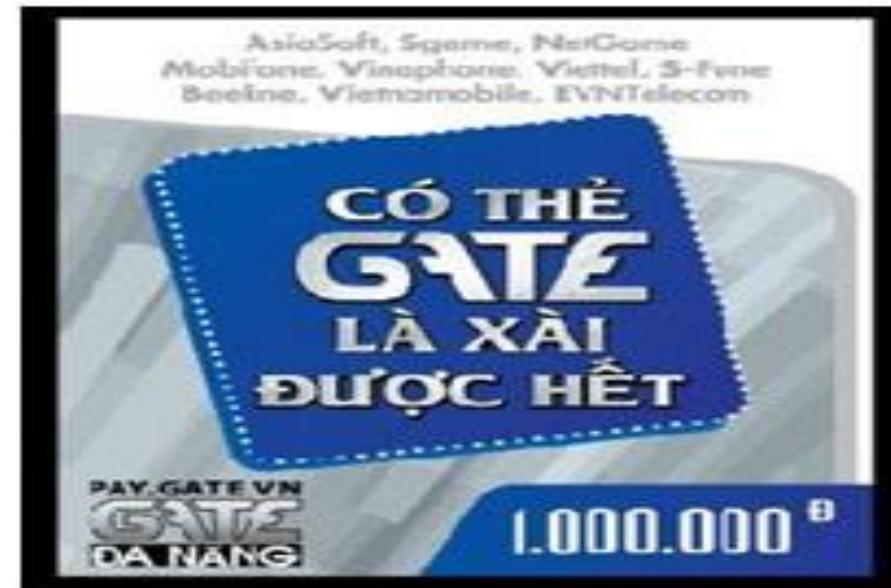
- Sản phẩm Công nghệ thông tin đã được ngân hàng nhà nước cấp phép hoạt động trung gian thanh toán điện tử
- Ví điện tử Payoo hiện đang dẫn đầu thị phần dịch vụ thanh toán trung gian tại Việt Nam.



CÁC DỊCH VỤ THANH TOÁN PHỐ BIÊN Ở VIỆT NAM

2.Thẻ nạp tiền đa năng

- Các loại thẻ nạp tiền vào TK game đã có thêm tính năng nạp tiền cho ĐTDĐ, trả cước phí học trực tuyến, mua hàng qua mạng, sử dụng cho nhiều loại dịch vụ trực tuyến khác nhau...Vd: Vcoin của VTC, Zing xu của VNG hoặc nạp thẻ Bạc của FPT Online...
- Bạn có thể chọn mua thẻ cào thông thường để lấy mã số nạp tiền hoặc mua mã số qua đại lý, máy bán mã số tự động...Hay nạp tiền bằng cách sử dụng Internet Banking, SMSBanking, Mobile Banking...



CÁC ĐIỀU KIỆN THAM GIA THANH TOÁN TRỰC TUYẾN QUỐC TẾ, VIỆT NAM

- Cần 1 TK chấp nhận thanh toán thẻ tại một ngân hàng (Merchant Account) và 1 Payment Gateway nếu muốn bán hàng trên mạng.
- Thẻ tín dụng được coi là hợp lệ khi có đủ 2 điều kiện sau:
- Thẻ được cung cấp bởi NH/tổ chức cung cấp dịch vụ xử lý thanh toán trên mạng (Issuer).
- Thẻ còn đủ khả năng chi trả cho hàng hóa hoặc dịch vụ định mua.

CÁC ĐIỀU KIỆN THAM GIA THANH TOÁN TRỰC TUYẾN QUỐC TẾ, VIỆT NAM

1. Đối với người sử dụng dịch vụ

- Phải đăng ký các loại thẻ thanh toán điện tử của các NH và sử dụng thẻ này để thanh toán với bên bán hàng, thuê bao dịch vụ.
- Các loại thẻ thanh toán quốc tế như Visa, Master,... có thể thực hiện giao dịch trong nước và ngoài nước, các loại thẻ khác chỉ có thể thanh toán phạm vi trong nước.

CÁC ĐIỀU KIỆN THAM GIA THANH TOÁN TRỰC TUYẾN QUỐC TẾ, VIỆT NAM

2. Đối với doanh nghiệp bán hàng

- Phải có phương tiện thực hiện thanh toán điện tử.
- Hiện nay, một số nhà cung cấp dịch vụ dùng các máy POS kiểm tra tính hợp lệ của các tài khoản của người thanh toán và thực hiện các giao dịch ngay tức thời khi người mua cần thanh toán qua thẻ mà họ sở hữu.

CÁC ĐIỀU KIỆN THAM GIA THANH TOÁN TRỰC TUYẾN QUỐC TẾ, VIỆT NAM

2. Đối với doanh nghiệp bán hàng

- Với các DN kinh doanh trên web thì web này sẽ có Module liên kết với NH sở hữu thẻ của bên bán.
- Khi khách hàng đưa ra thông tin yêu cầu thanh toán, thông tin này sẽ được chuyển đến các NH này hay NCC dịch vụ xử lý thanh toán qua mạng Online Payment để thực hiện việc kiểm tra xác thực tài khoản có hợp lệ và gởi lại cho bên bán. Nếu bên bán chấp nhận thì việc thanh toán sẽ được thực hiện.

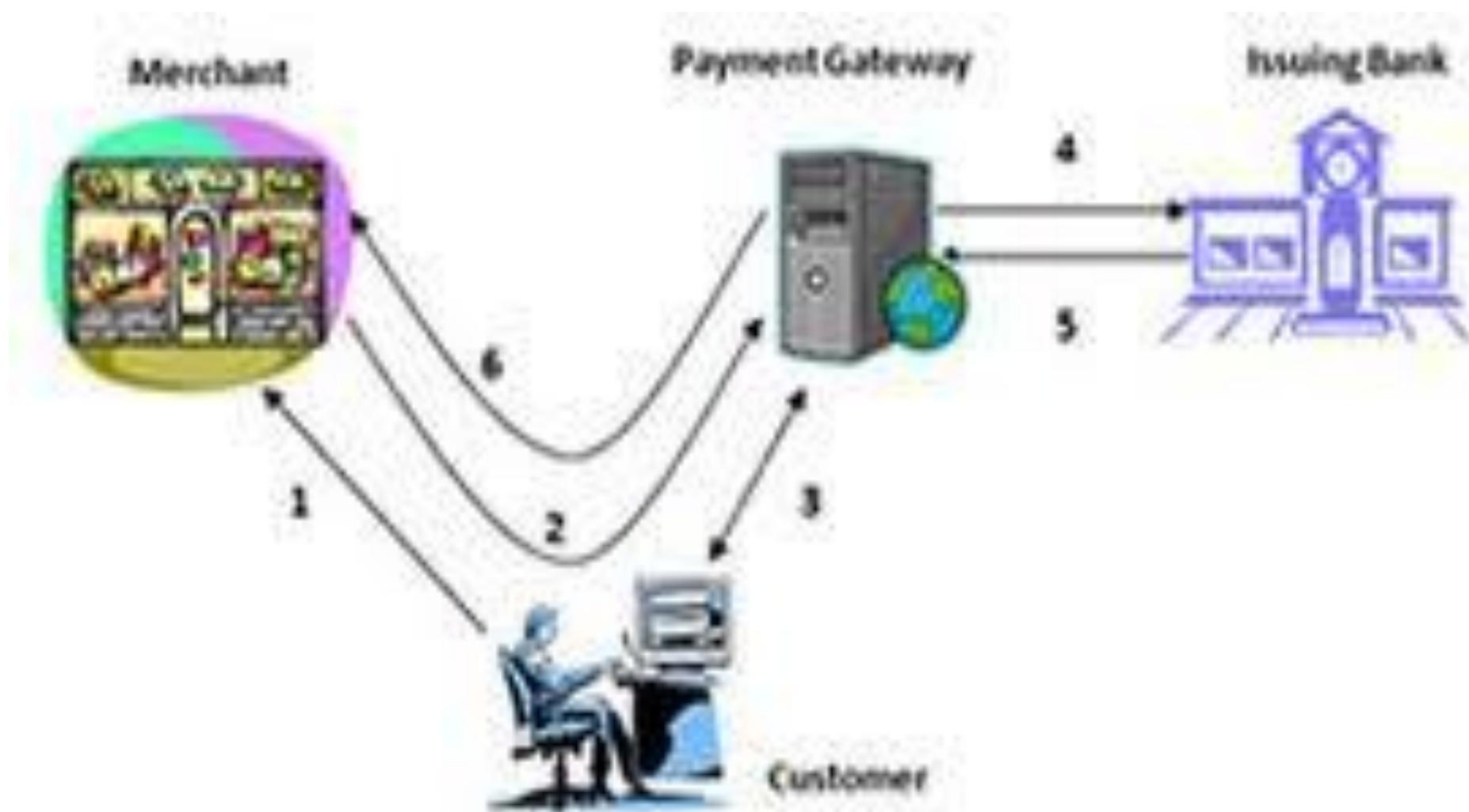
QUY TRÌNH THỰC HIỆN THANH TOÁN TRỰC TUYẾN

1.Thanh toán bằng thẻ tín dụng Credit card

- Người mua đặt lệnh mua hàng trên web, sau đó khai báo thông tin thẻ tín dụng.
- Thông tin→NH của người bán hoặc đến NCC dịch vụ xử lý thanh toán qua mạng payment gateway mà người bán đã chọn(sẽ gửi thông tin thẻ tới dịch vụ cung cấp thẻ và NH phát hành thẻ để kiểm tra tính hợp lệ ,khả năng thanh toán của thẻ)
- Thông tin được giải mã gửi về cho người bán.
- Người bán dựa thông tin phản hồi quyết định bán hay không bán.

QUY TRÌNH THỰC HIỆN THANH TOÁN TRỰC TUYẾN

1. Thanh toán bằng thẻ tín dụng Credit card



QUY TRÌNH THỰC HIỆN THANH TOÁN TRỰC TUYẾN

2. Thanh toán qua thẻ quốc tế

- Khách hàng đặt mua sản phẩm hay dịch vụ
 - khách hàng cung cấp các thông tin thẻ
 - hệ thống sẽ kiểm tra thẻ có hợp lệ, còn đủ chi trả cho món hàng, dịch vụ định mua hay không.
- Nếu các thông số đều thỏa mãn → tổ chức tín dụng cung cấp thẻ sẽ gửi mã số xác nhận chi trả cho DN, kèm theo các thông số về đơn hàng. Đồng thời, số tiền khách hàng thanh toán sẽ được chuyển ngay vào TK TMĐT của DN.

QUY TRÌNH THỰC HIỆN THANH TOÁN TRỰC TUYẾN

2. Thanh toán qua thẻ quốc tế



QUY TRÌNH THỰC HIỆN THANH TOÁN TRỰC TUYẾN

3. Thanh toán qua VDC-OPG

- Đây là hệ thống thanh toán phối hợp giữa VDC và NH Cổ Phần Thương Mại Á Châu ACB.
- Để tham gia VDC-OPG, tổ chức-cá nhân cần: có website cung cấp hàng hóa,dịch vụ trên Internet;được ACB chấp nhận là đại lý thanh toán thẻ trực tuyến; được VDC cho quyền sử dụng dịch vụ; cài đặt chứng thực điện tử VDC và ACB cấp.

LỢI ÍCH VÀ HẠN CHẾ THỰC HIỆN THANH TOÁN TRỰC TUYẾN VIỆT NAM

1. Lợi ích

- ❖ Tiết kiệm chi phí ,thời gian
- ❖ Tạo thuận lợi cho các bên giao dịch.
- ❖ Chi phí vận hành rất thấp
- ❖ Không bị giới hạn bởi không gian địa lý
- ❖ Giảm thiểu rủi ro mất tiền, tiền giả, nhầm lẫn... sẽ giảm bớt được việc thiếu minh bạch so với giao dịch bằng tiền mặt.

LỢI ÍCH VÀ HẠN CHẾ THỰC HIỆN THANH TOÁN TRỰC TUYẾN VIỆT NAM

2. Hạn chế

- ❖ Thủ tục chưa thật hợp lí
- ❖ Gian lận tín dụng
- ❖ Vấn đề bảo mật thông tin

NHẬN XÉT VÀ ĐÁNH GIÁ VỀ LOẠI HÌNH THANH TOÁN TRỰC TUYẾN

- Sự phát triển mạnh mẽ của số thuê bao điện thoại và người sử dụng internet góp phần làm cho thị trường thanh toán trực tuyến Việt Nam thêm sôi động.
- Việc triển khai các hoạt động thanh toán trực tuyến nhằm tiết giảm tối đa thời gian, nhân lực là một biện pháp đang được nhiều doanh nghiệp tìm đến để tiết giảm tối đa chi phí trong bối cảnh khủng hoảng hiện nay.

NHẬN XÉT VÀ ĐÁNH GIÁ VỀ LOẠI HÌNH THANH TOÁN TRỰC TUYẾN

Tuy nhiên loại hình thanh toán trực tuyến tại Nước ta hiện nay còn nhiều bất cập, cần giải quyết một số vấn đề sau:

- Thị trường thương mại điện tử Việt Nam thiếu đồng bộ
 - Thị trường thương mại điện tử Việt Nam thiếu cơ sở để tin
- Để khắc phục tình trạng này thì Chính phủ cần hoàn thiện hệ thống văn bản pháp lý về Thương Mại Điện Tử

LỢI ÍCH VÀ RỦI RO

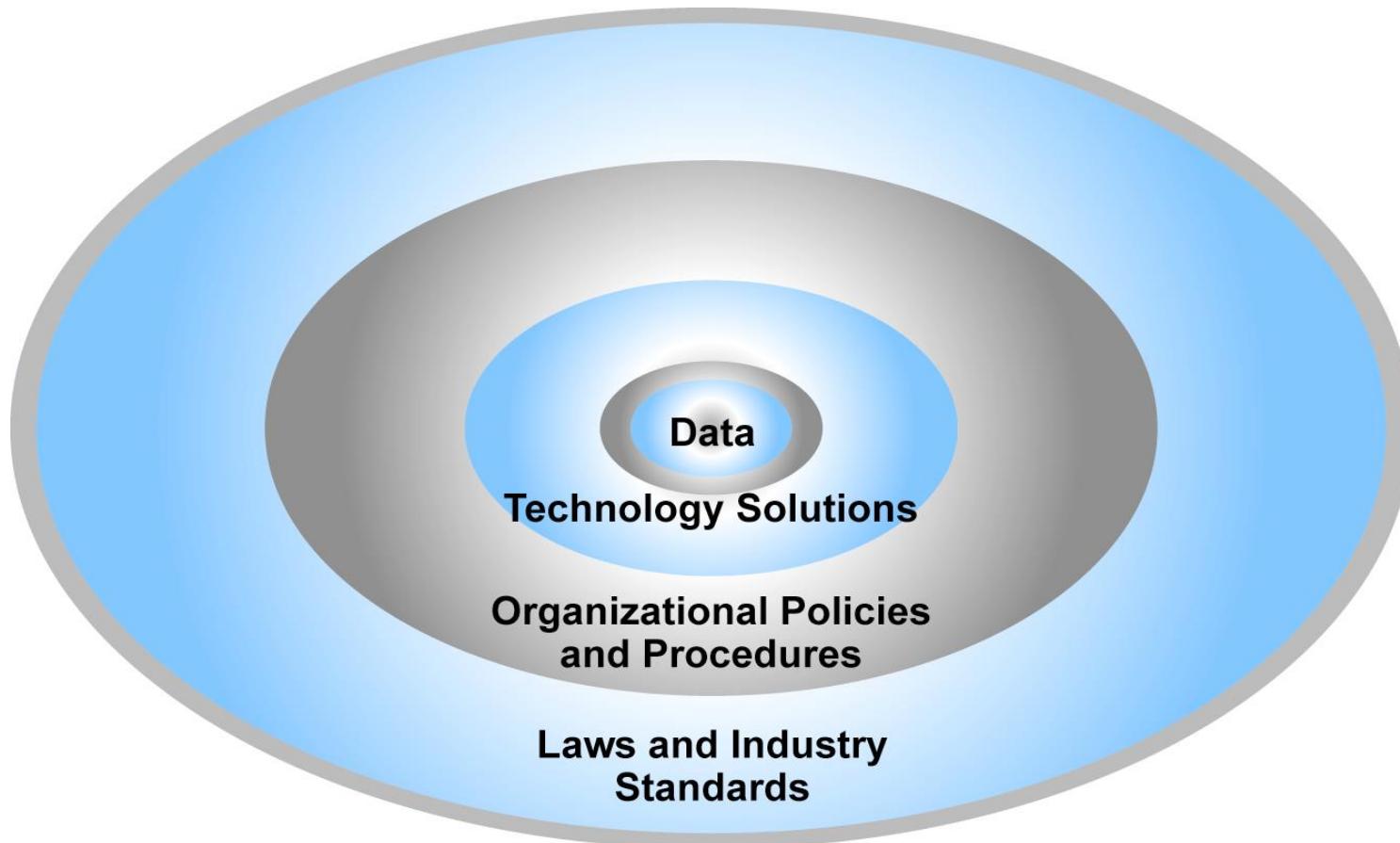
- Lợi ích của thanh toán trực tuyến

- * Người mua trả tiền nhanh chóng và trực tiếp
- * Người bán nhận tiền một cách nhanh nhất
- * Bất kỳ lúc nào 24/24
- * Hạn chế rủi ro và bất tiện khi thanh toán tiền mặt
- * Chi phí giao dịch giảm đáng kể

LỢI ÍCH VÀ RỦI RO

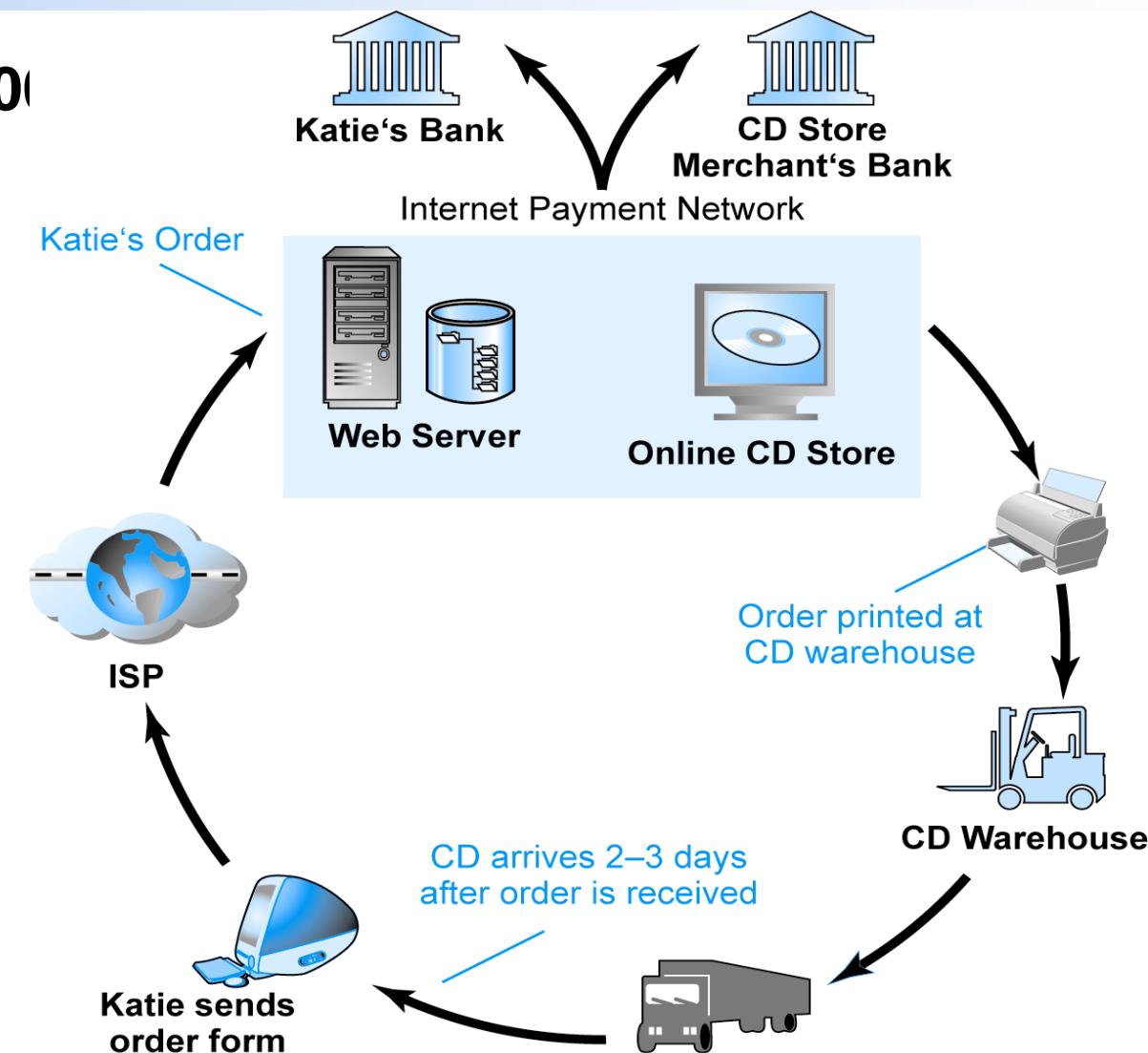
- ❖ **Rủi ro và khó khăn khi thanh toán trực tuyến**
 - * Sử dụng thẻ giả mạo
 - * Website giả mạo
 - * Tội phạm mạng Internet dòm ngó “ ví điện tử”
 - * Trở ngại về nhận thức của người dân & doanh nghiệp
 - * 3,2% website VN cho phép thanh toán trực tuyến.
 - * Khó khăn về quyết toán thuế

The E-commerce Security Environment



A Typical E-commerce Transaction

- SOURCE: Boncella, 2000



Vulnerable Points in an E-commerce Environment

Security Risks

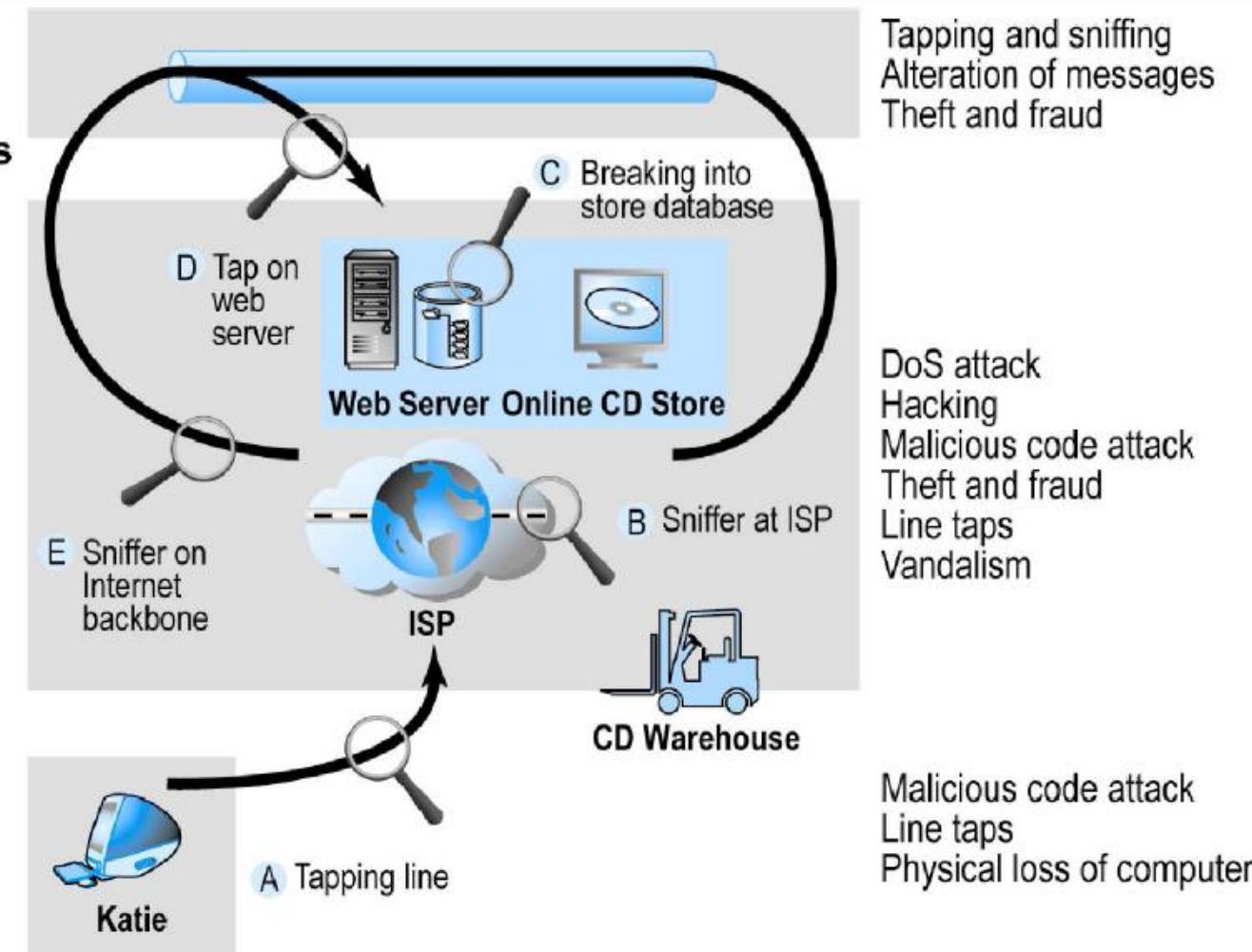
Internet communications

Servers

ISP
Merchant
Banks

Clients

Business
Home



Most Common Security Threats in the E-commerce Environment

- Malicious code
 - Viruses
 - Worms
 - Trojan horses
 - Bots, botnets
- Unwanted programs
 - Browser parasites
 - Adware
 - Spyware

Most Common Security Threats (cont.)

- Phishing

- Deceptive online attempt to obtain confidential information
- Social engineering, e-mail scams, spoofing legitimate Web sites
- Use of information to commit fraudulent acts (access checking accounts), steal identity

- Hacking and cybervandalism

- Hackers vs. crackers
- Cybervandalism: Intentionally disrupting, defacing, destroying Web site
- Types of hackers: White hats, black hats, grey hats

Most Common Security Threats (cont.)

- Credit card fraud/theft
 - Hackers target merchant servers; use data to establish credit under false identity
- Spoofing
- Pharming
- Spam/junk Web sites
- Denial of service (DoS) attack
 - Hackers flood site with useless traffic to overwhelm network
 - Distributed denial of service (DDoS) attack

Most Common Security Threats (cont.)

- Sniffing
 - Eavesdropping program that monitors information traveling over a network
- Insider jobs
 - Single largest financial threat
- Poorly designed server and client software
- Mobile platform threats
 - Same risks as any Internet device
 - Malware, botnets, vishing/smishing