Mật mã và An ninh mạng

Chương 6: An toàn Intermet

Chương 6: An toàn Intermet

6.1 Các kiểu tấn công trên Internet

6.2 Bảo mật thư điện tử

6.3 Bảo mật IP

6.4 Bảo mật WEB

6.5 Bảo mật mạng không dây

6.1 Các kiểu tấn công trên Internet

1. **TCP/IP Actacks**
2. **Virus**
3. **Mã độc**

1. TCP/IP Actacks

a) Tấn công TCP SYN Flood

b) Giả mạo địa chỉ IP (IP Spoofing)

a) Tấn công TCP SYN Flood

- Tấn công trực tiếp vào máy chủ bằng cách tạo ra một số lượng lớn các kết nối TCP nhưng không hoàn thành các kết nối này.
- Hacker sử dụng cơ chế bắt tay ba bước trong quá trình thiết lập kết nối giữa hai thực thể TCP.
- Máy hacker sử dụng một địa chỉ giả mạo và gửi hàng loạt bản tin yêu cầu kết nối tới máy tính nạn nhân với bit SYN được bật (bước 1)
- Nạn nhân nhận được gói tin này ngay lập tức nó sẽ dành một phần bộ nhớ cho kết nối này, máy tính nạn nhân nhận được yêu cầu trên thì trả lời lại với bản tin bit ACK, SEQ được bật (bước 2) và chờ để hacker trả lời
- Nhưng hacker không trả lời điều này sẽ làm cho máy tính nạn nhân luôn ở trong tình trạng chờ và dần dần sẽ cạn kiệt tài nguyên không thể phục vụ được nữa.

b) Giả mạo địa chỉ IP (IP Spoofing)

Địa chỉ IP giả mạo liên quan đến việc tạo ra các gói TCP/IP sử dụng địa chỉ IP giả với mục đích để che giấu danh tính hoặc giả mạo danh tính chủ sở hữu của địa chỉ IP được sử dụng.

- Tấn công từ chối dịch vụ (Denial of Service, DoS)
- Tấn công từ chối dịch vụ phản xạ nhiều vùng (Distributed Reflection DOS-DRDoS)
- Tấn công môi trường xác thực bằng địa chỉ IP
- Kiểu tấn công người đứng giữa (Man in The Middle Attack)

b) Giả mạo địa chỉ IP (IP Spoofing)

Tấn công từ chối dịch vụ (Denial of Service Attack, DoS):

- Hacker có thể gửi một số lượng lớn các gói tin yêu cầu kết nối (SYN) tới máy nạn nhân mà không cần quan tâm phản hồi (ACK) vì Hacker sẽ không nhận được bất kỳ gói tin phản hồi từ các nạn nhân
- Tất cả gói phản hồi sẽ được hướng tới các địa chỉ IP giả mạo.
- Danh tính của kẻ tấn công cũng sẽ không được tiết lộ.
- Cuộc tấn công này làm cho nạn nhân bị loại khỏi dịch vụ

b) Giả mạo địa chỉ IP (IP Spoofing)

DRDoS:

- Mục tiêu chính của DRDoS là chiếm đoạt toàn bộ băng thông của máy nạn nhân, làm tắc nghẽn hoàn toàn đường kết nối từ máy nạn nhân vào xương sống của Internet và làm tiêu hao tài nguyên.
- Trong suốt quá trình máy nạn nhân bị tấn công bằng DRDoS, không một máy khách nào có thể kết nối được vào máy nạn nhân đó
- Tất cả các dịch vụ chạy trên nền TCP/IP như: DNS, HTTP, FTP, POP3, ... đều bị vô hiệu hóa.

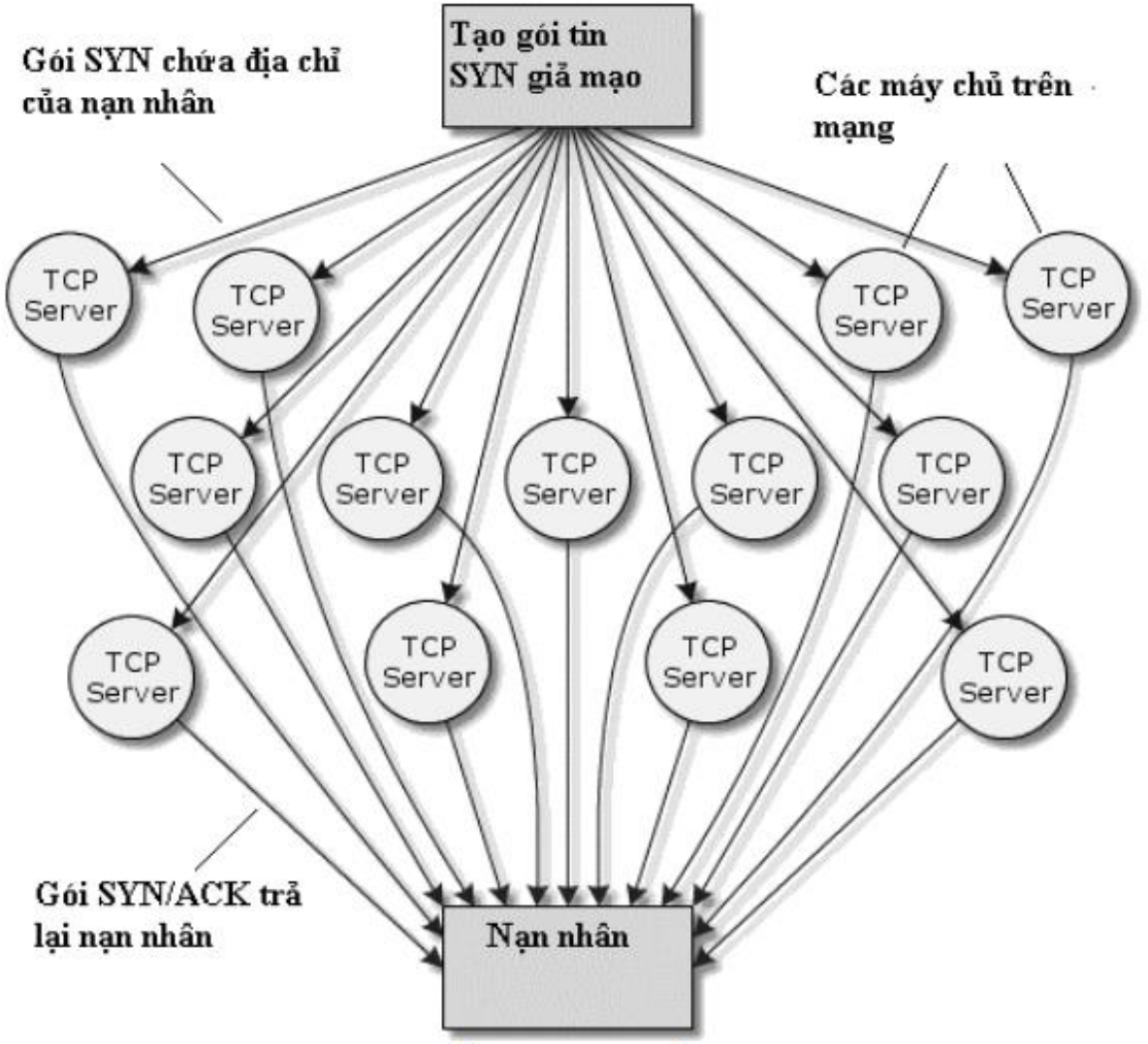
b) Giả mạo địa chỉ IP (IP Spoofing)

DRDoS:

- Hacker sử dụng các server phản xạ, hacker sẽ gửi yêu cầu kết nối (SYN) tới các server có bandwidth rất cao trên mạng – server phản xạ, các gói tin yêu cầu kết nối này mang địa chỉ IP giả - chính là địa chỉ IP của máy nạn nhân.
- Các server phản xạ này gửi lại máy nạn nhân các gói SYN/ACK dẫn tới hiện tượng nhân băng thông.

b) Giả mạo địa chỉ IP (IP Spoofing)

DRDoS:



b) Giả mạo địa chỉ IP (IP Spoofing)

Tấn công môi trường xác thực bằng địa chỉ IP:

- Trong trường hợp mạng nội bộ, xác thực bằng địa chỉ IP, không cần một tên đăng nhập hoặc mật khẩu để truy cập.
- Hacker có thể giả địa chỉ IP để có được quyền truy cập trái phép vào máy tính nạn nhân mà không xác thực.

b) Giả mạo địa chỉ IP (IP Spoofing)

Kiểu tấn công ngươi đứng giữa (Man in The Middle Attack):

- Can thiệp vào một phiên liên lạc được xác thực giữa hai máy tính A và B.
- Hacker sau khi hoàn thành các bước xác thực sẽ giả mạo địa chỉ IP của một nạn nhân A hoặc B đã được xác thực và nhận được các gói tin qua lại giữa hai máy A và B.

Các biện pháp chống lại tấn công IP Spoofing

- Dùng mật mã xác thực: Mã hoá traffic giữa các thiết bị (giữa 2 router, hoặc giữa 2 hệ thống đầu cuối và router) bằng một IPSec tunnel.
- Dùng danh sách kiểm tra truy cập Access Control List (ACL) trên các interface của router.
- Bộ lọc các gói dữ liệu: Ngăn chặn các gói tin gửi đến, chúng không đáp ứng các tiêu chí chính sách bảo mật.
- Sử dụng lớp trên: Kết hợp cơ chế phòng vệ ở tầng trên có thể ngăn chặn IP giả mạo như sử dụng số thứ tự trong trương số thứ tự của gói tin TCP ở tầng giao vận như vậy kẻ tấn công phải đoán được số thứ tự cũng trước khi giả mạo gói tin.

2. Virus

a) Malware là gì?

Malware (hay phần mềm độc hại) là thuật ngữ mô tả các chương trình hoặc mã độc có khả năng cản trở hoạt động bình thương của hệ thống bằng cách xâm nhập, kiểm soát, làm hỏng hoặc vô hiệu hóa hệ thống mạng, máy tính, máy tính bảng và thiết bị di động,…

2. Virus

b) Dấu hiệu nhận biết Malware.

- Máy tính chạy chậm
- Bạn bị làm phiền bởi quảng cáo pop-up
- Hệ thống liên tục gặp sự cố, bị đóng băng
- Dung lượng ổ cứng giảm bất thường
- Tài nguyên hệ thống tiêu hao bất thường

2. Virus

b) Dấu hiệu nhận biết Malware.

- Trang chủ của trình duyệt mặc định thay đổi mà không có sự cho phép của bạn.
- Các thanh công cụ, tiện ích mở rộng hoặc plugin mới được thêm vào trình duyệt
- Các chương trình anti-virus ngừng hoạt động và không cập nhật được
- Bạn nhận được thông báo đòi tiền chuộc từ Malware
- Tuy nhiên, trong vài trường hợp không có dấu hiệu cụ thể nào

2. Virus

c) Nguyên nhân bị Malware

- Truy cập các trang web độc hại, tải trò chơi, file nhạc nhiễm Malware, cài đặt thanh công cụ/phần mềm từ nhà cung cấp lạ, mở tệp đính kèm email độc hại (malspam) hoặc các dữ liệu tải xuống không được quét bởi phần mềm bảo mật
- Tải nhầm các ứng dụng độc hại ngụy trang dưới dạng các ứng dụng hợp pháp
- Tải ứng dụng ở các nguồn không đáng tin cậy
- Vô tình cài đặt các phần mềm bổ sung đi kèm với ứng dụng (potentially unwanted program) chứa Malware

2. Virus

d) Các loại Malware phổ biến

- Virus: Loại chương trình này vô cùng nguy hiểm vì có khả năng sinh sôi, lây lan ra khắp hệ thống phần mềm, gây thiệt hại phần cứng,… với tốc độ rất nhanh. Nếu không khắc phục kịp thời, mọi thông tin, dữ liệu, thậm chí là thiết bị đều sẽ mất kiểm soát
- Worm: Là con sâu và chương trình này còn độc hại hơn cả virus. Bởi Worm có thể tự sinh sôi, hoạt động mà không chịu bất kỳ sự tác động, điều khiển nào đến từ con người cả. Thậm chỉ khi đã bị "tiêu diệt" rồi thì vẫn có khả năng tự tái tạo, hoạt động lại như bình thường

2. Virus

d) Các loại Malware phổ biến

- Trojan: Phần mềm được xây dựng như một chương trình chính chủ, hợp pháp và uy tín. Được quảng cáo và sở hữu chức năng bảo vệ, giúp máy tính tránh khỏi sự xâm nhập, tấn công của Virus. Thực chất Trojan giống như một cánh cổng mở ra và cho phép hàng triệu loại Virus khác nhau tiến công, gây hại cho máy tính
- Spyware: hoàn toàn không có chức năng hủy hoại dữ liệu nhưng lại là chuyên gia theo dõi, sao chép và quan sát hoạt động của người dùng. Bất kỳ dữ liệu nào được nhập, xuất ra khỏi thiết bị đều được Spyware ghi nhận, cung cấp lại cho những kẻ gian mà không ai hay biết

2. Virus

d) Các loại Malware phổ biến

- Rootkit: Kể từ khi người dùng cài đặt phần mềm này vào thiết bị, Rootkit ngay lập tức tấn công và tước quyền quản trị. Khi này các tin tắc có thể tự do truy cập trái phép, vượt qua được bất cứ "bức tường bảo vệ" nào một cách dễ dàng. Đánh cấp dữ liệu, theo dõi hành vi người dùng một cách ung dung mà không có bất kỳ cảnh báo lỗi hệ thống nào diễn ra
- Ransomware: Ngăn bạn truy cập vào thiết bị và mã hóa dữ liệu, sau đó buộc bạn phải trả tiền chuộc để lấy lại chúng. Ransomware được xem là vũ khí của tội phạm mạng vì nó thường dùng các phương thức thanh toán nhanh chóng bằng tiền điện tử.

2. Virus

f) Cách phòng tránh Malware

- Cảnh giác với các web có domain kết thúc bằng tập hợp các chữ cái riêng lẻ, và có đuôi không giống như bình thường (.com, .vn, .org,...).
- Tránh nhấp vào các quảng cáo pop-up khi bạn lướt web
- Không nên mở các file lạ có đính kèm trên email
- Không nên tải các phần mềm từ các website không đáng tin cậy
- Thường xuyên cập nhật hệ điều hành, ứng dụng
- Không nên tải ứng dụng từ các nguồn bên thứ 3
- Không nên nhấp vào các liên kết lạ

3. Mã độc

a) Khái niệm

Phần mềm độc hại được tạo ra với động cơ xấu, gây hại cho người sử dụng.

Có 2 loại cơ bản:

- Loại tồn tại ký sinh trong chương trình chủ.
- Loại tồn tại độc lập

3. Mã độc

a) Khái niệm

Các phần mềm tồn tại ký sinh trong phần mềm chủ:

- Không phải là một chương trình hoàn chỉnh mà chỉ là một đoạn mã, không có khả năng tự hoạt động
- Thường được chèn vào một chương trình hoàn chỉnh nào đó (gọi là chương trình chủ).
- Ví dụ: virus máy tính, bom logic, backdoor, Trojan.

3. Mã độc

a) Khái niệm

Loại phần mềm độc hại tồn tại độc lập:

- Là các chương trình hoàn chỉnh, có khả năng tồn tại độc lập
- Có thể được lên lịch và chạy bởi hệ điều hành.
- Ví dụ: Sâu máy tính (worm) và bot (tay sai gây ra tấn công DoS)

3. Mã độc

b) Backdoor (trapdoor)

- Là một cổng bí mật để xâm nhập vào chương trình, giúp cho ngươi nào biết nó thì có thể nhanh chóng xâm nhập vào chương trình mà không cần phải thực hiện đầy đủ các thủ tục về an toàn thông tin thông thường.
- Có thể là độc hại nhưng cũng có thể là hữu ích, tùy vào mục đích của ngươi sử dụng nó.
- Sử dụng backdoor như một cách để sửa lỗi và kiểm thử các chương trình phần mềm (maintenance hook). Backdoor phải được loại bỏ khi chương trình đã được hoàn thiện
- Backdoor trở thành mối đe dọa khi những lập trình viên xấu sử dụng nó để xâm nhập vào chương trình một cách trái phép.

3. Mã độc

c) Bom logic

- Là một đoạn mã lệnh được chèn vào một chương trình chính thống và nó được kích hoạt khi một điều kiện nào đó thỏa mãn (ngày, tháng cụ thể, sự xuất hiện của một tập tin cụ thể hoặc việc chạy một chương trình cụ thể).
- Một khi được kích hoạt, bom logic sẽ thực hiện các hoạt động gây hại như thay đổi nội dung tệp tin, xóa toàn bộ các tệp tin, dừng toàn bộ hệ thống, …

3. Mã độc

d) Ngựa Trojan

- Là một chương trình hoặc một thủ tục câu lệnh bề ngoài có vẻ là hữu ích, vô hại nhưng bên trong lại chứa một đoạn mã thực hiện những chức năng gây hại.
- Thường là các chương trình thu hút được ngươi dùng như game, phần mềm tiện ích, …
- Các trình biên dịch đã bị thay đổi để chèn các đoạn mã lệnh vào chương trình được biên dịch nhằm tạo ra backdoor trong chức năng login

6.2 Bảo mật thư điện tử

Yêu cầu:

- Tính bảo mật nội dung tin gửi
- Xác thực người gửi mẩu tin
- Tính toàn vẹn của mẩu tin
- Tính chống từ chối gốc, chống từ chối của người gửi.

6.2 Bảo mật thư điện tử

1. Dịch vụ PGP
2. Mở rộng thư Internet đa mục đích/an toàn S/MIME

1. Dịch vụ PGP

- PGP (Pretty Good Privacy) là một dịch vụ về bảo mật và xác thực được sử dụng rộng rãi cho chuẩn an toàn thư điện tử.
- Được phát triển bởi Phil Zimmermann.
- Lựa chọn các thuật toán mã hoá tốt nhất để dùng, tích hợp thành một chương trình thống nhất, có thể chạy trên Unix, PC, Macintosh và các hệ thống khác
- Hoạt động: xác thực, bảo mật, nén, tương thích, quản lý khóa, …

Thao tác PGP – xác thực

- Người gửi tạo mẩu tin, sử dụng SHA-1 để sinh Hash 160 bit của mẩu tin, ký hash với RSA sử dụng khoá riêng của người gửi và đính kèm vào mẩu tin.
- Người nhận sử dụng RSA với khoá công khai của người gửi để giải mã và khôi phục bản hash, kiểm tra mẩu tin nhận sử dụng bản hash của nó và so sánh với bản hash đã được giải mã.

Thao tác PGP – bảo mật

- Người gửi tạo mẩu tin và số ngẫu nhiên 128 bit như khoá phiên cho nó, mã hoá mẩu tin sử dụng CAST-128/IDEA /3DES trong chế độ CBC với khoá phiên đó. Khoá phiên được mã sử dụng RSA với khoá công khai người nhận và đính kèm với mẩu tin.
- Người nhận sử dụng RSA với khoá riêng để giải mã và khôi phục khoá phiên. Khoá phiên được sử dụng để giải mã mẩu tin.

Thao tác PGP – bảo mật và xác thực

- Có thể sử dụng cả hai dịch vụ trên cùng một mẩu tin.
- Tạo chữ ký và đính vào mẩu tin, sau đó mã cả mẩu tin và chữ ký.
- Đính khoá phiên đã được mã hoá RSA/ElGamal

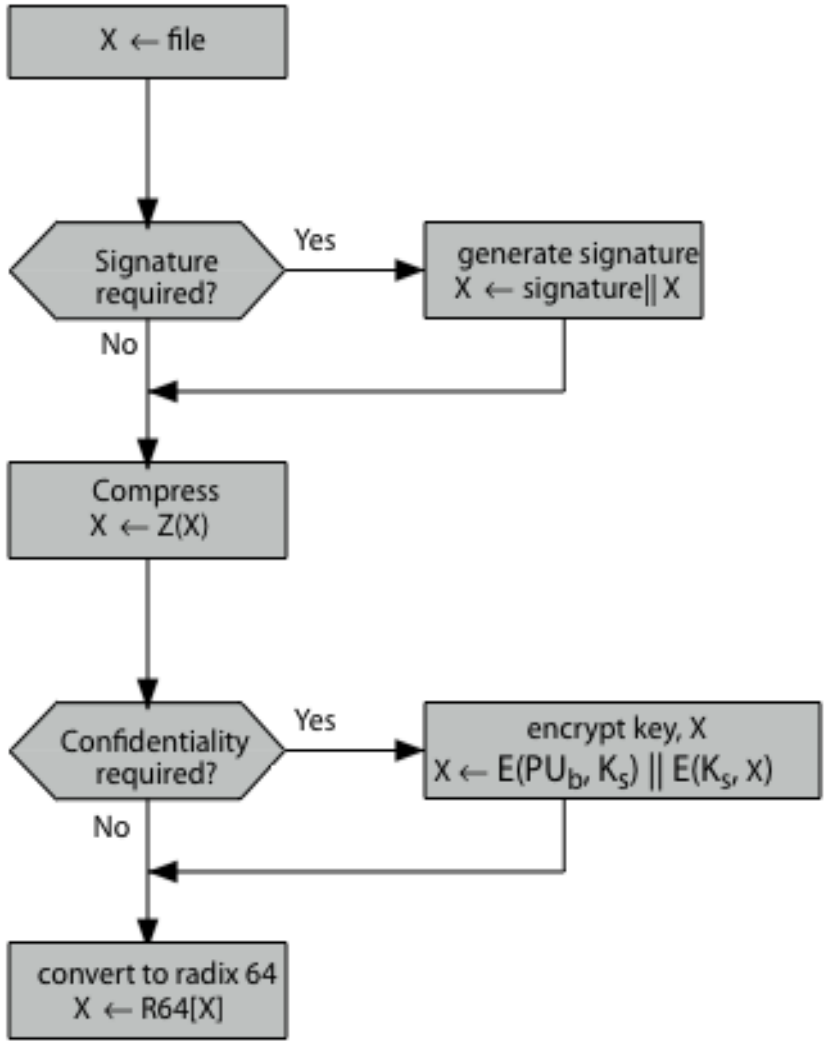
Thao tác PGP – nén

- Theo mặc định PGP nén mẩu tin sau khi ký nhưng trước khi mã.
- Cần lưu mẩu tin chưa nén và chữ ký để kiểm chứng về sau. Vì rằng nén là không duy nhất.
- Sử dụng thuật toán nén ZIP.

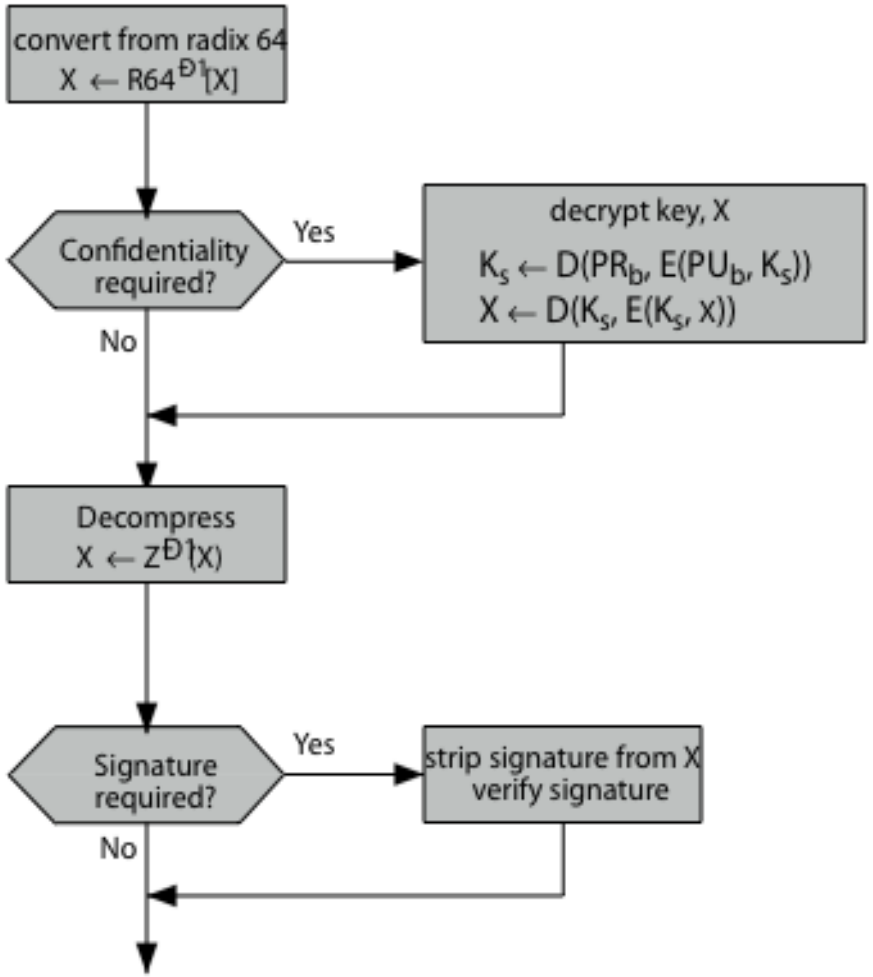
Thao tác PGP – tương thích thư điện tử

- Khi sử dụng PGP sẽ có dữ liệu nhị phân để gửi (mẩu tin được mã).
- Tuy nhiên thư điện tử có thể thiết kế chỉ cho văn bản. Vì vậy PGP cần mã dữ liệu nhị phân thô vào các ký tự ASCII in được. Sau đó sử dụng , ánh xạ 3 byte vào 4 ký tự in được và bổ sung kiểm tra thừa quay vòng CRC để phát hiện lỗi khi truyền. PGP sẽ chia đoạn mẩu tin nếu nó quá lớn.
- Cần có khoá phiên cho mỗi mẩu tin thuật toán Radix 64, có kích thước khác nhau: 56 bit – DES, 128 bit CAST hoặc IDEA, 168 bit Triple – DES, được sinh ra sử dụng dữ liệu đầu vào ngẫu nhiên lấy từ sử dụng trước và thời gian gõ bàn phím của người sử dụng

Thuật toán Radix 64



(a) Generic Transmission Diagram (from A)

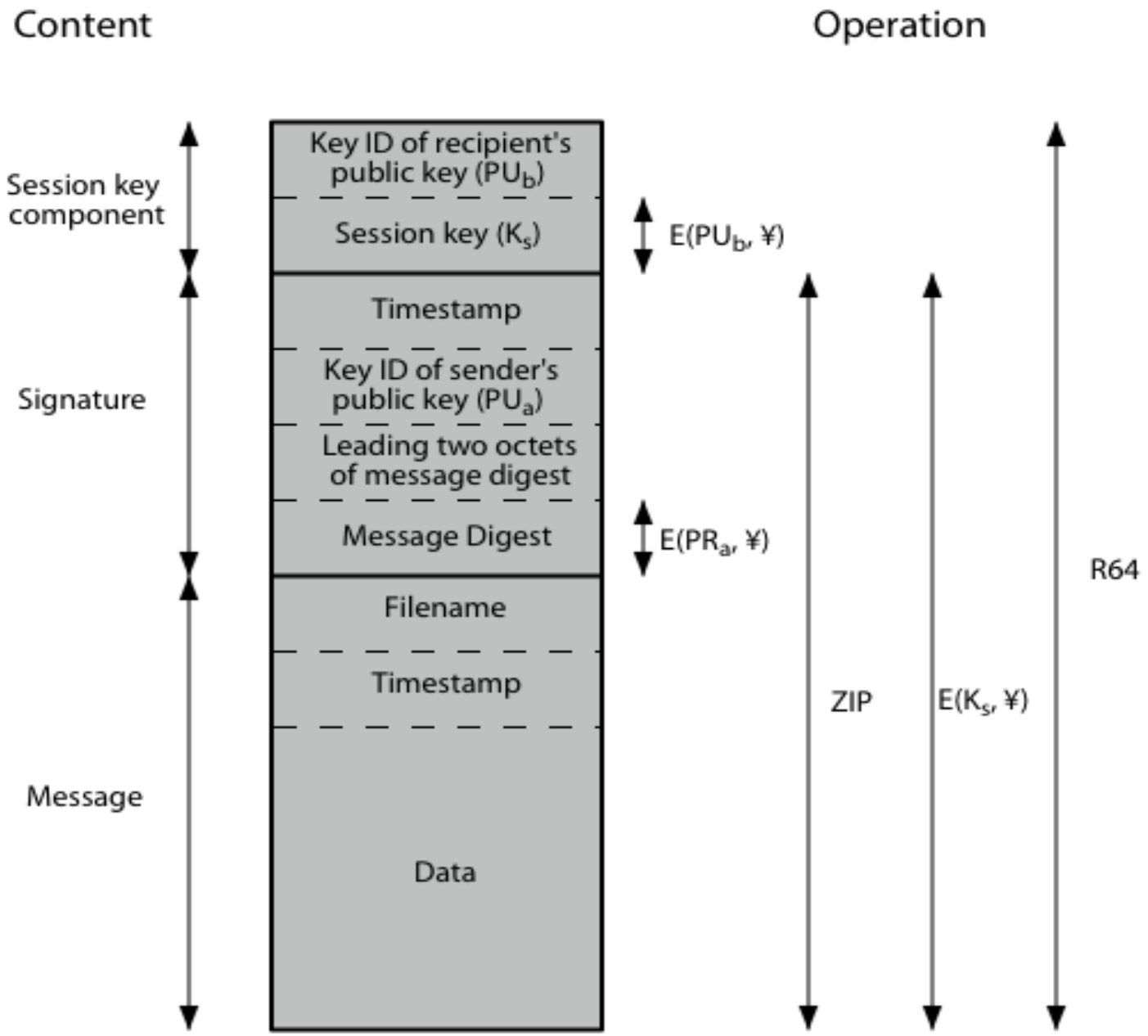


(b) Generic Reception Diagram (to B)

Khoá riêng và công khai của PGP

- Vì có nhiều khoá riêng và khoá công khai có thể được sử dụng, nên cần phải xác định rõ cái nào được dùng để mã khoá phiên trong mẩu tin.
- Có thể gửi khoá công khai đầy đủ với từng mẩu tin. Nhưng đều đó là không đủ, vì cần phải nêu rõ danh tính của người gửi. Do đó có thể sử dụng định danh khoá để xác định người gửi.
- Có ít nhất 64 bit có ý nghĩa của khoá và là duy nhất, có thể sử dụng định danh của khoá trong chữ ký.

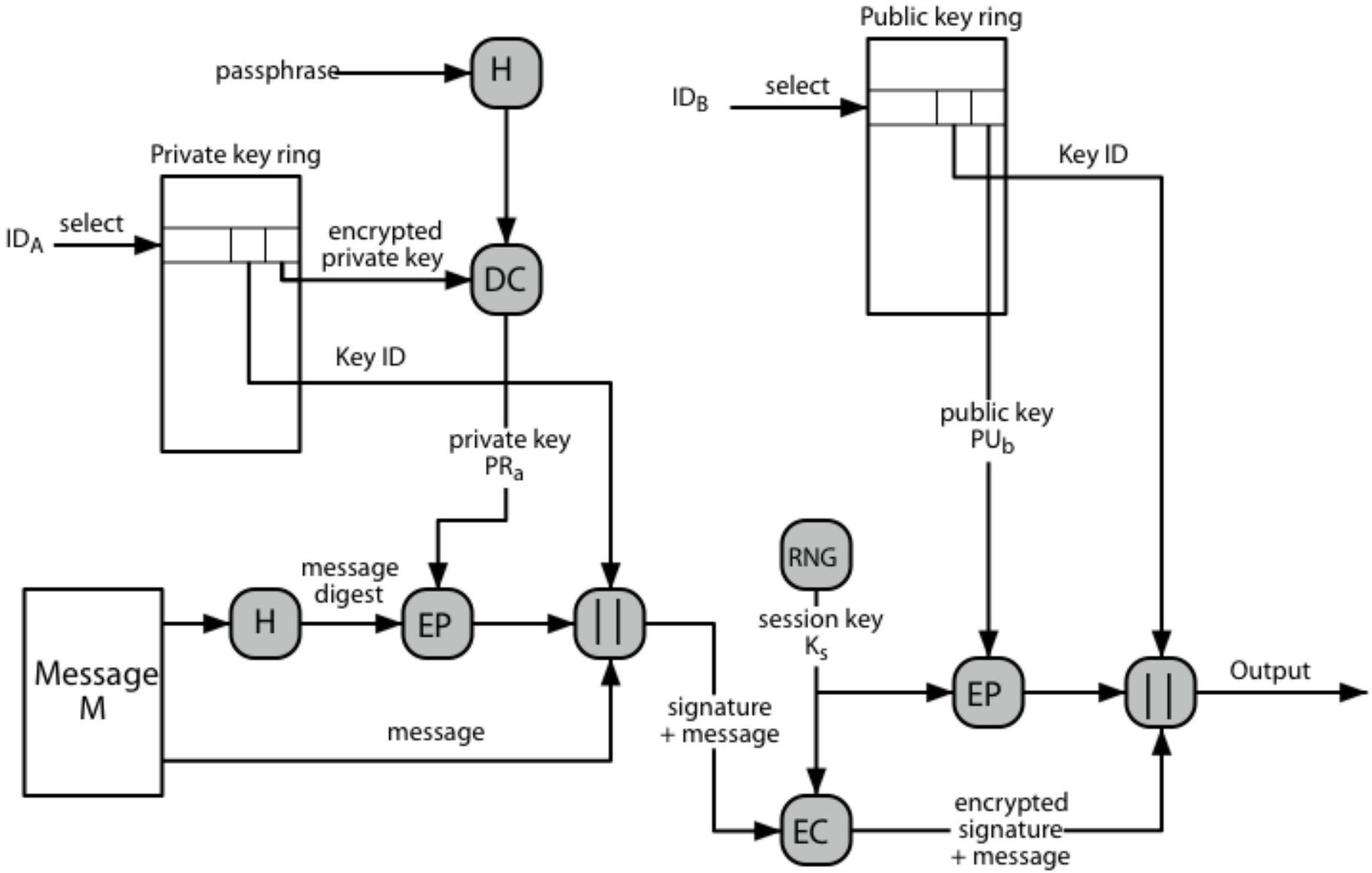
PGP Message Format



Các chùm khoá PGP

- Mỗi người sử dụng PGP có một cặp chùm khoá.
- Chùm khoá công khai chứa mọi khoá công khai của các người sử dụng PGP khác được người đó biết và được đánh số bằng định danh khoá (ID key).
- Chùm khoá riêng chứa các cặp khoá công khai/riêng của người đó được đánh số bởi định danh khoá và mã của khoá lấy từ giai đoạn duyệt hash. An toàn của khoá công khai như vậy phụ thuộc vào độ an toàn của giai đoạn duyệt.

Sinh mẩu tin PGP



Quản lý khoá PGP

- Tốt hơn hết dựa vào chủ quyền chứng nhận.
- Mỗi người sử dụng có một CA của mình.
- Có thể ký khoá cho người sử dụng mà anh ta biết trực tiếp. Cần tin cậy khóa đã được ký, và tin cậy các khoá mà các người khác ký khi dùng một dây chuyền các chữ ký đến nó.
- Chùm khoá chứa cả các chỉ dẫn tin cậy.
- Người sử dụng có thể thu hồi khoá của họ.

2. S/MIME

- Mở rộng thư Internet đa mục đích/an toàn S/MIME (Multipurpose Internet Mail Extension).
- Thư điện tử Internet RFC822 gốc chỉ có văn bản, MIME cung cấp hỗ trợ cho nhiều kiểu nội dung và mẩu tin có nhiều phần với mã hoá dữ liệu nhị phân thành dạng văn bản.
- S/MIME tăng cường tính an toàn cho thư điện tử, có trong nhiều tác nhân thư điện tử như MS Outlook, Mozilla, Mac Mail, …

Các chức năng S/MIME

- Nội dung thư được mã hoá và liên kết khoá
- Dữ liệu rõ ràng được ký, mẩu tin tương minh và mã hoá chữ ký trên bản nén
- Dữ liệu đóng phong bì và ký, lồng nhau các thực thể ký và mã

Các thuật toán mã hóa S/MIME

- Các chữ ký điện tử DSS và RSA,
- Các hàm hash: SHA-1 và MD5
- Mã khoá phiên: Elgamal & RSA
- Mã mẩu tin: AES, Triple-DES, RC2/40, …
- MAC: HMAC với SHA-1.
- Có quá trình để đối thoại quyết định sử dụng thuật toán nào

Các mẩu tin S/MIME

- S/MIME bảo vệ các thực thể MIME với chữ ký, mã hoặc cả hai tạo thành các đối tượng đóng gói MIME.
- Có phạm vi các kiểu nội dung khác nhau: dữ liệu đóng phong bì, dữ liệu được ký, dữ liệu rõ ràng được ký, yêu cầu đăng ký, chứng nhận mẩu tin

Quá trình chứng nhận S/MIME

- S/MIME sử dụng chứng nhận X.509 phiên bản 3.
- Quản trị việc sử dụng kết hợp sơ đồ phân cấp CA của X.509 và Web niềm tin của PGP.
- Mỗi client có một danh sách các giấy chứng nhận cho CA tin cậy và có các giấy chứng nhận và cặp khoá công khai/riêng của mình.
- Chứng nhận cần được ký bởi các CA tin cậy.

Chủ quyền chứng nhận CA

- Có một số CA mọi người đều biết. Verisign là một CA được sử dụng rộng rãi.
- Verisign xuất bản một số kiểu định danh điện tử.
- Tăng mức kiểm tra và kéo theo độ tin cậy.

6.3 Bảo mật IP: Giải pháp IPSec

IPSec (Internet Protocol Security) là một bộ giao thức phục vụ cho an ninh tầng IP thông qua cơ chế tác động lên các gói tin tầng IP để đảm bảo 3 mục tiêu:

1) Xác thực và toàn vẹn của thông tin
2) Bảo mật
3) Bảo vệ chống lại tấn công phát lại

6.3 Bảo mật IP: Giải pháp IPSec

- Cơ chế cài đặt ở tầng IP làm cho việc sử dụng họ giao thức này trong suốt đối với tầng ứng dụng.
- Đây là một giải pháp tổng quát chung cho cộng đồng sử dụng Internet, được xây dựng bởi nhóm làm việc chuyên trách (IETF IPSec Working Group).

6.3 Bảo mật IP: Giải pháp IPSec

IPSec là bộ ba giao thức chính sau, cung cấp những dịch vụ thành phần

- ✓ Giao thức trao chuyển khóa IKE (Internet key exchange): chịu trách nhiệm khởi tạo cái gọi là liên kết an toàn (security association - SA), tức là một nhóm các thông tin điều khiển và tham số để sử dụng cho các thuật toán an toàn bảo mật cho cho liên kết, trong đó có các khóa sử dụng cho thuật toán mật mã và xác thực.
- ✓ Giao thức xác thức AH (Authentication Header): chỉ cung cấp cơ chế xác thực và bảo vệ tính toàn vẹn của gói tin, không đảm bảo tính bảo mật
- ✓ Giao thức đóng gói an toàn ESP (Encapsulating Security Payload): có 2 mức, mức cơ bản chỉ cung cấp dịch vụ bảo mật và mức nâng cao cung cấp toàn bộ tính bảo mật, xác thực và nguyên vẹn (tức là bao gồm cả các chức năng của AH).

6.3 Bảo mật IP: Giải pháp IPSec

Cả hai giao thức AH và ESP này có thể hoạt động trong hai chế độ khác nhau:

- Chế độ giao vận (transport mode)
- Chế độ "đường hầm" (tunnel mode)

6.3 Bảo mật IP: Giải pháp IPSec

Chế độ giao vận (transport mode):

- Dữ liệu từ tầng trên (TCP/UDP) được "bao bọc" theo một nghĩa nào đó (để đảm bảo xác thực và/hoặc bí mật) nhưng khối điều khiển IP header thì vẫn để nguyên.
- Với ESP, toàn bộ dữ liệu truyền tải (IP payload) ngoại trừ IP header sẽ được mật mã và có thể được xác thực (tùy vào mức lựa chọn).
- Với AH, thì dữ liệu truyền tải và một phần được lựa chọn của IP header sẽ được xác thực

6.3 Bảo mật IP: Giải pháp IPSec

Chế độ "đường hầm" (tunnel mode):

- Toàn bộ dữ liệu, kể cả IP header, được bao bọc lại và một IP header mới được chèn thêm vào để chuyển tiếp trên mỗi chặng (giữa 2 router cùng hệ thống được cài IPSec).
- Với ESP, toàn bộ gói tin IP gốc (kể cả IP header) sẽ được mật mã và có thể được xác thực.
- Với AH, việc xác thực được thực hiện trên toàn bộ gói tin IP gốc và một phần được lựa chọn của IP header mới thêm vào để chuyển tiếp trên mỗi chặng.

6.3 Bảo mật IP: Giải pháp IPSec

IPSec có thể được sử dụng để bảo vệ các đương truyền dữ liệu giữa:

- Một cặp 2 máy (địa chỉ IP) tức là host-to-host,
- Giữa một cặp cổng an toàn (security gateways) tức là network-to-network,
- Giữa một cổng và một máy tức là network-to-host.

6.4 Bảo mật Web

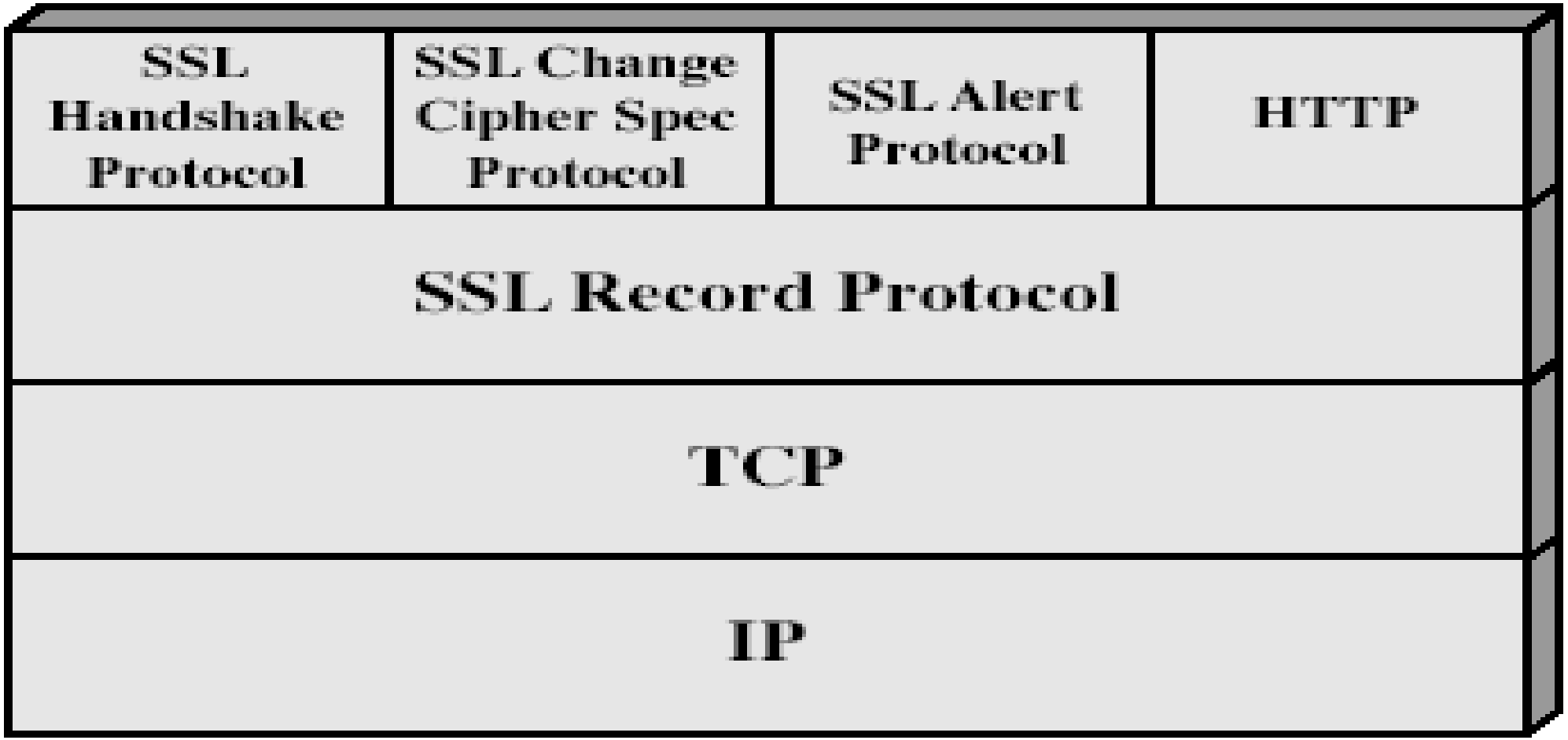
a) SSL (Secure Socket Layer)

b) Kiến trúc SSL

a) SSL (Secure Socket Layer)

- SSL là dịch vụ an toàn tầng vận chuyển.
- Một giải pháp bảo mật hàng đầu trên Internet.
- Ban đầu được phát triển bởi Netscape. Sau đó phiên bản 3 của nó được thiết kế cho đầu vào công cộng và trở thành chuẩn Internet, được biết đến như an toàn tầng vận chuyển TLS (Transport Layer Security).
- SSL sử dụng giao thức TCP để cung cấp dịch vụ đầu cuối đến cuối tin cậy và có 2 tầng thủ tục.

b) Kiến trúc SSL



b) Kiến trúc SSL

- Là một chồng xếp của các giao thức (protocol stack)
- SSL nằm ngay phía trên TCP.
- Các giao thức con của SSL được tổ chức thành 2 lớp con
- Tầng con dưới SSL Record Protocol xử lý mã hóa tất cả các thông điệp từ trên giao xuống.
- Tầng con trên là các giao thức con làm nhiệm vụ quản lý điều khiển (SSL handshake/ Change Cipher Spec/ Alert protocol) và các giao thức khai thác ứng dụng HTTPS

b) Kiến trúc SSL

2 khái niệm cơ bản:

- Phiên (Section):
  - ✓ Liên kết giữa người sử dụng và máy chủ
  - ✓ Được tạo bởi thủ tục HandShake Protocol
  - ✓ Xác định một tập các tham số mã hoá
  - ✓ Có thể chia sẻ bởi kết nối SSL lặp
- Kết nối (Connection)
  - ✓ Kênh truyền an toàn cụ thể kết nối giữa 2 tiến trình cụ thể trên 2 cổng cụ thể
  - ✓ Gắn chặt với 1 phiên SSL

Giao thức bản ghi SSL (SSL Record Protocol)

Xử lý thông tin mà tầng ứng dụng chuyển xuống, mật mã, đóng gói để chuyển xuống tầng IP

- Phân ra thành các gói phù hợp, nén dữ liệu, thêm mã xác thực (MAC)
- Mã hóa, chèn thêm thông tin điều khiển (SSL Record Header)

SSL Change Cipher Spec Protocol

- Đây là giao thức thay đổi đặc tả mã SSL
- Chỉ định các thuật toán mã đối xứng và hàm băm.

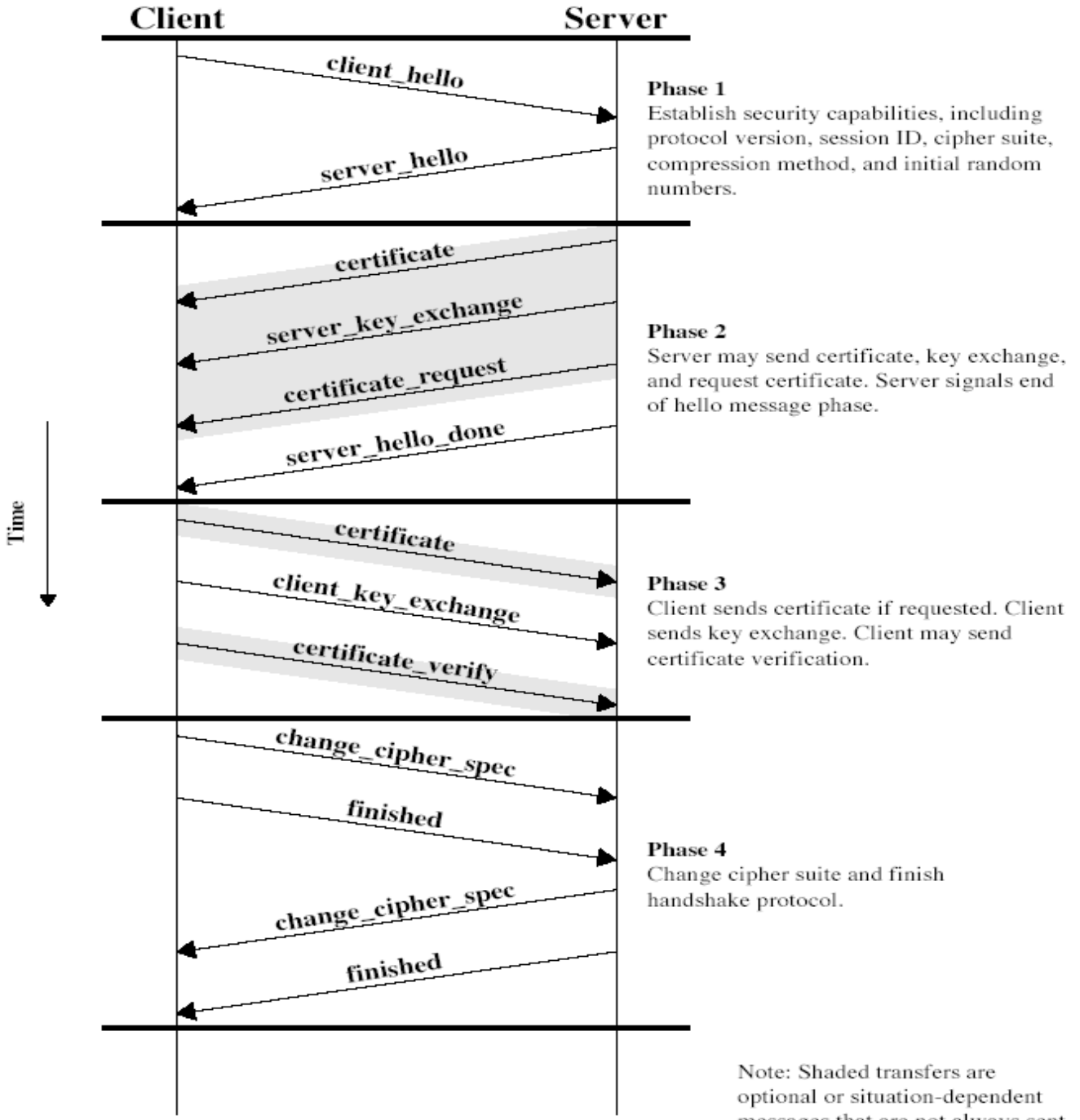
SSL Alert Protocol

- Đây là giao thức nhắc nhở SSL.
- Truyền đi lời nhắc của SSL liên quan cho thành viên
- Nhắc nhở đặc biệt:
  - ✓Cảnh báo: mẩu tin không chờ đợi, bản ghi MAC tồi, lỗi giải nén, lỗi Handshake, tham số không hợp lệ
  - ✓Nhắc nhở: đóng ghi chú, không chứng nhận, chứng nhận tồi, chứng nhận không được hỗ trợ, chứng nhận bị thu hồi, chứng nhận quá hạn, chứng nhận không được biết đến.

SSL Handshake Protocol

- Đây là giao thức bắt tay SSL
- Giao thức này cho phép máy chủ và máy trạm:
  - ✓ Xác thực nhau
  - ✓ Thỏa thuận thuật toán mã hoá và MAC
  - ✓ Thỏa thuận khoá mã sẽ dùng
- Nó bao gồm một loạt các thông tin:
  - ✓ Thiết lập các khả năng an toàn
  - ✓ Xác thực máy chủ và trao đổi khoá
  - ✓ Xác thực máy trạm và trao đổi khoá
  - ✓ Kết thúc

SSL Handshake Protocol



6.5 Bảo mật mạng không dây

1. Mạng không dây (WLAN) là Gì?

- WLAN (wireless local area network) là mạng cục bộ không dây
- Là phương thức phân phối mạng không dây cho phép nhiều thiết bị kết nối với Internet bằng cách sử dụng các giao thức chuẩn.

2. Thành phần chính của mạng không dây

Một mạng cục bộ không dây (WLAN) thông thương gồm có 2 thành phần:

- Các thiết bị truy nhập không dây (Wireless Client)
- Các điểm truy nhập (AP-access Point).

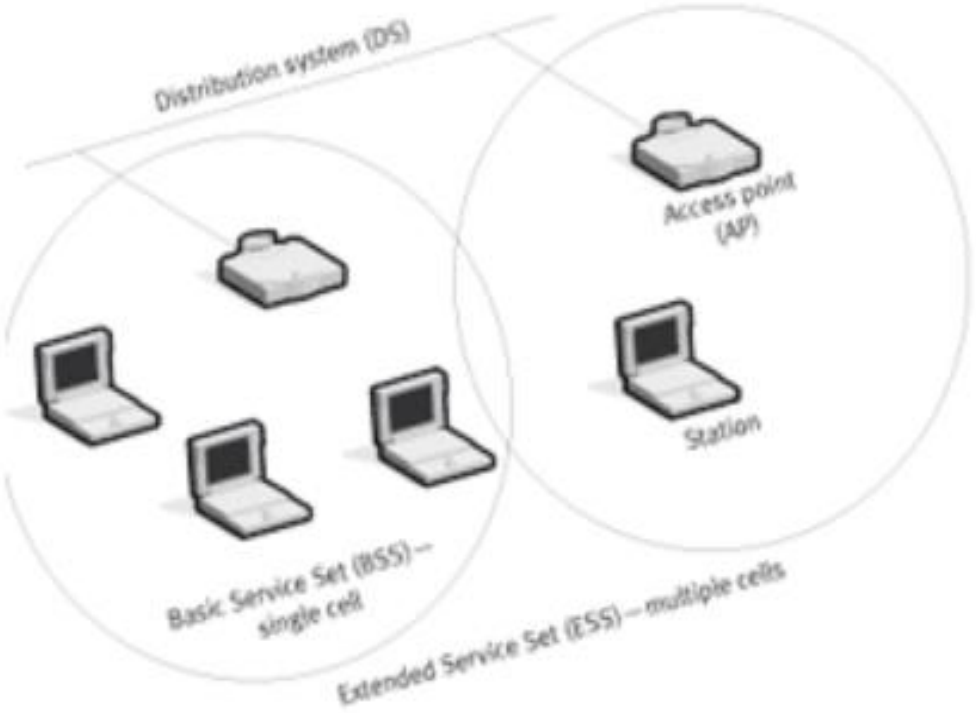
2. Thành phần chính của mạng không dây

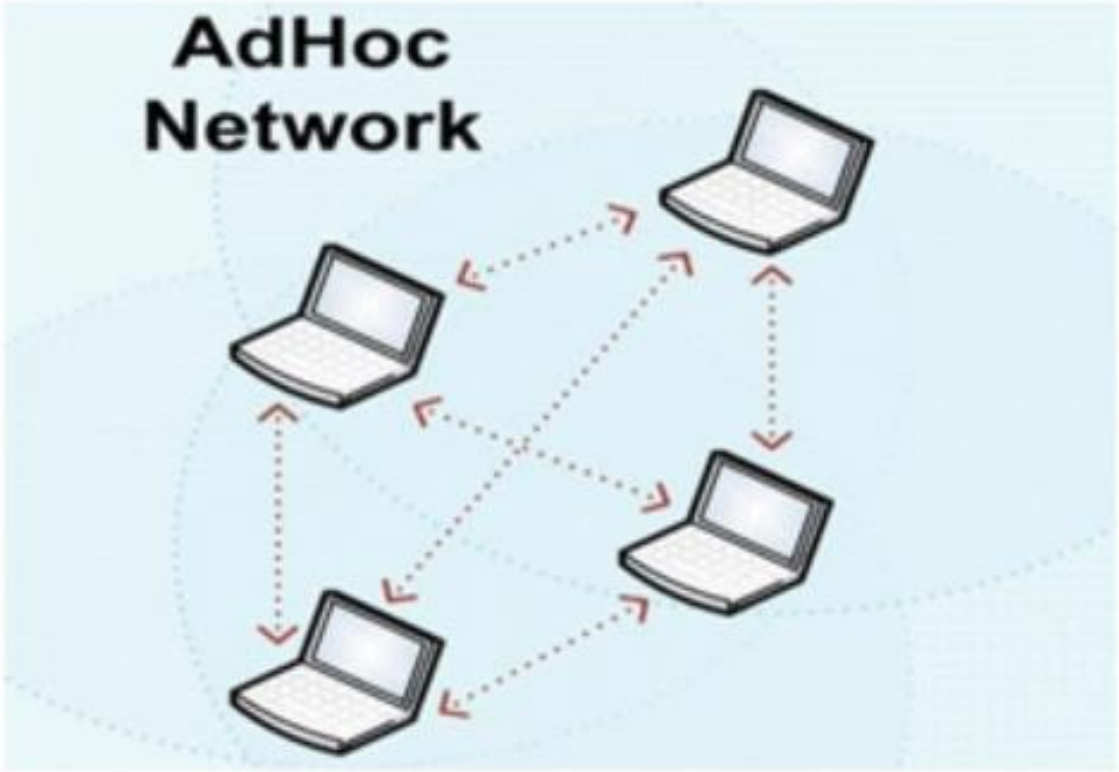
Có hai loại mạng không dây cơ bản: Ad-hoc và Infrastructure

- Kiểu Ad-hoc: Mỗi máy trong mạng giao tiếp trực tiếp với nhau thông qua các thiết bị không dây mà không dùng đến các thiết bị định tuyến (Wireless Router), hay thu phát không dây (Access point).
- Kiểu Infrastructure: Các máy trong mạng sử dụng một hay nhiều thiết bị định tuyến hay thiết bị thu phát để thực hiện trao đổi với nhau

2. Thành phần chính của mạng không dây

Có hai loại mạng không dây cơ bản: Ad-hoc và Infrastructure





3. Các chuẩn mạng không dây

- Chuẩn IEEE 802.11 ra mắt năm 1977 biểu thị một tập hợp các chuẩn WLAN được phát triển bởi ủy ban chuẩn hóa IEEE LAN/MAN.
- IEEE 802.11 là đặc tả đặc tả mạng cục bộ không dây, sử dụng phương pháp truy nhập CSMA/CA với các chuẩn:
  - ✓ IEEE 802.11a (băng tần 5.8GHz).
  - ✓ IEEE 802.11b (băng tần 2.4GHz).
  - ✓ IEEE 802.11g (băng tần 2.4GHz).
  - ✓ IEEE 802.11ac (băng tần 5GHz).
  - ✓ và IEEE 802.11i.

3. Các chuẩn mạng không dây

- IEEE 802.11b là chuẩn không dây được sử dụng phổ biến nhất hiện nay.
- Với số lượng lớn các nhà cung cấp cho các đối tượng khách hàng là các doanh nghiệp, gia đình hay các tổ chức, cơ quan nhà nước.
- IEEE 802.11b giống như HomeRF và bluetooth, sử dụng băng tần 2.4GHz và phương pháp điều biến tuyến tính được biết đến là CCK (complementary code keying) sử dụng các mã thay đổi của công nghệ trải phổ trực tiếp DSSS (Direct Sequence Spread Stpectrum).

4. Tầm quan trọng bảo mật mạng không dây

Lợi ích mà mạng không dây:

- Sự tiện lợi: Kết nối dễ dàng, không vướng víu bởi dây.
- Khả năng di động: Cho phép người dùng có thể truy cập Internet ở bất cứ đâu.
- Triển khai dễ dàng: Mạng không dây chỉ cần một điểm truy cập. Với mạng dùng cáp, người dùng có thể tốn thêm các chi phí lắp đặt và triển khai hệ thống.
- Khả năng mở rộng: Dễ dàng nâng cấp, đáp ứng tức thì nhu cầu người dùng về số lượng người kết nối mà không cần lắp thêm trang thiết bị.

4. Tầm quan trọng bảo mật mạng không dây

Các bất lợi như:

- vấn đề bảo mật
- phạm vi kết nối hẹp
- độ tin cậy kém do dễ bị nhiễu sóng
- tốc độ chậm dần nếu số ngươi kết nối lớn.

4. Tầm quan trọng bảo mật mạng không dây

- Vấn đề bảo mật là mối quan tâm hàng đầu.
- Bảo mật mạng không dây là vô cùng cần thiết
- Việc kết nối với mạng một cách lặng lẽ, khó kiểm soát của các tin tặc.
- Rất dễ bị hack hơn mạng có dây.
- Dẫn đến rủi ro lớn cho dữ liệu và hệ thống mạng cá nhân, hay doanh nghiệp.

5. Các giao thức bảo mật WLAN

- Giao thức WEP (Wired Equivalent Privacy)
- Giao thức bảo toàn dữ liệu với khóa theo thời gian TKIP (Temporal Key Integrity Protocol)
- Giao thức WPA (Wi-fi Protected Access)
- Giao thức WPA3 (Wi-fi Protected Access)