CHƯƠNG II

CÁC VẤN ĐỀ VÀ GIẢI PHÁP CƠ BẢN TRONG CÁC HỆ PHÂN TÁN

NỘI DUNG

- Truyền thông
- Định danh
- Đồng bộ
- Tiến trình trong các hệ thống phân tán
- Quản trị giao dịch và điều khiển tương tranh
- Phục hồi và chịu lỗi
- Bảo mật
- Tính nhất quán và vấn đề nhân bản

BẢO MẬT

NỘI DUNG

- Giới thiệu bảo mật
- Các kênh bảo mật
- Kiểm soát truy nhập
- Quản lý bảo mật

GIỚI THIỆU BẢO MẬT

- Bảo mật bao gồm việc đảm bảo an toàn và an ninh cho hệ thống, nó trùm toàn bộ hệ thống phân tán.
- Hệ thống phân tán luôn bị đe dọa bởi các nguy cơ mất bảo mật. Nguy cơ có thể xuất hiện trên mạng hoặc trong mỗi nút mạng.
- Các mối nguy cơ thường trực:
  - Đánh cắp (Interception): Thông tin bị đánh cắp trên đường truyền hoặc ngay tại nơi lưu trữ.
  - Gián đoạn (Interruption): làm mất hoặc hỏng dữ liệu, dịch vụ.
  - Thay đổi (Modification): thay đổi dữ liệu hoặc can thiệp vào các dịch vụ làm cho chúng không còn giữ được các đặc tính ban đầu.
  - Giả mạo (Fabrication): thêm vào dữ liệu ban đầu các dữ liệu hay hoạt động đặc biệt mà không thể nhận biết được để ăn cắp thông tin hoặc phục vụ cho mục đích riêng.

CÁC CHÍNH SÁCH BẢO MẬT

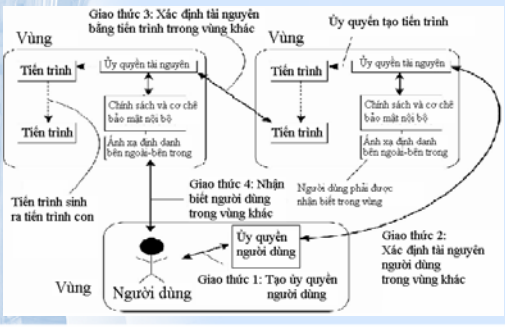
- **Mật mã** (Cryptography): thực hiện chuyển đổi dữ liệu theo một quy tắc nào đó thành dạng mới mà những người không có thẩm quyền khó có thể nhận biết được.
- **Xác thực** (Authentication): cơ chế để nhận dạng đúng đối tượng sử dụng (Người dùng, máy khách, máy chủ…)
- **Ủy quyền** (Authorization).: phân định quyền hạn cho mỗi thành phần đã đăng nhập thành công vào hệ thống. Quyền hạn này là các quyền sử dụng dịch vụ, truy cập dữ liệu…
- **Lưu vết** (Auditing): Lưu quá trình truy nhập tài nguyên (dịch vụ, dữ liệu) của đối tượng sử dụng.

Nguyễn Xuân Anh, anhcz@yahoo.com

VÍ DỤ KIẾN TRÚC BẢO MẬT CỦA Globus

- Globus là hệ thống điện toán lưới hoạt động trong môi trường nhiều vùng quản trị
- Các thao tác nội bộ chỉ phụ thuộc chính sách bảo mật vùng cục bộ
- Các thao tác bên ngoài đòi hỏi phải được nhận biết trong mỗi vùng thao tác thực hiện
- Thao tác giữa các thực thể khác vùng đòi hỏi cơ chế xác thực lẫn nhau
- Xác thực bên ngoài thay thế xác thực nội bộ
- Kiểm soát truy nhập tài nguyên chỉ phụ thuộc bảo mật nội bộ
- Người sử dụng có thể giao quyền cho các tiến trình
- Các tiến trình trong một vùng có thể chia sẻ quyền sử dụng

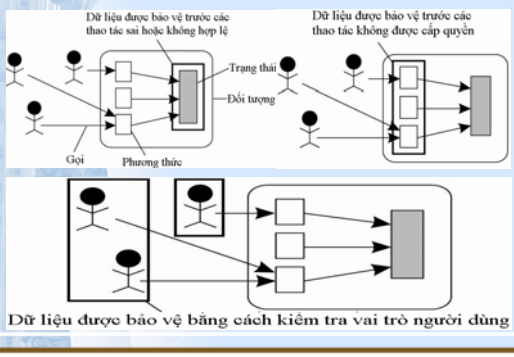
VÍ DỤ KIẾN TRÚC BẢO MẬT CỦA Globus



CÁC VẤN ĐỀ THIẾT KẾ BẢO MẬT

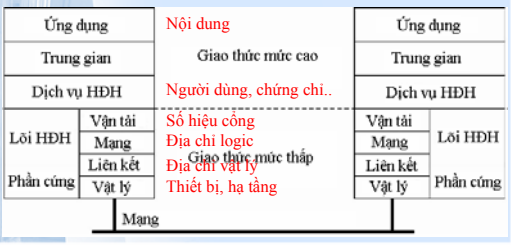
- Xác định trọng tâm kiểm soát
  - Bảo vệ dữ liệu: Bất chấp các thao tác thực hiện, dữ liệu vẫn luôn được toàn vẹn.
  - Xác định thao tác được phép gọi: Xác định các thao tác được phép thực hiện trên dữ liệu.
  - Phân quyền người dùng: Xác định người dùng và vai trò của người dùng mà không quan tâm đến thao tác người đó thực hiện
- Phân lớp cơ chế bảo mật: Lựa chọn phương án bảo mật cho từng lớp.
- Phân tán cơ chế bảo mật: Cơ chế bảo mật phụ thuộc vào hệ thống (hệ điều hành) cục bộ.
- Tính đơn giản của cơ chế bảo mật: Giải pháp bảo mật phải đơn giản nhưng vẫn bảo đảm yêu cầu chính sách bảo mật

TRỌNG TÂM KIỂM SOÁT



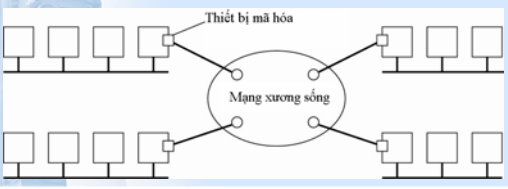
PHÂN LỚP CƠ CHẾ BẢO MẬT

- Cần phân biệt bảo mật với tin tưởng (trust)
- Xác định cơ chế bảo mật tùy thuộc vào sự tin tưởng máy khách (người dùng)



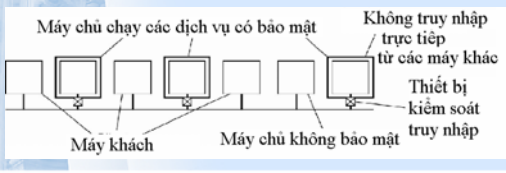
PHÂN LỚP CƠ CHẾ BẢO MẬT

- Đặt thiết bị mã hóa trước khi tham gia vào xương sống
- Trong hệ thống phân tán, bảo mật thường đặt ở mức trung gian.
- Bảo mật hệ thống phân tán phải được thực hiện tổng hợp từ bảo mật các lớp



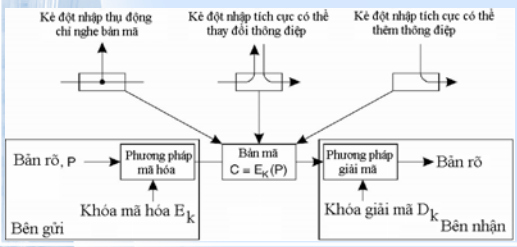
PHÂN TÁN CƠ CHẾ BẢO MẬT

- Cơ sở tính toán tin cậy (TCB): Tập các cơ chế bảo mật trong hệ thống các máy tính để bảo đảm chính sách bảo mật.
- TCB càng nhỏ càng tốt, nếu được xây dựng trên hệ điều hành mạng thì phụ thuộc vào hệ điều hành của từng máy.



MẬT MÃ

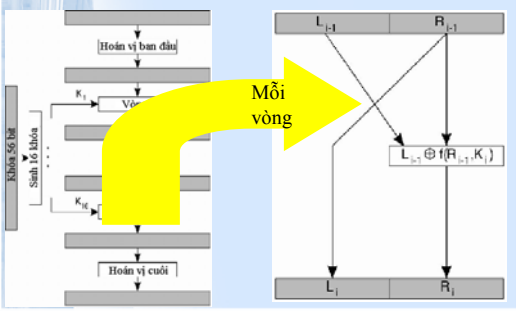
- Cơ chế bảo mật cơ bản trong hệ phân tán là mã mật.
- Bên gửi mã hóa thông điệp cần truyền (bản rõ) và gửi thông điệp đã mã hóa (bản mã), bên nhận sẽ giải mã thông điệp nhận được thành thông điệp ban đầu.



PHÂN LOẠI MẬT MÃ

- Qui ước ký hiệu:
  - $K_{A,B}$: Khóa bí mật chia sẻ giữa A và B
  - K_A^+: Khóa công khai của A
  - K_A^-: Khóa riêng của A
- Mật mã đối xứng (symmetric cryptosystem):khóa mã hóa và khóa giải mã là giống nhau
- Mật mã bất đối xứng (asymmetric cryptosystem):khóa mã hóa và khóa giải mã là khác nhau

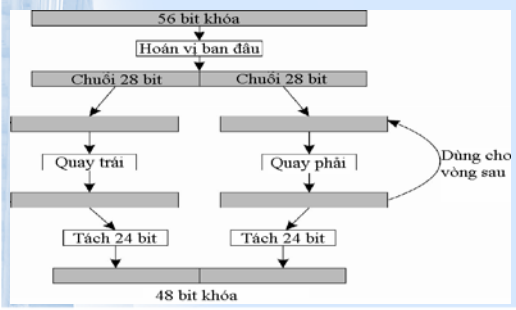
MẬT MÃ ĐỐI XỨNG
DES (Data Encryption Standard)



MÔ TẢ THUẬT TOÁN MẬT MÃ ĐỐI XỨNG
DES (Data Encryption Standard)

- Thực hiện trên các khối dữ liệu 64 bit. Mỗi khối được mã hóa qua 16 vòng lặp, mỗi vòng có một khóa mã hóa 48 bit riêng. 16 khóa này được sinh ra từ 56 bit khóa chính.
- Đầu vào của vòng lặp mã hóa thứ i là dữ liệu đã được mã hóa của vòng lặp thứ (i-1).
- 64 bit dữ liệu qua mỗi vòng lặp được chia thành hai phần bằng nhau: $\mathbf{L}_{i-1}$ và $\mathbf{R}_{i-1}$, và cùng bằng 32 bit. Phần dữ liệu bên phải R_{i-1} được lấy làm phần bên trái của dữ liệu cho vòng sau: $R_{i-1} = L_i$. Hàm f với đầu vào là R_{i-1} và khóa $\mathbf{K}_i$ sinh ra khối 32 bit được **XOR** với $\mathbf{L}_{i-1}$ để sinh ra $\mathbf{R}_i$.
- Sinh khóa: Mỗi khóa 48 bit cho mỗi vòng lặp được sinh ra từ khóa chính 56 bit. Hoán vị khóa chính, chia đôi thành hai phần 28 bit. Tại mỗi vòng, mỗi một nửa đó sẽ quay trái một hoặc hai bit, sau đó lấy ra 24 bit kết hợp với 24 bit của nửa còn lại tạo ra khóa.
- Để tăng tính bảo mật, có thể cải tiến bằng cách mã hóa hai lần.

SINH KHÓA CỦA THUẬT TOÁN
DES (Data Encryption Standard)



Nguyễn Xuân Anh, anhcz@yahoo.com

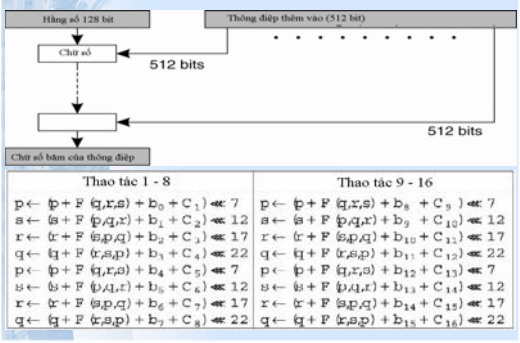
MẬT MÃ BẤT ĐỐI XỨNG
MÃ HÓA KHÓA CÔNG KHAI (RSA)

- Một khóa sẽ được giữ bí mật còn một khóa được công khai.
- Sinh khóa riêng và khóa công khai cần 4 bước:
  - Chọn 2 số nguyên tố lớn khác nhau p và q
  - Tính n = p.q và z = (p-1).(q-1)
  - Chọn một số tự nhiên d sao cho 1<d<z và nguyên tố cùng nhau với z
  - Tính toán e sao cho e.d =1 mod z (tìm số tự nhiên x sao cho e=(x.z+1)/d cũng là số tự nhiên).
- Có thể dùng d để giải mã và e dùng để mã hóa. Công khai một trong hai số này tùy trường hợp.

HÀM BĂM MD5

- Hàm tính toán chuỗi 128 bit từ bất kỳ xâu ký tự nào.
- Thông điệp được chia thành các chuỗi 512 bit.
- Giải thuật MD5 chính hoạt động trên trạng thái 128-bit, được chia thành 4 từ 32-bit, với ký hiệu *A*, *B*, *C* và *D*
- Quá trình xử lý khối tin bao gồm 4 vòng; mỗi vòng có 16 tác vụ giống nhau dựa trên hàm phi tuyến F, cộng mô đun và dịch trái.
- Có 4 khả năng cho hàm *F*, mỗi cái được dùng khác nhau cho mỗi vòng:
  F(x,y,z) = (x AND y) OR (NOT x) AND z)
  G(r,y,z) = (x AND z) OR (y AND (NOT z)
  H(x,y,z) =x XOR y XOR z
  I (z,y,z) =y XOR (x OR (NOT z))
- Sau khi thực hiện tính toán sẽ ghép 4 từ A, B, C, D.

HÀM BĂM MD5



Thao tác 1 - 8	Thao tác 9 - 16
$p \leftarrow (p + F(q,r,s) + b_0 + C_1) \lll 7$	$p \leftarrow (p + F(q,r,s) + b_8 + C_9) \lll 7$
$s \leftarrow (s + F(p,q,r) + b_1 + C_2) \lll 12$	$s \leftarrow (s + F(p,q,r) + b_9 + C_{10}) \lll 12$
$r \leftarrow (r + F(s,p,q) + b_2 + C_3) \lll 17$	$r \leftarrow (r + F(s,p,q) + b_{10} + C_{11}) \lll 17$
$q \leftarrow (q + F(r,s,p) + b_3 + C_4) \lll 22$	$q \leftarrow (q + F(r,s,p) + b_{11} + C_{12}) \lll 22$
$p \leftarrow (p + F(q,r,s) + b_4 + C_5) \lll 7$	$p \leftarrow (p + F(q,r,s) + b_{12} + C_{13}) \lll 7$
$s \leftarrow (s + F(p,q,r) + b_5 + C_6) \lll 12$	$s \leftarrow (s + F(p,q,r) + b_{13} + C_{14}) \lll 12$
$r \leftarrow (r + F(s,p,q) + b_6 + C_7) \lll 17$	$r \leftarrow (r + F(s,p,q) + b_{14} + C_{15}) \lll 17$
$q \leftarrow (q + F(r,s,p) + b_7 + C_8) \lll 22$	$q \leftarrow (q + F(r,s,p) + b_{15} + C_{16}) \lll 22$

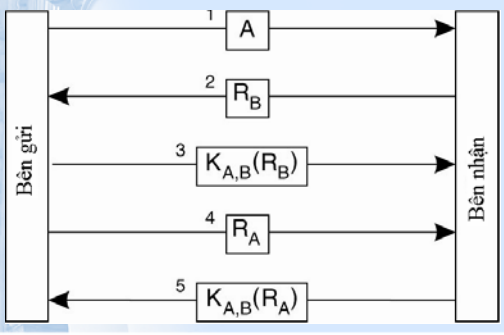
KÊNH BẢO MẬT

- Mô hình khách/chủ khá thuận tiện trong các hệ thống phân tán.
- Trao đổi thông tin giữa khách và chủ cần được thực hiện trên kênh truyền có bảo mật
- Hai vấn đề nổi bật trong kênh truyền có bảo mật:
  - Cơ chế xác thực:
    - Dựa trên khóa bí mật
    - Dựa trên trung tâm phân phối khóa
    - Dựa trên khóa công khai
  - Tính toàn vẹn và bí mật của thông điệp
- Giải pháp truyền thông nhóm có bảo mật

XÁC THỰC DỰA TRÊN KHÓA BÍ MẬT

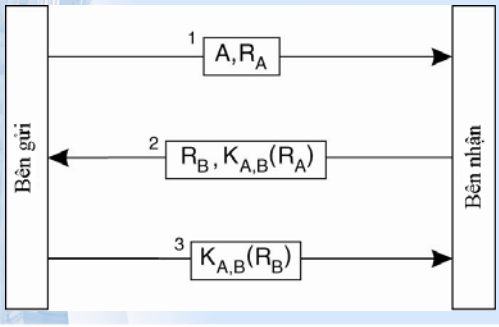
- Bên gửi muốn giao tiếp với bên nhận sẽ gửi một yêu cầu A tới bên nhận.
- Bên nhận trả lời bằng một yêu cầu R_B.
- Bên gửi sẽ mã hóa yêu cầu R_B bằng khóa bí mật $K_{A,B}$ và gửi cho bên nhận.
- Bên nhận xác thực được bên gửi nhờ nhận biết được yêu cầu R_B đã gửi trong thông điệp vừa nhận.
- Bên gửi muốn xác thực bên nhận sẽ tiếp tục gửi yêu cầu R_A tới bên nhận. Bên nhận sẽ lại mã hóa R_A bằng khóa bí mật $K_{A,B}$ đó và gửi về cho bên nhận.
- Hai bên đã xác thực thành công, quá trình trao đổi thông tin chính thức có thể bắt đầu.

XÁC THỰC DỰA TRÊN KHÓA BÍ MẬT



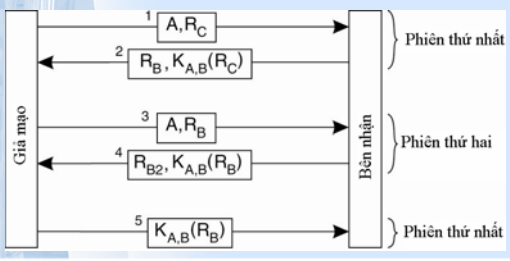
Nguyễn Xuân Anh, anhcz@yahoo.com

XÁC THỰC DỰA TRÊN KHÓA BÍ MẬT



TẤN CÔNG PHẢN XẠ (reflection attack)

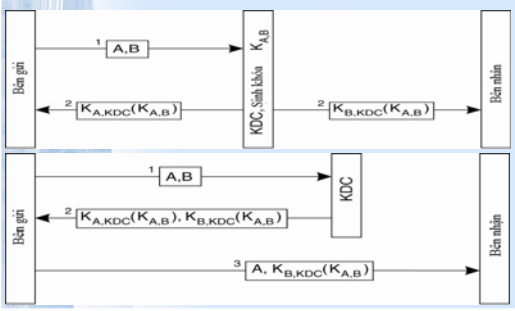
- Phiên thứ nhất giả làm bên gửi
- Phiên thứ hai nhận khóa K_{AB}



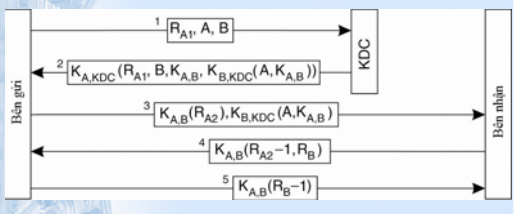
XÁC THỰC DỰA TRÊN TRUNG TÂM PHÂN PHỐI KHÓA

- Nếu hệ thống gồm N máy, mỗi máy phải chia sẻ một khóa bí mật với N-1 máy còn lại thì hệ thống cần quản lý N.(N-1)/2 khóa, và mỗi máy phải quản lý N-1 khóa. Nếu N lớn sẽ rất khó khăn trong việc quản lý. Do đó, để khắc phục hiện tượng trên ta sử dụng trung tâm phân phối khóa KDC (Key Distribution Center).
- Nguyên lý hoạt động: Bên gửi sẽ gửi thông điệp tới trung tâm phân phối khóa thông báo muốn giao tiếp với bên nhận. KDC có hai cách tiếp cận:
  - Cách 1: gửi cho cả bên gửi và bên nhận một bản tin có chứa khóa bí mật $K_{A,B}$. Thông điệp gửi cho bên nhận sẽ được mã hóa bằng $K_{A,KDC}$. Bản tin gửi cho bên gửi sẽ được mã hóa bằng $K_{B,KDC}$.
  - Cách 2: KDC sẽ gửi cả hai bản tin chứa khóa bí mật $K_{A,KDC}$ (KA,B) và $K_{B,KDC}$ (KA,B) cho bên gửi và bên gửi có nhiệm vụ gửi cho bên nhận khóa đã được KDC mã hóa $K_{B,KDC}$ (KA,B)

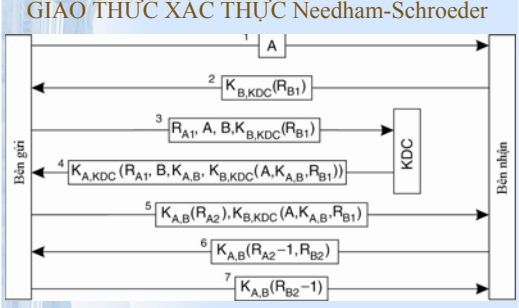
XÁC THỰC DỰA TRÊN TRUNG TÂM PHÂN PHỐI KHÓA



GIAO THỨC XÁC THỰC Needham-Schroeder



GIẢI PHÁP CHỐNG GIẢ MẠO TRONG GIAO THỨC XÁC THỰC Needham-Schroeder

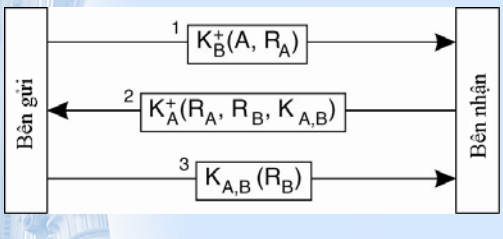


Nguyễn Xuân Anh, anhcz@yahoo.com

XÁC THỰC DỰA TRÊN KHÓA CÔNG KHAI

- Bên gửi mã hóa yêu cầu bằng khóa công khai K^{+}_{B} của bên nhận.
- Bên nhận là nơi duy nhất có thể giải mã thông điệp đó bằng K^{-}_{B}. Bên nhận sẽ mã hóa yêu cầu của bên gửi cùng với yêu cầu của chính mình và khóa $K_{A,B}$ vừa tạo ra bằng khóa công khai K^{+}_{A} của bên gửi nhằm xác thực bên gửi.
- Bên gửi sẽ gửi lại cho bên nhận yêu cầu R_B của bên nhận đã gửi đi để xác thực.

XÁC THỰC DỰA TRÊN KHÓA CÔNG KHAI

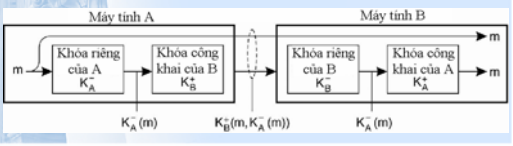


ĐẢM BẢO TÍNH TOÀN VẸN VÀ TÍNH BÍ MẬT CỦA THÔNG ĐIỆP

- Tính toàn vẹn: Thông điệp được bảo vệ trước những thay đổi lén lút
- Tính bí mật: Thông điệp không bị đánh cắp và đọc trộm.
- Đảm bảo tính bí mật bằng cách mã hóa thông điệp trước khi gửi, nhưng đảm bảo tính toàn vẹn là vấn đề khá phức tạp.
- Các giải pháp:
  - Sử dụng chữ ký số cho thông điệp
  - Tạo khóa cho mỗi phiên làm việc

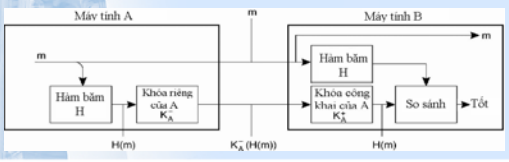
CHỮ KÝ SỐ SỬ DỤNG RSA

- Bên gửi sẽ mã hóa thông điệp bằng khóa riêng K^{-}_{A} của mình, sau đó sẽ mã hóa tiếp nội dung bản tin và phiên bản chữ kí bằng khóa công khai K^{+}_{B} của bên nhận.
- Bản mã được truyền đi cùng bản tin m.
- Bên nhận giải mã thông điệp, lấy phiên bản chữ kí của m và so sánh với m để xác thực thông điệp được gửi từ bên gửi, kiểm tra xem nội dung có thay đổi hay không.



CHỮ KÝ SỐ SỬ DỤNG HÀM BĂM

- Hàm băm H dùng để tính toán một thông điệp có độ dài cố định là một chuỗi bit từ một bản tin có độ dài tùy ý.
- Bên gửi tạo chữ ký của thông điệp m bằng hàm băm H và mã hóa bằng khóa riêng của mình.
- Chữ ký sẽ được truyền đi cùng bản tin m.
- Bên nhận giải mã thông điệp và thực hiện so sánh với bản tin m đã được truyền đi để xác định được rằng bản tin này gửi từ bên gửi đó và đã được kí bằng chữ kí số.



KHÓA PHIÊN

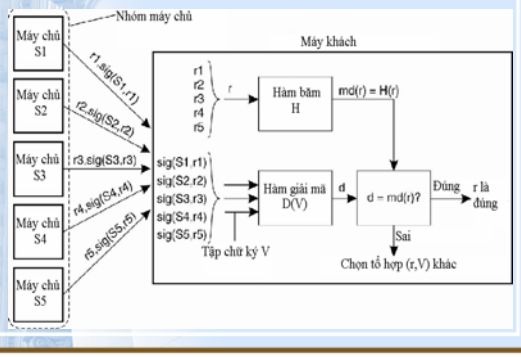
- Trong kênh truyền thông có bảo mật, sau khi xác thực sẽ tiến hành trao đổi thông tin chính thức.
- Mỗi kênh truyền thông đó được xác định bởi một đỉnh dannh gọi là khóa phiên.
- Khi kết thúcphiên thì khóa phiên tương ứng cũng bị hủy bỏ.

Nguyễn Xuân Anh, anhcz@yahoo.com

TRUYỀN THÔNG NHÓM CÓ BẢO MẬT

- Các giải pháp cho truyền thông nhóm bí mật:
  - Giải pháp 1: Tất cả các thành viên trong nhóm dùng chung một khóa bí mật để mã hóa và giải mã các thông điệp. Điều kiện tiên quyết cho mô hình này là phải đảm bảo tất cả các thành viên trong nhóm giữ bí mật khóa.
  - Giải pháp 2: Dùng một khóa bí mật cho từng cặp thành viên trong nhóm. Khi một thành viên để lộ thông tin thì các thành viên khác sẽ không gửi thông điệp cho thành viên đó nhưng vẫn sử dụng khóa bí mật cũ. Với mô hình này phải duy trì tới N (N-1)/2 khóa.
  - Giải pháp 3: Mỗi một thành viên trong nhóm sẽ phải duy trì một cặp khóa công khai và khóa riêng, trong đó khóa công khai được dùng bởi tất cả thành viên trong nhóm.
- Vấn đề bí mật các máy chủ nhân bản

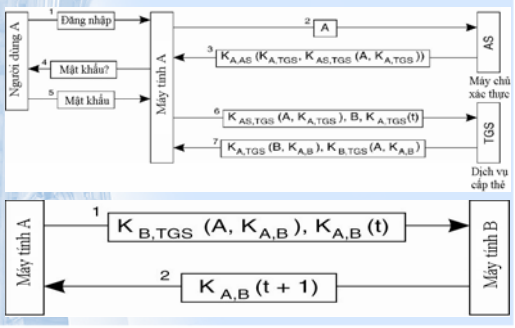
BÍ MẬT CÁC MÁY CHỦ NHÂN BẢN



VẤN ĐỀ BẢO MẬT NGHIÊM NGẶT

- Toàn bộ thệ thống phân tán phải được bảo mật nghiêm ngặt
- Giải pháp Kerberos được sử dụng rộng rãi trong việc bảo mật nghiêm ngặt các hệ thống
- Kerberos dựa trên giao thức xác thực Needham-Schroeder để thiết lập kênh bí mật giữa máy khách và máy chủ

THIẾT LẬP KÊNH BÍ MẬT TRONG Kerberos

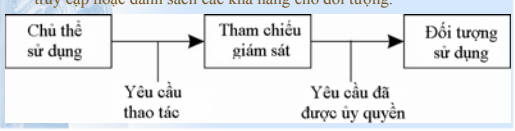


KIỂM SOÁT TRUY NHẬP

- Trong mô hình khách chủ, sau khi thiết lập kênh bí mật, máy khách có thể gửi các yêu cầu để máy chủ thực hiện.
- Máy chủ sẽ kiểm tra quyền truy nhập trước khi thực thi các yêu cầu trên đối tượng.
- Các quyền thao tác trên đối tượng bao gồm: Tạo (CREATE), thay đổi (ALTER, RENAME), xóa (DROP)… đọc (READ), ghi (WRITE), xóa (DELETE)
- Các phương pháp kiểm soát:
  - Ma trận kiểm soát truy nhập
  - Tường lửa
  - Mã di động bí mật
  - Từ chối dịch vụ

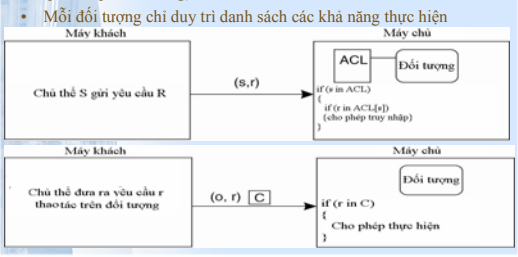
MA TRẬN KIỂM SOÁT TRUY NHẬP

- Ma trận kiểm soát truy nhập được cấu thành từ hàng (biểu diễn cho chủ thể) và cột (biểu diễn cho đối tượng).
- Phần tử M[s,o] chứa danh sách các thao tác mà chủ thể S được phép thực hiện trên đối tượng O.
- Khi chủ thể S gọi một phương thức của đối tượng O, thành phần giám sát sẽ kiểm tra danh sách trong M[s,o], nếu không xuất hiện trong danh sách này thì lời gọi bị hủy bỏ.
- Thông thường hệ thống phải làm việc với rất nhiều dùng nên kích thước ma trận sẽ lớn. Giải pháp khác là dùng danh sách kiểm soát truy cập hoặc danh sách các khả năng cho đối tượng.



DANH SÁCH KIỂM SOÁT TRUY NHẬP

- Mỗi đối tượng duy trì danh sách các thao tác hợp lệ của các chủ thể. Thực chất đây là cách thể hiện ma trận dưới dạng vector (bỏ qua các phần tử rỗng).
- Mỗi đối tượng chỉ duy trì danh sách các khả năng thực hiện

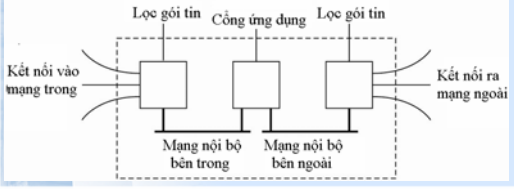


MIỀN BẢO VỆ

- ACL tuy đã khắc phục được nhược điểm của ma trận kiểm soát truy nhập nhưng vẫn có kích thước lớn.
- Miền bảo vệ là một tập các cặp (đối tượng, truy nhập hợp lệ), mỗi cặp này sẽ cho một đối tượng và các thao tác hợp lệ trên nó.
- Mỗi yêu cầu đều thuộc một miền bảo vệ nào đó. Khi một yêu cầu gửi đến, thành phần giám sát sẽ tìm trong miền bảo vệ tương ứng yêu cầu này.
- Để đạt hiệu quả cao hơn, người ta dùng kết hợp miền bảo vệ với việc phân nhóm các đối tượng.

TƯỜNG LỬA

- Tường lửa dùng để ngăn chặn các luồng không được phép.
- Thông thường chặn gói tin hoặc nội dung tại lớp ứng dụng
- Tham chiếu mô hình phân tầng mạng để đưa ra chính sách kiểm soát truy nhập
- Hai loại danh sách kiểm soát truy nhập: Cho phép (permit) hay từ chối (deny)



MÃ DI ĐỘNG BÍ MẬT

- Việc di trú mã trong hệ thống phân tán tiềm ẩn nguy cơ mất bảo mật.
- Khi Agent di chuyển trên mạng Internet, chủ sở hữu Agent muốn chúng không bị các máy tính cố tình làm hại đánh cắp hoặc thay đổi dữ liệu chứa trong các Agent đó.
- Bản thân máy tính của người dùng cũng cần được bảo vệ trước những Agent độc hại.

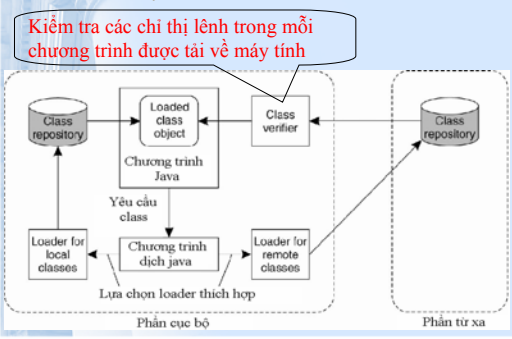
BẢO VỆ Agent

- Agent di chuyển giữa các máy tính để thu thập thông tin.
- Mã độc trên mỗi máy tính có thể thâm nhập thông tin của mỗi Agent.
- Agent được bảo vệ bằng cách ghi lại lịch sử với thuộc tính chỉ được thêm, sử dụng mã hóa công khai.

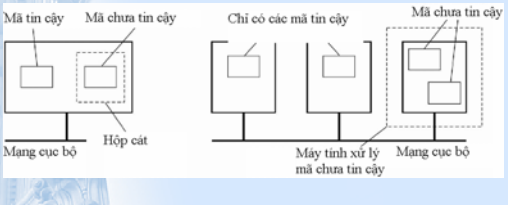
BẢO VỆ MÁY TÍNH

- Agent thâm nhập máy tính có thể chứa mã độc hại
- Cần phải kiểm tra mã lệnh của các Agent hoặc của các chương trình được tải về máy tính.
- Giải pháp hộp cát (sandbox): Kiểm soát toàn bộ các chỉ thị lệnh trong cách chương trình được tải về máy tính.
- Giải pháp khu xử lý (PlayGround): Tách riêng các mã di động trên máy tính khác

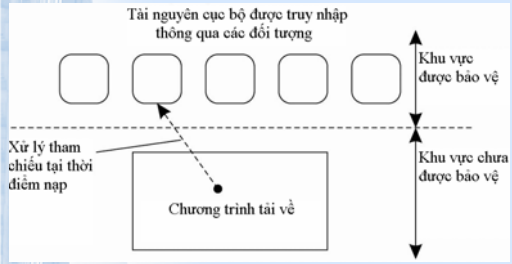
SỬ DỤNG Sandbox TRONG Java



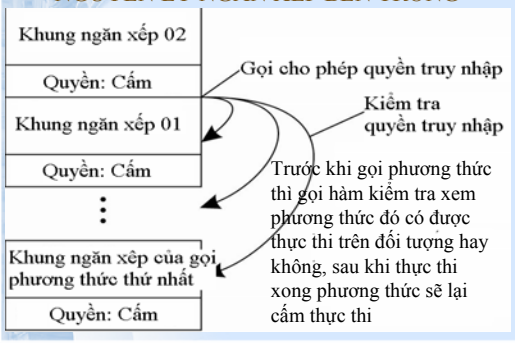
GIẢI PHÁP TÁCH THỰC THI MÃ DI ĐỘNG



NGUYÊN LÝ SỬ DỤNG THAM CHIẾU ĐỐI TƯỢNG



NGUYÊN LÝ NGĂN XẾP BÊN TRONG



TỪ CHỐI DỊCH VỤ

- Việc kiểm soát truy nhập được đảm bảo bằng cách chỉ có những tiến trình đã được ủy quyền mới có thể truy nhập tài nguyên.
- Kẻ tấn công lợi dụng đặc điểm này để làm tê liệt hệ thống, hệ thống sẽ từ chối ngay cả những tiến trình đã được ủy quyền. Hình thức tấn công này gọi là từ chối dịch vụ (DoS).
- Vấn đề ngày càng phức tạp bằng hình thức tấn công từ chối dịch vụ phân tán (DDoS)
- Chưa có biện pháp riêng để chống lại DDoS, hiện nay vẫn chủ yếu dựa vào việc theo dõi lưu lượng mạng và thiết bị định tuyến sẽ loại bỏ những gói tin xuất phát từ địa chỉ nào đó

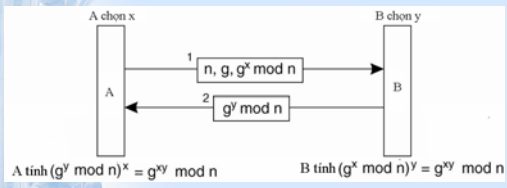
QUẢN LÝ BẢO MẬT

- Quản lý khóa mật mã
  - Thiết lập khóa
  - Phân phối khóa
- Quản lý nhóm các máy chủ
- Quản lý ủy quyền

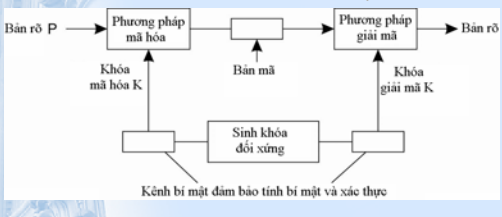
THIẾT LẬP KHÓA

- Bên A và bên B đều tạo ra hai số lớn là n và g - hai số này có thể được công khai.
- Bên A sẽ tạo ra một số lớn khác là x, bên B tạo ra số lớn y và giữ bí mật chúng.
- Bên A sẽ gửi cho bên B: n, g và (g^x mod n). Bên B sẽ thực hiện tính (g^x mod n)^y= g^{xy} mod n. do đó sẽ xác định được khóa bí mật x của bên A.
- Bên B cũng gửi cho bên A (g^y mod n). Bên A thực hiện tính toán (g^y mod n)^x= g^{xy} mod n nhờ đó cũng xác định được khóa bí mật y của bên B.

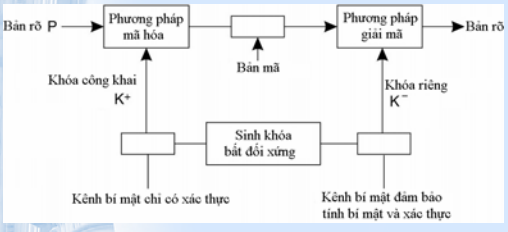
NGUYÊN LÝ THIẾT LẬP KHÓA



PHÂN PHỐI KHÓA BÍ MẬT



PHÂN PHỐI KHÓA CÔNG KHAI

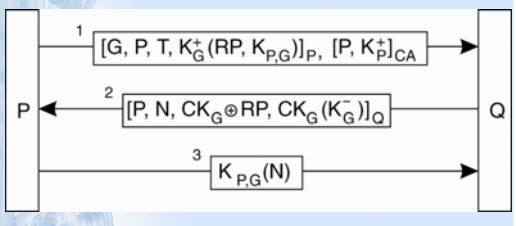


CÁC PHƯƠNG PHÁP HỦY CHỨNG CHỈ

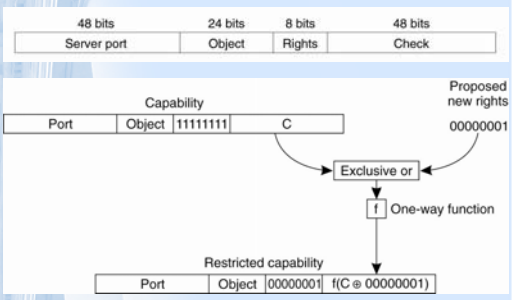
- Sử dụng danh sách các chứng chỉ bị hủy bỏ CRL (certification revocation list). Khi máy khách kiểm tra một chứng chỉ thì nó cũng kiểm tra trong danh sách CRL để kiểm tra xem chứng chỉ này đã bị hủy hay chưa. Như thế mỗi client phải được cập nhật danh sách này thường xuyên.
- Mỗi chứng chỉ tự động hết hiệu lực sau một thời gian xác định nào đó. Nhưng nếu muốn hủy chứng chỉ trước thời gian đó thì vẫn phải dùng đến danh sách CRL như trên.
- Giảm thời gian tồn tại có hiệu lực của một chứng chỉ xuống gần bằng 0. Khi đó máy khách phải thường xuyên kiểm tra chứng chỉ để xác đinh thời gian có hiệu lực của khóa công khai.

QUẢN LÝ NHÓM BÍ MẬT

BÍ MẬT NHẬN THÀNH VIÊN MỚI



CÁC KHẢ NĂNG VÀ CHỨNG CHỈ THUỘC TÍNH



CẤU TRÚC CHUNG CỦA ỦY QUYỀN ĐẠI DIỆN

SỬ DỤNG ỦY QUYỀN ĐỂ ĐẠI DIỆN VÀ CHỨNG MINH SỞ HỮU QUYỀN TRUY NHẬP