2.6 Các giao thức bảo mật trên mạng Internet

- Bảo mật giao thức PPP (Layer 2).
- Tunneling Protocols.
- IPsec (Layer 3).
- Secure Shell (SSH) (Layer 4).
- HTTP/S – on top of SSH (Layer 4,5).
- Bảo mật E-Mail (Layer 5).
- Bảo mật Wireless network.

63

Chương 3

HẠ TẦNG KIẾN TRÚC KHÓA CÔNG KHAI (PKI)

64

TRƯỜNG ĐẠI HỌC MỞ TP. HCM
Cơ hội học tập cho mọi người

Nội dung

- Khái niệm.
- CA – Certificate Authorities.
- RAs and LRAs.
- Certificates (Chứng chỉ).
- Mô hình uỷ quyền (Trust Models).

65

TRƯỜNG ĐẠI HỌC MỞ TP. HCM
Cơ hội học tập cho mọi người

3.1 Khái niệm

- Một PKI (Public Key Infrastructure) cho phép người sử dụng dùng một mạng công cộng không bảo mật để trao đổi thông tin một cách an toàn bằng cách sử dụng một cặp khóa công khai + khóa riêng tư được cung cấp từ một nhà cung cấp chứng thực được tín nhiệm (CA - Certificate Authority).
- PKI phải đảm bảo có đủ các đặc tính sau:
  - Tính bí mật (Confidentiality)
  - Tính toàn vẹn (Integrity)
  - Tính xác thực (Authentication)
  - Tính không thể chối từ (Non-Repudiation)

66

TRƯỜNG ĐẠI HỌC MỞ TP. HCM
Cơ hội học tập cho mọi người

Khái niệm (tt)

- Một cơ sở hạ tầng khóa công khai bao gồm:
  - Một nhà cung cấp chứng thực số (CA) chuyên cung cấp và xác minh các chứng chỉ số, bao gồm khóa công khai hoặc thông tin về khóa công khai
  - Tổ chức quản lý đăng ký (Registration Authority (RA)) đóng vai trò thẩm tra cho CA trước khi một chứng chỉ số được cấp phát tới người yêu cầu
  - Thực thể cuối (End Entity – EE): đối tượng sử dụng chứng nhận (tổ chức, cá nhân, dịch vụ trên máy tính,…)
  - Chứng nhận khóa công khai (Public Key Certificate)
  - Kho lưu trữ chứng nhận (*Certificate Repository – CR)*

67

TRƯỜNG ĐẠI HỌC MỞ TP. HCM
Cơ hội học tập cho mọi người

Khái niệm (tt)

68

TRƯỜNG ĐẠI HỌC MỞ TP. HCM
Cơ hội học tập cho mọi người

Khái niệm (tt)

- Một số ứng dụng của PKI:
  - Mã hóa Email hoặc xác thực người gửi Email (OpenPGP or S/MIME).
  - Mã hóa và xác thực văn bản (các tiêu chuẩn chữ ký XML * hoặc ma hoa XML * khi văn bản được thể hiện dưới dạng XML).
  - Xác thực người dùng ứng dụng (Đăng nhập bằng thẻ thông minh, nhận thực người dùng trong SSL).
  - Các giao thức truyền thông an toàn dùng kỹ thuật Bootstrapping (IKE, SSL): trao đổi khóa bằng khóa bất đối xứng, mã hóa bằng khóa đối xứng.

69

TRƯỜNG ĐẠI HỌC MỞ TP. HCM
Cơ hội học tập cho mọi người

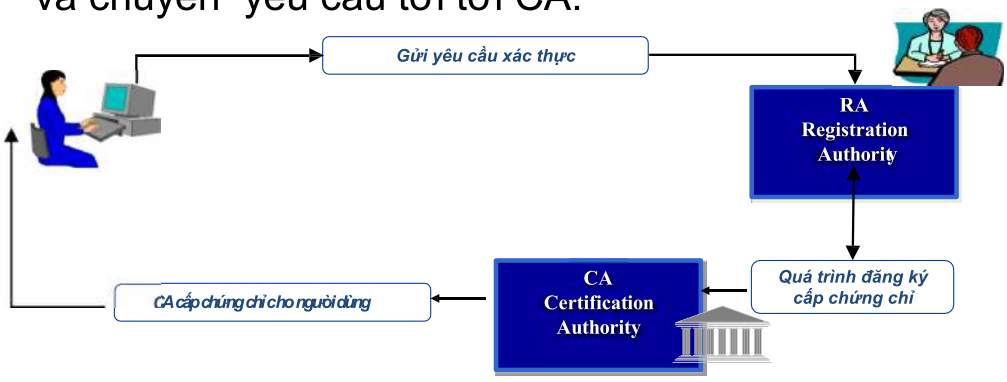
3.2 CA – Certificate Authorities

- CA là một tổ chức chuyên cung cấp các chứng chỉ dùng để xác thực cho người dùng trên một mạng máy tính cùng các khóa công khai để mã hóa thông tin
- Các chứng chỉ số (Certificate) sẽ được dùng vào các mục đích khác nhau, ví dụ như mã hóa dữ liệu, mã hóa thư điện tử, mã hóa website…
- CA thực hiện việc kiểm soát kết hợp với RA để xác minh thông tin về một chứng chỉ số mà người yêu cầu xác thực đưa ra:
  - RA xác nhận thông tin của người cần xác thực
  - CA cung cấp chứng chỉ

70

3.3 RAs and LRAs

- Là các tổ chức được CA ủy quyền nhằm thực hiện một số chức năng như tiếp nhận đăng ký, xác minh đối tượng xin cấp hành chứng chỉ xác thực và chuyển yều cầu tới tới CA.



71

RAs and LRAs (tt)

- Các chức năng của RA:
  - Xác thực cá nhân chủ thể đăng ký chứng chỉ
  - Kiểm tra tính hợp lệ của thông tin do chủ thể cung cấp
  - Xác nhận quyền của chủ thể đối với những thuộc tính chứng chỉ được yêu cầu
  - Kiểm tra chủ thể có thực sự sở hữu khóa riêng đang được đăng ký hay không (chứng minh sở hữu)
  - Tạo cặp khóa bí mật/công khai
  - Khởi tạo qua trình đăng ký cho chủ thể với CA
  - Lưu trữ/khôi phục khóa
  - Phân phối thẻ bài vật lý chứa khóa riêng (Smart Card)

72

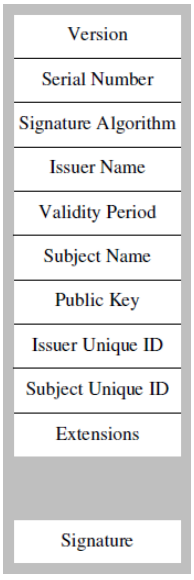
3.4 Certificates (Chứng chỉ).

- Là tập tin điện tử dùng để xác minh danh tính một chủ thể, bao gồm:
  - Thông tin của chủ thể
  - Khóa công khai của chủ thể
  - Chữ ký số của CA cấp
  - Thời gian hợp lệ
- Có nhiều loại chứng chỉ, một trong số đó là :
  - Chứng chỉ khóa công khai X.509
  - Chứng chỉ khóa công khai đơn giản (Simple public key certificates - SPKC).
  - Chứng chỉ Pretty Good Privacy (PGP).
  - Chứng chỉ thuộc tính (Attribute Cercitificates - AC)

73

3.4.1 Chứng chỉ - chuẩn x-509

- Là định dạng được sử dụng phổ biến và được hầu hết các nhà cung cấp chứng chỉ PKI triển khai.
- Do hội viễn thông quốc tế (ITU) đưa ra lần đầu tiên năm 1988.
- Chứng chỉ số gồm 2 thành phần:
  - Các trường cơ bản cần thiết phải có trong chứng chỉ.
  - Một số trường trường mở rộng dùng để xác định và đáp ứng yêu cầu bổ sung của hệ thống.



74

Chứng chỉ - chuẩn x-509

- Các thuộc tính của chứng chỉ:
  - Version : Xác định số phiên bản của chứng chỉ.
  - Certificate Serial Number : Do CA gán, là định danh duy nhất của chứng chỉ.
  - Signature Algorithm ID : Chỉ ra thuật toán CA sử dụng để ký số chứng chỉ. Có thể là thuật toán RSA hoặc DSA…
  - Issuer : chỉ ra CA cấp và ký chứng chỉ.
  - Validity Period : khoảng thời gian chứng chỉ có hiệu lực. Trường này xác định thời gian chứng chỉ bắt đầu
  - Subject: xác định thực thể mà khóa công khai của thực thể này xác nhận. Tên của subject phải duy nhất đối với mỗi thực thể CA xác nhận

75

Chứng chỉ - chuẩn x-509

- Các thuộc tính của chứng chỉ (tt)
  - Subject public key infomation: chứa khóa công khai và những tham số liên quan ; xác định thuật toán (ví dụ RSA hoặc DSA) được sử dụng cùng với khóa.
  - Issuer Unique ID : là trường không bắt buộc, trường này cho phép sử dụng lại tên của subject khi quá hạn. Trường hợp này cũng ít được sử dụng.
  - Extensions: chỉ có trong chứng chỉ v3.
  - Certification Authority's Digital Signature : chữ ký số của CA được tính từ những thông tin trên chứng chỉ với khóa riêng và thuật toán ký số được chỉ ra trong trường Signature Algorihm Identifier của chứng chỉ

76

Chứng chỉ - chuẩn x-509

- Tính toàn vẹn của chứng chỉ được đảm bảo bằng chữ ký số của CA trên chứng chỉ.
- Khóa công khai của CA được phân phối đến người sử dụng chứng chỉ theo một số cơ chế bảo mật trước khi thực hiện các thao tác PKI.
- Người sử dụng kiểm tra hiệu lực của chứng chỉ được cấp với chữ ký số của CA và khóa công khai của CA

77

Chứng chỉ - chuẩn x-509

- Các thuộc tính mở rộng của chứng chỉ:
  - Authority Key Indentifier: chứa ID khóa công khai của CA dùng để kiểm tra chữ ký số trên chứng chỉ. Nó cũng được sử dụng để phân biệt giữa các cặp khóa do một CA sử dụng (trong trường hợp nếu CA có nhiều hơn một khóa công khai). Trường này được sử dụng cho tất cả các chứng chỉ tự ký số (CA- certificates).
  - Subject Key Identifier: chứa ID khóa công khai có trong chứng chỉ dung để phân biệt giữa các khóa nếu như có nhiều khóa được gắn vào trong cùng chứng chỉ của người sử dụng (nếu chủ thể có nhiều hơn một khóa công khai).

78

Chứng chỉ - chuẩn x-509

- Các thuộc tính mở rộng của chứng chỉ:
  - Key Usage: chứa một chuỗi bít được dùng để xác định (hoặc hạn chế) chức năng hoặc dịch vụ được hỗ trợ qua việc sử dụng khóa công khai trong chứng chỉ.
  - Extended Key Usage: chứa một hoặc nhiều OIDs (định danh đối tượng - Object Identifier) để xác định cụ thể việc sử dụng khóa công khai trong chứng chỉ. Bao gồm các giá trị:
    - (1) Xác thực server TLS
    - (2) Xác thực client TLS
    - (3) Ký Mã
    - (4) Bảo mật email
    - (5) Thời gian hiệu lực

79

Chứng chỉ - chuẩn x-509

- Các thuộc tính mở rộng của chứng chỉ:
  - CRL Distribution Point: chỉ ra vị trí của CRL tức là nơi hiện có thông tin thu hồi chứng chỉ
    - URI (Uniform Resource Indicator)
    - Địa chỉ của x-509
    - LDAP server
  - Private Key Usage Period: thời gian sử dụng của khóa riêng gắn với khóa công khai trong chứng chỉ.
  - Certificate Policies: chỉ ra dãy các chính sách OIDs gắn với việc cấp và sử dụng chứng chỉ

80

Chứng chỉ - chuẩn x-509

- Các thuộc tính mở rộng của chứng chỉ:
  - Policy Mappings: chỉ ra các chính sách xác thực tương đương giữa hai miền CA, được dùng trong việc thiết lập xác thực chéo và kiểm tra đường dẫn chứng chỉ.
  - Subject Alternative Name: chỉ ra những dạng tên lựa chọn gắn với người sở hữu chứng chỉ:
    - Địa chỉ e-mail
    - Địa chỉ IP
    - Địa chỉ URI…
  - Issuer Alternative Name : chỉ ra những dạng tên lựa chọn gắn với người cấp chứng chỉ.

81

Chứng chỉ - chuẩn x-509

- Các thuộc tính mở rộng của chứng chỉ:
  - Subject Directory Attributes: dãy các thuộc tính gắn với người sở hữu chứng chỉ. Trường mở rộng này không được sử dụng rộng rãi. Nó được dùng để chứa những thông tin liên quan đến đặc quyền.
  - Basic Constrains Field: true/false, cho biết đây có phải là chứng chỉ CA hay không
  - Path Length Contraint: độ dài tối đa của đường dẫn chứng chỉ có thể được thiết lập.
    - zero: CA chỉ có thể cấp chứng chỉ cho thực thể cuối, không cấp chứng chỉ cho những CA khác

82

Chứng chỉ - chuẩn x-509

- Các thuộc tính mở rộng của chứng chỉ:
  - Name Constrainsts: được dùng để bao gồm hoặc loại trừ các nhánh trong những miền khác nhau trong khi thiết lập môi trường tin tưởng giữa các miền PKI
  - Policy Constraints: được dùng để bao gồm hoặc loại trừ một số chính sách chứng chỉ trong khi thiết lập môi trường tin tưởng giữa các miền PKI

83

3.4.2 Thu hồi chứng chỉ

- X.509 cho phép kiểm tra chứng chỉ trong những trường hợp sau:
  - Chứng chỉ không bị thu hồi.
  - Chứng chỉ đã bị CA cấp thu hồi.
  - Chứng chỉ do một tổ chức có thẩm quyền mà CA ủy thác có trách nhiệm thu hồi chứng chỉ đã thu hồi.
- Để duy trì tính nhất quán và khả năng kiểm tra, CA yêu cầu :
  - Duy trì bản ghi kiểm tra chứng chỉ thu hồi.
  - Cung cấp thông tin trạng thái thu hồi.
  - Công bố CRLs khi CRL là danh sách trống.

84

Thu hồi chứng chỉ

- Các trường hợp chứng chỉ không hợp lệ:
  - Hết thời gian hiệu lực
  - Khóa riêng của chủ thể bị xâm phạm.
  - Thông tin chứa trong chứng chỉ bị thay đổi.
  - Khoá riêng của CA cấp chứng chỉ bị xâm phạm.
- Khi chứng chỉ không hợp lệ, cần có một cơ chế để thông báo đến người sử dụng:
  - Công bố CRLs định kỳ hoặc khi cần thiết.
  - Dùng phương pháp trực tuyến Online Certificate Status Protocol.

85

Thu hồi chứng chỉ

- CRLs

Version number	
Signature	
Issuer	
This update	
Next update	
User certificate serial number	Date of revocation
Revocation reason	
User certificate serial number	Date of revocation
Revocation reason	
CRL extensions	

86

TRƯỜNG ĐẠI HỌC MỞ TP. HCM
Cơ hội học tập cho mọi người

3.5 Mô hình ủy quyền (Trust Models)

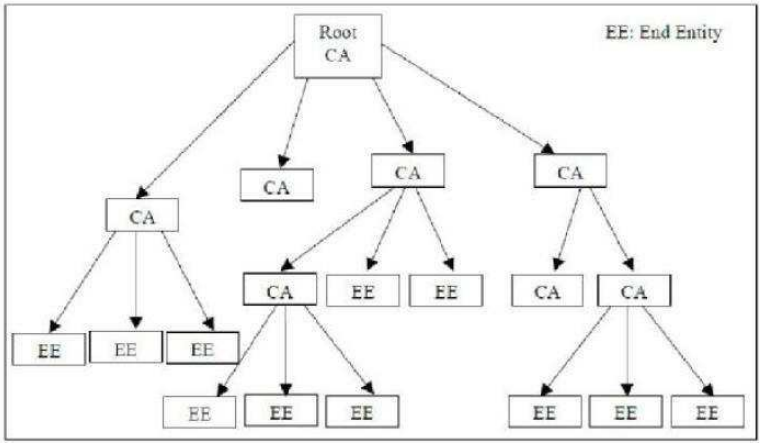
- Hierarchical (phân cấp)
- Bridge.
- Mesh (mắt lưới - xác thực chéo)
- Hybrid.

87

TRƯỜNG ĐẠI HỌC MỞ TP. HCM
Cơ hội học tập cho mọi người

Mô hình Hierarchical

- Đây là mô hình PKI mà trong đó mỗi thực thể sẽ giữ bản sao khóa công khai của root CA và kiểm tra đường dẫn của chứng chỉ bắt đầu từ chữ ký CA gốc



88

TRƯỜNG ĐẠI HỌC MỞ TP. HCM
Cơ hội học tập cho mọi người

Hierarchical (tt)

- Ưu điểm:
  - Có thể dùng trực tiếp cho những tổ chức có phân cấp và độc lập: doanh nghiệp, tổ chức chính phủ, quân đội,..
  - Cho phép thực thi chính sách và chuẩn thông qua hạ tầng cơ sở
  - Dễ vận hành giữa các tổ chức khác nhau

89

TRƯỜNG ĐẠI HỌC MỞ TP. HCM
Cơ hội học tập cho mọi người

Hierarchical (tt)

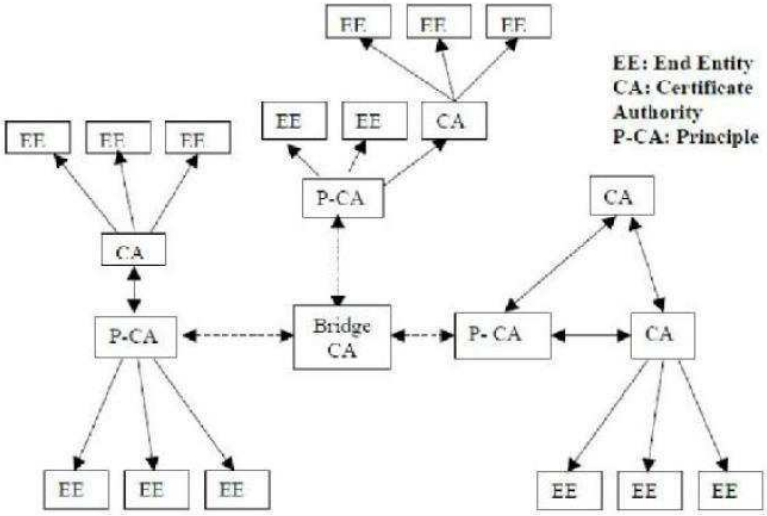
- Nhược điểm:
  - Không thích hợp đối với môi trường mà mỗi miền khác nhau có chính sách và giải pháp PKI khác nhau
  - Các tổ chức có thể không tin vào tổ chức khác
  - Không thích hợp cho những mối quan hệ ngang hàng giữa chính phủ và doanh nghiệp
  - Các tổ chức thiết lập CA trước đó có thể không muốn trở thành một phần của mô hình
  - Chỉ có một CA gốc → Khi khóa bí mật của CA bị xâm phạm, khóa công khai mới của CA gốc phải phân phối đến tất cả end - user

90

TRƯỜNG ĐẠI HỌC MỞ TP. HCM
Cơ hội học tập cho mọi người

Mô hình Bridge

- Do US Federal PKI phát triển



91

TRƯỜNG ĐẠI HỌC MỞ TP. HCM
Cơ hội học tập cho mọi người

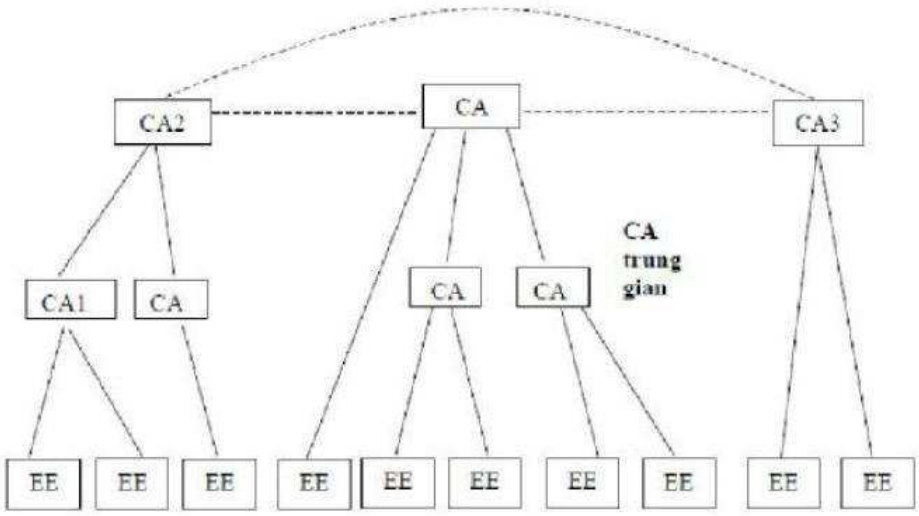
Mô hình Bridge (tt)

- CA trung tâm gọi là hub/bridge CA
- Mỗi CA gốc thiết lập xác thực với CA trung tâm
- Tất cả thực thể đều giữ khóa công khai của CA cục bộ, không có khóa của CA trung tâm
- Ưu điểm:
  - Không phân cấp
  - Giảm số xác thực chéo
  - Tránh được các nhược điểm của mô hình mạng
- Nhược điểm:
  - Khó thiết lập Bridge CA

92

TRƯỜNG ĐẠI HỌC MỞ TP. HCM
Cơ hội học tập cho mọi người

Mô hình Mesh

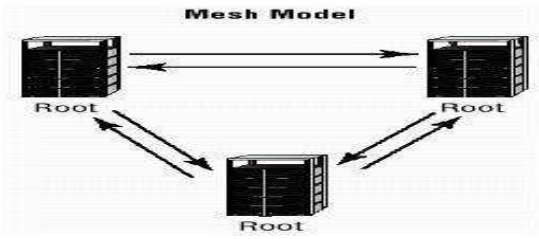


93

TRƯỜNG ĐẠI HỌC MỞ TP. HCM
Cơ hội học tập cho mọi người

Mô hình Mesh

- Có nhiều CA gốc xác thực chéo với nhau
- Mỗi CA có thể nằm trong mô hình phân cấp hoặc mô hình Mesh khác
- Có thể liên kết các miền khác nhau thông qua các thuộc tính BasicContraints, Name Contraints, PolicyMapping, PolicyContraints của x-509 v3 mở rộng



94

TRƯỜNG ĐẠI HỌC MỞ TP. HCM
Cơ hội học tập cho mọi người

Mô hình Mesh

- Ưu điểm:
  - Linh hoạt, phù hợp nhu cầu giao tiếp đa dạng
  - Cho phép những nhóm người sử dụng khác nhau có thể tự do phát triển và thực thi các chính sách và chuẩn khác nhau
  - Tính cạnh tranh cao
  - Khắc phục được nhược điểm của mô hình phân cấp
- Nhược điểm:
  - Số xác thực chéo lớn (n^2)
  - Phức tạp và khó quản lý

95

Chương 4

CÁC HỆ MẬT MÃ

96