ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC BÁCH KHOA
KHOA KHOA HỌC VÀ KỸ THUẬT MÁY TÍNH

BÁO CÁO – TÍNH TOÁN LƯỚI

AN NINH TRÊN LƯỚI

Giáo viên hướng dẫn: TS. Phạm Trần Vũ
Sinh viên thực hiện: Trần Ngọc Cường 11076009
Nguyễn Huynh 11076030

Tp.HCM, Tháng 5/2012

Mục lục

Mục Lục ảnh:

I. Tổng quan về security

1. Các khái niệm căn bản:

An ninh mạng ra đời với 3 mục tiêu chính:

- Đề phòng (prevention), ngăn chặn các cuộc tấn công bằng các chính sách an ninh, đây là trường hợp tốt nhất, vì hệ thống của chúng ta vẫn được đảm bảo an toàn, kẻ tấn công chưa gây ra tác động thay đổi nào đối với hệ thống.
- Phát hiện (detection) ra kẻ tấn công khi các chính sách an ninh bị vi phạm. Trong trường hợp này, hệ thống có thể đã bị tác động, thay đổi nhưng vẫn làm việc bình thường, kẻ xâm phạm bị phát hiện, hệ thống và những người quản trị có các phản hồi hợp lý để kịp thời xử lý các vi phạm và ngăn chặn kẻ tấn công.
- Phục hồi (recovery) hệ thống: dừng một cuộc tấn công, đồng thời sửa chữa khắc phục sự cố để hệ thống tiếp tục hoạt động. Hệ thống có thể đã bị tác động, thay đổi không mong muốn do cuộc tấn công gây ra trước khi được sửa chữa khắc phục.

Về mặt an toàn thông tin, an toàn dữ liệu, an ninh mạng phải đảm bảo các yếu tố sau:

- Tính bảo mật (confidentiality): những người có quyền mới được thấy nội dung dữ liệu. Để đạt được yêu cầu này, dữ liệu sẽ được mã hóa trước khi gửi, bên nhận sẽ giải mã để lấy được nội dung dữ liệu.
- Tính toàn vẹn (Integrity): Dữ liệu phải được giữ nguyên vẹn, và chỉ các quá trình điều khiển có thẩm quyền mới được thay đổi dữ liệu.
- Tính sẵn sàng (availabity): Dữ liệu phải luôn ở trạng thái sẵn sàng khi cần thiết.

Về mặt con người và hoạt động của họ, có những mối quan tâm sau:

- Xác thực người dùng (authentication): đảm bảo rằng người dùng chính xác là bản thân họ chứ không phải là ai khác. Có nhiều kĩ thuật được sử dụng để xác thực người dùng: sử dụng password , sinh trắc học (nhận diện vân tay, khuôn mặt), dùng thẻ thông minh hoặc các chứng nhận. Trước khi bắt đầu một dịch vụ, sẽ có một cơ chế để xác thực người dùng, phổ biến nhất là sử dụng mô hình đăng nhập bằng tên người dùng (user name) và mật khẩu (password). Xác thực liên quan mật thiết với vấn đề cấp quyền cho người dùng.
- Sự cấp quyền (authorization): cho phép người dùng được truy cập dữ liệu nào hoặc dịch vụ nào đó mà họ được phép. Sự cấp quyền xác định xem, một tác vụ có được phép thực thi đối với người dùng đang yêu cầu tác vụ này hay không. Hiện tại, vấn đề cấp quyền thường dựa trên các thông tin lưu tại máy chủ, và phổ biến nhất là sử dụng danh sách điều khiển truy cập, Access Control Lists (ACL), tương ứng với file và thư mục. Danh sách điều khiển truy cập là các tập tin liệt kê các cá nhân có quyền đăng nhập vào một tài khoản, hay các tập tin cấu hình ghi tên các người dùng được phép truy cập, thực thi tác dụng nào đó trên một node (node có thể xem tương ứng với một máy tính). Trọng hệ thống phân bố, sự cấp quyền còn hỗ trợ cơ chế ủy quyền (delegation), trong trường hợp này, người dùng hoặc process trong thẩm quyền của mình, có thể cấp quyền cho một người dùng khác hoặc process khác mà mình tin tưởng thực thi tác vụ tại một node nào đó, hoặc một process nào đó.

- Sự đảm bảo (assurance): Chắc chắn rằng hệ thống an ninh hoạt động đúng đắn. Ngược lại với cơ chế cấp quyền – nhà cung cấp dịch vụ quyết định xem một tác vụ có được phép thực thi với phạm vi quyền hạn của người dùng đó hay không; cơ chế đảm bảo cho phép người yêu cầu dịch vụ lựa chọn nhà cung cấp thỏa mản các tiểu chuẩn của mình về an ninh, sự tin cậy, và những đặc tính khác. Cơ chế đảm bảo thường được hiện thực thông qua chứng chỉ (certificate) được kí xác nhận bởi một bên thứ 3, bên thứ 3 này phải được người dùng biết và tin tưởng thì chứng chỉ mới hợp lệ.
- Chống thoái thác (non-repudiation) :Người dùng không thể phủ nhận hành động họ đã thực hiện.
- Sự kiểm tra (auditability): Ghi nhận lại người dùng đã làm gì đối với dữ liệu hoặc sử dụng dịch vụ nào. Nhờ vậy, trong trường hợp có sự đột nhập, người điều hành hệ thống có thể xác định chính xác những gì đã thực thi và bằng tên đăng nhập của người dùng nào.

Ngoài ra còn một số mối quan tâm khác như:

- Sự tín nhiệm (trust): Người dùng có thể tin tưởng giao cho hệ thống thực thi một tác vụ quan trọng nào đó một cách an toàn, như xử lý, lưu trữ và trao đổi các dữ liệu nhạy cảm.
- Tính đáng tin cậy của hệ thống (reliability): Cần đảm bảo rằng hệ thống sẽ thực thi điều gì bạn muốn, và khi bạn muốn. Ngoài ra hệ thống không làm gì thêm.
- Tính riêng tư (privacy): trong một chừng mực nào đó, không ai có thể biết được người dùng là ai và đang làm gì.

2. Mật mã hóa (Cryptography)

Mật mã hóa là phương tiện phổ biến nhất cung cấp cơ chế an ninh, mật mã hóa được sử dụng với 4 mục tiêu chính:

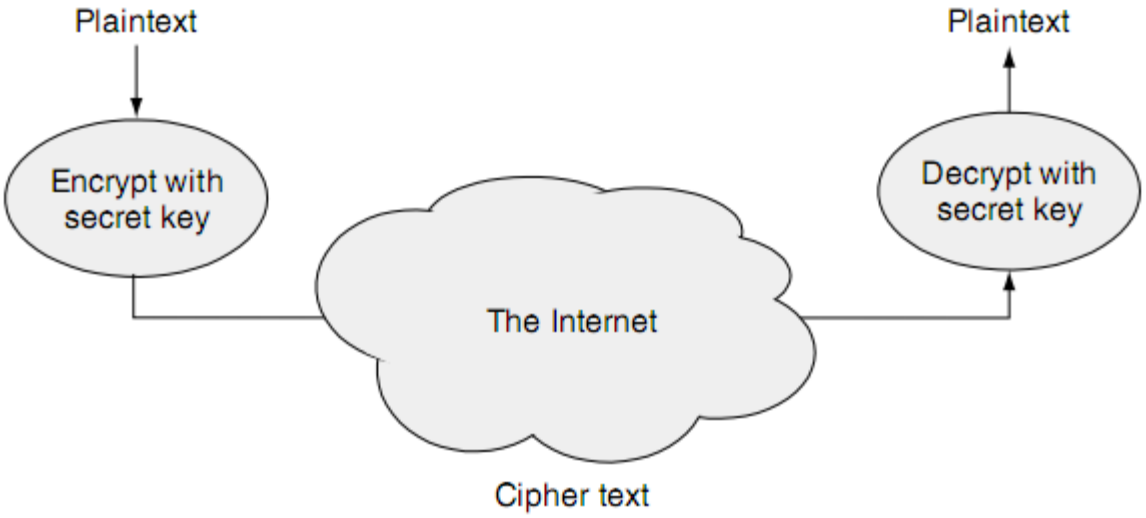
- Tính bảo mật thông điệp (message confidentiality): Chỉ người nhận có quyền mới có thể lấy được nội dung thông điệp đã được mã hóa khi gửi.
- Tính toàn vẹn thông điệp (message integrity): người nhận có thể xác định được liệu thông điệp có bị thay đổi trong quá trình truyền tải hay không.
- Xác thực phía gửi (sender authentication): Người nhận có thể xác định được người gửi, và xác định thông điệp mình nhận được chính xác là từ phía người gửi mà mình mong muốn (chứ không phải là một người khác mạo nhận và gửi thông điệp này).
- Chống thoái thác đối với bên gửi (sender non-repudiation): Bên gửi không thể phủ nhận là mình đã gửi thông điệp một khi họ đã thực hiện việc gửi.

Thông thường, không phải hệ thống nào cũng hiện thực đầy đủ tất cả các mục tiêu trên.

a. Hệ thống mã hóa đối xứng (symmetric cryptosystems):

Trong hệ thống mã hóa đối xứng, dữ liệu được mã hóa bằng một khóa (encrypted key) trở thành các ký hiệu không thể đọc được. Các ký hiệu này chỉ có thể đọc được khi giải mã trở thành dạng ban đầu bằng khóa đã dùng để mã hóa. Ngoài việc bảo vệ tính bảo mật của dữ liệu, mật mã hóa còn bảo đảm tính toàn vẹn dữ liệu. để thực hiện điều này, ta thêm vào phần tổng kiểm tra (checksum) trước khi mã hóa; bên nhận khi nhận được thông điệp sẽ kiểm tra lại checksum này sau khi giải mã. Hình 1.1 minh họa một hệ thống mã hóa đối xứng.

Một trong những phương pháp mã hóa đối xứng nổi tiếng là DES (Data Encryption Standard): DES gồm 2 thành phần: một giải thuật và một khóa. Giải thuật của DES gồm nhiều vòng lặp, mỗi vòng lặp thực hiện việc hoán đổi và thay thế dữ liệu. DES dùng chung một khóa cho việc mã hóa và giải mã dữ liệu. Giải thuật của DES được công khai rộng rãi, vì vậy nếu một người biết khóa tương ứng thì có thể lấy được nội dung thông điệp.



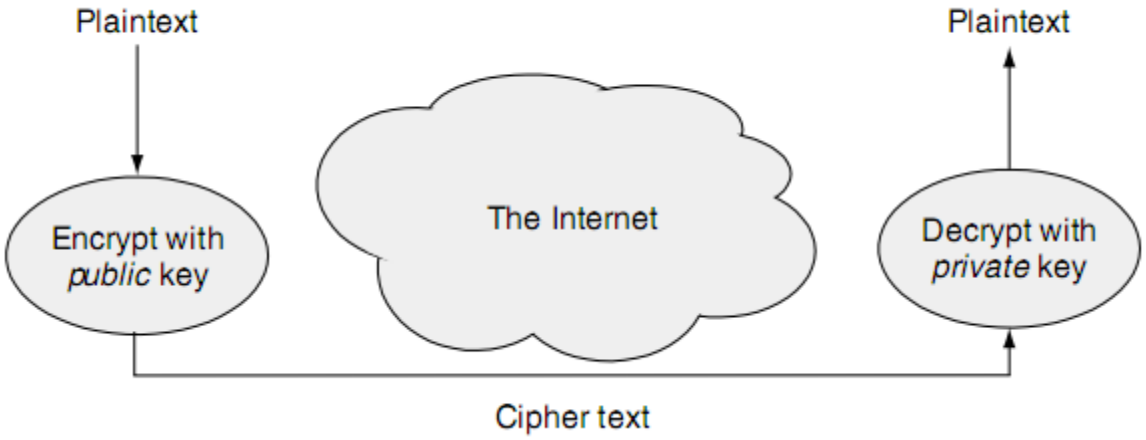
Hình 1.1: Hệ thống mã hóa khóa đối xứng

b. Hệ thống mã hóa bất đối xứng (Asymmetric cryptosystems):

Trong hệ thống mã hóa bất đối xứng, việc mã hóa và giải mã được thực hiện dựa trên một cặp khóa. Cặp khóa này được sinh ra bởi một giải thuật, tuy nhiên ngoại trừ người tạo ra cặp khóa, những người khác nếu biết thông tin một khóa thì khó có thể suy luận được khóa còn lại. Trong 2 khóa, có 1 khóa được công bố cho mọi người biết gọi là khóa công khai, khóa còn lại được giữ bí mật gọi là khóa riêng. Điểm thuận lợi của hệ mã hóa bất đối xứng là khóa công khai có thể được công bố cho mọi người biết. Việc giải mã để lấy nội dung thông điệp chỉ có thể được thực hiện bởi người sở hữu khóa riêng.

Mã hóa bất đối xứng còn được gọi là mã hóa khóa công khai (public-key cryptography).

Một trong những hệ thống mã hóa khóa công khai nổi tiếng là RSA. RSA cho phép xác thực, mã hóa dựa trên 2 khóa: một khóa riêng và một khóa công khai, cặp khóa này được sinh ra dựa trên các phép tính toán học. Việc sử dụng cặp khóa này tương tự như đã đề cập bên trên. Hình 1.2 minh họa một hệ thống sử dụng cặp khóa công khai.



Hình 1.2: hệ thống mã hóa khóa công khai

c. Chữ ký điện tử (digital signatures):

Tính toàn vẹn thông điệp được đảm bảo bằng hệ mã hóa bất đối xứng thông qua chữ kí điện tử, giúp xác thực các thông tin số. Chữ ký điện tử là môt chuỗi các bit tuân theo một tiêu chuẩn nào đó.

Hầu hết chữ kí điện tử hoạt động dựa trên hệ mã hóa bất đối xứng. Khi bên gửi muốn gửi một thông điệp và cần chứng minh mình là chủ thể gửi đi thông điệp này, bên gửi sẽ mã hóa thông điệp dùng khóa riêng của mình, rồi gửi kèm phần mã hóa này với thông điệp gốc. Bên nhận dùng khóa công khai của bên gửi để giải mã phần thông điệp đã mã hóa và so sánh với thông điệp gốc, bằng cách này bên nhận có thể xác nhận được bên gửi vì chỉ bên gửi mới biết khóa riêng tương ứng với khóa công khai trên để có thể mã hóa thông điệp. Thường thông điệp sẽ được hash trước khi mã hóa, bằng cách này, việc mã hóa sẽ nhanh hơn và chữ kí điện tử sẽ ngắn hơn giúp làm giảm kích thước toàn thông điệp gửi.

d. Chứng chỉ dựa trên khóa công khai (Public-key certificate):

Chứng chỉ dựa trên khóa công khai là một tập tin gồm khóa công khai, thông tin định danh như tên, cùng với chữ ký của tổ chức cấp chứng thực (Certificate Authority (CA)) trên tất cả các thông tin trên. CA là người đảm bảo khóa công khai trong chứng chỉ thuộc về người có tên trong chứng chỉ.

Chứng chỉ cần thiết trong hệ thống mã hóa khóa công khai. Vì mỗi người đều có thể tạo cho mình cặp khóa công khai-riêng tư, nên trường hợp sau có thể xảy ra nếu chứng chỉ không được sử dụng: người gửi gửi thông tin riêng tư được mã hóa với khóa công khai của bên nhận mà người gửi biết, tuy nhiên, một người thứ ba giả mạo người nhận, tự nhận rằng mình là người mà người gửi đang cần trao đổi thông điệp cùng với khóa công khai của người đó, nếu người gửi tin vào điều này thì thông tin có thể bị lộ với người thứ 3 đang giả mạo bên nhận vì họ biết khóa bí mật tương ứng với khóa công khai mà họ cung cấp cho bên gửi. Khi có sự can thiệp của tổ chức cấp chứng thực, kiểu tấn công này có thể được ngăn chặn. Trên diện rộng, có thể có nhiều tổ chức cấp chứng chỉ, nên một người có thể không biết hoặc không tin một tổ chức cấp chứng chỉ của một người khác. Để đảm bảo tính tin cậy của

chứng chỉ, mỗi chứng chỉ có thể gồm khóa công khai của CA cùng với chữ ký của CA cấp cao hơn. Quá trình này dẫn tới một cây phân cấp chứng chỉ và đồ thị phức tạp biểu diễn mối quan hệ tin tưởng.

Hạ tầng khóa công khai (Public Key Infrastructure – PKI) là một phần mềm quản lý chứng chỉ. Trong hệ thống X.509 PKI, sự phân cấp chứng chỉ được tổ chức thành một cây theo chiều từ trên xuống, trong đó chứng chỉ gốc nằm ở đỉnh của cây, và đại diện cho CA nổi tiếng rộng rãi mà người dùng không cần phải xác thực CA này. Một chứng chỉ có thể bị thu hồi nếu khóa bí mật tương ứng của nó bị lộ tẩy. Trong trường hợp này, trước khi sử dụng chứng chỉ, ta cần xem xét danh sách các chứng chỉ bị thu hồi. Chứng chỉ gồm các thành phần sau:

- Một khóa công khai được ký;
- Một tên, có thể là tên người, tên máy tính hoặc tên một tổ chức;
- Thời hạn có hiệu lực của chứng chỉ;
- Địa chỉ URL của danh sách thu hồi.

Chứng chỉ phổ biến nhất là ITU-T X.509, là một file dễ hiểu có cấu trúc như sau:

- Chủ thể: là tên người dùng;
- Khóa công khai của chủ thể: gồm khóa và thông tin khác liên quan tới khóa như giải thuật dùng để sinh khóa;
- Chủ thể cấp chứng chỉ: tên của CA.
- Chữ ký điện tử: ký trên tất cả các thông tin của chứng chỉ và dùng khóa riêng của CA.

Để xác nhận chữ ký điện tử này, tra cần khóa công khai của CA, thông tin này có thể tìm thấy trong chứng chỉ của CA.

e. Tổ chức cấp chứng chỉ (Certificate Authority - CA):

Tổ chức cấp chứng chỉ cấp phát các chứng chỉ, công khai các chứng chỉ hợp lệ để mọi người có thể truy cập sử dụng, thu hồi các chứng chỉ hết hạn hoặc bị lộ khóa riêng ứng với khóa công khai trong chứng chỉ, và cập nhật danh sách chứng chỉ bị thu hồi. CA cũng cần giữ lại thông tin các giao dịch của mình.

CA cấp phát chứng chỉ cá nhân cho người dùng, cho phép họ xác thực mình với một thực thể khác, hoặc dùng cho chữ ký điện tử của mình. CA cũng cấp phát chứng chỉ cho host và dịch vụ cho phép các host hoặc dịch vụ này xác thực mình khi kết nối vào mạng.

Một số CA cấp phát chứng chỉ nhằm xác thực CA cấp dưới của mình.

CA cấp phát chứng chỉ dựa trên khóa công khai có nghĩa là CA tin tưởng người sở hữu chứng chỉ này, và họ thực sự là bản thân họ chứ không phải ai khác giả danh. Một bên thứ ba khi sử dụng chứng chỉ của một người cần phải tin tưởng vào CA của người đó, đây là cơ chế nhằm đảm bảo danh định của người sở hữu chứng chỉ.

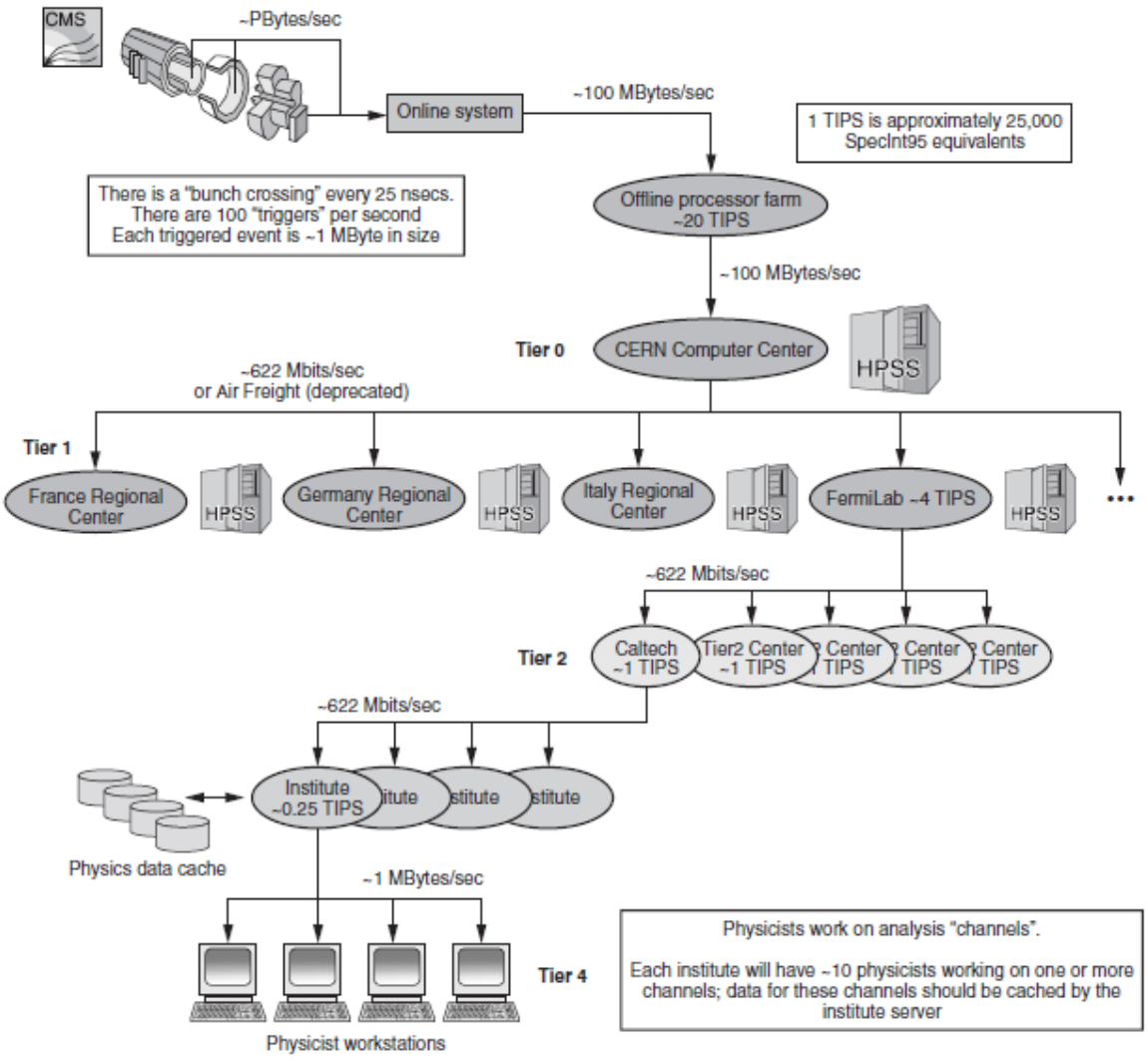
f. Tường lửa (firewalls):

Tường lửa là thành phần phần cứng hoặc phần mềm được thêm vào mạng lưới để ngăn chặn các giao tiếp bị cấm bởi chính sách quản trị của tổ chức. Có 2 loại tường lửa: truyền thống và cá nhân. Tường lửa truyền thống là một thiết bị mạng chuyên dụng hoặc máy tính đặt ở

các đường ra vào của mạng, nhằm lọc tất cả các thông tin vào hoặc ra khỏi mạng. Ngược lại, tường lửa cá nhân là một ứng dụng lọc thông tin vào và ra một máy tính đơn.
Tường lửa truyền thống thường hoạt động ở tầng mạng hoặc tầng vận chuyển trong mô hình TCP/IP. Tường lửa cá nhân hoạt động ở tầng ứng dụng trong mô hình TCP/IP.
Cấu hình đúng đắn cho một tường lửa đòi hỏi người dùng có kĩ năng, hiểu biết tốt về giao thức mạng và an ninh. Sai lầm dù nhỏ trong cấu hình tường lửa có thể làm cho tường lửa trở nên vô giá trị.

II. Nguyên lý chung của security on grid

1. Ví dụ về an ninh trên lưới:



Hình 2.1: Sự chia sẻ dữ liệu từ máy gia tốc hạt lớn(Large Hadron Collider) của CERN trong thí nghiệm Compact Muon Solenoid

Hình 2.1 minh họa một thí nghiệm trong dự án Grid, thí nghiệm Compact Muon Solenoid, cho thấy những thách thức về an ninh trong hệ thống lưới. Trong thí nghiệm này, dữ liệu thu được từ máy gia tốc hạt lớn (Large Hadron Collider) ở phòng thí nghiệm CERN tại Thụy Sĩ sẽ được hơn 2000 nhà khoa học của 150 trường đại học và phòng thí nghiệm ở 34 quốc gia tham gia phân tích.

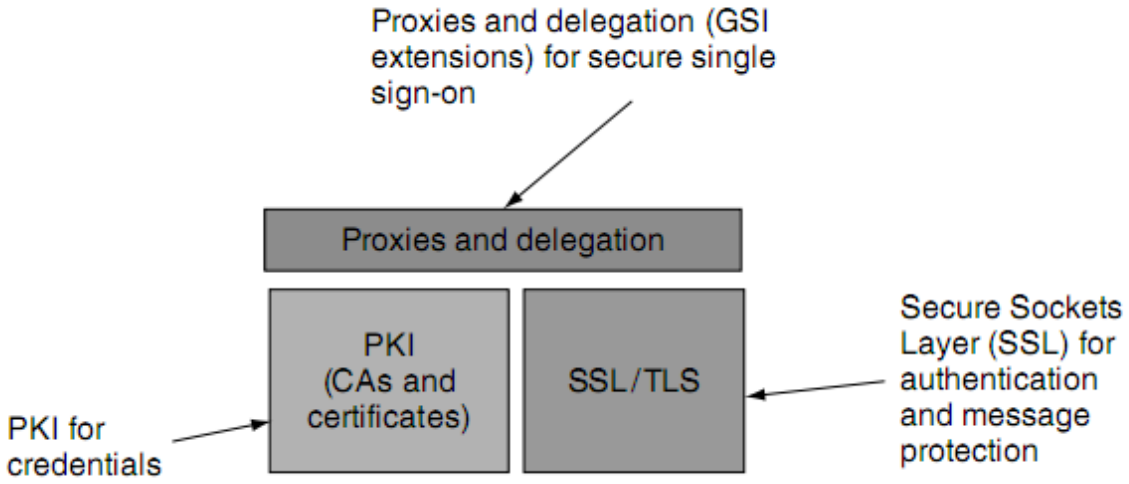
Việc chia sẻ, xử lý và ảo hóa dữ liệu, các tài nguyên máy tính, mạng đưa đến các đòi hỏi phức tạp về lưu trữ, băng thông và sức mạnh tính toán. Các đòi hỏi an ninh cũng phát sinh tương ứng:

- Dữ liệu sẽ di chuyển và được truy cập từ nhiều trung tâm ở các quốc gia khác nhau với các cơ chế và chính sách an ninh khác nhau.
- Cộng đồng tham gia hệ thống lưới có thể cần truy cập dữ liệu từ nhiều tổ chức và quốc gia với các chính sách an ninh khác nhau.
- Cần thiết lập mối quan hệ tin tưởng giữa các trung tâm, các tổ chức tham gia vào hệ thống lưới, điều này đưa đến sự ra đời của chính sách truy cập từ xa với các mức độ khác nhau.
- Vấn đề toàn vẹn và bảo mật dữ liệu cần phải được bảo đảm trong quá trình truyền tải, trao đổi dữ liệu giữa các bên.
- Các vấn đề trên và còn nhiều vấn đề khác đều cần phải quan tâm, chúng có đặc điểm chung là trải rộng trên nhiều vùng quản lý khác nhau với các quyền truy cập, mức độ tin tưởng, thỏa thuận dịch vụ khác nhau.

2. Hạ tầng an ninh lưới (Grid Security Infrastructure (GSI)):

An ninh lưới dựa trên GSI, là một tiêu chuẩn của forum quốc tế về tính toán lưới (Global Grid Forum - GGF). GSI là một tập hợp các công cụ, thư viện, và giao thức được sử dụng trong Globus, và những middleware lưới (grid middleware) khác, nhằm cho phép người dùng và ứng dụng truy cập vào tài nguyên lưới một cách an toàn. GSI dựa trên hạ tầng khóa công khai – PKI, gồm tổ chức cấp chứng chỉ và chỉ chỉ X.509. GSI cung cấp các thành phần:

- Hệ hống khóa công khai;
- Xác thực tương hỗ thông qua chứng chỉ số;
- Cơ chế ủy quyền và đăng nhập một lần (single sign-on).



Hình 2.2: Hạ tầng an ninh lưới

a. Giới thiệu:

GSI là tập hợp các kĩ thuật thông dụng và đáng tin cậy. GSI cung cấp tính riêng tư, toàn vẹn dữ liệu và xác thực người dùng dựa trên chứng chỉ. Tất cả các yếu tố trên không phải luôn cần thiết trong quá trình giao tiếp, tuy nhiên, một giao tiếp an toàn dựa trên GSI ít nhất phải được xác thực. Tính toàn vẹn dữ liệu có thể được kích hoạt hoặc bỏ qua, việc mã hóa cũng tương tự, có thể được hiện thực hoặc bỏ qua tùy nhu cầu người dùng.

b. Xác thực tương hỗ thông qua chứng chỉ số:

GSI sử dụng chứng chỉ X.509 để bảo đảm việc xác thực an toàn. Xác thực tương hỗ có nghĩa là cả 2 bên tham gia trong một lần giao tiếp xác thực lẫn nhau, và cả 2 bên phải tin tưởng vào chứng chỉ của CA đã ký cho chứng chỉ của phía còn lại, tức là tin tưởng vào CA cấp chứng chỉ cho phía đối tác của mình. Ngược lại, không tồn tại sự tin tưởng và quá trình xác thực thất bại.

c. Cơ chế ủy quyền và đăng nhập một lần:

GSI cho phép người dùng tạo và ủy quyền cho các process thay mặt người dung thực thi trên các tài nguyên ở xa; điều này quan trọng khi các ứng dụng cần sử dụng nhiều tài nguyên ở các nơi khác nhau. Giấy ủy nhiệm đại diện có thời gian sống ngắn, nó cho phép người dùng chỉ cần xác thực một lần, sau đó được phép thực thi các tác vụ khác nhau mà không cần phải xác thực lại.

3. Các chế độ cấp quyền trong GSI

GSI hỗ trợ 3 chế độ cấp quyền ở cả phía máy chủ và máy khách.

Sự cấp quyền phía máy chủ: Dựa trên chế độ cấp quyền, máy chủ sẽ chấp nhận hoặc từ chối một yêu cầu an ninh.

- None: không có sự cấp quyền nào được thực hiện.

- Self: máy khách được phép sử dụng một dịch vụ lưới nếu định danh của máy khách giống với định danh của dịch vụ.
- Gridmap: tập tin gridmap chứa một danh sách những người dùng có quyền, tương tự như danh sách điều khiển truy cập ACL. Chỉ những người dùng được liệt kê trong tập tin gridmap của dịch vụ được phép gọi dịch vụ.

Sự cấp quyền phía máy khách: máy khách trong GSI có thể lựa chọn một dịch vụ ở xa hay không tùy thuộc vào tính hợp lệ của giấy ủy nhiệm an ninh.

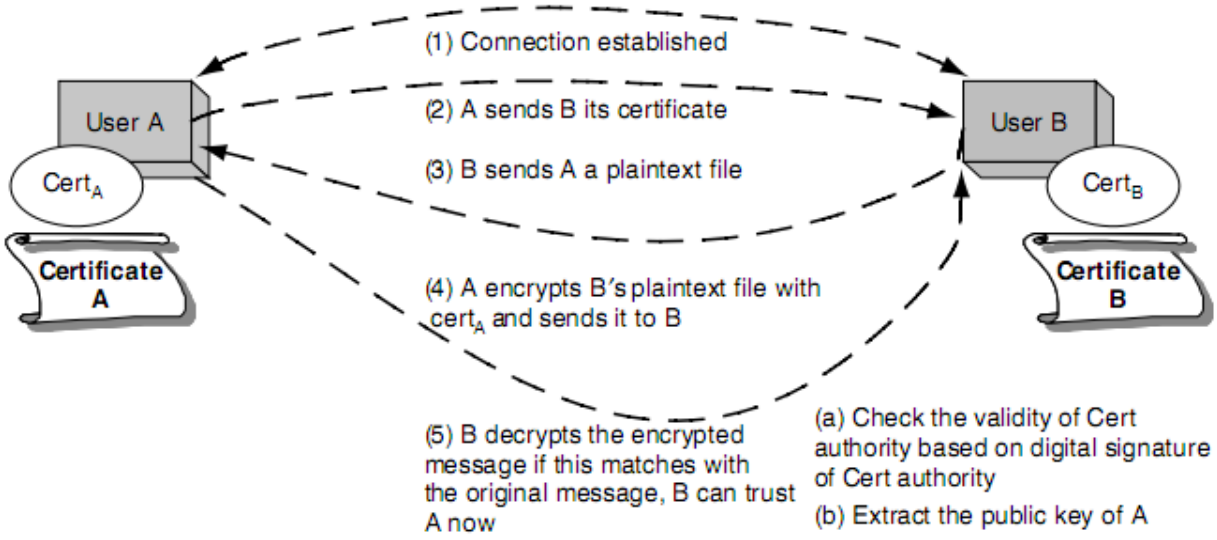
- None: không có sự cấp quyền nào được thực thi.
- Self: máy khách cho phép một yêu cầu nếu định danh của dịch vụ giống với định danh của máy khách. Nếu cả phía máy chủ và máy khách đều sử dụng chế độ phân quyền self, một dịch vụ chỉ có thể được gọi thực thi nếu định danh của nó giống với định danh của máy khách.
- Host: máy khách sẽ cấp quyền cho một yêu cầu an ninh nếu máy host trả về định danh có chứa tên của host đó. Điều này được thực hiện thông qua chứng chỉ của host.

a. Yêu cầu một chứng chỉ:

Để lấy một chứng chỉ, người dùng đầu tiên phải sinh ra cặp khóa. Khóa riêng được lưu trữ dưới dạng mã hóa và được bảo vệ bằng mật khẩu để đảm bảo tính an toàn. Khóa công khai được gửi tới CA cùng với yêu cầu chứng chỉ. CA thường gồm nhiều tổ chức đăng ký (Registration Authorities - RA). RA xác nhận lại yêu cầu xem đã hợp lý chưa: tên đăng kí phải là duy nhất đối với CA, và là tên thực sự của người dùng, sau đó CA ký trên yêu cầu chứng chỉ và cấp phát chứng chỉ này cho người dùng.

b. Xác thực tương hỗ:

GSI sử dụng Secure Sockets Layer (SSL) trong giao thức xác thực tương hỗ. Trước khi xác thực, các bên liên quan phải tin tưởng vào các CA ký trên chứng chỉ của các bên. Mỗi bên đều có chứng chỉ của bên còn lại, tức là có khóa công khai của nhau. Quá trình xác thực được minh họa trong hình:



Hình 2.3: Quá trình xác thực tương hỗ

- Bên A thiết lập kết nối với bên B. Để bắt đầu quá trình xác thực, A đưa cho B chứng chỉ của mình. Nhờ vào chứng chỉ này, B biết A là ai, khóa công khai của A, và CA nào đứng ra bảo đảm cho chứng chỉ này.
- B kiểm tra chữ ký số của CA để đảm bảo rằng chứng chỉ hợp lệ và CA thực sự ký trên chứng chỉ này chứ không phải là một ai khác giả mạo chữ ký. Ở đây, B phải tin vào CA của bên A.
- B sau đó gửi một mẫu văn bản chưa mã hóa cho A, yêu cầu A mã hóa nó và gửi lại mình.
- A dùng khóa riêng mã hóa thông điệp B yêu cầu, và gửi lại cho B. B giải mã thông điệp trên dùng khóa công khai của A. Nếu kết quả giống với thông điệp ban đầu, B biết A chính xác là người mà chứng chỉ đã ghi, và B tin tưởng vào A.
- Thao tác tương tự xảy ra theo chiều ngược lại để A xác thực B.
- Lúc này, A và B thiết lập kênh truyền với nhau và tin tưởng lẫn nhau để có thể thực hiện các giao dịch.

c. Trao đổi giấy ủy nhiệm:

Mặc định, GSI không thiết lập kênh giao tiếp mã hóa giữa các thực thể sau khi thực thi quá trình xác thực tương hỗ, nhằm giảm chi phí mã hóa. Tuy nhiên, việc trao đổi ủy nhiệm có thể được thực hiện khi cần thiết. GSI cung cấp toàn vẹn dữ liệu trong quá trình giao tiếp.

d. Bảo vệ khóa bí mật:

Khóa bí mật nên được lưu trữ trong một file, sau đó mã hóa file này bằng mật khẩu, lưu vào nơi an toàn trong máy tính. Điều này giúp đảm bảo khóa bí mật không bị lộ với một bên thứ ba không mong muốn.

e. Sự ủy thác và đăng nhập một lần:

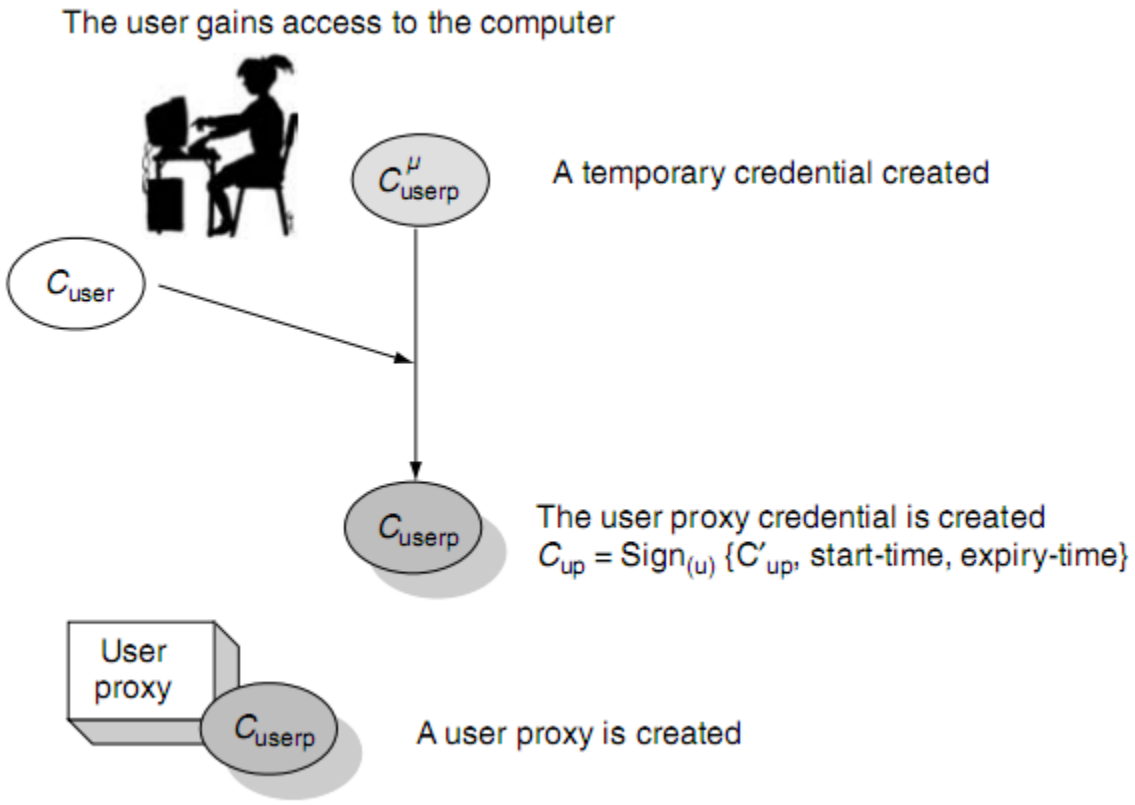
Sự ủy thác trong GSI giúp làm giảm số lần người dùng phải nhập mật khẩu khi cần thực thi một tác vụ nào khác trong chuỗi công việc của mình. Trong trường hợp một công việc cần sử dụng nhiều nguồn tài nguyên, hoặc một bên thứ ba đang đại diện cho người dùng để thực thi công việc – trên nguyên tắc, mỗi lần như vậy cần một lần xác thực tương hỗ và người dùng phải nhập mật khẩu, điều này rất mất thời gian và có thể không cần thiết trong nhiều trường hợp. Vì vậy, để tránh điều này, giấy ủy nhiệm được tạo ra để tránh sự phiền hà phải nhập lại mật khẩu nhiều lần.

Giấy ủy nhiệm gồm một chứng chỉ mới với một bộ khóa công khai - khóa bí mật mới. Chứng chỉ mới này chứa định danh của người sở hữu, và bổ sung thêm một số thông tin cho biết đây là giấy ủy nhiệm. Lần này, chủ sỡ hữu ký trên chứng chỉ mới. Chứng chỉ cũng chứa thông tin về thời gian mà chứng chỉ đại diện này tồn tại, sau thời gian này, chứng chỉ đại diện hết hiệu lực và không có giá trị sử dụng nữa. Chứng chỉ đại diện do đó có thời gian sống giới hạn, thời gian sống của chứng chỉ đại diện phải nhỏ hơn chứng chỉ gốc.

Khóa bí mật của bên ủy nhiệm phải được giữ an toàn. Vì khóa này không tồn tại lâu, nó thường được lưu trên hệ thống file cục bộ và không cần phải mã hóa. Khi giấy ủy nhiệm

được tạo ra và lưu trữ, người dùng có thể sử dụng chứng chỉ đại diện và khóa bí mật cho những lần xác thực tương hỗ mà không cần phải nhập mật khẩu.

Việc xác thực tương hỗ có khác biệt khi giấy ủy nhiệm được sử dụng. Phía liên quan nhận được chứng chỉ của bên đại diện (chứng chỉ này được người sở hữu gốc ký) cùng với chứng chỉ của người sở hữu gốc. Trong suốt quá trình xác thực tương hỗ, khóa công khai của chủ sở hữu được sử dụng để đánh giá tính hợp lệ của chứng chỉ đại diện. Sau đó, khóa công khai của CA tiếp tục được dùng để đánh giá chứng chỉ của người sở hữu. Điều này tạo ra một chuỗi tin tưởng từ CA tới bên đại diện thông qua người chủ sở hữu, trong đó bên đại diện thay mặt cho chủ sở hữu trong khoảng thời gian sống quy định trên chứng chỉ đại diện.



Hình 2.4: Quá trình tạo giấy ủy nhiệm

4. Các vấn đề còn tồn tại với an ninh trên lưới:

a. Vấn đề trong xác thực:

Trên Grid, cả 2 phía xác thực thông qua khóa công khai được chứng nhận bởi CA. Vấn đề có thể phát sinh nếu CA xác định nhầm định danh của một người, việc này có thể xảy ra nếu kẻ giả mạo cung cấp đủ bằng chứng để yêu cầu CA cấp chứng chỉ, hoặc do sự thiếu sót phía CA khi cấp phát chứng chỉ bị kẻ mạo danh lợi dụng. Vì vậy, CA nên công khai chính sách của mình đề người dùng biết được họ hoạt động như thế nào, và mức độ tin tưởng đến mức nào.

b. Vấn đề với bên đại diện (Proxies):

Cơ chế ủy quyền cho bên đại diện hữu dụng trong quyền cấp quyền cục bộ mà không cần liên hệ với người dùng cho mỗi thao tác trên các tài nguyên hoặc dịch vụ ở xa. Tuy nhiên có một số trở ngại có thể ảnh hưởng đến an ninh trên lưới:

- Khóa bí mật của bên đại diện được lưu trữ trên hệ thống ở xa ngoài tầm quản lý trực tiếp của người dùng. Tuy nhiên, khóa này lại được sử dụng để ký trên thông điệp mà hạ tầng lưới tin tưởng như thể do người dùng ký trực tiếp.
- Khi tạo chứng chỉ đại diện, người dùng thực hiện các thao tác tương tự CA trên giấy ủy nhiệm; tuy nhiên, người dùng không phát hành chính sách cấp chứng chỉ hay quá trình thu hồi chứng chỉ.

Nếu hệ thống ở xa bị thỏa hiệp, khóa bí mật của bên đại diện sẽ bị lộ, nếu người dùng biết được điều này, vẫn không có quá trình thu hồi chứng chỉ. Một số hiện thực của lưới giảm nguy cơ trên bằng cách quy định thời gian sống của giấy ủy quyền ngắn. Tuy nhiên vấn đề vẫn có thể xảy ra và gây ra hậu quả không mong muốn.

c. Vấn đề cấp quyền:

Cấp quyền là cơ chế quyết định xem người dùng có quyền sử dụng dịch vụ nào, ở mức độ nào. Trong hệ thống lưới, thường người chủ của dịch vụ cấp phát quyền cho người dùng, bằng cách ánh xạ định danh của người dùng lên một tài khoản cục bộ, và quy định các dịch vụ tương ứng với tài khoản đó. Vấn đề là với mỗi người dùng, dịch vụ hoặc tài nguyên, cần có một chỉ mục trong tập tin gridmap, số lượng này có thể rất lớn, và nhà quản trị hệ thống không thể điều khiển trực tiếp mà chuyển sang cơ chế cấp quyền mặc định cho hầu hết người dùng, và lỗ hổng bảo mật có thể khai thác vì điều này.

Khi người dùng được cấp phát quyền càng nhiều, dịch vụ hoặc tài nguyên càng dễ dàng bị thỏa hiệp. Nếu giấy ủy quyền của người dùng bị đánh cắp và không thu hồi kịp thời, các dịch vụ và tài nguyên có thể trong tình trạng nguy hiểm.

III. Hiện thực về bảo mật của grid

Phần này của bài báo cáo trình bày về hiện thực về bảo mật của hai middleware thông dụng nhất hiện nay là unicore, phiên bản 6 và globus, phiên bản 4.

Một số thuật ngữ kỹ thuật được trình bày trong phần báo cáo này gồm có:

certificate: Chứng chỉ dùng cho xác thực.

CA: Tổ chức cung cấp các chứng chỉ.

RA: Tổ chức đăng ký chứng chỉ.

PKI (Public key infrastructure): Là một hệ thống các qui tắc nhằm thiết lập khả năng quản lý khóa công khai như định dạng, cấp, xác thực, thu hồi, quản lý, lưu trữ.

Site: Unicore quản lý hạ tầng của mình theo cách phân loại thành từng khu vực (site) riêng biệt.

certificate revocation lists: Danh sách các chứng chỉ đã bị thu hồi bởi CA.

Gateway: Mỗi site trong unicore được đại diện bởi một gateway.

CSR (certificate signing request): Trong hạ tầng mã hóa khóa công khai, CSR được tạo ra bởi ứng dụng và gửi tới CA nhằm yêu cầu xác thực.

SOAP (Simple object access protocol): Chuẩn đưa ra nhằm định nghĩa cấu trúc hiện thực của một web service để truyền tải qua mạng.

GRAM: Một thành phần nằm trong grid dùng để xác định, truyền tải, quản lý, thu hồi các job trên hạ tầng lưới.

Grid-mapfile: Tập tin lưu trử trong Globus Toolkit nhằm chứa các chứng chỉ ứng với từng người dùng cụ thể.

GridFTP: Một phương pháp truyền tải dữ liệu được định nghĩa trong Globus Toolkit nhằm cung cấp khả năng truyền tải dữ liệu đạt hiệu quả cao, an toàn, tin cậy dùng trong grid được hiện thực dựa trên giao thức FTP.

Web service: Chuẩn hiện thực các ứng dụng hoạt động trên nền web.

SAML (Security Assertion Markup Language): Ngôn ngữ đặc tả dựa trên chuẩn XML nhằm truyền tải các thông tin về xác thực và phân quyền giữa các phân vùng trên mạng.

OASIS (Organization for the Advancement of Structured Information Standards): Tổ chức toàn cầu làm nhiệm vụ thúc đẩy sự phát triển và thống nhất các tiêu chuẩn dịch vụ web thông qua sự hợp tác giữa các doanh nghiệp lớn trong nghành.

TLS (Transport layer security): Là một giao thức cung cấp khả năng truyền tải thông tin bảo mật qua mạng internet.

X.509 Certificate: Là một hiện thực cho PKI nhằm cung cấp khả năng quản lý các khóa công khai, các chứng chỉ, định dạng các khóa và chứng chỉ.

CAS (Central Authentication Service): Cung cấp khả năng quản lý đăng nhập trên nhiều ứng dụng mạng khác nhau thông qua việc cho phép đăng nhập một lần duy nhất vào hệ thống.

1. Hiện thực security trên unicore

Trong phần này của báo cáo tập trung vào cơ chế xác thực của Unicore dựa trên hạ tầng mã hóa khóa công khai theo tiêu chuẩn của x.509. Phần báo này dựa trên bài báo “An analysis

of Unicore Security model" của tác giả T. Goss-Walter và các cộng sự. Trong phần báo cáo này đề cập tới mô hình PKI mà Unicore áp dụng, chính sách một U-CA duy nhất và nhiều RA, cách thức bảo mật của một ứng dụng khi thực hiện tác vụ trong Unicore.

a. Unicore public key infrastructure (U-PKI)

Trong hệ thống Unicore việc hiện thực về bảo mật được dựa trên mô hình PKI hay còn gọi là U-PKI. U-PKI được hiện thực dựa trên mô hình X.509 với một CA và nhiều RA.

Hạ tầng xác thực của U-PKI gồm có:

- Một Trust Root CA.
- Một Unicore CA.
- Certificate revocation lists (CRLs) của Root CA và U-CA.
- Các Unicore RA.
- Gateway certificates cho mỗi Unicore Gateway
- NJS certificate nhằm phân phối các job con cho các Unicore V-site.
- Client hoặc user certificate cho các user đã được chấp nhận vào hệ thống.

Mục tiêu ban đầu của Unicore là xây dựng một VO (Virtual Organization) được tạo thành từ các trung tâm tính toán lớn, các phòng ban, viện nghiên cứu và các trang web bao gồm cả công khai và nội bộ.

Các site trong cùng một VO được kết nối thông qua một hạ tầng mạng chung và phổ biến, do đó nảy sinh các vấn đề về bảo vệ tính toàn vẹn, riêng tư của dữ liệu khi được truyền tải qua mạng internet.

Để đảm bảo tính an toàn của dữ liệu và xác thực người dùng, Unicore sử dụng mô hình PKI với chứng chỉ (certificate) được dùng nhằm:

- Xác thực người dùng.
- Xác thực các Unicore Gateway.
- Xác thực các NJS (dùng để phân phối các sub-jobs)
- ký xác thực các job và các software.

Trong mô hình xác thực của Unicore, có hai tầng xác thực với tầng đầu tiêng bao gồm Root CA và U-CA. Root CA đóng vai trò là CA được tin tưởng tuyệt đối và có chức năng xác thực cho Unicore CA. Tuy nhiên Root CA lại hoạt động độc lập và không thuộc về hệ thống Unicore, Root CA chịu trách nhiệm xác thực cho U-CA và đảm bảo tính toàn vẹn của U-CA. CRL của Root CA có trách nhiệm thu hồi các certificate được ký bởi Root CA cũng như bởi U-CA.

Unicore CA trong mô hình hiện tại là một CA độc lập và là trung tâm của cộng đồng Unicore. Chứng chỉ của Unicore CA được ký xác thực bởi root CA và có thể dùng để chứng thực các user và các server còn lại trong hệ thống. U-CA còn sở hữu một CRL riêng nhằm thực hiện thu hồi các chứng chỉ đã quá hạn sử dụng hoặc bị vi phạm về bảo mật. Trong Unicore các Root CA, U-CA và các CRL tương ứng của chúng đều có thể được truy cập bởi người dùng. Các chứng chỉ ở tầng thấp hơn chỉ có thể có giá trị nếu chứng chỉ ở tầng cao hơn chúng trong trường hợp này là của U-CA và Root CA là có giá trị.

Tầng thấp hơn trong mô hình chứng thực của Unicore là user, Gateway và NJS, chúng được ký bởi U-CA và cũng có thể được thu hồi bởi U-CA khi hết hiệu lực. Certificate của user được sử dụng khi muốn xác thực với gateway trên site mục tiêu nhằm thực thi các job, chứng thực (endorse) job thông qua việc ký bằng khóa riêng của mình hoặc ủy quyền (consign) các job tới một site trong hệ thống. Một cách hình tượng, chứng chỉ của User trong hệ thống Unicore tương đương với chứng minh thư điện tử của user đó.

Đối với Gateway, certificate được dùng để xác thực Gateway với user. Khi thực hiện đăng nhập từ xa vào một Unicore site (U-Site), người dùng cần phải xác thực Gateway muốn sử dụng, trong trường hợp này phía người dùng chỉ kiểm tra tính xác thực của chử ký được dùng để tạo nên certificate cho gateway. Người dùng trong quá trình xác thực này không biết đến khóa công khai của gateway.

Một loại khác của xác thực người dùng là sử dụng NJS Certificate để thiết lập các kết nối SSL tới các V-Sites (Virtual sites) và consign các sub-job ở đây. Các chứng chỉ dạng NJS Certificate trong trường hợp này dùng để chứng thực các NJS với các site mục tiêu.

Chi tiết về hiện thực của U-CA được trìn bày ở phần tiếp theo của báo cáo.

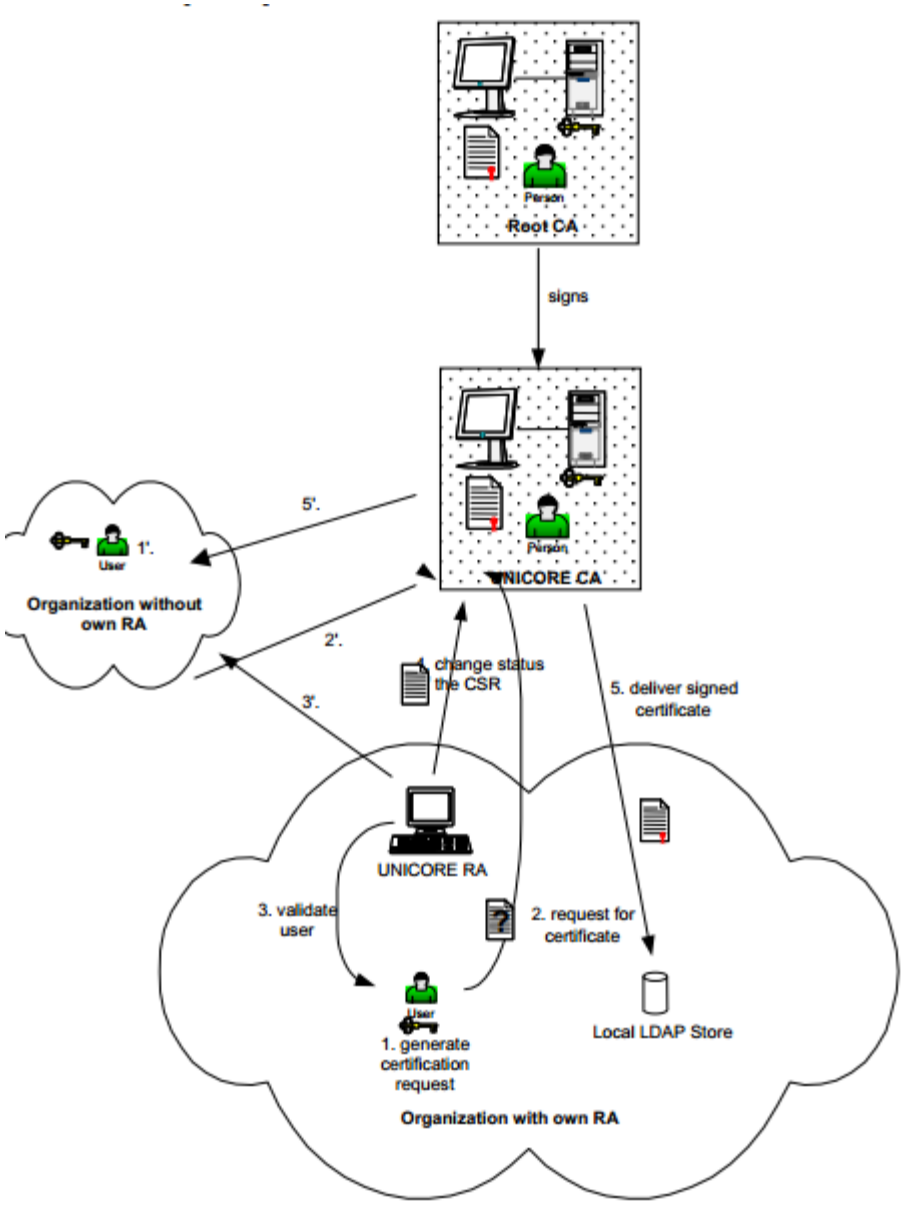
b. Kiến trúc của CA và RA.

Khả năng bảo mật của PKI được quyết định bởi ba yếu tố:

- Mức độ tin tưởng của việc xác thực người dùng thực hiện bởi RA trước khi các certificate được cấp phát cho người dùng.
- Mức độ an toàn của khóa riêng của người dùng được cất giử ở phía client.
- Mức đô tin cậy đối với chuỗi thao tác xác thực các certificate và khả năng CRL thực hiện xác thực cho từng kết nối.

Việc định danh người dùng thực hiện thông qua RAs bằng các kiểm tra ID card của người dùng. Mỗi đối tác trong hệ thống Unicore đều có sở hửu riêng một RA, được chứng nhận bởi U-CA, các đối tác nhỏ hơn không thể tạo riêng một RA có thể sử dụng RA của đối tác khác. Các bước để thông qua một chứng nhận cho người dùng gồm có:

- Người dùng tạo ra một một certificate signing request (CSR) với một cặp khóa bí mật và khóa công khai. Khóa bí mật được lưu trong kho chứa của client.
- CSR được gởi tới RA phù hợp. RA chỉ ra các thực hiện cách thực hiện xác thực cho người dùng. Xác thực có thể thực hiện thông qua: định danh trực tiếp (người dùng trực tiếp tới gặp RA) hoặc gián tiếp (thông qua video conferencing).
- RA xác thực người dùng và CSR của người dùng. Trong mô hình xác thực hiện tại chỉ có xác thực trực tiếp là được sử dụng.
- RA chuyển tiếp CSR tới U-CA. U-CA ký và tạo chứng chỉ cho CSR gởi trở lại cho user.



Hình 3.1: Quá trình cung cấp certificate trong Unicore

c. Quá trình bảo mật của một ứng dụng khi thực thi trong grid:

Một khi chứng chỉ đã được khởi tạo và phân phối tới user và site thích hợp. Các kết nối và phân phối các job có thể được bắt đầu. Có hai dạng thực thi có thể được thực hiện bởi user và server:

- Thiết lập một kênh kết nối sử dụng SSL.
- Endorsing (xác nhận) các AIOs (Unicore jobs) bằng cách ký xác thực trên chúng.
- Trước khi khởi chạy Unicore tất cả các đối tác trong hệ thống phải lấy về các chứng nhận của U-CA và root CA để có thể xác thực các chứng nhận của client và server về sau này.

Các kịch bản hoạt động có thể gồm:

- Thiết lập các kết nối SSL từ user side tới unicore side (hay target side). Khi site cần xác thực lẫn nhau thông qua các chứng nhận của mỗi bên.
- Endorse Unicore jobs: người dùng có thể chứng thực các job của mình bằng cách ký dùng khóa bí mật của mình. Chử ký này sau đó có thể xác thực thông qua chứng nhận của người dùng, chứng nhận được gửi kèm như một phần của job.
- Consign sub-jobs: Các NJS thực hiện consign các sub-jobs bằng cách phân phối chúng thông qua các SSL tới các V-Site phù hợp.

Ngoài ra trong mô hình của Unicore còn thực thiện ủy quyền (delegation) thông qua SAML assertions. Theo đó một thành phần phụ thêm được thêm vào header trong tệp SOAP được gửi đi tới các site mục tiêu.

d. Quá trình xác thực quyền của người dùng

Trước khi người dùng có thể thực submit các AJOs lên target system, người dùng cần thực hiện truy cập và xác thực người dùng cũng như xác thực quyền hạn của người dùng tại target site. Có hai thao tác cần được thực thi tại target site:

- User authentication: Dùng để thực hiện thiết lập kết nối SSL tới target site. Người dùng Unicore phải trình ra chứng chỉ xác nhận bản thân và Gateway trên target site cũng phải trình ra chứng chỉ xác nhận tương tự.
- User authorization: Trước khi người dùng có thể submit job lên trên target site, người dùng cần phải thực hiện xác thực quyền. NJS của target site thực hiện xác thực định danh của người dùng trên AJO thông qua cơ sở dữ liệu của Unicore (Unicore user database – UUDB).

2. Hiện thực security trên Globus

Globus toolkit hiện thực bảo mật theo chuẩn GSI, theo đó cho phép việc bảo mật ở tranport-lever và message-lever. GT4.0 hiện thực bảo mật cho web service (ws) và pre web service (pre-ws). Trong bài báo cáo này tập trung chủ yếu cho web service, pre-ws sử dụng cùng một cơ chế authentication tương tự như ws nhưng chi tiết về hiện thực của ứng dụng và chuẩn bảo mật của thông điệp nằm ngoài phạm vi của báo cáo này.

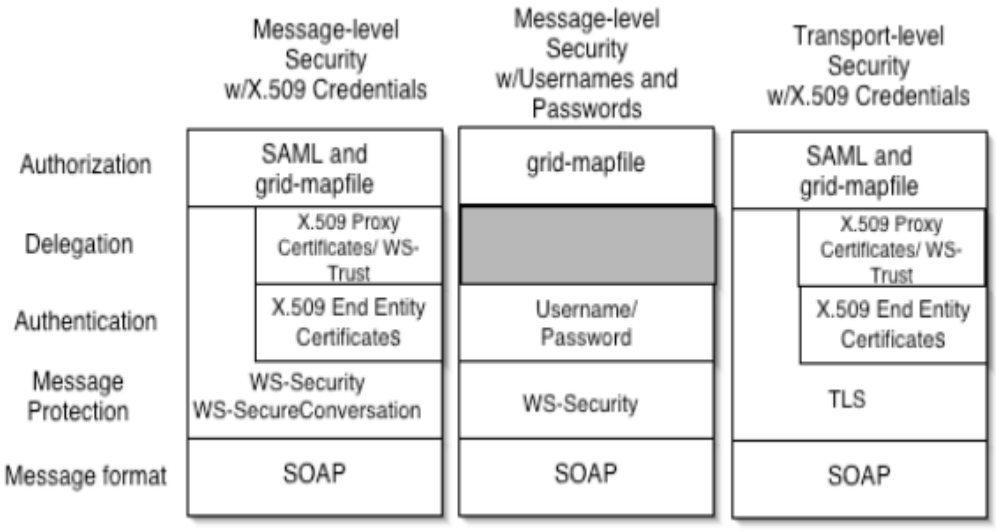
a. Transport-level và message-level Security:

GT4.0 hỗ trợ bảo mật ở tầng transport-level và message-level ở phiên bản hiện tại và cả cho những phiên bản tiếp theo. Bảo mật ở tầng message-level nhằm cung cấp khả năng bảo mật theo chuẩn WS-Security và WS-secureConversation nhằm bảo vệ nội dung thông điệp cho các SOAP message. Bảo mật ở tầng transport-level nhằm cung cấp khả năng xác thực thông qua TLS/SSL được hổ trợ bởi X.509 proxy certificate. Hiện tại việc hiện thực bảo mật ở tầng message-level bị giới hạn về mặt hiệu năng, do đó GT4.0 sử dụng transport-level theo mặc định và việc thay đổi sang message-level có thể được kích hoạt nếu cần thiết.

Nếu hiện thực của message-level được cải thiện theo như mục tiêu của dự án Globus, tầng message-level sẽ được thiết lập như là phương thức bảo mật mặc định. Tuy nhiên, bảo mật ở transport-level vẫn sẽ được yêu cầu.

b. Các layer bảo mật theo mô hình GSI:

GSI được hình thành dựa vào bốn yêu cầu chính: bảo vệ thông điệp (message protection), xác thực (authentication), ủy quyền (delegation) và phân quyền (authorization). Các chuẩn bảo mật khác nhau được sử dụng trong mô hình bảo mật của GT4.0: TLS, WS-Security hay WS-SecureConversation được sử dụng như là công cụ bảo mật đi kèm với SOAP. X.509 End Entity Certificates hoặc Username và Password được sử dụng như là phương thức ủy nhiệm xác thực.
X.509 Proxy certificates và WSTrust được dùng cho delegation. SAML Assertions được dùng để xác định quyền.



Hình 3.2: Mô hình bảo mật theo từng tầng của GT4.0 và các chuẩn được sử dụng

c. Bảo vệ thông điệp (message protection):

GT4.0 sử dụng SOAP trong hiện thực web service, việc mã hóa thông điệp có thể được hiện thực thông qua tầng transport-level với giao thức TLS hoặc tầng message-level bằng cách ký và mã hóa thông điệp. Chi tiết về từng cách hiện thực sẽ được trình bày như bên dưới.

Bảo vệ thông điệp ở tầng Transport-level:

Bảo vệ thông điệp ở tầng Transport thông qua giao thức TLS cho phép mã hóa toàn bộ thông điệp qua đó đảm bảo tính toàn vẹn của dữ liệu và tính riêng tư của dữ liệu. Như đã trình bày ở phần trên, transport-level cung cấp hiệu suất hoạt động cao hơn so với message-level, do đó vẫn là phương thức được ưu tiên sử dụng. tuy nhiên trong tương lai, thông qua việc nâng cao hiệu suất làm việc của message-level security việc chuyển dần từ transport-level sang message-level có thể được dự đoán trước.

Transport-level security được sử dụng kết hợp với chứng thực X.509 để xác thực, hoặc có thể không cần chứng thực mà chỉ tập trung vào tính toàn vẹn thông qua chế độ hoạt động "anonymous transport-level security ". Trong chế độ này, việc xác thực có thể được thực hiện ở một tầng khác. Ví dụ: Việc xác thực thông qua username và password chứa trong thông điệp SOAP, hoặc kênh kết nối được tin tưởng tuyệt đối mà không cần thông qua xác thực.

Bảo vệ thông điệp ở tầng Message-level:

Trong định dạng của SOAP cho phép hiện thực phần bảo mật cho payload thông qua bất kỳ một cơ chế bảo mật nào, ví dụ: chữ ký số, mã hóa, đảm bảo tính toàn vẹn. Qua đó hiện thực GSI trong GT4.0 có thể được chọn lựa phương pháp phù hợp để bảo vệ thông điệp SOAP mà có thể áp dụng cho tất cả ứng dụng dựa trên nền tảng GT4.0 web service.

GSI hiện thực hai chuẩn bảo mật cho web service là WS-Security standard và WS-SecureConversation. Tuy nhiện hiện tại việc bảo mật cho web service vẫn chỉ dừng lại ở các specification tức là các định dạng về mặt kỹ thuật mà chưa được hiện thực hóa thành chuẩn quy ước. WS-Security standard, được định nghĩa bởi OASIS, đưa ra một framework cho phép thực hiện bảo mật trên nội dung của thông điệp SOAP; GSI sử dụng phương thức bảo mật này nhằm cung cấp khả năng bảo mật cho các thông điệp độc lập, ví dụ thông điệp không nằm trong một ngữ cảnh bảo mật được thống nhất trước giữa bên nhận và gửi (như thông tin về khóa và CA được tin tưởng của hai bên).

WS-SecureConvertsation là một chuẩn được bảo trợ bởi IBM và Microsoft cho phép thực hiện các thao tác trao đổi thông điệp để khởi tạo ban đầu cho một ngữ cảnh trao đổi thông điệp bảo mật được dùng cho các thông điệp được trao đổi về sau, mục tiêu của phương pháp này nhằm giảm thiểu chi phí về tính toán trong thông điệp. Lưu ý khi sử dụng WS-SecureConvertsatation chỉ được sử dụng khi đi kèm với chứng thực X.509 nhằm thực hiện xác thực trong các bước tiếp theo của phiên làm việc (session).

Cả hai chuẩn WS-Security standard và WS-SecureConvertsation đều được hiện thực một cách độc lập với phương pháp xác thực được sử dụng trong GSI. Do đó, GSI có thể sử dụng chứng thực X.509 hoặc username và password trong phần xác thực. Khi chứng thực X.509 được dùng nhằm định danh, WS-Security và WS-SecureConvertsation được sử dụng bởi GSI sẽ cung cấp thêm các cơ chế bảo mật bổ sung như (các cơ chế này có thể được kết hợp với nhau):

- Bảo vệ tính toàn vẹn (integrity protection): Bên nhận có thể đảm bảo thông điệp là nguyên vẹn như lúc được truyền tải.
- Mã hóa (encryption): Thông điệp được bảo mật để đảm bảo nội dung không được tiết lộ ra bên ngoài.
- Chống phát lại (Replay prevention): Bên nhận có thể xác thực rằng thông điệp nhận được không bị lặp lại từ một thông điệp trước đó.

d. Authentication và delegation

GSI ban đầu hỗ trợ xác thực (authentication) và khả năng chuyển tiếp (delegation) thông qua sử dụng chứng thực X.509 và khóa công khai. Phiên bản GT4.0 còn hỗ trợ xác thực thông qua username và password.

Chứng thực X.509:

GSI sử dụng X.509 end entity certificates (EECs) để định danh các đối tượng như người dùng và dịch vụ. X.509 EECs cho phép định danh mỗi đối tượng một chức chỉ duy nhất mà chỉ đối tượng đó sở hửu và phương pháp để truy cập chứng chỉ này thông qua bên thứ ba thông qua hệ thống khóa bất đối xứng. X.509 ECCs hiện thực dựa trên một số chuẩn có liên

quan. Các tổ chức phát triển grid trên khắp thế giới có thể đưa ra chứng chỉ và cơ quan xác thực chứng chỉ thông qua sử dụng các phần mềm từ bên thứ ba để dựng nên X.509 ECCs và áp dụng cho GSI và Globus Toolkit.

GSI cũng hỗ trợ delegation và single sign-on thông qua sử dụng chuẩn X.509 Proxy Certificate. Proxy Certificate cho phép dựa trên X.509ECCs để thực hiện delegation các tác vụ lên trên một khu vực khác. Trong tác vụ xác thực và phân quyền, GSI coi X.509 EECs và Proxy Certificate với vai trò tương đương nhau.

Xác thực thông qua X.509 có thể thực hiện thông qua TLS, nếu muốn bảo mật ở tầng transport hoặc thông qua chử ký trong WS-Security, nếu muốn bảo mật ở tầng message.

Globus toolkit hỗ trợ ba dạng của Proxy Certificate:

- *Old:* Được hình thành từ bản drafting của RFC 3820, một phát thảo ban đầu và chưa chính thức. Việc sử dụng của bản này bị hạn chế và chỉ dùng trong trường hợp bắt buộc khi muốn giao tiếp với các phiên bản Globus cũ.
- *GT4 Default:* Phiên bản này được hiện thực theo đặc tả từ RFC 3820. Được tạo ra theo mặc định khi gọi lệnh $grid-proxy-init. Nhưng phiên bản này không được sử dụng trong các phiên bản tiếp theo của Globus toolkit.
- *Fully RFC 3820 compliant:* Phiên bản này được hiện thực với khả năng tương thích hoàn toàn với RFC 3820 và có thể được tạo ra thông qua lệnh $grid-proxy-init-rfc. Phiên bản này được dự định trở thành tùy chọn mặc định trong các phiên bản tiếp theo của Globus Toolkit.

Một số hiện thực khác của Proxy Certificate có thể vẫn còn tồn tại, tuy nhiên đây là các hiện thực có từ trước chuẩn RFC 3820. Các hiện thực này không còn được hỗ trợ và không đáng tin cậy trong sử dụng.

Mọi phiên bản của Proxy Certificate đều hỗ trợ đối số "limited", ví dụ $grid-proxy-init –limited. Viêc cung cấp đối số này cho phép chứng chỉ Proxy bị giới hạn khả năng tính toán, ví dụ chỉ sử dụng cho GridFTP mà không dùng dược cho GRAM.

e. Delegation

GT4.0 cho phép delegation một service bằng việc cung cấp một giao diện cho phép người dùng delegate thông qua chứng nhận X.509 Proxy Certificate. Giao diện đưa ra được dựa trên đặc tả về WS-Trust.

f. Xác thực dựa trên Username và password

GSI có thể sử dụng WS-Security cùng với Username và password dạng văn bản text như được đặc tả trong WS-Security standard. Cơ chế này cho phép hổ trợ các ứng dụng dựa trên nền web-service trở nên tương thích hơn đối với WS-I, sẽ được trình bày ở phần sau của bài báo cáo. Lưu ý, khi sử dụng username và password như cách thay cho chứng thực X.509. GSI chỉ có thể cung cấp chế độ xác thực mà không có các chế độ khác như delegate, confident, integrity và replay prevention. Ngoài ra, GSI còn hỗ trợ việc sử dụng username và pasword cùng với chế độ anonymous trong security ở tầng transport.

g. Authorization

Grid-mapfile đã được sử dụng trong các phiên bản trước của GT4.0 và trong phiên bản 4.0 chức năng của grid-mapfile còn cung cấp khả năng kiểm soát hoạt động (access control) trong qua một danh sách các người dùng được phân quyền. GT4.0 sử dụng chuẩn SAML từ OASIS. SAML định nghĩa một định dạng chung cho các dạng quyền về bảo mật và giao thức để tiếp cận các quyền đó. GSI sử dụng SAML AuthorizationDecision để quản lý các quyền theo hai cách:

- Giao thức CAS (community Authorization Service) tạo ra SAML AuthorizationDecision trong việc quản lý và phân hoạch quyền của các thành viên trong CAS trong các service.
- GSI sử dụng các phương thức gọi hàm, được định nghĩa trong SAML AuthorizationDecision protocol của GGF, nhằm cung cấp khả năng sử dụng một dịch vụ quyết định quyền hạn từ một bên thứ ba, chẳng hạn PERMIS, nhằm quản lý khả năng truy suất của các request gởi tới GT4-base service.

h. Khả năng tương thích với WS-I:

GSI hiện tại cung cấp những hỗ trợ ban đầu cho WS-I Basic Security Profile ở những hiện thực có thể hỗ trợ được. Khi GSI sử dụng username và password cho việc định danh, các giao thức được đặc tả nhằm có thể tương thích với WS-I.

i. Xu hướng phát triển của Globus toolkit:

Phân quyền dựa trên từng vai trò riêng biệt là một yêu cầu cấp thiết trong grid. Các dịch vụ như PERMIS và VOMS sử dụng hệ thống phân quyền mà trong đó các quyền được gán trực tiếp thành các đối số cho các người dùng đã không còn phù hợp với yêu cầu của các hệ thống phân quyền hiện tại. Một phương án đang được triển khai nhằm cung cấp khả năng tương thích cho Shibboleth vào Globus toolkit, nhằm cung cấp một cơ chế gán quyền khác vào hệ thống phân quyền của GT.

Một thách thức lớn phải giải quyết khi thực hiện phân quyền dựa trên các đối số là việc hiện vẫn chưa có một phương pháp tổng thể nhằm cho phép các đối số này được giao tiếp từ vùng cung cấp quyền tới các dịch vụ mà các đối số này qui định. Ngoài ra hiện vẫn chưa có chuẩn chung để mô tả các cách mà các đối số này quyết định các chính sách dịch của mình. Một công việc khác hiện đang được khởi động là việc phân tầng của WS-Security Standard nhằm cung cấp khả năng vận chuyển các chứng thực khác nhau từ phía client tới phía service.

IV. Tổng kết đánh giá về bảo mật trong môi trường grid

Grid security hiện nay vẫn là một thách thức lớn. Các nhà phát triển middleware đưa ra những giải pháp khác nhau nhằm giải quyết vấn đề này. Trong xu hướng hiện nay muốn thực hiện xác nhập các hệ thống grid với nhau thành một hệ thống lớn hơn làm nảy sinh các vấn đề với chính sách bảo mật trong môi trường grid. Các vấn đề này hiện vẫn đang được tìm cách giải quyết.

Đối với Globus toolkit sử dụng cơ chế proxy certificates để đơn giản hóa các thao tác truy cập và cho phép delegation, đồng thời hướng đến thực hiện single-sign-on. Trong khi đó với Unicore, không hiện thực cho một cơ chế tương đương. Do đó, khi hệ thống Globus và Unicore được tích hợp sẽ dẫn đến những vấn đề phát sinh như:

- Thông tin về người dùng submit các job chỉ được thấy ở Globus gateway sẽ không thể được quản lý bởi các site sử dụng unicore gateway.
- Khả năng bảo vệ tính toàn vẹn và riêng tư của job sẽ không còn khi di chuyển sang unicore site.

Ngoài ra các chính sách bảo mật do các CA đặt ra thay đổi theo từng trường hợp và việc thay đổi các chính sách bảo mật này sẽ dẫn tới những kết quả khác nhau, trong nhiều trường hợp là không thể thay đổi theo một chuẩn chung duy nhất. Tuy nhiên, việc hiện thực xác thực hiện nay trong môi trường grid đều chủ yếu thông qua chứng chỉ X.509 trong đó các CA đóng vai trò quyết định mức độ tin tưởng của chứng chỉ.

Trong các hiện thực hiện tại của mình, GT4.0 hướng tới mô hình dịch vụ và sử dụng cơ chế bảo mật thông qua các chuẩn bảo mật dùng cho các web service. Tuy nhiên các chuẩn này hiện vẫn được xây dựng và hiệu suất hoạt động không cao do vấn đề khó khăn về chi phí overhead trong thông điệp muốn bảo mật. Do đó, dẫn tới việc GT4.0 tuy có đưa ra hỗ trợ bảo mật theo những chuẩn mới nhưng vẫn phải dùng các phương pháp bảo mật theo các chuẩn cũ làm mặc định.

V. Tài liệu tham khảo

1. The Grid 2-Blueprint for a new computing infrastructure - The Elsevier Series in Grid Computing.
2. The Grid Core Technologies – Maozhen Li, Mark Baker.
3. An analysis of Unicore Security model – T. Goss-Walter.
4. Globus toolkit Version 4 Grid Security Infrastructure: A standard Perspective – Globus security teams