Tạp chí Tin học và Điều khiển học, T.20, S.4 (2004), 305–318

PHÁT TRIỂN GIAO THỨC XÁC THỰC KIỂU KERBEROS KẾT HỢP KIỂM SOÁT TRUY NHẬP DỰA TRÊN VAI CHO HỆ THỐNG QUẢN LÍ TÀI NGUYÊN

LÊ THANH[1], NGUYỄN THÚC HẢI[2]

[1] *Trường Đại học Sư phạm Thể dục Thể thao Hà Tây*
[2] *Khoa Công nghệ thông tin, Trường Đại học Bách khoa Hà Nội*

Abstract. In the resource management system, the security infrastructure is one of the most important components. Here, we focuses on analysing and designing the authentication protocol of Kerberise type which is combinated with role-based access control in an organizational Intranet (named Kerberos-role). Being different from Kerberos, the three-way authentication, Kerberos-role protocol achieve two-way authentication with aims to facilitate a simple user interface of the system while keeping the security strength of the first one.

Tóm tắt. Trong hệ thống quản lí tài nguyên, cơ sở hạ tầng an ninh, an toàn là một trong những thành phần quan trọng nhất. Ở đây, chúng tôi tập trung vào việc phân tích và thiết kế một giao thức xác thực dựa trên giao thức xác thực Kerberos được kết hợp với kiểm soát truy nhập dựa trên vai (gọi là Kerberos-role). Khác với Kerberos là một giao thức xác thực ba bước, Kerberos-role thực hiện một xác thực hai bước tạo cho giao diện người dùng đơn giản hơn nhưng vẫn giữ được sức mạnh an toàn của xác thực Kerberos.

1. MỞ ĐẦU

Đối với hệ thống quản lí tài nguyên của một tổ chức (Resource Management System, viết tắt là RMS), hạ tầng cơ sở an ninh, an toàn là một thành phần tối quan trọng, thường bao gồm: xác thực, kiểm soát truy nhập và kiểm toán. Trong phạm vi bài báo này, chúng tôi trình bày việc phân tích, thiết kế giao thức Kerberos-role dựa trên giao thức xác thực Kerberos trong đó tích hợp thông tin vai của định danh hệ thống vào trong vé dịch vụ dùng cho kiểm soát truy nhập dựa trên vai. Đặc biệt, chúng tôi chú trọng vào việc chứng minh tính đúng đắn, tính hợp lệ và hiệu quả của các giao thức Kerberos-role con dựa trên các khái niệm, kí hiệu và định đề của logic BAN.

2. CÁC VẤN ĐỀ LIÊN QUAN

2.1. Xác thực

2.1.1. *Các phương pháp xác thực*

Dựa trên kĩ thuật mật mã khóa, các phương pháp xác thực được chia thành hai loại:
- Loại 1: xác thực dựa trên mật mã khóa bất đối xứng (khóa công khai).

- Loại 2: xác thực dựa trên mật mã khóa đối xứng (khóa bí mật).

Tiêu biểu cho loại 1 là xác thực dựa trên giấy chứng nhận. Tiêu biểu cho loại 2 là xác thực Kerberos [1]. Xác thực Kerberos là một giao thức xác thực dựa trên giao thức Needham-Schroeder dùng khóa bí mật. Nó được phát triển ở giao thức trao đổi khóa MTI (Matsumoto, Tahashima, Imai - 1988) nhằm cung cấp một miền các tiện ích xác thực và an toàn sử dụng trong mạng máy tính campus Athena và các hệ thống mở khác. Giao thức Kerberos đã trải qua một số lần sửa đổi và nâng cấp từ kinh nghiệm và phản hồi của các tổ chức người dùng. Phiên bản mới nhất của giao thức này là version 5. Ở đây chúng ta xây dựng cơ sở hạ tầng xác thực dựa trên mật mã khóa đối xứng.

2.1.2. *Hệ thống xác thực Kerberos*

- Cấu trúc và chức năng các thành phần: Kerberos là một hệ thống xác thực dựa trên mật mã khóa đối xứng [1]. Việc xác thực là thành công khi một đối tác chứng tỏ việc biết một bí mật chia sẻ gọi là vé với một đối tác khác. Kerberos dựa trên hai dịch vụ: dịch vụ xác thực A (Authentication service) và dịch vụ cấp phát vé T (Ticket granting service). Hai dịch vụ này hợp thành trung tâm phân phối khóa KDC (Key Distribution Center). Dịch vụ xác thực A chịu trách nhiệm sản sinh các khóa đối xứng dựa trên password dùng cho các định danh hệ thống của Kerberos, đồng thời sản sinh các khóa phiên đối xứng dùng cho các phiên giao tiếp với dịch vụ cấp phát vé T và phát hành các vé T. Dịch vụ cấp phát vé T chịu trách nhiệm sản sinh các khóa đối xứng cho các phiên giao tiếp với Server dịch vụ và phát hành các vé dịch vụ.

- Vé Kerberos và bộ xác thực: Vé Kerberos và bộ xác thực là hai kiểu giấy ủy nhiệm phối hợp thực hiện chức năng xác thực. Vé được dùng nhiều lần và cho một Server biết liệu vé có hợp lệ không và ai là Client. Một vé Kerberos là một thông báo được mã hóa gồm tên Client (C), tên Server (S), địa chỉ Client (addr), thời gian phát hành vé (t_1), thời gian hết hiệu lực của vé (t_2), thời gian sống của vé (t_f), thời gian làm mới vé (t_n) và khóa phiên giao tiếp giữa Client và Server ($K_{C,S}$). Nó được thể hiện như sau: $\{\text{ticket}(C,S)\}K_S$, trong đó K_S là khóa riêng của S, $\text{ticket}(C,S) = (C, S, \text{addr}, t_1, t_2, t_f, t_n, K_{C,S})$. Bộ xác thực được một Client sản sinh sẽ cho Server biết ai là Client. Bộ xác thực được gán tem thời gian để sử dụng một lần, nên nó được dùng để ngăn chặn việc tái sử dụng vé. Bộ xác thực là một thông báo gồm tên Client (C), địa chỉ Client (addr), thời gian hiện tại (t), được mã hóa bằng một khóa phiên giao tiếp Client với Server. Cụ thể nó có dạng: $\{\text{auth}(C)\}K_{C,S}$, trong đó $\text{auth}(C) = (C, \text{addr}, t)$.

- Các giao thức xác thực Kerberos:

Bước 1: Lấy khóa phiên và vé giao tiếp với T từ dịch vụ xác thực A

1. $C \to A : (C, T, n)$;
2. $A \to C : (\{K_{C,T}, n\}K_C, \{\text{ticket}(C,T)\}K_T)$.

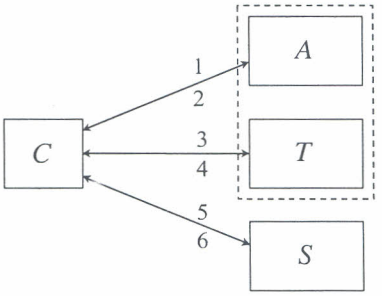
Bước 2: Lấy khóa phiên và vé giao tiếp với S từ dịch vụ cấp phát vé T

3. $C \to T : (\{\text{auth}(C)\}K_{C,T}, \{\text{ticket}(C,T)\}K_T, S, n)$;
4. $T \to C : (\{K_{C,S}, n\}K_{C,T}, \{\text{ticket}(C,S)\}K_S)$.

Bước 3: Truy nhập dịch vụ S khi dùng vé giao tiếp với S

5. $C \to S : (\{\text{auth}(C)\}K_{C,S}, \{\text{ticket}(C,S)\}K_S, n, \text{Request})$;
6. $S \to C : (\{n\}K_{C,S}, \text{Response})$.

Mã hiệu n (none) là một số tuần tự do thành phần Client tạo ra dùng để kiểm tra tính hợp lệ của lời đáp, Request là yêu cầu của C gửi tới S, Response là đáp ứng của S cho C.



Hình 1. Xác thực ba bước trong Kerberos

2.2. Logic xác thực BAN

Michael Burrows, Martin Abadi và Roger Needham mô tả logic xác thực (1990) mà ta gọi tắt là logic BAN [2]. Logic BAN đã được áp dụng để phân tích nhiều giao thức như giao thức Needham–Schroeder và giao thức Kerberos.

2.2.1. *Các khái niệm và kí hiệu của logic BAN*

$P \equiv X$: Đối tượng P tin cậy X là đúng. X có thể đúng, có thể sai, nhưng P hành động như thể X là đúng.

$P \lhd X$: Đối tượng P nhận được một thông báo chứa X. P có thể thực hiện việc giải mã để rút X từ thông báo. P có khả năng lặp lại X trong các thông báo gửi cho các đối tượng khác. X có thể là một mệnh đề hoặc một mục dữ liệu đơn giản như là một mã hiệu (hoặc kết hợp cả hai).

$P \mid\sim X$: Đối tượng P được coi là đã gửi một thông báo chứa X ở một thời điểm nào đó trong quá khứ. Điều này ngụ ý P tin cậy X khi nó gửi thông báo.

$P \Rightarrow X$ (P có quyền hạn đối với X): Đối tượng P được ủy thác như một đối tượng có thẩm quyền về X.

$\#(X)$: X là mới. Ví dụ: Đối tượng P gửi cho đối tượng Q một thông báo chứa mã hiệu n, Q gửi lại cho P một thông báo chứa X và mã hiệu n này thì X được coi là mới.

$P \overset{K}{\longleftrightarrow} Q$: P và Q được giao quyền sử dụng khóa bí mật K. K là một khóa bí mật giữa P và Q và có thể giữa các đối tượng khác được P và Q ủy nhiệm.

Nếu K là một khóa thì $\{X\}K$ được hiểu là X được mã hóa với khóa K. Nếu X và Y là các mệnh đề thì từ đây ta viết X, Y nghĩa là X và Y.

2.2.2. *Các luật suy diễn của logic BAN*

Biểu thị sự kết hợp của mệnh đề X và mệnh đề Y kéo theo mệnh đề Z, ta viết: $\frac{X,Y}{Z}$.

Các luật suy diễn chính của logic BAN như sau:

- Luật ý nghĩa thông báo:

$$\frac{P \equiv P \overset{K}{\longleftrightarrow} Q, P \lhd \{X\}K}{P \equiv Q \mid\sim X}.$$

Nếu P tin rằng nó chia sẻ khóa bí mật K với Q và nếu P nhận được một thông báo chứa X được mã hóa bằng khóa K thì P tin rằng Q đã gửi X (tức là Q đã tin tưởng X và đã gửi một thông báo chứa X).

- Luật kiểm tra mã hiệu:

$$\frac{P \models \#(X), P \models Q \sim X}{P \models Q \models X}.$$

Nếu P tin rằng X là mới và nếu P tin rằng Q đã gửi X thì P tin rằng Q đang tin cậy X. Chú ý là X phải không bị mã hoá. Nếu X bị mã hóa thì Q đơn thuần chỉ là lặp lại một mệnh đề đã mã hóa và Q không cần thiết tin cậy vào X.

- Luật quyền hạn:

$$\frac{P \models Q \mapsto X, P \models Q \models X}{P \models X}.$$

Nếu P tin rằng Q có quyền hạn đối với X trong bất cứ trường hợp nào và nếu P tin rằng Q đang tin cậy X thì P phải tin X, vì Q có thẩm quyền hơn hẳn P trong vấn đề này.

Ngoài ra còn một số luật suy diễn khác của logic BAN như:

$$\frac{P \lhd (X, Y)}{P \lhd X}, \quad \frac{P \models \#(X)}{P \models \#(X, Y)}, \quad \frac{P \models (X, Y)}{P \models X}.$$

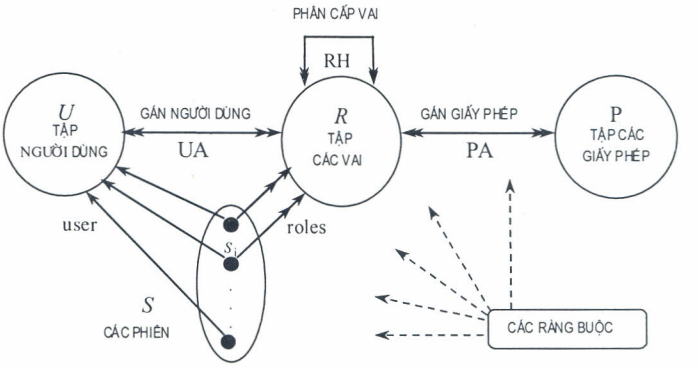
Luật suy diễn thứ nhất nói rằng P có thể quan sát từng thành phần của thông báo nếu nó quan sát được tất cả các thành phần của thông báo đó. Luật suy diễn thứ hai nói rằng nếu một thành phần của một thông báo là mới thì các thành phần khác của thông báo đó cũng được coi là mới. Luật suy diễn thứ ba nói rằng nếu P tin vào một thông báo thì P tin vào từng thành phần của thông báo này.

2.3. Kiểm soát truy nhập dựa trên vai

Hệ thống kiểm soát truy nhập thường dựa trên ba chính sách: chính sách kiểm soát truy nhập tùy ý DAC (Discretionary Access Control), chính sách kiểm soát truy nhập bắt buộc MAC (Mandatory Access Control), chính sách kiểm soát truy nhập dựa trên vai RBAC (Role-Based Access Control). Chính sách kiểm soát truy nhập tùy ý DAC thì quá yếu đối với việc kiểm soát hiệu quả các thông tin đòi hỏi một độ bảo mật, trong khi chính sách kiểm soát truy nhập bắt buộc MAC thì lại quá nghiêm ngặt không có tính linh hoạt. Kiểm soát truy nhập dựa trên vai RBAC là một lựa chọn đầy triển vọng thay thế cho kiểm soát truy nhập tùy ý và kiểm soát truy nhập bắt buộc. Bởi vì RBAC có thể được cấu hình để thực thi kiểm soát truy nhập tuỳ ý hoặc để thực thi kiểm soát truy nhập bắt buộc (chính sách được thực thi là chuỗi cấu hình chi tiết nhiều thành phần RBAC) [5].

Một họ chung các mô hình RBAC (được gọi là RBAC96) được Ravi Sandhu và cộng sự định nghĩa [4]. Hình 2 minh họa mô hình tổng quát nhất trong họ này. Một người dùng là một con người hoặc một tác tử tự trị (autonomous agent), một vai là một chức năng công việc hoặc một tiêu đề công việc bên trong một tổ chức với một số ngữ nghĩa được kết hợp đối với việc cấp quyền và trách nhiệm được gán cho một thành viên của vai. Một giấy phép là một sự phê chuẩn của một hình thức truy nhập cụ thể tới một hoặc nhiều đối tượng trong hệ thống hoặc một số đặc quyền để thực hiện các hoạt động đặc biệt. Các vai được tổ chức theo thứ tự bộ phận $\geq$ sao cho nếu $x \geq y$ thì vai x kế thừa các giấy phép của vai y. Các

thành viên của x rõ ràng là các thành viên của y, nhưng ngược lại không đúng. Trong các trường hợp như thế, chúng ta nói x là cấp trên đối với y. Mỗi phiên liên hệ một người dùng với một số vai có thể. Một người dùng thiết lập một phiên và kích hoạt một số tập con các vai mà người dùng này là thành viên của chúng (trực tiếp hay gián tiếp qua phân cấp vai). Mô hình RBAC96 có các thành phần sau đây:



Hình 2. Mô hình RBAC96,
$\leftrightarrow\!\!\!\!\rightarrow$: tương ứng nhiều - nhiều, $\longrightarrow\!\!\!\!\!\rightarrow$: tương ứng một - nhiều

U là tập hợp người dùng, R là tập hợp các vai, P là tập hợp các giấy phép, S là tập hợp các phiên.

- UA $\subseteq U \times R$, quan hệ gán người dùng cho vai (User Assignment).
- PA $\subseteq P \times R$, quan hệ gán giấy phép cho vai (Permission Assignment).
- RH $\subseteq R \times R$, quan hệ phân cấp vai thứ tự bộ phận (Role Hierarchy).
  (vai x là cấp trên của vai y thì được viết là $x \geq y$).
- Hàm user: $S \to U$, ánh xạ mỗi phiên s_i tới một người dùng u_i (không thay đổi trong suốt phiên làm việc): $u_i = \text{user}(s_i)$.
- Hàm roles: $S \to 2^R$, ánh xạ mỗi phiên s_i tới một tập vai
  $\text{roles}(s_i) \subseteq \{r \mid (\exists r' \geq r)(\text{user}(s_i), r') \in UA\}$ (có thể thay đổi cùng với thời gian).
- Phiên s_i có tập các giấy phép là $\bigcup_{r \in \text{roles}(s_i)} \{p \mid (\exists r'' \leq r)[(p, r'') \in PA]\}$.
- Có một tập hợp các ràng buộc tác động vào giá trị của các thành phần khác nhau được liệt kê ở trên (cụ thể là các quan hệ PA, UA, RH và các hàm user, hàm roles cũng như các phiên làm việc S) và cho kết quả là được phép hay bị cấm. Đây là một mặt quan trọng của RBAC96.

Trong bài báo này, chúng tôi bước đầu kết hợp kiểm soát truy nhập dựa trên vai và một xác thực kiểu Kerberos thành một khối nhằm xây dựng bộ giao thức làm cơ sở cho hạ tầng an ninh, an toàn của một hệ thống quản lí tài nguyên.

3. XÂY DỰNG HỆ THỐNG XÁC THỰC KERBEROS-ROLE

3.1. Các chức năng thành phần

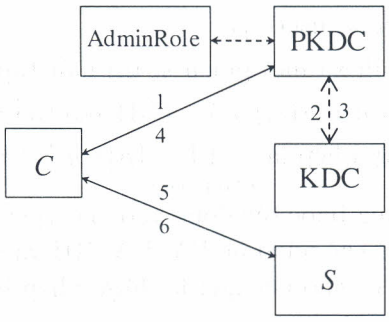
Hệ thống xác thực của chúng tôi vẫn sử dụng các giấy ủy nhiệm Kerberos: vé Kerberos

và bộ xác thực. Một vé truyền tải thông tin định danh của một Client do dịch vụ phân phối khóa KDC chứng thực dùng cho một dịch vụ cụ thể. Một bộ xác thực là một bằng chứng chứng tỏ rằng vé được phát hành từ đầu cho Client chứ không phải là vé ăn cắp.

Khác với Kerberos, ở đây vé giao tiếp giữa Client và dịch vụ chứa cả vai của Client để dùng cho kiểm soát truy nhập dựa trên vai. Sau khi đã xác thực tên định danh an toàn của Client và tính hợp lệ của vé, kết quả kiểm soát truy nhập dựa trên vai sẽ cho phép hay cấm Client truy nhập dịch vụ này. Ở đây một tên định danh an toàn là một tên định danh hệ thống được bảo vệ bằng các cơ chế xác thực và kiểm soát truy nhập trong hệ thống. Chúng tôi gọi hệ thống xác thực của mình là xác thực Kerberos-role ngụ ý kết hợp xác thực kiểu Kerberos với kiểm soát truy nhập dựa trên vai (role).

Các chức năng của hệ thống xác thực Kerberos-role được chia thành ba phần: thành phần Client, thành phần dịch vụ phân phối khóa KDC (Key Distribution Center) và thành phần dịch vụ quản trị PKDC (hoạt động như một Proxy của dịch vụ KDC). Bên cạnh đó là thành phần AdminRole đảm nhiệm việc quản lí và cập nhật vai cho các định danh Client để xây dựng các vé giao tiếp dịch vụ có chứa vai của Client. AdminRole được tích hợp trong hệ thống RMS. Trong phạm vi bài báo này chúng tôi không đi vào phân tích cơ chế hoạt động của AdminRole.

Dịch vụ KDC được thiết kế là một dịch vụ quản lí hai cơ sở dữ liệu bảo vệ giao dịch: cơ sở dữ liệu xác thực và cơ sở dữ liệu vé. Dịch vụ KDC là định danh an toàn tin cậy duy nhất trong RMS. Tất cả các định danh an toàn khác đều được xác thực dựa trên nó. Để việc quản lí hệ thống xác thực được dễ dàng, chỉ có các định danh quản trị của KDC mới có khả năng truy nhập tới dịch vụ KDC. Ban đầu, một định danh quản trị ngầm định được đăng kí trong cơ sở dữ liệu xác thực của KDC. Các định danh quản trị được các dịch vụ quản trị sử dụng. Các dịch vụ quản trị được tích hợp với các nhiệm vụ của dịch vụ RMS. Dịch vụ KDC chủ yếu hoàn thành ba chức năng: chức năng đăng kí và cập nhật định danh an toàn, chức năng sản sinh vé phiên, chức năng làm mới vé.



Hình 3. Xác thực hai bước trong Kerberos-role

Khác với Kerberos, trong hệ thống này, khi một Client yêu cầu truy nhập một dịch vụ thì chỉ phải thực hiện xác thực hai bước (Client không cần biết việc xác thực giữa KDC và PKDC).

Bước 1: Lấy khóa phiên và vé giao tiếp với dịch vụ S

1. $C \rightarrow$ PKDC : (C, addr, S, n) (thực hiện trên tầng socket an toàn SSL);

4. PKDC $\rightarrow C : \{K_{C,S}, n, \{\text{ticket}(C,S)\}K_S\}K_C$.

Bước 2: Truy nhập dịch vụ S khi dùng khóa phiên và vé giao tiếp với S

5. $C \rightarrow S : (\{\text{auth}(C)\}K_{C,S}, \{\text{ticket}(C,S)\}K_S, \{n, \text{Request}\}K_{C,S})$;

6. $S \rightarrow C : (\{n\}K_{C,S}, \text{Response})$.

3.2. Các giao thức xác thực Kerberos-role

Ta xây dựng năm giao thức con: giao thức đăng kí định danh an toàn, giao thức lấy vé dịch vụ, giao thức yêu cầu dịch vụ, giao thức cập nhật định danh an toàn và giao thức làm mới vé. Ta gọi là các giao thức xác thực Kerberos-role hàm ý kiểu giao thức xác thực Kerberos, trong đó nhúng vai (role) của định danh an toàn vào vé dịch vụ. Trong hệ thống RMS, mỗi định danh an toàn đều cần được đăng kí trong dịch vụ KDC để sản sinh khóa riêng của nó trước khi định danh an toàn này có thể giao tiếp với các định danh an toàn khác. Dịch vụ KDC ban đầu tự mình đăng kí vào trong cơ sở dữ liệu xác thực. Dịch vụ KDC là dịch vụ đầu tiên được triển khai trong hệ thống.

- PKDC sử dụng tên ngầm định D trong cơ sở dữ liệu xác thực của KDC để lấy vé dịch vụ tới KDC (thực hiện trên tầng socket an toàn Security Socket Layer - SSL):

1. PKDC $\rightarrow$ KDC : $(D, \text{addr}, \text{KDC}, n)$ (thực hiện trên SSL);

2. KDC $\rightarrow$ PKDC : $\{ \text{K}_{\text{D,KDC}}, n, \{\text{ticket}(D, \text{KDC})\}K_{\text{KDC}}\}K_D$.

- PKDC dùng giao thức cập nhật định danh an toàn (nói trong 3.2.4) để cập nhật tên mới PKDC và password mới p cùng vai của PKDC vào trong cơ sở dữ liệu xác thực của KDC:

1. PKDC $\rightarrow$ KDC : $(\{\text{auth}(D)\}K_{D,\text{KDC}}, \{\text{ticket}(D, \text{KDC})\}K_{\text{KDC}},$
$\{D, \{D, \text{PKDC}, p\}K_D, \text{role}(\text{PKDC}), n\}K_{D,\text{KDC}})$;

2. KDC $\rightarrow$ PKDC : $\{n\}K_{\text{PKDC}}$

PKDC dùng tên mới PKDC và password mới p để giải mã thông báo và nhận được n chứng tỏ việc cập nhật thành công.

- PKDC dùng tên mới PKDC để lấy vé dịch vụ tới KDC:

1. PKDC $\rightarrow$ KDC : (PKDC, addr, KDC, n) (thực hiện trên SSL);

2. KDC $\rightarrow$ PKDC : $\{K_{\text{PKDC, KDC}}, n, \{\text{ticket}(\text{PKDC}, \text{KDC})\}K_{\text{KDC}}\}K_{\text{PKDC}}$.

Kể từ đây PKDC có vé dịch vụ và khóa phiên giao tiếp với KDC.

3.2.1. *Giao thức đăng kí định danh an toàn*

1. $C \rightarrow$ PKDC : $(C, \text{password}, n)$ (thực hiện trên SSL);

2. PKDC $\rightarrow$ KDC : $(\{\text{auth}(\text{PKDC})\}K_{\text{PKDC,KDC}}, \{\text{ticket}(\text{PKDC,KDC})\}K_{\text{KDC}},$
$\{C, \text{password}, \text{role}(C), n\}K_{\text{PKDC,KDC}})$;

3. KDC $\rightarrow$ PKDC : $\{\{n\}K_C\}K_{\text{PKDC}}$;

4. PKDC $\rightarrow C$: $\{n\}K_C$.

Để đăng kí, một định danh an toàn trước tiên cần có giấy chứng nhận của dịch vụ PKDC sao cho nó có thể có một cách an toàn để đệ trình tên và password của mình và một mã hiệu n cho dịch vụ PKDC (n là một số tuần tự được thành phần Client của hệ thống sản sinh và dùng một lần khi giao tiếp với một dịch vụ). Ở đây, có thể dùng giao thức https cho việc truyền an toàn ban đầu (tầng socket an toàn Security Socket Layer - SSL). Khi dịch vụ PKDC có được

tên và password của một client C, nó kích hoạt AdminRole để có được vai role(C) của Client C này. Rồi nó mã hóa bộ dữ liệu $(C, \text{password}, \text{role}(C), n)$ khi dùng khóa phiên $K_{\text{PKDC,KDC}}$ giao tiếp giữa PKDC và KDC và gửi bản mã cho dịch vụ KDC. Khi dịch vụ PKDC yêu cầu dịch vụ KDC, nó cũng cần tự xác thực với dịch vụ KDC bằng cách gửi cho KDC một bộ xác thực của mình $\{\text{auth(PKDC)}\}K_{\text{PKDC,KDC}}$, một vé $\{\text{ticket(PKDC,KDC)}\}K_{KDC}$ giao tiếp với KDC. Sau khi giải mã vé bằng khóa riêng K_{KDC} rồi dùng khóa phiên $K_{\text{PKDC,KDC}}$ có được để giải mã bộ xác thực và KDC so sánh nội dung của bộ xác thực và vé. Nếu kết quả hợp lệ thì trước yêu cầu đăng kí tên định danh an toàn của client C, KDC sẽ kiểm tra tính duy nhất của tên định danh an toàn và sản sinh một khóa riêng K_C (ta có thể dùng khóa DES) dựa trên password và tên của Client C. Khi mọi việc đã thành công, KDC trả lại PKDC thông báo $\{\{n\}K_C\}K_{\text{PKDC}}$. PKDC giải mã thông báo được $\{n\}K_C$ và gửi kết quả này cho Client C mà chỉ nó mới có thể giải mã bằng password đã đăng kí của định danh an toàn yêu cầu ban đầu (mã hiệu n báo nhận tốt).

Việc giải thích hoạt động của các bước giao thức khác được chúng ta xây dựng trong 3.2 thì tương tự như trên.

3.2.2. *Giao thức lấy vé dịch vụ*

1. $C \to$ PKDC : (C, addr, S, n) (thực hiện trên SSL);
2. PKDC $\to$ KDC : $(\{\text{auth(PKDC)}\}K_{\text{PKDC,KDC}}, \{\text{ticket(PKDC,KDC)}\}K_{\text{KDC}}, \{C, \text{addr}, \text{role}(C), S, n\}K_{\text{PKDC,KDC}})$;
3. KDC $\to$ PKDC : $\{\{K_{C,S}, n, \{\text{ticket}(C, S)\}K_S\}K_C\}K_{\text{PKDC}}$;
4. PKDC $\to C$: $\{K_{C,S}, n, \{\text{ticket}(C, S)\}K_S\}K_C$

$\text{ticket}(C, S) = (C, \text{addr}, \text{role}(C), S, t_1, t_2, t_f, t_n, K_{C,S})$.

3.2.3. *Giao thức yêu cầu dịch vụ*

1. $C \to S$: $(\{\text{auth}(C)\}K_{C,S}, \{\text{ticket}(C, S)\}K_S, \{n, \text{Request}\}K_{C,S})$;
2. $S \to C$: $(\{n\}K_{C,S}, \text{Response})$.

Trong đó: $\text{auth}(C) = (C, \text{addr}, t), \text{ticket}(C, S) = (C, \text{addr}, \text{role}(C), S, t_1, t_2, t_f, t_n, K_{C,S})$.

3.2.4. *Giao thức cập nhật định danh an toàn*

1. $C \to$ PKDC : $(C, \{C, C', p\}K_C, n)$ (thực hiện trên SSL);
2. PKDC $\to$ KDC : $(\{\text{auth(PKDC)}\}K_{\text{PKDC,KDC}}, \{\text{ticket(PKDC,KDC)}\}K_{\text{KDC}}, \{C, \{C, C', p\}K_C, \text{role}(C'), n\}K_{\text{PKDC, KDC}})$;
3. KDC $\to$ PKDC : $\{\{n\}K_{C'}\}K_{\text{PKDC}}$;
4. PKDC $\to C$: $\{n\}K_{C'}$.

Client có tên cũ là C, tên mới là C' và password mới là p (hoặc password cũ nếu password không cần thay đổi).

3.2.5. *Giao thức làm mới vé*

Đây là chức năng của riêng trung tâm phân phối khóa KDC. Nó làm mới các vé hết hạn và các vé cũ không hợp lệ trong cơ sở dữ liệu vé. Theo định kì, thành phần KDC kiểm tra các vé $\text{ticket}(C, S)$ trong cơ sở dữ liệu vé của mình để làm mới thời gian phát hành vé t_1, thời gian hết hiệu lực của vé t_2, thời gian sống của vé t_f và gán thời điểm làm mới vé t_n. Vé cũ

của client C giao tiếp với dịch vụ S: $\text{ticket}(C,S) = (C, \text{addr}, \text{role}(C), S, t_1, t_2, t_f, t_n, K_{C,S})$ và vé mới là $\text{ticket}'(C,S) = (C, \text{addr}, \text{role}(C), S, t'_1, t'_2, t'_f, t'_n, K_{C,S})$.

4. ÁP DỤNG LOGIC BAN PHÂN TÍCH GIAO THỨC KERBEROS-ROLE

4.1. Phân tích giao thức trường hợp tổng quát

Để đơn giản, ta kí hiệu lại: KDC là S, PKDC là P, $\text{auth}(A) = (T_A, A)$ và $\text{ticket}(A,B) = (A, B, \text{role}(A), T_{AB}, K_{AB})$. Trong đó T_A là thời gian hiện tại khi phát hành bộ xác thực $\text{auth}(A)$, T_{AB} là tem thời gian bao gồm t_1, t_2, t_f, t_n trong vé $\text{ticket}(A,B)$, K_{AB} là khóa phiên giao tiếp giữa A và B. Địa chỉ addr của Client được hiểu là gộp vào định danh của Client.

Trong hệ thống đang xét, ta có các giả thiết được thừa nhận ban đầu:

$$\begin{cases} S \models P \overset{K_P}{\longleftrightarrow} S, \quad S \models A \overset{K_A}{\longleftrightarrow} S, \quad A \models \forall K.(S \mapsto A \overset{K}{\longleftrightarrow} B), \quad B \models \#(T_A), \; B \models \#(T_{AB}), \\ P \models P \overset{K_P}{\longleftrightarrow} S, \quad A \models A \overset{K_A}{\longleftrightarrow} S, \quad B \models \forall K.(S \mapsto A \overset{K}{\longleftrightarrow} B), \quad B \models S \mapsto \text{role}(A), \\ S \models S \overset{K_S}{\longleftrightarrow} S, \quad S \models B \overset{K_B}{\longleftrightarrow} S, \quad A \models \forall K.(S \mapsto \#(A \overset{K}{\longleftrightarrow} B)), \; S \models A \overset{K_{AB}}{\longleftrightarrow} B, \\ S \models \#(T_P), \quad B \models B \overset{K_B}{\longleftrightarrow} S, \quad B \models \forall K.(S \mapsto \#(A \overset{K}{\longleftrightarrow} B)), \; S \models \#(A \overset{K_{AB}}{\longleftrightarrow} B). \end{cases} \tag{4.1}$$

Trường hợp tổng quát ta có giao thức:

1. $A \to P : (A, B, n)$ (thực hiện trên SSL);
2. $P \to S : (\{T_P, P\}K_{PS}, \{P, S, \text{role}(P), T_{PS}, K_{PS}\}K_S, \{A, B, \text{role}(A), n\}K_{PS})$;
3. $S \to P : \{\{K_{AB}, \{A, B, \text{role}(A), T_{AB}, K_{AB}\}K_B, n\}K_A\}K_P$;
4. $P \to A : \{K_{AB}, \{A, B, \text{role}(A), T_{AB}, \text{K}_{AB}\}\text{K}_B, n\}K_A$;
5. $A \to B : (\{T_A, A\}K_{AB}, \{A, B, \text{role}(A), T_{AB}, K_{AB}\}K_B, \{M, n\}K_{AB})$;
6. $B \to A : (\{n\}K_{AB}, \text{Response})$.

Response là đáp ứng của B khi nhận được thông báo 5 từ A, M là một thông báo hoặc yêu cầu của A gửi cho B. Thông báo 1 không thuộc vào đặc tính logic của giao thức. Các thông báo còn lại có dạng hình thức sau:

2. $P \to S : (\{T_P, P \overset{K_{PS}}{\longleftrightarrow} S\}K_{PS}, \{T_{PS}, P \overset{K_{PS}}{\longleftrightarrow} S, \text{role}(P)\}K_S, \{A, B, \text{role}(A), n\}K_{PS})$;
3. $S \to P : \{\{A \overset{K_{AB}}{\longleftrightarrow} B, \{T_{AB}, A \overset{K_{AB}}{\longleftrightarrow} B, \text{role}(A)\}K_B, n\}K_A\}K_P$;
4. $P \to A : \{A \overset{K_{AB}}{\longleftrightarrow} B, \{T_{AB}, A \overset{K_{AB}}{\longleftrightarrow} B, \text{role}(A)\}K_B, n\}K_A$;
5. $A \to B : (\{T_A, A \overset{K_{AB}}{\longleftrightarrow} B\}K_{AB}, \{T_{AB}, A \overset{K_{AB}}{\longleftrightarrow} B, \text{role}(A)\}K_B, \{M, n\}K_{AB})$;
6. $B \to A : (\{A \overset{K_{AB}}{\longleftrightarrow} B, n\}K_{AB}, \text{Response})$.

Bổ đề 1. *Với các giả thiết được thừa nhận ban đầu* (4.1), *khi B nhận được từ A thông báo sau:*

$$(\{T_A, A \overset{K_{AB}}{\longleftrightarrow} B\}K_{AB}, \{T_{AB}, A \overset{K_{AB}}{\longleftrightarrow} B, \text{role}(A)\}K_B, \{M, n\}K_{AB}), \tag{1}$$

thì: $B \models A \overset{K_{AB}}{\longleftrightarrow} B, B \models A \models A \overset{K_{AB}}{\longleftrightarrow} B, B \models \text{role}(A), B \models A \sim M$.

Chứng minh. Khi B nhận được thông báo (1) thì $B \lhd \{T_{AB}, A \overset{K_{AB}}{\longleftrightarrow} B, \text{role}(A)\}K_B$. Vì $B \models B \overset{K_B}{\longleftrightarrow} S$ nên theo luật ý nghĩa thông báo ta có $B \models S \sim (T_{AB}, A \overset{K_{AB}}{\longleftrightarrow} B, \text{role}(A))$.

Vì $B \models \#(T_{AB})$ nên $B \models \#(T_{AB}, A \overset{K_{AB}}{\longleftrightarrow} B, \text{role}(A))$. Theo luật kiểm tra mã hiệu ta được: $B \models S \models (T_{AB}, A \overset{K_{AB}}{\longleftrightarrow} B, \text{role}(A))$. Suy ra $B \models S \models A \overset{K_{AB}}{\longleftrightarrow} B$ và $B \models S \models \text{role}(A)$. Vì $B \models \forall K.$ $(S \mapsto A \overset{K}{\longleftrightarrow} B)$ nên $B \models S \mapsto A \overset{K_{AB}}{\longleftrightarrow} B$. Mà $B \models S \mapsto \text{role}(A)$, nên từ luật quyền hạn ta được $B \models A \overset{K_{AB}}{\longleftrightarrow} B$ và $B \models \text{role}(A)$. Khi nhận được thông báo (1) thì $B \lhd \{T_A, A \overset{K_{AB}}{\longleftrightarrow} B\}K_{AB}$. Vì $B \models A \overset{K_{AB}}{\longleftrightarrow} B$ nên theo luật ý nghĩa thông báo ta có $B \models A \vdash (T_A, A \overset{K_{AB}}{\longleftrightarrow} B)$. Vì $B \models \#(T_A)$ nên $B \models \#(T_A, A \overset{K_{AB}}{\longleftrightarrow} B)$. Dùng luật kiểm tra mã hiệu ta được $B \models A \models (T_A, A \overset{K_{AB}}{\longleftrightarrow} B)$. Suy ra $B \models A \models A \overset{K_{AB}}{\longleftrightarrow} B$. Khi nhận được thông báo (1) thì $B \lhd \{M, n\}K_{AB}$. Vì $B \models A \overset{K_{AB}}{\longleftrightarrow} B$ nên theo luật ý nghĩa thông báo ta có $B \models A \vdash M$. Vậy: $B \models A \overset{K_{AB}}{\longleftrightarrow} B, B \models A \models A \overset{K_{AB}}{\longleftrightarrow} B$, $B \models \text{role}(A), B \models A \vdash M$. Ta thấy: vì $B \models \text{role}(A)$, tức B tin rằng A có vai là role(A), nên B sẽ thực hiện kiểm soát truy nhập dựa trên vai của A. Nếu A được phép truy nhập B thì B đáp ứng yêu cầu M.

Định lý 1. *Với các giả thiết được thừa nhận ban đầu* (4.1)*, giao thức trong trường hợp tổng quát nêu trên là hợp logic và đạt được các mục tiêu xác nhận sau:*

$$A \models A \overset{K_{AB}}{\longleftrightarrow} B \qquad A \models B \models A \overset{K_{AB}}{\longleftrightarrow} B \qquad B \models A \vdash M$$
$$B \models A \overset{K_{AB}}{\longleftrightarrow} B \qquad B \models A \models A \overset{K_{AB}}{\longleftrightarrow} B \qquad B \models \text{role}(A)$$

Chứng minh. Khi S nhận được thông báo 2, theo Bổ đề 1 thì $S \models P \overset{K_{PS}}{\longleftrightarrow} S$, $S \models \text{role}(P)$, $S \models P \models P \overset{K_{PS}}{\longleftrightarrow} S$ và $S \models P \vdash (A, B, \text{role}(A), n)$. Nghĩa là S tin rằng mình đang giao tiếp với P và P có vai role(P). Vì $S \models \text{role}(P)$ và role(P) cho phép P truy nhập S nên S đáp ứng yêu cầu của P, cụ thể là: S đáp ứng yêu cầu của P bằng một thông báo mã hóa chứa khóa phiên và vé giao tiếp giữa A và B trong thông báo 3. Khi P nhận được thông báo 3, vì $P \models P \overset{K_P}{\longleftrightarrow} S$ nên ta có $P \lhd \{A \overset{K_{AB}}{\longleftrightarrow} B, \{T_{AB}, A \overset{K_{AB}}{\longleftrightarrow} B, \text{role}(A)\}K_B, n\}K_A$. Do đó P có thể gửi cho A thông báo 4. Khi A nhận được thông báo 4, vì $A \models A \overset{K_A}{\longleftrightarrow} S$ nên theo luật ý nghĩa thông báo ta được: $A \models S \vdash (A \overset{K_{AB}}{\longleftrightarrow} B, \{T_{AB}, A \overset{K_{AB}}{\longleftrightarrow} B, \text{role}(A)\}K_B, n)$. A gửi cho P mã hiệu n và nhận lại được n do đó $A \models \#(A \overset{K_{AB}}{\longleftrightarrow} B, \{T_{AB}, A \overset{K_{AB}}{\longleftrightarrow} B, \text{role}(A)\}K_B, n)$. Áp dụng luật kiểm tra mã hiệu, ta được $A \models S \models (A \overset{K_{AB}}{\longleftrightarrow} B, \{T_{AB}, A \overset{K_{AB}}{\longleftrightarrow} B, \text{role}(A)\}K_B, n)$. Suy ra $A \models S \models (A \overset{K_{AB}}{\longleftrightarrow} B)$. Vì $A \models \forall K.$ $(S \models A \overset{K}{\longleftrightarrow} B)$, nên $A \models (S \models A \overset{K_{AB}}{\longleftrightarrow} B)$. Áp dụng luật quyền hạn, ta được $A \models A \overset{K_{AB}}{\longleftrightarrow} B$. Hơn nữa khi A nhận được thông báo 4 thì vì $A \models A \overset{K_A}{\longleftrightarrow} S$ nên:

$$A \lhd (A \overset{K_{AB}}{\longleftrightarrow} B, \{T_{AB}, A \overset{K_{AB}}{\longleftrightarrow} B, role(A)\}K_B, n).$$

Suy ra $A \lhd \{T_{AB}, A \overset{K_{AB}}{\longleftrightarrow} B, \text{role}(A)\}K_B$ và $A \lhd n$.

Vậy A có thể xây dựng thông báo 5 và chuyển cho B. Khi B nhận được thông báo 5, theo Bổ đề 1 thì: $B \models A \overset{K_{AB}}{\longleftrightarrow} B$, $B \models A \models A \overset{K_{AB}}{\longleftrightarrow} B$, $B \models \text{role}(A)$, $B \models A \vdash M$.

Vì $B \models \text{role}(A)$, tức B tin rằng A có vai là role(A), nên B sẽ thực hiện kiểm soát truy nhập dựa trên vai của A. Nếu A được phép truy nhập B thì B đáp ứng yêu cầu M và gửi thông báo 6 cho A (Nếu A không được phép truy nhập B thì B gửi thông báo từ chối truy nhập. Ở đây ta không xét chi tiết kiểm soát truy nhập dựa trên vai). Khi A nhận được thông báo 6, vì $A \models A \overset{K_{AB}}{\longleftrightarrow} B$ nên theo luật ý nghĩa thông báo ta có $A \models B \vdash (A \overset{K_{AB}}{\longleftrightarrow} B, n)$. A gửi cho B

mã hiệu n và nhận lại được n nên $A \models \#(A \overset{K_{AB}}{\longleftrightarrow} B, n)$. Do đó theo luật kiểm tra mã hiệu ta được $A \models B \models (A \overset{K_{AB}}{\longleftrightarrow} B, n)$. Suy ra $A \models B \models A \overset{K_{AB}}{\longleftrightarrow} B$.

Tóm lại:

$$A \models A \overset{K_{AB}}{\longleftrightarrow} B \qquad A \models B \models A \overset{K_{AB}}{\longleftrightarrow} B \qquad B \models A \mathrel{|\sim} M$$
$$B \models A \overset{K_{AB}}{\longleftrightarrow} B \qquad B \models A \models A \overset{K_{AB}}{\longleftrightarrow} B \qquad B \models \text{role}(A)$$

4.2. Phân tích các giao thức con trong giao thức Kerberos-role:

Giao thức lấy vé dịch vụ:

1. $A \to P : (A, B, n)$ (thực hiện trên SSL);
2. $P \to S : (\{T_P, P\}K_{PS}, \{P, S, \text{role}(P), T_{PS}, K_{PS}\}K_S, \{A, B, \text{role}(A), n\}K_{PS})$;
3. $S \to P : \{\{K_{AB}, \{A, B, \text{role}(A), T_{AB}, K_{AB}\}K_B, n\}K_A\}K_P$;
4. $P \to A : \{K_{AB}, \{A, B, \text{role}(A), T_{AB}, K_{AB}\}K_B, n\}K_A$.

Thông báo 1 không thuộc vào đặc tính logic của giao thức. Các thông báo còn lại có dạng hình thức sau:

2. $P \to S : (\{T_P, P \overset{K_{PS}}{\longleftrightarrow} S\}K_{PS}, \{T_{PS}, P \overset{K_{PS}}{\longleftrightarrow} S, \text{role}(P)\}K_S, \{A, B, \text{role}(A), n\}K_{PS})$;
3. $S \to P : \{\{A \overset{K_{AB}}{\longleftrightarrow} B, \{T_{AB}, A \overset{K_{AB}}{\longleftrightarrow} B, \text{role}(A)\}K_B, n\}K_A\}K_P$;
4. $P \to A : \{A \overset{K_{AB}}{\longleftrightarrow} B, \{T_{AB}, A \overset{K_{AB}}{\longleftrightarrow} B, \text{role}(A)\}K_B, n\}K_A$.

Hệ quả 1. *Với các giả thiết được thừa nhận ban đầu* (4.1), *thì giao thức lấy vé dịch vụ nêu trên đạt được các mục tiêu xác nhận:* $A \models A \overset{K_{AB}}{\longleftrightarrow} B, A \lhd \{T_{AB}, A \overset{K_{AB}}{\longleftrightarrow} B, \text{role}(A)\}K_B$ *và* $A \lhd n$.

Chứng minh. Đây chính là các bước giao thức từ 1 đến 4 ở trường hợp tổng quát. Theo chứng minh ở Định lý 1 thì các mục tiêu xác nhận của Hệ quả 1 là đạt được.

Hệ quả 1 cho thấy A nhận được khóa phiên K_{AB} và vé mã hóa $\{\text{ticket}(A, B)\}K_B$ để giao tiếp với B. Vé này chứa role(A) là vai của A để B thực hiện kiểm soát truy nhập dựa trên vai đối với A.

Giao thức yêu cầu dịch vụ:

1. $A \to B : (\{T_A, A\}K_{AB}, \{A, B, \text{role}(A), T_{AB}, K_{AB}\}K_B, \{Request, n\}K_{AB})$.

Request là một yêu cầu dịch vụ do A gửi cho B. Thông báo 1 có dạng hình thức sau:

1. $A \to B : (\{T_A, A \overset{K_{AB}}{\longleftrightarrow} B\}K_{AB}, \{T_{AB}, A \overset{K_{AB}}{\longleftrightarrow} B, \text{role}(A)\}K_B, \{Request, n\}K_{AB})$.

Hệ quả 2. *Với các giả thiết được thừa nhận ban đầu* (4.1), *thì giao thức yêu cầu dịch vụ nêu trên đạt được các mục tiêu xác nhận:*

$$B \models A \overset{K_{AB}}{\longleftrightarrow} B, B \models A \models A \overset{K_{AB}}{\longleftrightarrow} B, B \models \text{role}(A), B \models A \mathrel{|\sim} Request.$$

Chứng minh. Hệ quả này suy trực tiếp từ Bổ đề 1.

Hệ quả 2 cho thấy: B nhận được khóa phiên K_{AB} và yêu cầu Request từ A; B tin rằng A có vai role(A) nên thực hiện kiểm soát truy nhập dựa trên vai role(A) của A. Nếu A được phép truy nhập B thì B sẽ đáp ứng yêu cầu Request của A (nếu A không được phép truy

nhập B thì A nhận được thông báo từ chối dịch vụ).

Giao thức đăng kí định danh an toàn:

1. $A \to P$: $(A, \text{password}, n)$ (thực hiện trên SSL);
2. $P \to S$: $(\{T_P, P\}K_{PS}, \{P, S, \text{role}(P), T_{PS}, K_{PS}\}K_S, \{A, \text{password}, \text{role}(A), n\}K_{PS})$;
3. $S \to P$: $\{\{n\}K_A\}K_P$;
4. $P \to A$: $\{n\}K_A$

n là mã hiệu do A tạo ra ban đầu, password là mật khẩu của client A. Thông báo 1 không thuộc vào đặc tính logic của giao thức. Các thông báo còn lại có dạng hình thức sau:

2. $P \to S$: $(\{T_P, P \overset{K_{PS}}{\longleftrightarrow} S\}K_{PS}, \{T_{PS}, P \overset{K_{PS}}{\longleftrightarrow} S, \text{role}(P)\}K_S, \{A, \text{password}, \text{role}(A), n\}K_{PS})$;
3. $S \to P$: $\{\{A \overset{K_A}{\longleftrightarrow} S, n\}K_A\}K_P$;
4. $P \to A$: $\{A \overset{K_A}{\longleftrightarrow} S, n\}K_A$.

Bổ đề 2. *Với các giả thiết được thừa nhận ban đầu* (4.1), *khi A nhận được từ P thông báo*

$$\{A \overset{K_A}{\longleftrightarrow} S, n\}K_A \tag{2}$$

thì $A \models S \models A \overset{K_A}{\longleftrightarrow} S$ và $A \lhd n$ (n là mã hiệu A gửi cho P trước thông báo (2)*).*

Chứng minh. Khi A nhận được thông báo (2), vì $A \models A \overset{K_A}{\longleftrightarrow} S$ nên: $A \models S \vdash (A \overset{K_A}{\longleftrightarrow} S, n)$ và $A \lhd (A \overset{K_A}{\longleftrightarrow} S, n)$, do đó $A \lhd n$. A nhận lại được mã hiệu n nên $A \models \#(A \overset{K_A}{\longleftrightarrow} S, n)$. Do đó $A \models S \models (A \overset{K_A}{\longleftrightarrow} S, n)$. Thế thì $A \models S \models A \overset{K_A}{\longleftrightarrow} S$ và $A \lhd n$. Về ý nghĩa, việc A giải mã thành công thông báo (2) để có được n chứng tỏ việc A có khóa riêng K_A là đúng.

Định lý 2. *Với các giả thiết được thừa nhận ban đầu* (4.1), *thì giao thức đăng kí định danh an toàn nêu trên là hợp logic và đạt được các mục tiêu xác nhận: $A \models S \models A \overset{K_A}{\longleftrightarrow} S$ và $A \lhd n$.*

Chứng minh. Ta xét trường hợp $P \equiv A$, $S \equiv B$, theo Bổ đề 1, khi S nhận được thông báo 2 thì $S \models P \overset{K_{PS}}{\longleftrightarrow} S$, $S \models P \models P \overset{K_{PS}}{\longleftrightarrow} S$, $S \models \text{role}(P)$, $S \models P \vdash (A, \text{password}, \text{role}(A), n)$. Vì $\text{role}(P)$ cho phép P có quyền truy nhập S, nên S đáp ứng yêu cầu của P bằng cách sản sinh ra khóa phiên K_A ứng với $(A, \text{password})$, lưu trữ bộ $(A, K_A, \text{role}(A))$ trong cơ sở dữ liệu xác thực của mình, đồng thời gửi thông báo 3 cho P báo nhận đã thực hiện yêu cầu của P. Khi P nhận được thông báo 3, vì $P \models P \overset{K_P}{\longleftrightarrow} S$ nên: $P \lhd \{A \overset{K_A}{\longleftrightarrow} S, n\}K_A$ và P có thể chuyển thông báo 4 cho A. Khi A nhận được thông báo 4, theo Bổ đề 2 thì: $A \models S \models A \overset{K_A}{\longleftrightarrow} S$ và $A \lhd n$. Việc A giải mã thành công thông báo 4 để có được n chứng tỏ việc A có khóa riêng K_A là đúng và việc đăng kí định danh an toàn đã thành công.

Giao thức cập nhật định danh an toàn:

1. $A \to P$: $(A, \{A, A', p\}K_A, n)$ (thực hiện trên SSL);
2. $P \to S$: $(\{T_P, P\}K_{PS}, \{P, S, \text{role}(P), T_{PS}, K_{PS}\}K_S, \{A, \{A, A', p\}K_A, \text{role}(A'), n\}K_{PS})$;
3. $S \to P$: $\{\{n\}K_{A'}\}K_P$;
4. $P \to A'$: $\{n\}K_{A'}$.

n là mã hiệu do A tạo ra ban đầu, p là mật khẩu của client A'. Thông báo 1 không thuộc

vào đặc tính logic của giao thức. Các thông báo còn lại có dạng hình thức sau:

2. $P \to S$:
$(\{T_P, P \overset{K_{PS}}{\longleftrightarrow} S\}K_{PS}, \{T_{PS}, P \overset{K_{PS}}{\longleftrightarrow} S, \text{role}(P)\}K_S, \{A, \{A, A', p\}K_A, \text{role}(A'), n\}K_{PS})$;

3. $S \to P$: $\{\{A' \overset{K_{A'}}{\longleftrightarrow} S, n\}K_{A'}\}K_P$;

4. $P \to A'$: $\{A' \overset{K_{A'}}{\longleftrightarrow} S, n\}K_{A'}$.

Định lý 3. *Với các giả thiết được thừa nhận ban đầu* (4.1)*, thì giao thức cập nhật định danh an toàn nêu trên là hợp logic và đạt được các mục tiêu xác nhận* $A' \models S \models A' \overset{K_{A'}}{\longleftrightarrow} S$ *và* $A' \lhd n$.

Chứng minh. Khi S nhận được thông báo 2, theo Bổ đề 1 thì $S \models P \overset{K_{PS}}{\longleftrightarrow} S$, do đó $S \lhd (A, \{A, A', p\}K_A, \text{role}\,(A'), n)$ nên $S \lhd \{A, A', p\}K_A$. Mà $S \models A \overset{K_A}{\longleftrightarrow} S$ nên $S \lhd (A, A', p)$. Hơn nữa, khi S nhận được thông báo 2, theo Bổ đề 1 thì $S \models P \models P \overset{K_{PS}}{\longleftrightarrow} S$, $S \models \text{role}(P)$, $S \models P \sim (A, \text{role}\,(A'), n)$. Vì vai $\text{role}(P)$ cho phép P có quyền truy nhập S, nên S đáp ứng yêu cầu của P bằng cách sản sinh ra khóa phiên $K_{A'}$ ứng với (A', p), lưu trữ bộ $(A', K_{A'}, \text{role}(A'))$ trong cơ sở dữ liệu của mình thay cho bộ $(A, K_A, \text{role}(A))$, đồng thời gửi thông báo 3 cho P. Khi P nhận được thông báo 3, vì $P \models P \overset{K_P}{\longleftrightarrow} S$ nên $P \lhd \{A' \overset{K_{A'}}{\longleftrightarrow} S, n\}K_{A'}$ và P có thể chuyển thông báo 4 cho A' (định danh mới của client A). Khi A' nhận được thông báo 4, áp dụng Bổ đề 2 cho cặp (A', S) thay cho cho cặp (A, S) thì: $A' \models S \models A' \overset{K_{A'}}{\longleftrightarrow} S$ và $A' \lhd n$. Việc A' giải mã thành công thông báo 4 để có được n chứng tỏ A' có khóa riêng $K_{A'}$ là đúng và việc cập nhật định danh an toàn đã thành công.

Giao thức làm mới vé:

Theo định kì, S làm mới các vé đã hết hạn: làm mới thời gian phát hành vé t_1, thời gian hết hiệu lực của vé t_2, thời gian sống của vé t_f và gán thời điểm làm mới vé t_n. Dưới dạng hình thức, vé dành cho giao tiếp giữa Client A và dịch vụ B là: vé cũ $(A, B, \text{role}(A), T_{AB}, K_{AB})$; vé mới $(A, B, \text{role}(A), T'_{AB}, K_{AB})$. Đây là chức năng của riêng trung tâm phân phối khóa S, nên ta không xét tính logic của giao thức.

5. KẾT LUẬN

Trong phạm vi bài báo này, chúng tôi trình bày việc thiết kế các giao thức xác thực Kerberos-role tích hợp thông tin vai của định danh an toàn vào trong vé dịch vụ nhằm thực hiện xác thực kết hợp với kiểm soát truy nhập dựa trên vai. Các giao thức xác thực của chúng tôi dựa trên các giao thức xác thực của Kerberos version 5, với việc sử dụng các cơ chế an toàn cơ bản của Kerberos: bộ xác thực, vé, khóa riêng và khóa phiên. Khác với Kerberos (là một xác thực ba bước), Kerberos-role thực hiện một xác thực hai bước tạo cho giao diện người dùng đơn giản hơn nhưng vẫn giữ được sức mạnh an toàn của xác thực Kerberos.

TÀI LIỆU THAM KHẢO

[1] B. Clifford Neuman and Theodore Ts'o, Kerberos: An authentication service for computer networks, *IEEE Communications* **32** (9) (1994) 33–38.

[2] Burrows M., Abadi M., and Needham R., A logic of authentication, *ACM Transactions Computer Systems* **8** (1990) 18–36.

[3] George Coulouris, Jean Dollimore, and Tim Kindberg, *Distributed Systems - Concepts and Design*, Queen Mary and Westfield College - University of London, Addison-Wesley Publishing Company, second edition, 1994.

[4] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. youman, Role-based access control models, *IEEE Computer* **29** (2) (1996) 38–47.

[5] Sylvia Osborn, Ravi Sandhu, and Qamar Munawer, Configuring role-based access control to enforce mandatory and discretionary access control policies, *ACM Transactions on Information and System Security* **3** (2) (2000) 85–106.

Nhận bài ngày 15 - 9 - 2003
Nhận lại sau sửa ngày 10 - 11 - 2004