CHỨNG THỰC NGƯỜI DÙNG SỬ DỤNG MÃ GRAY ỨNG DỤNG TRONG ĐÀO TẠO TRÊN MẠNG

Trần Ngọc Bảo
Nguyễn Đình Thúc

ABSTRACT

Mutual authentication is vital concept to network security and incorporated to proprietary security solutions.If the mutual authentication is proprietary implemented, it can stop man-in-the-middle attacks, session high-jacking and replay attacks.

In this paper, we present a new mutual authentication protocol based on Gray code, integrate with Moodle system to verify user authentication. Proposed protocol can be implemented in client/server mode, where the server stores and manages account of all users, says certificate authority (CA).

KEYWORDS

Wireless Lan Security, Authentication, Moodle, e-Learning

TÓM TẮT

Chứng thực lẫn nhau là một khái niệm quan trọng trong lĩnh vực an ninh mạng. Giao thức này có khả năng ngăn chặn các hình thức tấn công qua người trung gian và replay [3] .

Trong bài báo này chúng tôi trình bày giao thức chứng thực lẫn nhau dựa vào mã Gray [1], thực nghiệm vào quá trình chứng thực người dùng trong hệ thống nguồn mở Moodle phục vụ đào tạo trực tuyến. Giao thức xây dựng được triển khai theo mô hình client-server, trong đó server đóng vai trò lưu trữ, quản lý thông tin truy cập của các client và xác nhận quyền đăng nhập hệ thống, được gọi là CA (Cetificated Authentication) server. Mỗi client sẽ được cấp tài khoản để truy cập hệ thống.

TỪ KHÓA

Wireless Lan Security, Authentication, Moodle, e-Learning

I. GIỚI THIỆU

Ngày nay, nhu cầu học tập, đào tạo trực tuyến thông qua hệ thống mạng ngày càng trở nên phổ biến. Bên cạnh những thuận lợi, hệ thống đào tạo trực tuyến cũng chứa đựng rất nhiều rủi ro và nguy cơ tấn công từ bên ngoài. Vì vậy, khi thực hiện triển khai hệ thống đào tạo trực tuyến thì vấn đề an toàn cần được xem xét và giải quyết. Làm thế nào để ngăn chặn những người lạ truy cập vào hệ thống? Trong bài báo này chúng tôi trình bày một giải pháp an ninh cho việc triển khai hệ thống nguồn mở Moodle phục vụ công tác đào tạo từ xa tại khoa Toán – Tin học, Trường Đại học Sư phạm Tp.HCM. Trong giải pháp này chúng tôi đề xuất và cài đặt một giao thức chứng thực dựa trên mã gray để thực hiện chứng thực người dùng hệ thống. Giao thức được triển khai theo mô hình client-server.

II. GIAO THỨC CHỨNG THỰC NGƯỜI DÙNG

2.1 Thông tin chứng thực

Hệ thống chứng thực người dùng sử dụng giao thức chứng thực lẫn nhau dựa vào mã Gray được triển khai theo mô hình client-server, trong đó server đóng vai trò quản lý, lưu trữ và cấp tài khoản truy cập cho các client và xác nhận quyền đăng nhập hệ thống, được gọi là CA Server.

– Mỗi client sẽ được cấp tài khoản để truy cập hệ thống bao gồm:

• Username: thông tin dùng để đăng

nhập hệ thống;

• COG (Client Original Gray): mã Gray gốc;

• T_0: thời điểm cấp tài khoản (ddMMyyyy hhmmss);

• T: chu kỳ phát sinh mã Gray (được tính bằng đơn vị giây);

• D: hệ số sử dụng trong quá trình phát sinh Gray code;

• CGAL (Client Gray Accessed List): danh sách chứa mã gray đã sử dụng trong các lần truy cập trước, số lượng phần tử của danh sách cố định với mỗi client được ký hiệu là N ($N \leq N_{Max}$).

– Server đóng vai trò quản lý, lưu trữ và cấp tài khoản truy cập hệ thống của các client, thông tin của mỗi client được lưu trữ trên server gồm các thông tin:

• Username: thông tin dùng để đăng nhập hệ thống;

• SOG (Server Original Gray): mã Gray gốc;

• T_0: thời điểm cấp tài khoản (ddMMyyyy hhmmss);

• T: chu kỳ phát sinh mã Gray (được tính bằng đơn vị giây);

• D: hệ số sử dụng trong quá trình phát sinh Gray code;

• SGAL (Server Gray Accessed List): danh sách chứa mã gray mà client đã sử dụng trong các lần truy cập trước, số lượng phần tử của danh sách cố định với mỗi client được ký hiệu là N ($N \leq N_{Max}$).

2.2 Qui trình cấp tài khoản

Mỗi client muốn đăng nhập hệ thống cần phải có một tài khoản. Qui trình cấp tài khoản cho client được thực hiện theo các bước sau:

(1) Chọn Username tương ứng cho client;

(2) Phát sinh ngẫu nhiên mã Gray gốc COG và SOG (có thể sử dụng mã gray nhị phân, tam phân hoặc m phân, COG = SOG); ghi nhận thời điểm phát sinh T_0;

(3) Phát sinh ngẫu nhiên giá trị D;

(4) Chọn/phát sinh ngẫu nhiên chu kỳ phát sinh mã Gray T;

(5) Phát sinh ngẫu nhiên danh sách CGAL và SGAL chứa N mã Gray (CGAL = SGAL);

(6) Phát sinh ngẫu nhiên khóa M_k (Master key dùng để mã hóa liệu trong quá trình cấp tài khoản và chứng thực);

(7) Tạo Cert bằng cách mã hóa các thông tin với Mk;

Cert1 = AES(M_k,COG, T, T_0, D, CGAL)

Cert2 = AES(M_k,SOG, T, T_0, D, SGAL)

(8) Gởi thông tin tài khoản gồm Cert1, username, M_k cho client

(9) Lưu thông tin tài khoản tương ứng với tài khoản đã cấp cho client gồm Cert2, username, M_k vào server.

(Cert1 có thể được cấp theo dạng thẻ truy cập hoặc USB, username, M_k sẽ được nhập trong quá trình cấu hình module client, trong trường hợp client bị mất USB và bị lộ username cũng không bị ảnh hưởng đến thông tin tài khoản, vì được mã hóa bởi M_k).

Sau khi nhận được Cert1, username, khóa M_k client sử dụng thông tin này để đăng nhập hệ thống theo quy trình chứng thực trong mục 3.3.

2.3 Qui trình chứng thực

Client muốn truy cập hệ thống phải thực hiện đăng nhập và chứng thực theo qui trình sau:

(1) Client gởi thông điệp đăng nhập hệ thống:

– Chọn ngẫu nhiên một mã Gray trong danh sách CGAL, được ký hiệu là CG_i (phần tử ở vị trí thứ i từ đầu danh sách CGAL);

– Tạo giá trị nonce bằng cách mã hóa CG_i với khóa M_k

nonce $= AES(M_k, CG_i)$

[hoặc nonce $= AES(M_k, CG_i,$ username)]

– Gởi username và nonce cho server AS

(2) AS Server xác nhận nonce và tạo Cert

– Nếu username không tồn tại (client mới), server gởi thông báo yêu cầu đăng ký tài khoản đăng nhập với admin của hệ thống và kết thúc quy trình chứng thực. (Việc đăng ký tài khoản thực hiện offline, được thực hiện theo quy trình cấp Cert được mô tả trong mục 3.3).

– Nếu username tồn tại thực hiện

• Giải mã nonce được CG_i

$CG_i = AES(M_k,$ nonce)

• Lấy danh sách SGAL tương ứng với username.

• Nếu CG_i không tồn tại trong danh sách SGAL kết thúc quy trình chứng thực, từ chối client đăng nhập hệ thống.

• Ngược lại (CG_i sẽ được tìm thấy ở vị trí thứ i trong danh sách SGAL) thực hiện tạo Cert gởi cho client.

• Chọn mã gray ở vị trí thứ i tính từ cuối danh sách trong danh sách SGAL, ký hiệu là CG_j;

• Tạo giá trị Cert bằng cách mã hóa CG_j với khóa M_k

Cert $= AES(M_k, CG_j)$

• Gởi Cert cho client.

(3) Client xác nhận Cert và tạo Session key

– Giải mã Cert được CG_j

$CG_j = AES(M_k,$ Cert)

– Nếu CG_j tồn tại ở vị trí thứ i tính từ cuối danh sách trong danh sách CGAL

• Tính $\Delta_{ij} = |i-j|$, trong đó i, j là vị trí của CG_i và CG_j trong danh sách CGAL (tính từ đầu danh sách)

• Tính mã Gray tại thời điểm t hiện tại theo qui tắc

$$CG_t = COG + \left[\frac{t - T_0}{T}\right] xD$$

$CG_{ij} = \Delta_{ij} + CG_t$

• Tạo Session key K_{ss} bằng cách mã hóa CG_{ij}, t với M_k

$K_{ss} = AES(M_k, CG_{ij})$

• Gởi Session key K_{ss} và thời điểm phát sinh t cho AS Server.

– Ngược lại kết thúc quy trình chứng thực, từ chối client đăng nhập hệ thống.

(4) AS Server kiểm tra tính hợp lệ của Session key K_{ss}

– Tạo Session key K'_{ss} từ giá trị t

• Tính $\Delta_{ij} = |i-j|$, trong đó i, j là vị trí của CG_i và CG_j trong danh sách SGAL (tính từ đầu danh sách)

• Tính mã Gray tại thời điểm hiện tại t theo qui tắc

$$CG_t = SOG + \left[\frac{t - T_0}{T}\right] xD$$

CGij $= \Delta_{ij} + CG_t$

• Tạo Session key K'_{ss} bằng cách mã hóa CG_{ij}, t với M_k

$K'_{ss} = AES(M_k, CG_{ij})$

– Kiểm tra tính hợp lệ của Kss

• Nếu $K_{ss} <> K'_{ss}$ thì thông báo không hợp lệ và từ chối client truy cập hệ thống;

• Ngược lại quá trình chứng thực thành công, cho phép client truy cập hệ thống

• Cập nhật giá trị CG_i và CG_j trong danh sách SGAL

$$CG_j = \frac{CG_i + CG_j + C_{ij}}{3}$$

$CG_i = CG_{ij}$

(5) Client cập nhật giá trị CG_i và CG_j trong danh sách CGAL

$$CG_j = \frac{CG_i + CG_j + C_{ij}}{3}$$

$CG_i = CG_{ij}$

K_{ss} là Session key, có thể sử dụng cho giai đoạn mã hóa dữ liệu (nếu cần).

Giá trị nonce và Cert được sử dụng trong (2) và (3) nhằm ngăn chặn hình thức tấn công replay từ hacker.

III. MOODLE VÀ CHỨNG THỰC NGƯỜI DÙNG

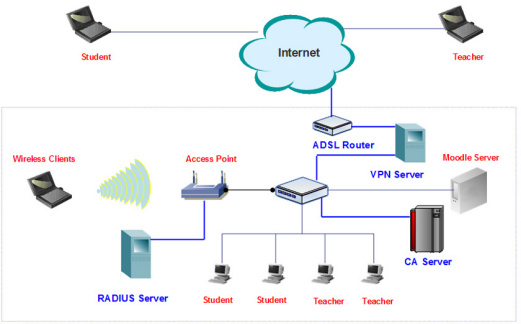
Moodle [2], [4] là một phần mềm mã nguồn mở sử dụng công nghệ LAMP (Linux – Apache – MySQL - PHP), đang được phát triển bởi một cộng đồng theo hướng đơn thể (module) để hỗ trợ cho giáo dục và được sử dụng phổ biến tại Việt Nam (ví dụ trang Web về đào tạo từ xa của Bộ Giáo Dục – Đào tạo [5]).

Phần mềm Moodle là một hệ thống tổ chức khoá học và đào tạo (LCMS/LMS) dựa trên Internet và các Web-based learning, với đối tượng phục vụ là: các trường phổ thông, cao đẳng, đại học, trung tâm, doanh nghiệp, các tổ chức kinh doanh, bệnh viện, thư viện, …

An ninh hệ thống Moodle là vấn đề được cộng đồng người sử dụng Moodle quan tâm. Trong bài báo này nhóm chúng tôi khảo sát hệ thống Moodle phiên bản 1.6 được sử dụng phục vụ đào tạo tại khoa Toán – Tin học, trường Đại học Sư Phạm Tp.HCM; trên cơ sở đó đề xuất một giải pháp nhằm cải thiện, nâng cao tính an toàn cho hệ thống Moodle. Giải pháp đề xuất bao gồm:

– Kiến trúc triển khai hệ thống được minh họa trong hình 1.

o Hệ thống triển khai bao gồm các máy tính cá nhân (PC), máy chủ và các thiết bị khác… kết nối với nhau qua hệ thống dây cáp truyền thống và các máy tính (hay thiết bị) không dây kết nối vào hệ thống có dây thông qua Access Point, các máy tính bên ngoài internet kết nối vào hệ thống thông qua VPN server.



Hình 1. Mô hình triển khai hệ thống Moodle tại Khoa Toán – Tin học Trường ĐHSP Tp.HCM.

• Hệ thống mạng cục bộ (LAN) - sẽ bao gồm các máy tính kết nối có dây thông qua Switch – Hub, máy chủ Moodle và CA server.

• Hệ thống mạng không dây (Wireless LAN) - WLAN sẽ bao gồm các máy tính không dây kết nối vào hệ thống mạng có dây (hoặc kết nối với nhau) thông qua Access Point và CA server.

• RADIUS server cung cấp dịch vụ xác nhận quyền truy cập và trao đổi khoá cho các thiết bị không dây dựa trên nền nghi thức EAP.

• VPN Gateway dùng để đảm bảo an toàn trao đổi thông điệp từ bên ngoài internet và hệ thống.

• CA server cung cấp dịch vụ xác nhận quyền truy cập vào hệ thống đào tạo Moodle của Khoa Toán – Tin học.

• Với mỗi loại người dùng, hệ thống được bảo vệ 2 lớp như sau:

• Với người dùng mạng có dây, kết nối cục bộ (LAN), hệ thống được bảo vệ bởi CA server.

• Với người dùng mạng không dây kết nối thông qua mạng WLAN, hệ thống được bảo vệ bởi RADIUS server và CA server. RADIUS sẽ được cấu hình cho phép dùng giao thức EAP cho quá trình xác nhận truy

cập EAP và WEP key dùng cho mã hóa dữ liệu của 802.11.

• Với người dùng mạng internet kết nối hệ thống thông qua WAN và VPN, hệ thống được bảo vệ bởi VPN server và CA server.

– Xây dựng cơ chế quản lý đăng nhập đồng thời để kiểm tra người dùng đăng nhập hệ thống, tại một thời điểm một tài khoản chỉ có thể đăng nhập hệ thống một lần. Chức năng này nhằm hạn chế người dùng sử dụng cùng một tài khoản để truy cập hệ thống ở nhiều máy khác nhau.

– Đề xuất giao thức chứng thực lẫn nhau dựa trên mã gray để thực hiện chứng thực người dùng. Thông tin chi tiết về giao thức đã được trình bày trong mục 2.

– Cài đặt hệ thống chứng thực đề xuất trong mục 2 để thực hiện kiểm tra người dùng trong quá trình đăng nhập hệ thống Moodle.

IV. KẾT LUẬN

Trong bài báo này nhóm chúng tôi đã trình bày một giao thức chứng thực dựa trên mã Gray để thực hiện chứng thực người dùng hệ thống Moodle. Giao thức có khả năng ngăn chặn các hình thức tấn công qua người trung gian, tấn công replay. Ngoài ra, dữ liệu sử dụng trong quá trình chứng thực đều được mã hóa, do đó giao thức này cũng có khả năng ngăn chặn được hình thức tấn công high-jacking.

Ngoài việc đề xuất một giao thức chứng thực lẫn nhau dựa trên mã gray như đã trình bày trong mục 2, nhóm chúng tôi cũng đề xuất mô hình an ninh triển khai hệ thống Moodle với các thành phần bảo vệ cho mỗi loại đối tượng người dùng (LAN, WLAN, WAN) truy cập hệ thống Moodle.

TÀI LIỆU THAM KHẢO

[1] Bùi Doãn Khanh (2006), "Hoán vị, mã gray và mã hóa thông tin", UFR 929, University of PARIS VI

[2] Lê Đức Long, Bùi Minh Từ Diễm, Trần Văn Hạo, Nguyễn Đình Thúc (2005), "Nghiên cứu thực nghiệm về các hệ LCMS/LMS nguồn mở", Báo cáo hội thảo Quốc gia lần thứ 8, Hải Phòng, Việt Nam.

[3] Nguyen Dinh Thuc, Tran Ngoc Bao (2007), "An Authentication Protocol based on Threshold Secret Sharing", Proceeding of ISSAT International Conference on Modeling of Complex Systems and Environments, HCMC, Vietnam

[4] Website chính thức của LCMS nguồn mở Moodle, http://moodle.org/course, http://moodle.org/mod/forum/discuss.php?d=35845

[5] Website đào tạo từ xa của Bộ Giáo dục – Đào tạo

http://el.edu.net.vn/