TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

KHOA CÔNG NGHỆ THÔNG TIN

ĐỒ ÁN 02:

Báo cáo lần 5:

End-to-End Encryption

Bổ sung chức năng nhóm chat

GV hướng dẫn:	**Sinh viên thực hiện:**
Nguyễn Văn Quang Huy	20127192 - Trần Anh Huy
Nguyễn Đình Thúc	20127066 – Nguyễn Nhật Quân

Thành phố Hồ Chí Minh, ngày 30 tháng 4 năm 2024

1. TỔNG QUAN

1.1. THÔNG TIN NHÓM: NHÓM 10

MSSV	Họ tên	Email
20127192	Trần Anh Huy	20127192@student.hcmus.edu.vn
20127066	Nguyễn Nhật Quân	20127066@student.hcmus.edu.vn

2. LÝ THUYẾT

2.1. MỤC TIÊU:

Dựa trên đồ án chính, nhóm thực hiển bổ sung chức năng nhóm chat, gồm tối thiểu 3 thành viên trở lên. Các người dùng cần đã xác thực nhau trước khi thêm vào nhóm. Người tạo nhóm lần đầu phải thêm ít nhất 2 người dùng đã xác thức để có thể tạo nhóm. Tin nhắn văn bản trong nhóm sẽ được mã hóa đầu cuối bằng khóa bí mật chung được chia sẽ bảo mật bằng thuật toán Diffie-Hellman.

2.2. MÔ TẢ:

Người dùng tạo nhóm sẽ nhấn vào nút tạo nhóm, sau đó chọn 2 người dùng bạn bè đã trao đổi khóa với người tạo nhóm. Điều này là cần thiết để người dùng xác thực lẫn nhau trước khi thêm vào nhóm.

Các thành viên nhóm chat, sẽ được trao đổi khóa theo thuật toán Diffie-Hellman dành cho 2 đối tượng trở lên để tạo khóa bí mật chung của nhóm chat. Các thành viên không cần chia sẻ khóa bí mật của mình cho nhau và cho hệ thống.

Nhóm chat sẽ có khả năng thêm thành viên mới và khi thêm thành công quá trình trao đổi khóa sẽ được tự động cập nhật dựa trên những người tham gia mới của nhóm chat

2.3. HƯỚNG TRIỂN KHAI GIAO THỨC TRAO ĐỔI KHÓA TRONG NHÓM 1:

Ý tưởng:

Thuật toán trao đổi khóa Diffie-Hellman tiêu chuẩn hoạt động trong nhóm tuần hoàn với trình tạo g , và dựa vào

$$y_A^{x_B} = (g^{x_A})^{x_B} = (g^{x_B})^{x_A} = y_B^{x_A}$$

với yA , yB được chuyển công khai và xA and xB được giữ bí mật

Với 3 đối tượng tham ta có như sau:

$$((g^{x_A})^{x_B})^{x_C} = ((g^{x_A})^{x_C})^{x_B} = ((g^{x_B})^{x_A})^{x_C} = ((g^{x_B})^{x_C})^{x_A} = ((g^{x_C})^{x_A})^{x_B} = ((g^{x_C})^{x_B})^{x_A}$$

Vì mỗi bên muốn giữ khóa riêng của mình nên mỗi phép tính lũy thừa cần được thực hiện tại các địa điểm khác nhau, điều đó có nghĩa là một số bên phải gửi kết quả bước thứ hai của mình cho các bên khác.

Giao thức khả thi có thể là:

1. A, B, C có các khóa bí mật là x_A, x_B, x_C.
2. A, B, C tính giá trị $y_A=g^{x_A}$, $y_B=g^{x_B}$, $y_C=g^{x_C}$.
3. A gửi y_A cho B, B gửi y_B cho C, C gửi y_C cho A.
4. A sẽ tính $\mathbf{Z}_{CA} = yc^{x_A}$, B tính $\mathbf{Z}_{AB} = y_A^{x_B}$, C tính $\mathbf{Z}_{BC} = y_B^{x_C}$.
5. A sẽ gửi $\mathbf{Z}_{CA}$ cho B, B gửi $\mathbf{Z}_{BA}$ cho C, C gửi $\mathbf{Z}_{BC}$ cho A.
6. A sẽ tính $k_{BCA} = \mathbf{Z}_{BC}^{x_A}$, B sẽ tính $k_{CAB} = \mathbf{Z}_{CA}^{x_B}$, C sẽ tính $k_{ABC} = \mathbf{Z}_{AB}^{x_C}$

Với Giao thức trên, 3 đối tượng tham sẽ biết được giá trị bí mật chung $k_{BCA} = k_{CAB} = k_{ABC}$
Mà vẫn đảm bảo bảo mật trong quá trình trao đổi khóa. Khóa chung này sẽ được dùng để mã hóa và giải mã tin nhắn trao đổi của các thành viên trong nhóm.

Với trường hợp nhóm có hơn 3 đối tượng, ta đơn giản là thêm 1 đối tượng vào vòng trao đổi. Lúc này A sẽ gửi cho B, B gửi cho C, C gửi cho D và D gửi cho A. Từ đó tính ra 4 khóa k có giá trị bằng nhau là đó là khóa bí mật chung của nhóm.

Vấn đề và Thách thức:

- Trong môi trường đa bên, mỗi thành viên sẽ cần trao đổi thông tin với từng thành viên khác để tạo ra các khóa chung. Điều này làm tăng số lượng trao đổi cần thiết và độ phức tạp của quy trình.

- Các thành viên cần tính toán và quản lý các khóa khác nhau cho từng thành viên trong nhóm.

- Việc quản lý các khóa chung cho từng cặp thành viên trong nhóm có thể trở nên phức tạp khi số lượng thành viên tăng lên.

- Trong một nhóm chat, các thành viên cần tin tưởng nhau về việc xử lý đúng thông tin trao đổi để tạo ra các khóa chung an toàn.

2.4. HƯỚNG TRIỂN KHAI GIAO THỨC TRAO ĐỔI KHÓA TRONG NHÓM 2:

Ý tưởng:
Tạo một khoá chung cho cả nhóm sử dụng, được quản lý và phân phát bởi người tạo nhóm.

Phương pháp này có thể được áp dụng trong một môi trường nhóm chat nhằm đảm bảo rằng mọi thành viên trong nhóm đều có thể mã hóa và giải mã thông tin bằng cùng một khoá.

Giao thức khả thi có thể là:

1. Khởi tạo khoá chung: Người tạo nhóm sử dụng giao thức Diffie-Hellman để tạo ra một khoá chung. Khoá

này được tạo từ một căn cứ và một số nguyên tố được chọn trước, từ đó tính toán ra một giá trị khoá.

2. Phân phối khoá: Khoá chung này sau đó được chia sẻ cho các thành viên trong nhóm thông qua tin nhắn đã được mã hóa 1-1 giữa người tạo nhóm và mỗi thành viên. Việc sử dụng mã hóa đầu cuối (end-to-end encryption) trong giai đoạn này sẽ đảm bảo khoá chung không bị lộ cho bên ngoài hay kẻ tấn công.

3. Sử dụng khoá chung: Mỗi thành viên trong nhóm sử dụng khoá chung để mã hóa và giải mã các tin nhắn trong nhóm. Điều này đảm bảo rằng chỉ các thành viên có khoá mới có thể đọc được nội dung.

4. Quản lý khoá: Bất cứ khi nào có thành viên mới tham gia hoặc rời nhóm, người quản lý nhóm cần cập nhật và phân phối lại khoá chung để đảm bảo tính bảo mật của nhóm.

Vấn đề và Thách thức:

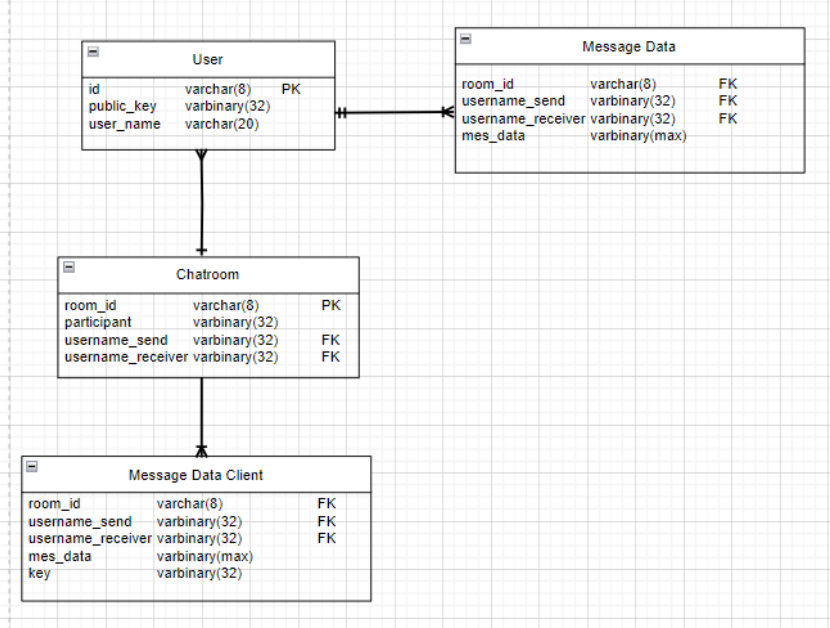
- Việc cần phải cập nhật và phân phối lại khoá chung mỗi khi có sự thay đổi thành viên có thể là quá trình phức tạp và dễ dẫn đến lỗi.

- Nếu khoá chung bị lộ, tất cả các thông tin trao đổi trong nhóm sẽ không còn đảm bảo tính bảo mật.

- Việc sử dụng một khoá chung có nghĩa là bất kỳ thành viên nào trong nhóm cũng có thể giải mã bất kỳ tin nhắn nào, điều này có thể gây ra vấn đề nếu có sự không tin tưởng giữa các thành viên.

- Việc phụ thuộc vào một khoá chung đòi hỏi khoá đó phải rất mạnh và được bảo vệ cẩn thận.

2.5. ENTITY RELATIONSHIP DIAGRAM CHO NHÓM CHAT:



2.6. KẾT LUẬN:

Mã hóa đầu cuối đóng vai trò quan trọng trong việc bảo vệ tính bảo mật và riêng tư của thông tin được trao đổi trong các cuộc trò chuyện nhóm. Qua việc triển khai các giao thức, nhóm chat có thể thiết lập một khóa chung an toàn mà không cần tiết lộ thông tin bí mật nào trong quá trình trao đổi khóa.

Việc ứng dụng phương pháp này không chỉ giúp đảm bảo an toàn cho thông tin được trao đổi, mà còn tăng cường sự tin tưởng của người dùng đối với nền tảng truyền thông. Tuy nhiên, cũng cần lưu ý rằng việc triển khai và quản lý giao thức mã hóa này phải được thực hiện một cách cẩn thận để tránh những lỗ hổng bảo mật tiềm ẩn.

Nhìn chung, sử dụng mã hóa đầu cuối và các giao thức trao đổi khóa mang lại lợi ích lớn cho việc bảo vệ thông tin trong nhóm chat. Qua đồ án lần này, nhóm cũng cảm thấy cần tiếp tục nghiên cứu và phát triển các phương pháp an toàn hơn nữa để đáp ứng nhu cầu ngày càng tăng về bảo mật thông tin trong môi trường truyền thông số.

HẾT