1. Khái niệm

1.1 Quan hệ khóa

Quan hệ khóa (Keying relationship) là trạng thái mà trong đó các bên tham gia truyền thông chia sẻ dữ liệu chia sẻ (thường là khóa hoặc thành phần tạo ra khóa) để sử dụng cho các kỹ thuật mã hóa. Các dữ liệu chia sẻ có thể gồm:

- Khóa bí mật
- Khóa công khai
- Các giá trị khởi tạo
- Các tham số bổ sung không bí mật.

1.2 Quản lý khóa

Quản lý khóa (Key management) là một tập các kỹ thuật cho phép thiết lập và duy trì các quan hệ khóa giữ các bên có thẩm quyền. Cụ thể, quản lý khóa gồm các kỹ thuật và thủ tục cho phép:

- Khởi tạo các người dùng hệ thống (system users) trong một vùng (domain);
- Sinh khóa, phân phối và cài đặt các dữ liệu khóa;
- Kiểm soát việc sử dụng các dữ liệu khóa;
- Cập nhật, thu hồi và hủy các dữ liệu khóa;
- Lưu, sao lưu/khôi phục và lưu trữ các dữ liệu khóa.

1.3 Phân phối khóa

Phân phối khóa (Key distribution) là một thành phần của quản lý khóa, trong đó các khóa mật mã được vận chuyển, hoặc trao đổi giữa các thực thể trong một hệ thống, hay giữa các bên tham gia phiên truyền thông.

2. Vai trò và các nguy cơ mất an toàn quản lý khóa

Quản lý khóa là một khâu có vai trò quan trọng trong việc đảm bảo tính bí mật, toàn vẹn, xác thực, không thể chối bỏ và dịch vụ chữ ký số của một hệ mã hóa. Khâu quản lý khóa được thực hiện phù hợp sẽ đảm bảo cho các thông tin khóa được an toàn, đặc biệt khi có nhiều thực thể tham gia truyền thông. Các thông tin khóa được đảm bảo an toàn là yếu tố tiên quyết cho việc đảm bảo tính an toàn của hệ mã hóa.

Đứng trên góc độ quản lý, vấn đề quản lý khóa phải luôn được thực hiện trong khuôn khổ chính sách an ninh (Security policies) cụ thể. Chính sách an ninh của cơ quan, tổ chức cần có các nội dung mô tả về quản lý khóa, bao gồm:

- Các thực tế và thủ tục cần thực hiện trong các khía cạnh kỹ thuật và quản trị khóa tự động hoặc thủ công;

- Trách nhiệm của các bên có liên quan;
- Các bản ghi dữ liệu cần phải lưu để tạo các báo cáo về các vấn đề có liên quan đến an toàn khóa.

Ngoài ra, việc phân tích, nhận dạng các nguy cơ đe dọa an toàn của khâu quản lý khóa là một việc cần thiết, từ đó có thể đề ra và áp dụng các biện pháp đảm bảo an toàn phù hợp. Các nguy cơ đối với quản lý khóa bao gồm:

- Các khóa bí mật bị lộ;
- Tính xác thực của các khóa bí mật và công khai bị thỏa hiệp (compromise). Tính xác thực bao gồm các hiểu biết và việc kiểm chứng thông tin nhận dạng của một bên mà khóa được chia sẻ;
- Sử dụng trái phép các khóa bí mật và công khai:

+ Sử dụng các khóa đã hết hiệu lực;

+ Sử dụng các khóa sai mục đích.

3. Phân loại khóa

Các khóa/chìa mật mã (Cryptographic key) có thể được phân loại theo (1) khả năng sử dụng và (2) thời gian sử dụng. Theo khả năng sử dụng, có thể chia các khóa thành 3 lớp:

3.1 Khóa chủ (Master key):

+ Là các khóa ở mức cao nhất và không được bảo vệ bằng các kỹ thuật mật mã.

+ Các khóa chủ thường được chuyển giao trực tiếp và được bảo vệ bằng các cơ chế kiểm soát vật lý.

3.2 Khóa dùng cho trao đổi khóa (Key – encrypting key):

+ Là những khóa được sử dụng để vận chuyển hoặc lưu trữ các khóa khác.

+ Các khóa này cũng có thể được bảo vệ bằng khóa khác.

3.3 Khóa dữ liệu (Data keys):

+ Là các khóa được sử dụng để mã hóa dữ liệu cho người dùng.

+ Thường là các khóa ngắn hạn.

Theo thời gian sử dụng, có thể chia các khóa thành 2 lớp:

3.4 Khóa dài hạn (long-term key):

+ Là các khóa được sử dụng trong một khoảng thời gian dài;

+ Gồm khóa chủ, khóa dùng cho trao đổi khóa, hoặc khóa dùng cho thỏa thuận khóa.

3.5 Khóa ngắn hạn:

+ Là các khóa được sử dụng trong một khoảng thời gian ngắn hoặc chỉ trong

một phiên làm việc;

+ Gồm các khóa được trao đổi trong quá trình trao đổi khóa, thỏa thuận khóa;
+ Thường được dùng để mã hóa dữ liệu của người dùng.

4. Phân phối khóa bí mật

4.1 Đặt vấn đề

Như đã đề cập trong mục 3.3.1, các hệ mã hóa khóa đối xứng, hay khóa bí mật (Secret key cryptosystem) có ưu điểm là tính an toàn cao và tốc độ xử lý nhanh do kích thước khóa tương đối nhỏ. Tuy nhiên, hạn chế lớn nhất của chúng là khó khăn trong quản lý và phân phối khóa bí mật – các khóa bí mật dùng chung phải được phân phối, chia sẻ an toàn đến các bên tham gia trước khi có thể thực hiện phiên truyền thông an toàn.

Vấn đề phân phối khóa bí mật được khái quát hóa thành bài toán phân phối n^2 khóa. Bài toán này phát biểu như sau: Nếu một hệ thống có n người dùng tham gia truyền thông sử dụng kỹ thuật mã hóa khóa đối xứng và mỗi cặp người dùng cần trao đổi thông tin an toàn, thì mỗi cặp người dùng cần chia sẻ một khóa bí mật duy nhất. Như vậy, mỗi người dùng cần sở hữu n-1 khóa bí mật và tổng số khóa cần quản lý trong hệ thống là $n(n-1)/2 \approx n^2$. Ví dụ, nếu hệ thống có 10 người dùng, tổng số khóa cần quản lý là 10×9/2 = 45 khóa; với 100 người dùng, số khóa là 100×99/2 = 4.950 khóa; và với 1000 người dùng, số khóa là 1000×999/2 = 499.500 khóa. Số khóa cần quản lý sẽ rất lớn nếu số người dùng lớn và việc quản lý số lượng lớn khóa đảm bảo an toàn là rất khó khăn.

Để giải quyết bài toán phân phối n^2 khóa và đảm bảo an toàn trong phân phối các khóa bí mật, một số mô hình và kỹ thuật phân phối khóa bí mật được đề xuất và ứng dụng, bao gồm:

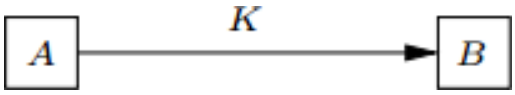
- Phân phối khóa điểm – điểm (Point-to-point key distribution)
- Trung tâm phân phối khóa (Key distribution center – KDC)
- Trung tâm dịch khóa (Key translation center – KTC)
- Sử dụng mã hóa khóa công khai để phân phối khóa bí mật.

Các mục tiếp theo mô tả chi tiết các mô hình và kỹ thuật phân phối khóa bí mật này.

4.2 Phân phối khóa điểm – điểm

Phân phối khóa điểm – điểm (Point-to-point key distribution) là hình thức phân phối khóa chỉ liên quan trực tiếp đến 2 thực thể tham gia truyền thông, như minh họa trên Hình 3.38. Hình thức phân phối khóa điểm – điểm có thể thực hiện thông qua các kênh tin cậy, như kênh truyền thuê riêng, hoặc thư bảo đảm. Phương pháp này có thể sử dụng với các trao đổi không thường xuyên và thích hợp với

các hệ thống cỡ nhỏ hoặc đóng kín. Nhược điểm của phương pháp này là trễ có thể lớn (như sử dụng thư bảo đảm) và các kênh tin cậy dùng riêng thường đắt tiền.

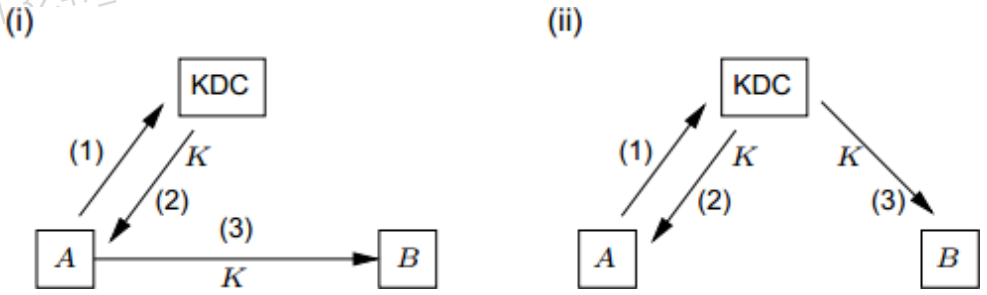


Hình 3.38. Phân phối khóa điểm – điểm

4.3 Trung tâm phân phối khóa

4.3.1 Giới thiệu

Trung tâm phân phối khóa (Key distribution center – KDC) là một trong các kỹ thuật được sử dụng rộng rãi để giải quyết bài toán n^2 khóa trong hệ thống có n người dùng. Mục tiêu là KDC tạo và phân phối khóa bí mật an toàn đến các thực thể trong hệ thống và giảm thiểu số lượng khóa dài hạn mà mỗi thực thể và KDC phải quản lý. Hình 3.39 biểu diễn mô hình hoạt động của hệ thống KDC gồm 3 thực thể: Trung tâm phân phối khóa KDC ký hiệu là T và 2 thực thể thành viên tham gia trao đổi khóa là A và B. Khóa bí mật cần trao đổi là K. Hoạt động của hệ thống KDC gồm 2 khâu: (1) Khởi tạo – thiết lập môi trường và các tham số hoạt động và (2) Thủ tục phân phối khóa sử dụng KDC.



Hình 3.39. Mô hình hoạt động của trung tâm phân phối khóa – KDC

4.3.2 Khởi tạo

Trong quá trình khởi tạo, thực thể A sở hữu khóa dài hạn K_{AT} và A chia sẻ K_{AT} với KDC T. Thực thể B sở hữu khóa dài hạn K_{BT} và B chia sẻ K_{BT} với KDC T. Trung tâm phân phối khóa T là một máy chủ tin cậy, cho phép hai bên A và B không trực tiếp chia sẻ thông tin khóa thiết lập kênh truyền thông an toàn sử dụng hai khóa dài hạn K_{AT} và K_{BT}.

4.3.3 Thủ tục phân phối khóa

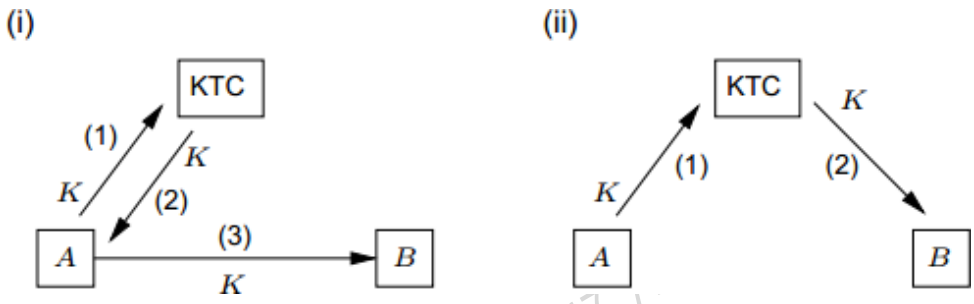
Hình 3.39 biểu diễn mô hình hoạt động của trung tâm phân phối khóa. Gọi E là hàm mã hóa, D là hàm giải mã, thủ tục phân phối khóa sử dụng KDC T như sau:

- A yêu cầu chia sẻ khóa với B;
- T sẽ tạo ra hoặc lấy khóa có sẵn K và mã hóa K thành $E_{KAT}(K)$ và gửi cho A;
- T cũng có thể gửi khóa cho B dưới dạng $E_{KBT}(K)$ thông qua A (hình i);
- T cũng có thể gửi khóa trực tiếp cho B dưới dạng $E_{KBT}(K)$ (hình ii);
- A nhận được $E_{KAT}(K)$, giải mã sử dụng K_{AT} để có được K: $D_{KAT}(E_{KAT}(K)) = K$
- B nhận được $E_{KBT}(K)$, giải mã sử dụng K_{BT} để có được K: $D_{KBT}(E_{KBT}(K)) = K$

4.4 Trung tâm dịch khóa

4.4.1 Giới thiệu

Trung tâm dịch chuyển khóa (Key translation center – KTC) là một trong các kỹ thuật được sử dụng rộng rãi để giải quyết bài toán n^2 khóa trong hệ thống có n người dùng. Vai trò của KTC tương tự KDC, tuy nhiên một bên tham gia truyền thông sẽ cung cấp khóa trao đổi. Mục tiêu là KTC chuyển khóa bí mật an toàn đến các thực thể còn lại tham gia truyền thông trong hệ thống và giảm thiểu số lượng khóa dài hạn mà mỗi thực thể và KTC phải quản lý. Điểm khác biệt của KTC so với KDC là KTC cho phép sinh khóa phân tán (các thực thể tự sinh khóa), còn KDC cho phép sinh khóa tập trung (KDC sinh khóa). Hình 3.40 biểu diễn mô hình hoạt động của hệ thống KTC gồm 3 thực thể: Trung tâm dịch chuyển khóa KTC ký hiệu là T và 2 thực thể thành viên tham gia trao đổi khóa là A và B. Khóa bí mật cần trao đổi là K. Hoạt động của hệ thống KTC gồm 2 khâu: (1) Khởi tạo – thiết lập môi trường và các tham số hoạt động và (2) Thủ tục phân phối khóa sử dụng KTC.



Hình 3.40. Mô hình hoạt động của trung tâm dịch chuyển khóa – KTC

a. Khởi tạo

Trong quá trình khởi tạo, thực thể A sở hữu khóa dài hạn K_{AT} và A chia sẻ K_{AT} với KTC T. Thực thể B sở hữu khóa dài hạn K_{BT} và B chia sẻ K_{BT} với KTC T. Trung tâm phân phối khóa T là một máy chủ tin cậy, cho phép hai bên A và B không trực tiếp chia sẻ thông tin khóa thiết lập kênh truyền thông an toàn sử dụng

hai khóa dài hạn K_{AT} và K_{BT}.

4.4.2 Thủ tục phân phối khóa

Hình 3.40 biểu diễn mô hình hoạt động của trung tâm dịch chuyển khóa. Gọi E là hàm mã hóa, D là hàm giải mã, thủ tục phân phối khóa sử dụng KTC T như sau:

- A tạo ra khóa K và mã hóa K thành $E_{KAT}(K)$ và gửi cho T;
- T nhận được $E_{KAT}(K)$, giải mã sử dụng K_{AT} thu được K: $D_{KAT}(E_{KAT}(K)) = K$
- Sau đó, T mã hóa khóa K sử dụng K_{BT} để có $E_{KBT}(K)$;
- T có thể gửi khóa cho B dưới dạng $E_{KBT}(K)$ thông qua A (hình i);
- T cũng có thể gửi khóa trực tiếp cho B dưới dạng $E_{KBT}(K)$ (hình ii);
- B nhận được $E_{KBT}(K)$, giải mã sử dụng K_{BT} để có được K: $D_{KBT}(E_{KBT}(K)) = K$

4.4.3 Ưu điểm và nhược điểm của quản lý khóa tập trung (KDC và KTC)

- Ưu điểm:

+ Hiệu quả trong lưu trữ khóa: mỗi bên chỉ cần duy trì một khóa bí mật dài hạn với bên tin cậy (không phải với bên trao đổi thông tin);

+ Tổng số khóa dài hạn cần lưu trữ là n khóa (so với n^2 khóa).

- Nhược điểm:

+ Cả hệ thống có thể bị mất an toàn nếu trung tâm quản lý khóa bị thỏa hiệp (bị điều khiển);

+ Trung tâm quản lý khóa có thể thành điểm nút cổ chai;

+ Dịch vụ sẽ phải ngừng nếu trung tâm quản lý khóa gặp trục trặc;

+ Cần có một máy chủ tin cậy ở chế độ trực tuyến.

4.4.4 Sử dụng mã hóa khóa công khai để phân phối khóa bí mật

Do các hệ mã hóa khóa công khai có ưu điểm là phân phối khóa công khai dễ dàng, có thể sử dụng mã hóa khóa công khai để phân phối khóa bí mật. Các giao thức SSL/TLS và PGP đều sử dụng phương pháp này một cách hiệu quả để trao đổi khóa bí mật, hoặc dữ liệu khóa bí mật cho phiên làm việc. Chi tiết về các giao thức này được đề cập ở mục 3.6.

Giả thiết bên A cần chuyển khóa bí mật Ks cho bên B. Các bước hai bên A và B cần thực hiện để chuyển khóa bí mật Ks từ A đến B sử dụng mã hóa khóa công khai như sau:

- B tạo cặp khóa, khóa công khai Kp và khóa riêng Kr;
- B gửi khóa công khai Kp của mình cho A (cần đảm bảo tính xác thực và

toàn vẹn của Kp);

- A sử dụng Kp để mã hóa khóa bí mật Ks tạo bản mã Cs và gửi cho B;
- B sử dụng khóa riêng Kr để giải mã Cs để khôi phục khóa bí mật Ks.

5. Phân phối khóa công khai

5.1 Giới thiệu

Khác với khóa bí mật, việc phân phối khóa công khai thuận lợi hơn do khóa công khai có thể trao đổi công khai giữa các thực thể tham gia truyền thông. Tuy nhiên, việc phân phối khóa công khai phải đảm bảo tính xác thực (authentic public keys). Tính xác thực của khóa công khai thể hiện ở 2 yếu tố: (1) tính toàn vẹn và chủ thể luôn xác định. Các phương pháp phân phối khóa công khai được sử dụng rộng rãi bao gồm:

- Trao đổi kiểu điểm-điểm thông qua kênh tin cậy;
- Truy nhập trực tiếp vào danh mục công cộng (public-key registry);
- Sử dụng một máy chủ trực tuyến tin cậy;
- Sử dụng một máy chủ không trực tuyến và chứng chỉ.

Phương pháp trao đổi khóa công khai kiểu điểm-điểm thông qua kênh tin cậy được thực hiện tương tự như phương pháp trao đổi khóa bí mật kiểu điểm-điểm đã được trình

bày ở mục 3.5.2.2. Các phương pháp phân phối khóa công khai còn lại được trình bày trong các mục tiếp theo.

5.2 Truy nhập trực tiếp vào danh mục công cộng (public-key registry)

Trong phương pháp này, một cơ sở dữ liệu công cộng tin cậy được thiết lập, trong đó mỗi bản ghi gồm tên người dùng và khóa công khai tương ứng. Cơ sở dữ liệu công cộng này có thể được vận hành bởi 1 bên tin cậy và người dùng có thể truy nhập khóa công khai từ cơ sở dữ liệu này nếu biết tên người dùng. Một phương pháp thực hiện được sử dụng phổ biến là cây xác thực khóa công khai (Tree authentication of public keys).

5.3 Sử dụng một máy chủ trực tuyến tin cậy

Trong phương pháp này, một máy chủ trực tuyến tin cậy được sử dụng để cung cấp truy nhập đến cơ sở dữ liệu công cộng các khóa công khai. Khóa công khai cần phân phối được ký sử dụng khóa riêng của máy chủ và gửi cho bên yêu cầu. Phương pháp này không đòi hỏi phải sử dụng kênh truyền bí mật. Bên yêu cầu sử dụng khóa công khai của máy chủ để xác thực chữ ký của máy chủ và qua đó kiểm tra tính xác thực, toàn vẹn của khóa. Phương pháp này có nhược điểm là máy chủ phải luôn trực tuyến để hệ thống có thể hoạt động và bản thân máy chủ có thể trở thành điểm nút cổ chai trong hệ thống.

5.4 Sử dụng một máy chủ không trực tuyến và chứng chỉ

Đây là phương pháp phân phối khóa dựa trên chứng chỉ khóa công khai (Public key certificate) được sử dụng rất rộng rãi trong bảo mật thông tin truyền trên mạng Internet. Các bước thực hiện của phương pháp này gồm:

- Bên A liên hệ với một bên tin cậy (được gọi là Cơ quan cấp chứng chỉ - Certification Authority (CA)) để đăng ký khóa công khai của mình và nhận được chữ ký xác nhận khóa công khai của CA;
- CA cấp một chứng chỉ (Certificate) cho khóa công khai của A, trong đó kết hợp khóa công khai của A với thông tin định danh của A sử dụng chữ ký số của CA;
- Khi A đã có chứng chỉ khóa công khai (Public key certificate), A có thể gửi khóa công khai cho các bên có liên quan bằng cách gửi chứng chỉ khóa công khai.
- Chứng chỉ khóa công khai cũng có thể được đưa vào danh mục công cộng và người dùng khác có thể truy nhập.

Chi tiết về chứng chỉ khóa công khai và quá trình cấp phát – sử dụng chứng chỉ đã được đề cập ở các mục 3.4.2 và 3.4.3.