TCVN TIÊU CHUẨN QUỐC GIA

TCVN 9696-2 : 2013
ISO 7498-2 : 1989

Xuất bản lần 1

CÔNG NGHỆ THÔNG TIN – LIÊN KẾT HỆ THỐNG MỞ - MÔ HÌNH THAM CHIẾU CƠ SỞ - PHẦN 2: KIẾN TRÚC AN NINH

Information technology - Open Systems Interconnection - Basic Reference Model - Part 2: Security architecture

HÀ NỘI - 2013

Mục lục **Trang**

Lời nói đầu

TCVN 9696-2:2013 hoàn toàn tương đương với ISO 7498-2:1989

TCVN 9696-2:2013 do Ban kỹ thuật tiêu chuẩn quốc gia TCVN/JTC 1 "*Công nghệ thông tin*" biên soạn, Tổng cục Tiêu chuẩn Đo lường Chất lượng đề nghị, Bộ Khoa học và Công nghệ công bố.

Bộ TCVN 9696 (ISO/IEC 7498) *Công nghệ thông tin - Liên kết hệ thống mở - Mô hình tham chiếu cơ sở*, gồm các phần sau đây:

- TCVN 9696-1:2013 (ISO/IEC 7498-1:1994) Phần 1: Mô hình cơ sở
- TCVN 9696-2:2013 (ISO 7498-2:1989) Phần 2: Kiến trúc an ninh
- TCVN 9696-3:2013(ISO/IEC 7498-3:1997) Phần 3: Đặt tên và ghi địa chỉ
- TCVN 9696-4:2013 (ISO/IEC 7498-4:1989) Phần 4: Khung tổng quát về quản lý

Lời giới thiệu

Bộ tiêu chuẩn này mô tả mô hình tham chiếu cơ sở về liên kết hệ thống mở (OSI). Tiêu chuẩn này thiết lập khung tổng quát cho việc phối hợp xây dựng các tiêu chuẩn hiện có và các tiêu chuẩn trong tương lai về liên kết các hệ thống.

Mục đích của OSI là cho phép liên kết các hệ thống máy tính không đồng nhất sao cho có thể đạt được việc truyền thông có ích giữa các quy trình ứng dụng. Tại các thời điểm khác nhau, các kiểm soát an ninh phải được thiết lập để bảo vệ thông tin trao đổi giữa hai quy trình ứng dụng. Các kiểm soát này nên có giá cao hơn giá trị tiềm năng trong việc nhận và sửa đổi dữ liệu hoặc tạo ra thời gian được yêu cầu để nhận dữ liệu rất lớn mà giá trị của dữ liệu bị mất mát.

Tiêu chuẩn này xác định các phần tử kiến trúc liên quan đến an ninh chung có thể áp dụng trong các trường hợp nhằm bảo vệ truyền thông giữa các hệ thống mở được yêu cầu. Trong khung tổng quát của mô hình tham chiếu, còn thiết lập các hướng dẫn và các ràng buộc nhằm cải tiến các tiêu chuẩn hiện có hoặc để xây dựng các tiêu chuẩn mới trong ngữ cảnh OSI để cho phép truyền thông an toàn và cung cấp một phương pháp tiếp cận nhất quán cho an ninh trong OSI

Bối cảnh trong an ninh sẽ có giúp ích trong việc lĩnh hội tiêu chuẩn này. Người sử dụng không am hiểu về an ninh nên đọc Phụ lục A trước.

Tiêu chuẩn này mở rộng mô hình tham chiếu cơ sở nhằm bao hàm các khía cạnh an ninh, các khía cạnh này là các phần tử kiến trúc chung của các giao thức truyền thông nhưng không được bàn đến trong mô hình tham chiếu cơ sở.

Công nghệ thông tin - Liên kết hệ thống mở - Mô hình tham chiếu cơ sở - Phần 2: Kiến trúc an ninh

Information technology - Open systems interconnection - Basic reference model - Part 2: Security Architecture

1 Phạm vi áp dụng

Tiêu chuẩn này:

a) Cung cấp mô tả chung về các dịch vụ an ninh và các cơ chế liên quan mà có thể được cung cấp bởi mô hình tham chiếu; và

b) Xác định các vị trí trong mô hình tham chiếu, các vị trí này có thể cung cấp dịch vụ và cơ chế.

Tiêu chuẩn này mở rộng lĩnh vực áp dụng của Bộ tiêu chuẩn TCVN 9696 nhằm kiểm soát truyền thông đảm bảo giữa các hệ thống.

Các dịch vụ, cơ chế an ninh cơ sở và sự sắp xếp của chúng được định danh cho tất cả các tầng của mô hình tham chiếu cơ sở. Ngoài ra, các mối quan hệ cấu trúc của các dịch vụ và cơ chế an ninh với mô hình tham chiếu cơ sở cũng được định danh. Các biện pháp an ninh bổ sung được yêu cầu trong các hệ thống cuối, các trạm và các tổ chức. Các biện pháp này áp dụng trong các ngữ cảnh ứng dụng khác nhau. Định nghĩa các dịch vụ an ninh nhằm hỗ trợ các biện pháp an ninh nằm ngoài phạm vi áp dụng của tiêu chuẩn này.

Các chức năng an ninh OSI đề cập đến các khía cạnh hữu hình của đường truyền thông, giúp các hệ thống cuối có thể truyền được thông tin bảo đảm. An ninh OSI không đề cập đến các biện pháp an ninh yêu cầu trong các hệ thống cuối, các trạm và các tổ chức, ngoại trừ nơi có liên quan đến lựa chọn và vị trí của các dịch vụ an ninh trong OSI. Các khía cạnh an ninh tiếp theo có thể được tiêu chuẩn hóa nhưng không nằm trong phạm vi của Bộ tiêu chuẩn này.

Tiêu chuẩn này bổ sung các khái niệm và các nguyên tắc có trong bộ tiêu chuẩn TCVN 9696 (ISO 7498) mà không sửa đổi các khái niệm và nguyên tắc đó. Tiêu chuẩn này không phải một đặc tả thực thi, cũng không phải là cơ sở đánh giá sự phù hợp của các thực thi thực.

2 Tài liệu viện dẫn

Các tài liệu viện dẫn sau là rất cần thiết cho việc áp dụng tiêu chuẩn. Đối với các tài liệu viện dẫn ghi năm công bố thì áp dụng bản được nêu. Đối với các tài liệu viện dẫn không ghi năm công bố thì áp dụng phiên bản mới nhất, bao gồm cả các sửa đổi.

TCVN 9696 (ISO 7498) Công nghệ thông tin – Liên kết hệ thống mở – Mô hình tham chiếu Cơ sở.

TCVN 9696-4:2013 (ISO 7598-4) Công nghệ thông tin – Liên kết hệ thống mở - Phần 4: Khung tổng quát quản lý.

ISO 7498/Add.1 Information processing systems – Open Systems Interconnection – Basic Reference Model – Addendum 1: Connectionless-mode transmission (Công nghệ thông tin – Liên kết hệ thống mở - Mô hình tham chiếu cơ sở - Phần bổ sung 1: Truyền dẫn chế độ không-kết nối.)

ISO 8648 Information processing systems – Open Systems Interconnection – Internal organization of the Network Layer (Công nghệ thông tin – Liên kết hệ thống mở - Tổ chức bên trong của tầng mạng)

3 Định nghĩa và từ viết tắt

3.1 Tiêu chuẩn này sử dụng các thuật ngữ sau đây:

a) Kết nối-tầng (N) ;

b) Truyền dẫn dữ liệu-tầng (N);

c) Thực thể-tầng (N);

d) Tiện ích-tầng (N);

e) Tầng (N);

f) Hệ thống mở

g) Các thực thể ngang hàng;

h) Giao thức-tầng (N);

i) Đơn vị dữ liệu giao thức-tầng (N);

k) Chuyển tiếp-tầng (N);

l) Xếp chuỗi;

m) Dịch vụ-tầng (N) ;

n) Đơn vị dữ liệu dịch vụ-tầng (N);

o) Dữ liệu người sử dụng-tầng (N);

p) Mạng con;

q)Tài nguyên OSI, và

s) Cú pháp truyền.

3.2 Tiêu chuẩn này sử dụng các thuật ngữ lấy từ các tiêu chuẩn tương ứng sau đây:

- Truyền dẫn chế độ không-kết nối (ISO 7498/Add.1)
- Hệ thống cuối (TCVN 9696)
- Chức năng chuyển tiếp và định tuyến (ISO 8648)
- Cơ sở thông tin quản lý (TCVN 9696-4:2013)

Ngoài ra, các từ viết tắt sau đây được sử dụng:

- OSI: liên kết hệ thống mở;
- SDU: đơn vị dữ liệu dịch vụ;
- SMIB: cơ sở thông tin quản lý an ninh; và
- MIB: cơ sở thông tin quản lý.

3.3 Tiêu chuẩn này áp dụng các định nghĩa sau đây:

3.3.1

Điều khiển truy cập (access control)

Ngăn ngừa việc sử dụng tài nguyên trái phép, bao gồm việc ngăn ngừa sử dụng tài nguyên không đúng cách.

3.3.2

Danh mục điều khiển truy cập (access control list)

Danh mục các thực thể cùng với các quyền truy cập của chúng, trong đó được phép truy cập tài nguyên.

3.3.3

Trách nhiệm giải trình (accountability)

Đặc tính đảm bảo rằng các hoạt động của một thực thể phải được theo dõi chỉ thực thể đó.

3.3.4

Mối đe dọa kích hoạt (active threat)

Mối đe dọa về việc cố ý thay đổi trạng thái của hệ thống.

CHÚ THÍCH – Các ví dụ về các mối đe dọa tích cực liên quan đến an ninh có thể là: sửa đổi các thông điệp, phát lại các thông điệp, chèn các thông điệp giả mạo, giả mạo là một thực thể có thẩm quyền và chối bỏ dịch vụ.

3.3.5

Kiểm định (audit)

Xem phần **kiểm định an ninh**.

3.3.6

Biên bản kiểm định (audit trail)

Xem phần **biên bản kiểm định an ninh**.

3.3.7

Xác thực (authentication)

Xem phần **xác thực nguồn gốc dữ liệu**, và **xác thực thực thể ngang hàng**.

CHÚ THÍCH – Trong tiêu chuẩn này, thuật ngữ "xác thực" được sử dụng kết hợp với tính toàn vẹn; thuật ngữ "tính toàn vẹn dữ liệu" được sử dụng để thay thế.

3.3.8

Thông tin xác thực (authentication information)

Thông tin sử dụng để thiết lập tính hiệu lực của định danh đã yêu cầu.

3.3.9

Trao đổi xác thực (authentication exchange)

Cơ chế đảm bảo định danh thực thể bằng trao đổi thông tin.

3.3.10

Cấp quyền (authorization)

Việc cấp quyền bao gồm cấp quyền truy cập dựa trên các quyền truy cập.

3.3.11

Tính sẵn có (availability)

Đặc tính có thể truy cập và sử dụng dựa trên yêu cầu bởi thực thể có thẩm quyền.

3.3.12

Khả năng (capability)

Thẻ lệnh được sử dụng như một thẻ định danh đối với tài nguyên sở hữu thẻ lệnh trao các quyền truy cập cho tài nguyên.

3.3.13

Kênh (Channel)

Đường truyền thông tin.

3.3.14

Bản mã (ciphertext)

Dữ liệu tạo ra thông qua việc sử dụng **bản mã**. Nội dung của dữ liệu kết quả là không có sẵn.

CHÚ THÍCH – Bản mã có thể là đầu vào của **mã hóa** sao cho đầu ra siêu mã hóa được tạo ra.

3.3.15

Bản rõ (cleartext)

Dữ liệu dễ hiểu, nội dung ngữ nghĩa của văn bản luôn có sẵn.

3.3.16

Tính mật (confidentiality)

Đặc tính mà thông tin không được tạo sẵn cho các cá nhân, thực thể hoặc các quy trình có thẩm quyền.

3.3.17

Thư ủy nhiệm (credentials)

Dữ liệu được truyền nhằm thiết lập định danh đã yêu cầu của thực thể.

3.3.18

Phân tích giải mã (cryptanalysis)

Phân tích hệ thống mật mã và/hoặc các đầu vào và đầu ra nhằm dẫn xuất các biến tin cậy và/hoặc dữ liệu nhảy cảm bao gồm **bản rõ.**

3.3.19

Giá trị kiểm tra mật mã (cryptographic checkvalue)

Thông tin mà được dẫn xuất bằng cách thực hiện việc biến đổi mật mã (xem phần **mật mã**) trên đơn vị dữ liệu.

CHÚ THÍCH – Việc dẫn xuất giá trị kiểm tra có thể được thực hiện trong một hoặc nhiều bước và là một kết quả của chức năng toán học của khóa và đơn vị dữ liệu. Giá trị này thường được sử dụng để kiểm tra tính toàn vẹn của đơn vị dữ liệu.

3.3.20

Mật mã (crytography)

Quy tắc bao gồm các nguyên tắc, phương tiện và phương pháp về việc biến đổi dữ liệu để giấu nội dung thông tin của nó, ngăn ngừa việc sửa đổi và/hoặc việc sử dụng trái phép.

CHÚ THÍCH – Mật mã xác định các phương pháp sử dụng trong việc mã hóa và giải mã. Sự tác động vào nguyên tắc, phương tiện hoặc phương pháp mật mã là phân tích giải mã.

3.3.21

Tính toàn vẹn dữ liệu (data integrity)

Đặc tính mà dữ liệu không bị thay đổi hoặc phá huỷ một cách trái phép.

3.3.22

Xác thực nguồn gốc dữ liệu (data origin authentication)

Chứng thực rằng nguồn dữ liệu đã nhận là được yêu cầu.

3.3.23

Giải mã (decipherment)

Sự ngược lại của **mã hoá** thuận nghịch tương ứng.

3.3.24

Giải mã (decryption)

Xem điều 3.3.23.

3.3.25

Từ chối dịch vụ (denial of service)

Ngăn ngừa việc truy cập trái phép các tài nguyên hoặc làm trễ các thao tác giới hạn thời gian.

3.3.26

Chữ ký số (digital signature)

Dữ liệu gắn với hoặc biến đổi mật mã của (xem phần **mật mã**), đơn vị dữ liệu cho phép người nhận đơn vị dữ liệu chứng minh nguồn và tính toàn vẹn của đơn vị dữ liệu và bảo vệ khỏi sự giả mạo chữ ký, ví dụ: bởi người nhận.

3.3.27

Mã hoá (encipherment)

Sự biến đổi mật mã của dữ liệu (xem phần **mật mã**) để tạo ra văn bản thuần tuý.

CHÚ THÍCH – Mã hoá phi thuận nghịch, là trường hợp mà quy trình giải mã tương ứng không được thực hiện.

3.3.28

Mã hoá (encryption)

Xem điều 3.3.27.

3.3.29

Mã hoá toàn trình (end-to-end encipherment)

Mã hoá dữ liệu trong hoặc tại hệ thống đầu cuối nguồn, với sự **giải mã** tương ứng chỉ xảy ra trong hoặc tại hệ thống cuối đích. (cũng xem **mã hoá từng kết nối**)

3.3.30

Chính sách an ninh dựa trên định danh (identity-based security policy)

Chính sách an ninh dựa trên các định danh và/hoặc các thuộc tính của người sử dụng, nhóm người sử dụng hoặc các thực thể hoạt động thay mặt cho người sử dụng và các tài nguyên/đối tượng đang được truy cập.

3.3.31

Tính toàn vẹn (integrity)

Xem phần **Tính toàn vẹn của dữ liệu**.

3.3.32

Khoá (key)

Chuỗi ký hiệu điều khiển các thao tác của **mã hoá** và **giải mã**.

3.3.33

Quản lý khoá (key management)

Việc tạo, lưu trữ, phân tán, xoá và ứng dụng các khoá theo **chính sách an ninh**.

3.3.34

Mã hoá từng kết nối (link-by-link encipherment)

Ứng dụng riêng lẻ của **mã hoá** dữ liệu trên mỗi kết nối của hệ thống truyền thông. (Cũng xem **mã hoá toàn trình**.)

CHÚ THÍCH - Sự kéo theo của việc mã hoá từng kết nối là dữ liệu sẽ tồn tại ở dạng văn bản thuần tuý trong các thực thể chuyển tiếp.

3.3.35

Phát hiện thao tác (manipulation detection)

Cơ chế được sử dụng để phát hiện xem liệu đơn vị dữ liệu có bị sửa đổi hay không (ngẫu nhiên hoặc cố ý)

3.3.36

Sự giả mạo (masquerade)

Thực thể giả mạo là một thực thể khác.

3.3.37

Sự chứng nhận (notarization)

Đăng ký dữ liệu với bên thứ ba tin cậy cho phép đảm bảo tính chính xác của các đặc điểm như nội dung, nguồn gốc, thời gian và việc phân phát.

3.3.38

Mối đe dọa bị động (passive threat)

Luồng thông tin chưa phơi bày không làm thay đổi trạng thái của hệ thống.

3.3.39

Mật khẩu (password)

Thông tin xác thực thường bao gồm một xâu các ký tự.

3.3.40

Xác thực thực thể ngang hàng (peer-entity authentication)

Chứng thực rằng thực thể ngang hàng trong một liên kết là một thực thể đã yêu cầu.

3.3.41

An ninh vật lý (physical security)

Các biện pháp sử dụng để cung cấp việc bảo vệ các tài nguyên chống lại các mối đe doạ ngẫu nhiên và có chủ ý.

3.3.42

Chính sách (policy)

Xem phần **chính sách an ninh**.

3.3.43

Sự riêng tư (privacy)

Quyền của cá nhân là kiểm soát hoặc tác động đến thông tin liên quan đến họ có thể được tập hợp hoặc lưu trữ bởi cá nhân và đến cá nhân mà thông tin có thể được phơi bày.

CHÚ THÍCH - Bởi vì thuật ngữ này liên quan đến quyền cá nhân nên nó có thể không chính xác lắm và việc sử dụng của nó nên được tránh ngoại trừ việc đẩy mạnh yêu cầu an ninh.

3.3.44

Sự chối bỏ (repudiation)

Sự từ chối bởi một trong các thực thể liên quan đến truyền thông tham giao vào tất cả hoặc một phần của truyền thông.

3.3.45

Điều khiển định tuyến (routing control)

Ứng dụng các quy tắc trong suốt quy trình định tuyến để chọn hoặc tránh các mạng, các kết nối hoặc các chuyển tiếp cụ thể.

3.3.46

Chính sách an ninh dựa trên quy tắc (rule-based security policy)

Chính sách an ninh dựa trên các quy tắc toàn cầu áp đặt cho tất cả người người sử dụng. Các quy tắc này dựa vào một so sánh về độ nhạy của các tài nguyên đang được truy cập và việc sở hữu các thuộc tính người sử dụng tương ứng, nhóm người sử dụng hoặc các thực thể hoạt động thay mặt người sử dụng.

3.3.47

Kiểm định an ninh (security audit)

Sự xem xét và kiểm tra độc lập với các bản ghi và hoạt động của hệ thống nhằm thử nghiệm tính đầy đủ của các bộ điều khiển hệ thống, đảm bảo sự phù hợp với chính sách đã thiết lập và các thủ tục vận hành nhằm phát hiện ra các vi phạm về an ninh và để khuyến cáo các thay đổi trong bộ điều khiển, chính sách và các thủ tục.

3.3.48

Theo dõi kiểm định an ninh (security audit trail)

Dữ liệu tập hợp và sử dụng để thuận lợi hoá cho kiểm định an ninh.

3.3.49

Nhãn an ninh (security label)

Đánh dấu ranh giới cho tài nguyên (có thể là đơn vị dữ liệu) trong đó đặt tên hoặc chỉ định các thuộc tính an ninh của tài nguyên đó.

CHÚ THÍCH – Đánh dấu và/hoặc gắn kết có thể rõ ràng hoặc không rõ ràng.

3.3.50

Chính sách an ninh (security policy)

Tập các tiêu chí về sự cung cấp các dịch vụ an ninh (cũng xem chính sách an ninh **dựa trên quy tắc** và **dựa trên định danh**)

CHÚ THÍCH - Một chính sách an ninh hoàn thiện sẽ đề cập đến nhiều mối quan tâm nằm ngoài phạm vi của OSI.

3.3.51

Dịch vụ an ninh (security service)

Dịch vụ đảm bảo an ninh của các hệ thống hoặc các chuyển giao dữ liệu được cung cấp bởi một tầng gồm các hệ thống mở truyền thông.

3.3.52

Bảo vệ trường lựa chọn (selective field protection)

Bảo vệ các trường cụ thể trong một thông điệp được truyền.

3.3.53

Độ nhạy (sensitivity)

Đặc tính của tài nguyên trong đó bao hàm giá trị hoặc tầm quan trọng của nó và có thể bao gồm khả năng bị xâm phạm.

3.3.54

Chữ ký (signature)

Xem phần **chữ ký số**.

3.3.55

Mối đe doạ (threat)

Sự vi phạm về an ninh.

3.3.56

Phân tích lưu lượng (traffic analysis)

Sự suy diễn thông tin từ quan sát các luồng lưu lượng (sự có mặt, sự vắng mặt, số lượng, hướng và tần số).

3.3.57

Tính mật của luồng lưu lượng (traffic flow confidentiality)

Dịch vụ tin cẩn bảo vệ khỏi sự phân tích lưu lượng.

3.3.58

Đệm lưu lượng (traffic padding)

Việc tạo ra các tình huống giao tiếp, các đơn vị dữ liệu và/hoặc dữ liệu không xác thực trong các đơn vị dữ liệu.

3.3.59

Chức năng tin cậy (trusted functionality)

Chức năng này được cho là đúng đối với một số tiêu chí, ví dụ: được thiết lập bởi một chính sách an ninh.

4 Ký hiệu

Ký hiệu về tầng được sử dụng giống với ký hiệu xác định trong bộ tiêu chuẩn TCVN 9696(ISO 7498)

Mặt khác, thuật ngữ "dịch vụ" không đủ điều kiện được sử dụng để đề cập đến dịch vụ an ninh.

5 Mô tả chung các dịch vụ và cơ chế an ninh

5.1 Tổng quát

Các dịch vụ an ninh có trong kiến trúc và các cơ chế an ninh OSI trong đó thực hiện các dịch vụ được nêu ra ở điều này. Các dịch vụ an ninh mô tả dưới đây là các dịch vụ an ninh cơ sở. Thực tế, chúng sẽ được gọi ra ở các tầng thích hợp và trong các liên kết thích hợp, thường với các dịch vụ và cơ chế không theo OSI nhằm thỏa mãn chính sách an ninh và/hoặc các yêu cầu của người sử dụng. Các cơ chế an ninh riêng có thể được sử dụng để thực hiện các liên kết của các dịch vụ an ninh cơ sở. Thực tế của hệ thống có thể thực hiện các liên kết riêng của các dịch vụ an ninh cơ sở đối với dẫn chứng trực tiếp.

5.2 Các dịch vụ an ninh

Các vấn đề được xem xét sau đây là các dịch vụ an ninh, các dịch vụ an ninh này có thể được cung cấp một cách tùy chọn trong khung tổng quát của mô hình tham chiếu OSI. Các dịch vụ xác thực yêu cầu thông tin xác thực bao gồm thông tin dự trữ cục bộ và dữ liệu được truyền (thư ủy nhiệm) nhằm thuận lợi hóa việc xác thực.

5.2.1 Xác thực

Các dịch vụ này cung cấp cho việc xác thực của thực thể truyền ngang hàng và nguồn dữ liệu như đã mô tả dưới đây.

5.2.1.1 Xác thực thực thể ngang hàng

Dịch vụ này khi được cung cấp bởi tầng (N) chứng thực cho thực thể-tầng (N+1) rằng thực thể ngang hàng là thực thể-tầng (N+1) đã yêu cầu.

Dịch vụ này được cung cấp để sử dụng tại lúc thiết lập hoặc tại các thời điểm trong suốt giai đoạn truyền dữ liệu của kết nối nhằm xác nhận các định danh của một hoặc nhiều thực thể kết nối nối với một hoặc nhiều các thực thể khác. Dịch vụ này cung cấp sự tin tưởng ở thời điểm sử dụng mà một thực thể cố gắng làm lại kết nối giả mạo hoặc trái phép trước đó. Các lược đồ xác thực thực thể ngang hàng một chiều và hai chiều cần hoặc không cần kiểm tra, có thể cung cấp các mức độ bảo vệ khác nhau.

5.2.1.2 Xác thực nguồn gốc dữ liệu

Dịch vụ này khi được cung cấp bởi tầng (N), cung cấp chứng thực cho thực thể-tầng (N+1) rằng nguồn dữ liệu là thực thể ngang hàng-tầng (N+1) đã yêu cầu.

Dịch vụ xác thực nguồn gốc dữ liệu cung cấp chứng thực của nguồn đơn vị dữ liệu. Dịch vụ không cung cấp việc bảo vệ khỏi việc sao chép hoặc sửa đổi các đơn vị dữ liệu.

5.2.2 Điều khiển truy cập

Dịch vụ này cung cấp chế độ bảo vệ để chống lại việc sử dụng trái phép các tài nguyên có thể truy cập qua OSI. Các tài nguyên này có thể là các tài nguyên OSI hoặc không theo OSI truy cập qua các giao thức OSI. Dịch vụ bảo vệ này có thể được áp dụng cho các kiểu truy cập tài nguyên khác nhau (ví dụ: việc sử dụng tài nguyên truyền; đọc, viết hoặc xóa nguồn thông tin; việc thực hiện một tài nguyên xử lý) hoặc cho tất cả các truy cập tài nguyên.

Điều khiển truy cập theo các chính sách an ninh khác nhau (xem điều 6.2.1.1).

5.2.3 Tính cẩn mật của dữ liệu

Các dịch vụ này cung cấp việc bảo vệ dữ liệu khỏi sự phơi bày trái phép.

5.2.3.1 Tính cẩn mật của kết nối

Dịch vụ này cung cấp tính cẩn mật của tất cả dữ liệu người sử dụng-tầng (N) trên kết nối-tầng (N).

CHÚ THÍCH – Phụ thuộc vào người sử dụng và tầng, nó có thể không thích hợp để bảo vệ tất cả dữ liệu, ví dụ: dữ liệu được tiến hành hoặc dữ liệu trong một yêu cầu kết nối.

5.2.3.2 Tính cẩn mật của không kết nối

Dịch vụ này cung cấp tính cẩn mật của tất cả dữ liệu người sử dụng-tầng (N) trong SDU không kết nối đơn-tầng (N).

5.2.3.3 Tính cẩn mật của trường lựa chọn

Dịch vụ này cung cấp tính cẩn mật của các trường lựa chọn trong dữ liệu người sử dụng-tầng (N) trên (Kết nối-tầng (N)hoặc trong SDU không kết nối đơn -tầng (N).

5.2.3.4 Tính cẩn mật của luồng lưu lượng

Dịch vụ này cung cấp việc bảo vệ thông tin, thông tin có thể được dẫn xuất từ việc quan sát các luồng lưu lượng.

5.2.4 Tính toàn vẹn của dữ liệu

Các dịch vụ này chống lại các mối de dọa tích cực và có thể có một trong các dạng mô tả dưới đây:

CHÚ THÍCH – Trên một kết nối, việc sử dụng dịch vụ xác thực thực thể ngang hàng tại điểm bắt đầu của kết nối và dịch vụ toàn vẹn dữ liệu trong suốt vòng đời của kết nối có thể cùng cung cấp sự chứng thực của nguồn đơn vị dữ

liệu truyền trên kết nối, tính toàn vẹn của các đơn vị dữ liệu đó và có thể cung cấp thêm việc xóa sao chép các đơn vị dữ liệu, ví dụ: bằng cách sử dụng các số chuỗi.

5.2.4.1 Tính toàn vẹn của chế độ kết nối có khôi phục

Dịch vụ này cung cấp tính toàn vẹn của tất cả dữ liệu người sử dụng-tầng (N)trên (Kết nối-tầng (N)và phát hiện mọi sửa đổi, chèn, xóa hoặc phát lại dữ liệu trong toàn bộ chuỗi SDU (cố gắng khôi phục).

5.2.4.2 Tính toàn vẹn của chế độ kết nối không khôi phục

Giống với điều 5.2.4.1 nhưng khác ở chỗ là không cố gắng khôi phục.

5.2.4.3 Tính toàn vẹn của kết nối trường lựa chọn

Dịch vụ này cung cấp tính toàn vẹn của các trường lựa chọn trong dữ liệu người sử dụng-tầng (N) của SDU-tầng (N) truyền qua một kết nối và xác định xem liệu các trường lựa chọn có được sửa đổi, chèn, xóa hoặc phát lại hay không.

5.2.4.4 Tính toàn vẹn của chế độ không-kết nối

Dịch vụ này, khi được cung cấp bởi tầng (N), cung cấp tính toàn vẹn đảm bảo cho thực thể-tầng (N+1) yêu cầu.

Dịch vụ này cung cấp tính toàn vẹn của SDU của chế độ không-kết nối đơn và xác định xem liệu SDU đã nhận có được sửa đổi hay không. Ngoài ra, có thể cung cấp một dạng phát hiện sự phát lại.

5.2.4.5 Tính toàn vẹn của chế độ không-kết nối trường lựa chọn

Dịch vụ này cung cấp tính toàn vẹn của các trường được chọn trong SDU của chế độ không-kết nối đơn và xác định xem liệu các trường đã chọn có được sửa đổi hay không.

5.2.5 Chống chối bỏ

Dịch vụ này có thể có một hoặc cả hai dạng.

5.2.5.1 Chống chối bỏ bằng chứng nguồn gốc dữ liệu

Người nhận dữ liệu được cung cấp bằng chứng nguồn gốc dữ liệu. Điều này sẽ bảo vệ mọi cố gắng của người gửi nhằm phủ nhận việc gửi nhầm dữ liệu hoặc nội dung của nó.

5.2.5.2 Chống chối bỏ bằng chứng của việc gửi dữ liệu

Người gửi dữ liệu được cung cấp bằng chứng của việc gửi dữ liệu. Điều này sẽ bảo mọi cố gắng sau đó của người nhận nhằm phủ nhận việc nhận nhầm dữ liệu hoặc nội dung của nó.

5.3 Các cơ chế an ninh cụ thể

Các cơ chế sau đây có thể được hợp nhất thành tầng (N) thích hợp nhằm cung cấp một số dịch vụ mô tả trong điều 5.2.

5.3.1 Mã hóa

5.3.1.1 Mã hóa cung cấp tính mật của dữ liệu hoặc thông tin luồng lưu lượng và có thể đóng vai trò quan trọng hay bổ sung số lượng cơ chế an ninh khác như đã mô tả trong các phần sau đây.

5.3.1.2 Các thuật ngữ mã hóa có thể là thuận nghịch hoặc phi thuận nghịch. Có hai phân loại về thuật toán mã hóa thuận nghịch:

a) Mã hóa đối xứng (ví dụ: khóa bí mật), tại đó nhận biết về khóa mã hóa bao hàm nhận thức về khóa giải mã và ngược lại; và

b) Mã hóa phi đối xứng (ví dụ: khóa công khai), tại đó nhận thức về khóa mã hóa không bao hàm nhận thức về khóa giải mã hoặc ngược lại. Hai khóa của hệ thống đôi khi được tham chiếu như "khóa công khai" và "khóa bí mật".

Các thuật toán mã hóa phi thuận nghịch có thể hoặc không thể sử dụng một khóa. Khi chúng sử dụng một khóa thì khóa này có thể là công khai hoặc bí mật.

5.3.13 Sự tồn tại của cơ chế mã hóa bao hàm việc sử dụng cơ chế quản lý khóa ngoại trừ trong trường hợp các thuật toán mã hóa phi thuận nghịch. Một số hướng dẫn về phương pháp quản lý khóa được đưa ra trong điều 8.4.

5.3.2 Các cơ chế chữ ký số

Các cơ chế này xác định hai thủ tục:

a) Ký tên một đơn vị dữ liệu; và

b) Xác nhận đơn vị dữ liệu đã ký tên.

Quy trình đầu tiên sử dụng thông tin bí mật (nghĩa là duy nhất và cẩn mật) của người ký tên. Quy trình thứ hai sử dụng các thủ tục và thông tin có sẵn một cách công khai mà thông tin bí mật của người ký tên không bị tìm ra.

5.3.2.1 Quy trình ký tên bao gồm việc mã hóa đơn vị dữ liệu hoặc việc tạo ra giá trị kiểm tra mật mã của đơn vị dữ liệu sử dụng thông tin bí mật của người ký tên như một khóa bí mật.

5.3.2.2 Quy trình xác nhận bao gồm việc sử dụng các thủ tục và thông tin công khai để xác định xem liệu chữ ký có được tạo ra với thông tin bí mật hay không.

5.3.2.3 Các đặc điểm chủ yếu của cơ chế chữ ký là chữ ký chỉ có thể được tạo ra bằng cách sử dụng thông tin bí mật của người ký tên. Do đó, khi chữ ký được xác nhận thì chứng tỏ nó là bên thứ ba (ví dụ: thẩm phán) tại mọi thời điểm mà chỉ có người giữ thông tin duy nhất có thể tạo ra chữ ký.

5.3.3 Các cơ chế điều khiển truy cập

5.3.3.1 Các cơ chế này có thể sử dụng định danh xác thực của thực thể hoặc thông tin về thực thể (như là thành viên trong tập các thực thể đã biết) hoặc các khả năng của thực thể, để xác định và giúp cho các quyền truy cập thực thể có hiệu lực. Nếu thực thể cố gắng sử dụng tài nguyên trái phép hoặc một tài nguyên được cấp quyền với kiểu truy cập không đúng thì chức

năng điều khiển truy cập sẽ chối bỏ mọi xâm phạm và có thể báo cáo sự cố nhằm mục đích tạo ra một cảnh báo và/hoặc ghi lại nó như một phần của bản theo dõi kiểm định an ninh. Mọi thông báo đến người gửi về chối bỏ truy cập đối với truyền dữ liệu chế độ không-kết nối có thể được cung cấp là kết quả của các bộ điều khiển truy cập tại điểm xuất phát.

5.3.3.2 Các cơ chế điều khiển truy cập có thể dựa trên việc sử dụng một hoặc nhiều vấn đề sau đây:

a) Các cơ sở thông tin điều khiển truy cập trong đó duy trì các quyền truy cập của các thực thể ngang hàng. Thông tin này có thể được duy trì bởi các trung tâm xác thực hoặc bởi thực thể được truy cập và có thể là dạng danh mục điều khiển truy cập hay ma trận của cấu trúc phân cấp hoặc phân tán. Điều này đảm bảo việc xác thực thực thể ngang hàng;

b) Thông tin xác thực như là mật khẩu, quyền sở hữu và việc thể hiện là bằng chứng của việc cấp quyền của thực thể truy cập.

c) Các khả năng, quyền sở hữu và việc thể hiện là bằng chứng của quyền truy cập thực thể hoặc tài nguyên xác định bởi khả năng;

CHÚ THÍCH: Khả năng nên dễ nhớ và được truyền tại theo cách đáng tin cậy.

d) Các nhãn an ninh, khi được kết hợp với một thực thể có thể được sử dụng để tạo hoặc chối bỏ truy cập, thông thường theo một chính sách an ninh;

e) Thời gian truy cập

f) Lộ trình truy cập, và

g) Thời lượng truy cập.

5.3.3.3 Các cơ chế điều khiển truy cập có thể được áp dụng tại điểm của liên kết truyền và/hoặc tại mọi điểm trung gian.

Các bộ điều khiển truy cập liên quan tại điểm xuất phát hoặc mọi điểm trung gian được sử dụng để xác định xem liệu người gửi có được phép giao tiếp với người nhận hay không và/hoặc để sử dụng các tài nguyên truyền được yêu cầu.

Yêu cầu của các cơ chế điều khiển truy cập mức ngang hàng tại giới hạn đến của đường truyền dữ liệu chế độ không-kết nối phải được biết đến là một quyền tiên tại điểm xuất phát và phải được ghi lại trong Cơ sở thông tin quản lý an ninh (xem điều 6.2 và điều 8.1).

5.3.4 Các cơ chế về tính toàn vẹn của dữ liệu

5.3.4.1 Hai khía cạnh về tính toàn vẹn của dữ liệu là: tính toàn vẹn của đơn vị dữ liệu hoặc trường đơn và tính toàn vẹn của dòng đơn vị dữ liệu hoặc trường. Nhìn chung, các cơ chế khác nhau được sử dụng để cung cấp hai kiểu dịch vụ này, mặc dù việc cung cấp kiểu thứ hai mà không có kiểu thứ nhất là không thực tế.

5.3.4.2 Xác định tính toàn vẹn của đơn vị dữ liệu đơn gồm hai quy trình, một là tại thực thể gửi và một là tại thực thể nhận. Thực thể gửi gắn cho đơn vị dữ liệu một định lượng mà là chức năng

của bản thân dữ liệu đó. Định lượng này có thể là thông tin bổ sung như mã kiểm tra khối hoặc giá trị kiểm tra mật mã và có thể được mã hóa. Thực thể nhận tạo ra một định lượng tương ứng và so sánh nó với định lượng đã nhận để xác định xem liệu dữ liệu có được sử đổi trên đường vận chuyển hay không. Bản thân cơ chế này không bảo vệ khỏi việc phát lại đơn vị dữ liệu đơn. Trong các tầng thích hợp của kiến trúc, việc phát hiện thao tác có thể dẫn đến hoạt động khôi phục (ví dụ: thông qua việc truyền lại hoặc chỉnh sửa lỗi) tại đó hoặc ở tầng cao hơn.

5.3.4.3 Đối với truyền dữ liệu chế độ kết nối, việc bảo vệ tính toàn vẹn của chuỗi các đơn vị dữ liệu (nghĩa là: bảo vệ khỏi việc sắp sai thứ tự, mất mát, phát lại và chèn hoặc sửa đổi dữ liệu) yêu cầu một vài dạng sắp xếp rõ ràng như là số chuỗi, tem thời gian hoặc dãy mật mã.

5.3.4.4 Đối với truyền dữ liệu chế độ không-kết nối, việc dán tem thời gian có thể được sử dụng để cung cấp một dạng bảo vệ giới hạn khỏi việc phát lại các đơn vị dữ liệu cá nhân.

5.3.5 Cơ chế trao đổi xác thực

5.3.5.1 Một số công nghệ có thể được áp dụng cho các trao đổi xác thực là:

a) Sử dụng thông tin xác thực như các mật khẩu-được cung ứng bằng một thực thể gửi và kiểm tra bằng một thực thể nhận;

b) Các kỹ thuật mật mã; và

c) Sử dụng các đặc điểm và/hoặc các quyền sở hữu thực thể.

5.3.5.2 Các cơ chế có thể được kết hợp thành tầng (N) nhằm cung cấp việc xác thực thực thể ngang hàng. Nếu cơ chế không hoàn thành việc xác thực thực thể thì sẽ dẫn đến việc chối bỏ hoặc kết thúc kết nối và cũng có thể tạo ra một thực thể trong bản theo dõi và/hoặc báo cáo kiểm định an ninh cho trung tâm quản lý an ninh.

5.3.5.3 Khi các kỹ thuật mật mã được sử dụng thì chúng có thể liên kết với các giao thức "thỏa hiệp" nhằm bảo vệ khỏi việc phát lại. (ví dụ: để đảm bảo tính sống động).

5.3.5.4 Các lựa chọn kỹ thuật trao đổi xác thực phụ thuộc và các trường hợp mà chúng được sử dụng. Trong nhiều trường hợp chúng cần được sử dụng với:

a) Tem thời gian và các đồng hồ đã đồng bộ hóa;

b) Thỏa hiệp hai và ba chiều (đối với việc xác thực đơn phương và song phương tương ứng); và

c) Các dịch vụ thừa nhận đạt được bởi chữ ký số và/hoặc các cơ chế chứng nhận.

5.3.6 Cơ chế đệm lưu lượng

Các cơ chế đệm lưu lượng có thể được sử dụng để cung cấp các mức bảo vệ khác nhau khỏi việc phân tích lưu lượng. Cơ chế này chỉ có thể hiệu quả nếu việc đệm lưu lượng được bảo vệ bởi dịch vụ đáng tin.

5.3.7 Cơ chế điều khiển định tuyến

5.3.7.1 Các tuyến có thể được chọn tự động bằng cách sắp xếp trước để sử dụng các mạng con, các chuyển tiếp hoặc kết nối đảm bảo.

5.3.7.2 Khi phát hiện ra các tấn công thao tác không đổi, các hệ thống cuối có thể chỉ dẫn cho nhà cung cấp dịch vụ mạng nhằm thiết lập một kết nối qua một tuyến khác.

5.3.7.3 Dữ liệu mang các nhãn an ninh nhất định có thể bị cấm bởi chính sách an ninh để đi qua các mạng con, chuyển tiếp hay kết nối nhất đinh. Người khởi tạo kết nối (hoặc người gửi đơn vị dữ liệu chế độ không-kết nối) có thể quy định các cảnh báo định tuyến, các cảnh báo này yêu cầu tránh các mạng con, các kết nối hoặc chuyển tiếp cụ thể.

5.3.8 Cơ chế chứng nhận

Các đặc tính về dữ liệu giao tiếp giữa hai hoặc nhiều thực thể, như là tính toàn vẹn, điểm xuất phát, thời gian và điểm đến có thể được bảo đảm bằng cách cung cấp cơ chế chứng nhận. Việc đảm bảo được cung cấp bởi bên thứ ba, bên thứ ba này được các thực thể truyền thông tin tưởng và mang thông tin cần thiết để cung cấp việc đảm bảo theo cách có thể chứng nhận được. Mỗi trường hợp truyền có thể sử dụng chữ ký số, mã hóa và các cơ chế toàn vẹn thích hợp với dịch vụ được cung cấp bởi bên thứ ba. Khi cơ chế chứng nhận này được gọi ra thì dữ liệu được giao tiếp giữa các thực thể truyền thông qua các thực thể truyền và bên thứ ba.

5.4 Các cơ chế an ninh thâm nhập

Điều này mô tả số lượng các cơ chế không đặc trưng cho bất kỳ dịch vụ riêng nào. Do đó, trong Điều 7, chúng không được mô tả rõ ràng trong bất kỳ tầng nào. Một số cơ chế an ninh này có thể được xem như các khía cạnh của quản lý an ninh (xem Điều 8). Nhìn chung, tầm quan trọng của các cơ chế này liên quan trực tiếp đến mức an ninh đã yêu cầu.

5.4.1 Chức năng tin cậy

5.4.1.1 Chức năng tin cậy phải được sử dụng nhằm mở rộng phạm vi áp dụng hoặc thiết lập tính hiệu quả của các cơ chế an ninh khác. Mọi chức năng cung cấp truy cập, các cơ chế an ninh cần đáng tin cậy.

5.4.1.2 Các thủ tục sử dụng nhằm đảm bảo rằng sự tin cậy được đặt trong phần mềm và phần cứng này nằm ngoài phạm vi áp dụng của tiêu chuẩn, trong mọi trường hợp chúng khác với mức độ đe dọa nhận thức và giá trị thông tin được bảo vệ.

5.4.1.3 Nhìn chung, các thủ tục này khó thực hiện. Các vấn đề có thể được giảm thiểu bằng cách lựa chọn một kiến trúc cho phép thực hiện các chức năng an ninh trong các mô đun mà có thể phân chia và cung cấp các chức năng không liên quan đến an ninh.

5.4.1.4 Việc áp dụng các bảo vệ liên kết trên tầng phải được cung cấp bởi các phương tiện khác, ví dụ: bởi chức năng tin cậy thích hợp.

5.4.2 Nhãn an ninh

Các tài nguyên bao gồm các mục dữ liệu có thể có các nhãn an ninh kết hợp với chúng, ví dụ: để chỉ ra mức độ nhạy. Cần truyền tải nhãn an ninh thích hợp với dữ liệu trên đường truyền. Nhãn an ninh có thể là dữ liệu bổ sung kết hợp với dữ liệu đã truyền hoặc có thể là tiềm tàng, ví dụ: được bao hàm bằng việc sử dụng khóa cụ thể để mã hóa dữ liệu hoặc được bao hàm bằng ngữ cảnh của dữ liệu như là nguồn hoặc tuyến. Các nhãn an ninh rõ ràng phải có định danh theo thứ tự mà chúng có thể được kiểm tra. Ngoài ra, các nhãn phải được gắn chặt với dữ liệu có liên kết với chúng.

5.4.3 Phát hiện sự việc

5.4.3.1 Việc phát hiện sự việc liên quan đến an ninh bao gồm việc phát hiện các vi phạm về an ninh và có cũng có thể bao gồm việc phát hiện các sự việc "bình thường" như là một truy cập thành công. Các sự việc liên quan đến an ninh có thể được phát hiện bởi các thực thể trong OSI bao gồm các cơ chế an ninh. Đặc tả này hình thành một sự việc được duy trì bởi Bộ quản lý sự việc (xem điều 8.3.1). Việc phát hiện các sự việc liên quan đến an ninh khác nhau có thể sinh ra các hoạt động sau đây:

a) Báo cáo sự việc cục bộ;

b) Báo cáo sự việc từ xa;

c) Ghi lại sự việc (xem điều 5.4.3); và

d) Hoạt động khôi phục (xem điều 5.4.4).

Các ví dụ về các sự việc liên quan đến an ninh là:

a) Vi phạm an ninh cụ thể;

b) Sự việc lựa chọn cụ thể; và

c) Đếm thừa số lần xảy ra.

5.4.3.2 Tiêu chuẩn hóa trong lĩnh vực này tính đến việc truyền thông tin liên quan đối với báo cáo sự việc và ghi lại sự việc, định nghĩa cú pháp và ngữ nghĩa được sử dụng cho việc truyền báo cáo sự việc và ghi lại sự việc.

5.4.4 Bản theo dõi kiểm định an ninh

5.4.4.1 Các bản theo dõi kiểm định an ninh cung cấp cơ chế an ninh có giá trị khi chúng cho phép phát hiện và điều tra các vi phạm an ninh bằng cách cho phép một kiểm định an ninh tiếp theo. Kiểm định an ninh là một bản xem xét độc lập và việc kiểm tra các bản ghi và các hoạt động của hệ thống nhằm kiểm tra tính đầy đủ của các bộ điều khiển hệ thống để đảm bảo sự phù hợp với chính sách đã thiết lập, các thủ tục điều hành và trợ giúp cho việc đánh giá mối nguy hại và khuyến cáo mọi thay đổi trong các bộ điều khiển, chính sách và các thủ tục. Kiểm định an ninh yêu cầu việc ghi thông tin liên quan đến an ninh trong bản theo dõi kiểm định an ninh, phân tích và báo cáo thông tin từ bản theo dõi kiểm định an ninh. Việc ghi lại được xem là cơ chế an ninh

và được mô tả trong phần này. Việc tạo ra báo cáo hoặc phân tích được xem là chức năng quản lý an ninh (xem 8.3.2).

5.4.4.2 Việc tập hợp thông tin theo dõi kiểm định an ninh được gắn với các yêu cầu khác nhau bằng cách quy định (các) loại sự việc liên quan đến an ninh được ghi (ví dụ: các vi phạm về an ninh hoặc việc hoàn thành các thao thác thành công).

Sự tồn tại của bản theo dõi kiểm định an ninh có thể hoạt động như một cản trở nhằm chống lại các nguồn tấn công đến an ninh.

5.4.4.3 Các xem xét theo dõi kiểm định an ninh OSI tính đến thông tin được ghi lại theo các điều kiện mà thông được ghi lại, định nghĩa cú pháp và ngữ nghĩa này được sử dụng cho việc trao đổi thông tin theo dõi kiểm định an ninh.

5.4.5 Khôi phục an ninh

5.4.5.1 Khôi phục an ninh đề cập đến các yêu cầu từ cơ chế ví dụ như các chức năng vận dụng và quản lý sự việc, nắm giữ các hoạt động khôi phục như một kết quả của việc áp dụng tập các quy tắc. Các hoạt động khôi phục này có thể là ba loại sau:

a) Tức thời;

b) Tạm thời; và

c) Dài hạn.

Ví dụ:

Các hoạt động tức thời có thể tạo ra việc tạm ngưng tức thời các thao tác, như là việc ngắt kết nối.

Các hoạt động tạm thời có thể làm mất hiệu lực tạm thời của thực thể.

Các hoạt động dài hạn có thể là một lời giới thiệu về thực thể trong "danh sách đen" hoặc việc thay đổi một khóa.

5.4.5.2 Các chủ đề tiêu chuẩn hóa bao gồm các giao thức về các hoạt động khôi phục và quản lý khôi phục an ninh (xem điều 8.3.3).

5.5 Minh họa mối quan hệ của các dịch vụ và cơ chế an ninh

Bảng 1 minh họa riêng các cơ chế hoặc kết hợp với các cơ chế khác, đôi khi được xem là phù hợp với điều khoản của mỗi dịch vụ. Bảng này thể hiện cái nhìn tổng quát về các mối quan hệ này nhưng không đáng tin cậy. Các dịch vụ và cơ chế tham chiếu đến bảng này được mô tả trong điều 5.2 và điều 5.3. Các mối quan hệ được mô tả đầy đủ hơn trong Điều 6.

6 Mối quan hệ của các dịch vụ, các cơ chế và các tầng

6.1 Các nguyên tắc sắp tầng an ninh

6.1.1 Các nguyên tắc sau đây được sử dụng để xác định việc định vị các dịch vụ an ninh cho các tầng và sự sắp xếp các cơ chế an ninh trong các tầng:

a) Số cách sắp tầng an ninh để có được dịch vụ nên được giảm thiểu;

Bảng 1

Cơ chế / Dịch vụ	Mã hóa	Chữ ký số	Điều khiển truy cập	Tính toàn vẹn của dữ liệu	Trao đổi tính xác thực	Đệm lưu lượng	Điều khiển định tuyến	Công chứng
Xác thực thực thể ngang hàng	Y	Y	•	•	Y	•	•	•
Xác thực nguồn gốc của dữ liệu	Y	Y	•	•	•	•	•	•
Dịch vụ điều khiển truy cập	•	•	Y	•	•	•	Y	•
Tính mật của chế độ kết nối	Y	•	•	•	•	•	Y	•
Tính mật của chế độ không kết nối	Y	•	•	•	•	•	•	•
Tính mật của trường lựa chọn	Y	•	•	•	•	•	Y	•
Tính mật của luồng lưu lượng	Y	•	•	•	•	Y	•	•
Tính toàn vẹn của chế độ kết nối có khôi phục	Y	•	•	Y	•	•	•	•
Tính toàn vẹn của chế độ kết nối không khôi phục	Y	•	•	Y	•	•	•	•
Tính toàn vẹn của chế độ kết nối trường lựa chọn	Y	•	•	Y	•	•	•	•

Bảng 1 (tiếp theo)

Tính toàn vẹn của chế độ không-kết nối	Y	Y	•	Y	•	•	•	•
Tính toàn vẹn của chế độ không-kết nối trường lựa chọn	Y	Y	•	Y	•	•	•	•
Chống chối bằng chứng xuất xứ	•	Y	•	Y	•	•	•	Y
Chống chối bỏ bằng chứng việc gửi	•	Y	•	Y	•	•	•	Y

Ghi chú: Y (Yes): Cơ chế được cho là phù hợp với cơ chế của nó hoặc kết hợp với các cơ chế khác.

- Cơ chế được cho là không phù hợp

b) Có thể chấp nhận xây dựng các hệ thống an toàn bằng cách cung cấp các dịch vụ an ninh trong nhiều tầng;

c) Chức năng bổ sung yêu cầu cho an ninh không nhất thiết sao chép các chức năng OSI hiện có;

d) Nên tránh xâm phạm đến sự độc lập của tầng;

e) Nên giảm thiểu số lượng chức năng đáng tin cậy;

f) Bất cứ nơi nào mà một thực thể phụ thuộc vào cơ chế an ninh cung cấp bởi một thực thể trong tầng thấp hơn, các tầng tức thời nên được cấu trúc theo một cách mà không thể thực hiện được việc xâm phạm an ninh;

g) Bất cứ khi nào có thể, các chức năng an ninh bổ sung của tầng nên được xác định theo cách mà việc thực hiện đóng vai trò như (các) mô đun độc lập không được ngăn ngừa; và

h) Tiêu chuẩn này được cho là áp dụng các hệ thống mở bao gồm các hệ thống cuối bao gồm cả bảy tầng và phát lại các hệ thống.

6.1.2 Các định nghĩa dịch vụ tại mỗi tầng có thể yêu cầu việc sửa đổi nhằm cung cấp các yêu cầu về các dịch vụ an ninh, liệu các dịch vụ đã yêu cầu có được cung cấp tại tầng đó hay không.

6.2 Mô hình dẫn chứng, quản lý và sử dụng dịch vụ được bảo vệ -tầng (N)

Điều này nên được trình bày cùng với Điều 8, trong đó bao gồm thảo luận chung về các vấn đề quản lý an ninh. Các dịch vụ và cơ chế an ninh có thể được kích hoạt bởi thực thể quản lý thông qua giao diện quản lý và/hoặc dẫn chứng dịch vụ.

6.2.1 Xác định các tính năng bảo vệ cho thể hiện truyền thông

6.2.1.1 Khái quát

Điều này mô tả dẫn chứng bảo vệ các thể hiện chế độ truyền kết nối và không-kết nối. Trong trường hợp truyền thông hướng kết nối, các dịch vụ bảo vệ thường được yêu cầu tại thời điểm thiết lập kết nối. Trong trường hợp về dẫn chứng dịch vụ không kết nối, việc bảo vệ được yêu cầu cho mỗi trường hợp của yêu cầu UNITDATA.

Để đơn giản hóa mô tả sau đây, thuật ngữ "yêu cầu của dịch vụ" được sử dụng cho việc thiết lập kết nối hoặc một yêu cầu UNITDATA. Dẫn chứng bảo vệ dữ liệu đã chọn có thể đạt được bằng cách yêu cầu bảo vệ trường lựa chọn. Ví dụ, điều này có thể được thực hiện bằng cách thiết lập một vài kết nối, mỗi kết nối với kiểu hoặc mức bảo vệ khác nhau.

Kiến trúc an ninh này cung cấp nhiều chính sách an ninh khác nhau bao gồm các chính sách dựa trên quy tắc, các chính sách dựa trên định danh và các chính sách là sự kết hợp của cả hai. Kiến trúc an ninh còn cung cấp cách bảo vệ được áp đặt về mặt hành chính, cách bảo vệ được lựa chọn động và sự kết hợp của cả hai.

6.2.1.2 Các yêu cầu của dịch vụ

Đối với mỗi yêu cầu của dịch vụ-tầng (N) , thực thể-tầng (N+1) có thể yêu cầu việc bảo vệ an ninh mục tiêu cần thiết. Yêu cầu của dịch vụ-tầng (N) sẽ quy định các dịch vụ an ninh cùng với các thông số và mọi thông tin bổ sung liên quan (như là các thông tin nhạy cảm và/hoặc các nhãn an ninh) nhằm bảo vệ an ninh mục tiêu.

Trước mỗi trường hợp truyền, tầng (N) phải truy cập Cơ sở thông tin quản lý an ninh (SMIB) (xem điều 8.1). SMIB chứa thông tin về các yêu cầu bảo vệ về mặt hành chính kết hợp với thực thể-tầng (N+1). Chức năng đáng tin cậy được yêu cầu để giúp cho các yêu cầu an ninh về mặt hành chính có hiệu lực.

Việc cung cấp các tính năng an ninh trong trường hợp chế độ truyền kết nối có thể yêu cầu thương thảo các dịch vụ án ninh. Các thủ tục yêu cầu cho việc thương thảo các cơ chế và thông số có thể được thực hiện như một thủ tục riêng biệt hoặc như một phần không thể thiếu được của thủ thục thiết lập kết nối thông thường.

Khi việc thương thảo được thực hiện như một thủ tục riêng biệt thì các kết quả thỏa thuận (nghĩa là các cơ chế và thông số an ninh cần cung cấp cho các dịch vụ an ninh này) được đưa ra trong Cơ sở thông tin quản lý an ninh (xem điều 8.1).

Khi việc thương thảo được thực hiện như một phần không thể thiếu của thủ tục thiết lập kết nối thường, các kết quả của việc thương thảo giữa thực thể-tầng (N) được lưu trữ tạm thời trong SMIB. Trước khi thương thảo, mỗi thực thể-tầng (N) sẽ truy cập SMIB đối với thông tin yêu cầu cho việc thương thảo.

Tầng (N) chối bỏ yêu cầu dịch vụ nếu nó vi phạm các yêu cầu về mặt hành chính được đăng ký trong SMIB đối với thực thể-tầng (N+1).

Tầng (N) cũng bổ sung cho dịch vụ bảo vệ các dịch vụ an ninh được xác định trong SMIB với tư cách bắt buộc nhằm bảo vệ an ninh mục tiêu.

Nếu thực thể-tầng (N+1)không quy định việc bảo vệ an ninh mục tiêu thì tầng (N) sẽ theo chính sách an ninh phù hợp với SMIB. Có thể bắt đầu truyền bằng cách sử dụng một cách bảo vệ an ninh mặc định trong dãy xác định thực thể-tầng (N+1) trong SMIB.

6.2.2 Điều khoản về các dịch vụ bảo vệ

Sau khi việc kết hợp các yêu cầu về mặt hành chính và các yêu cầu an ninh lựa chọn động được xác định như đã mô tả trong điều 6.2.1, tầng (N) sẽ cố gắng đạt được cách bảo vệ mục tiêu ở mức tối thiểu. Điều này có được bởi một trong hai hoặc cả hai phương pháp sau đây:

a) Gọi trực tiếp các cơ chế an ninh trong tầng (N); và/hoặc

b) Yêu cầu các dịch vụ bảo vệ từ tầng (N-1). Trong trường hợp này, phạm vi bảo vệ phải được mở rộng cho dịch vụ-tầng (N) bằng cách kết hợp chức năng đáng tin cậy và/hoặc các cơ chế an ninh cụ thể trong tầng (N).

CHÚ THÍCH – Không nhất thiết rằng tất cả chức năng trong tầng (N) phải đáng tin cậy.

Do đó, tầng (N) xác định nếu nó có thể bảo vệ mục tiêu đã yêu cầu. Nếu không việc truyền sẽ không xảy ra.

6.2.2.1 Thiết lập kết nối được bảo vệ -tầng (N)

Thảo luận sau đây đề cập đến việc cung cấp các dịch vụ trong tầng (N), (phản đối việc dựa vào dịch vụ-tầng (N-1)).

Trong các giao thức nhất định, để bảo vệ tốt mục tiêu thì chuỗi các thao tác là thành phần chủ chốt.

a) Điều khiển truy cập ngoài

Tầng (N) có thể áp đặt các bộ điều khiển truy cập mở, tức là nó có thể xác định (từ SMIB) xem liệu việc thiết lập (Kết nối-tầng (N) được bảo vệ có thể được thông qua hoặc ngăn cấm hay không.

b) Xác thực thực thể ngang hàng

Nếu việc bảo vệ mục tiêu bao gồm xác thực thực thể ngang hàng hoặc nếu được biết rằng thực thể-tầng (N) đích yêu cầu xác thực thực thể ngang hàng thì sẽ diễn ra một trao đổi xác thức. Điều này sử dụng các thỏa hiệp hai hoặc ba chiều để cung cấp xác thực đơn phương hoặc song phương khi yêu cầu.

Đôi khi, việc trao đổi xác thực có thể được hợp nhất thành các thủ thục thiết lập kết nối-tầng (N) . Ở các trường hợp khác, trao đổi xác thực có thể được thực hiện riêng rẽ từ việc thiết lập kết nối-tầng (N) .

c) Dịch vụ điều khiển truy cập

Thực thể-tầng (N) đến hoặc các thực thể trung gian có thể áp đặt các giới hạn điều khiển truy cập. Nếu thông tin cụ thể được yêu cầu bởi cơ chế điều khiển truy cập từ xa thì thực thể khởi tạo-tầng (N) cung cấp thông tin này trong giao thức-tầng (N) hoặc qua các kênh quản lý.

d) Tính mật

Nếu toàn bộ hoặc một dịch vụ tin cẩn được lựa chọn thì (Kết nối-tầng (N) phải được thiết lập. Điều này bảo gồm việc thiết lập (các) khóa thực hành và thương thảo các thông số mật mã đối với kết nối. Điều này có thể được thực hiện bằng cách sắp xếp trước trong trao đổi xác thực hoặc bởi giao thức riêng rẽ.

e) Tính toàn vẹn của dữ liệu

Nếu tính toàn vẹn của tất cả dữ liệu người sử dụng-tầng (N) có hoặc không có sự hồi phục, hay tính toàn vẹn của các trường phải được lựa chọn thì (Kết nối-tầng (N) phải được thiết lập. Điều này có thể có cùng kết nối với kết nối thiết lập để cung cấp dịch vụ đáng tin cậy và có thể cung cấp việc xác thực. Các xem xét giống nhau áp dụng cho các dịch vụ đáng tin cậy đối với kết nối được bảo vệ -tầng (N).

f) Các dịch vụ thừa nhận

Nếu việc thừa nhận với chứng cứ về nguồn gốc được lựa chọn thì các thông số mật mã chính xác phải được thiết lập hoặc việc liên kết với thực thể chứng nhận phải được thiết lập.

Nếu việc thừa nhận với chứng cứ về việc gửi được lựa chọn thì các thông số chính xác (khác với các thông số yêu cầu cho việc thừa nhận về nguồn gốc) phải được thiết lập hoặc việc liên kết với thực thể chứng nhận phải được thiết lập.

CHÚ THÍCH – Việc thiết lập thực thể-tầng (N) có thể không phải do sự bất đồng về các thông số mật mã (bao gồm việc không sở hữu các khóa chính xác) hoặc thông qua việc chối bỏ bởi cơ chế điều khiển truy cập.

6.2.3 Thao tác của Kết nối được bảo vệ -tầng (N)

6.2.3.1 Trong suốt giai đoạn truyền kết nối-tầng (N), các dịch vụ bảo vệ phải được cung cấp.

Các điều sau đây luôn có mặt tại ranh giới dịch vụ-tầng (N):

a) Xác thực thực thể ngang hàng (thỉnh thoảng);

b) Bảo vệ các trường lựa chọn, và

c) Báo cáo tác động tích cực (ví dụ, khi thao tác dữ liệu xảy ra và dịch vụ đang được cung cấp là "tính toàn vẹn của kết nối không được khôi phục")-xem điều 5.2.4.2).

Ngoài ra, các điều sau đây có thể được yêu cầu:

a) Bản ghi theo dõi kiểm định an ninh; và

b) Phát hiện và quản lý sự việc;

6.2.3.2 Các dịch vụ tuân theo ứng dụng lựa chọn là:

a) Tính mật;

b) Tính toàn vẹn của dữ liệu; và

c) Chống chối bỏ (bởi người nhận hoặc người gửi).

CHÚ THÍCH

1 Hai kỹ thuật được đề xuất đánh dấu các mục dữ liệu đã lựa chọn cho ứng dụng dịch vụ. Kỹ thuật đầu tiên bao gồm sự định kiểu mạnh. Cần biết trước rằng tầng trình diễn được áp dụng sẽ công nhận các kiểu mà yêu cầu các dịch vụ bảo vệ. Kỹ thuật thứ hai bao gồm một vài dạng ra cờ hiệu các mục dữ liệu riêng lẻ mà áp dụng các dịch vụ bảo vệ đã quy định.

2 Cần đảm bảo rằng một lý do cung cấp ứng dụng lựa chọn của của các dịch vụ thừa nhận có thể phát sinh từ các kịch bản sau đây. Một số dạng đàm thoại thương lượng xuất hiện qua một liên kết, trước khi cả hai thực thể-tầng (N) thỏa thuận rằng phiên bản cuối cùng của mục dữ liệu có thể chấp nhận lẫn nhau. Tại thời điểm đó, người nhận mong đợi có thể yêu cầu người gửi áp dụng các dịch vụ thừa nhận (của cả điểm gốc và điểm gửi đi) cho phiên bản được thỏa thuận của mục dữ liệu. Người gửi yêu cầu các dịch vụ này, truyền dẫn mục dữ liệu, sau đó nhận thông báo rằng mục dữ liệu đã được nhận. Các dịch vụ thừa nhận đảm bảo rằng nơi phát và nơi nhận mục dữ liệu đều được truyền thành công.

3 Cả hai dịch vụ thừa nhận (nghĩa là điểm gốc và điểm gửi đi) được khởi gọi từ nơi phát.

6.2.4 Điều khoản về truyền dữ liệu chế độ không-kết nối được bảo vệ

Không phải tất cả các dịch vụ an ninh đều có sẵn trong các giao thức của chế độ kết nối và các giao thức của chế độ không-kết nối. Nhất là bảo vệ khỏi việc xóa, chèn và phát lại. Khi được yêu cầu thì các dịch vụ an ninh phải được cung cấp tại các tầng cao hơn. Bảo vệ khỏi sự phát lại có thể được cung cấp bởi cơ chế tem thời gian. Ngoài ra, số lượng các dịch vụ an ninh khác không thể cung cấp cùng một mức độ chấp hành an ninh mà có thể thu được bởi các giao thức kết nối.

Các dịch vụ kết nối phù hợp với chế độ truyền dữ liệu không kết nối như sau:

a) Xác thực thực thể ngang hàng (xem điều 5.2.1.1);

b) Xác thực nguồn gốc của dữ liệu (xem điều 5.2.1.2);

c) Dịch vụ điều khiển truy cập (xem điều 5.2.2);

d) Tính mật của chế độ không-kết nối (xem 5.2.3.2);

e) Tính mật của trường lựa chọn (xem 5.2.3.3);

f) Tính toàn vẹn của chế độ không-kết nối (xem 5.2.4.4);

g) Tính toàn vẹn của chế độ không-kết nối trường lựa chọn (xem 5.2.4.5); và

h) Chống chối bỏ, nguồn gốc (xem điều 5.2.5.1).

Các dịch vụ được cung cấp bởi các cơ chế mã hóa, chữ ký, các cơ chế điều khiển truy cập, các cơ chế định tuyến, các cơ chế về tính toàn vẹn của dữ liệu và/hoặc các cơ chế chứng thực (xem điều 5.3).

Nơi gửi đường truyền dữ liệu chế độ không-kết nối phải đảm bảo rằng SDU đơn chứa tất cả các thông tin được yêu cầu nhằm giúp nó được chấp nhận tại điểm đến.

7 Xếp đặt các dịch vụ và cơ chế an ninh

Điều này xác định các dịch vụ an ninh được cung cấp trong khung tổng quát của mô hình tham chiếu cơ sở OSI và phác họa cách mà chúng đạt được. Việc cung cấp dịch vụ an ninh là tùy chọn, phụ thuộc vào các yêu cầu.

Dịch vụ an ninh cụ thể được định danh trong điều này được cung cấp một cách tùy chọn bởi tầng riêng biệt, nếu không được quy định thì dịch vụ an ninh sẽ được cung cấp bởi các cơ chế an ninh vận hành trong tầng đó. Như đã mô tả trong Điều 6, nhiều tầng yêu cầu cung cấp các dịch vụ an ninh riêng biệt. Các tầng này không thể tự cung cấp các dịch vụ an ninh, nhưng có thể sử dụng các dịch vụ an ninh thích hợp đang được cung cấp trong các tầng thấp nhất. Thậm chí khi không có dịch vụ an ninh nào được cung cấp trong một tầng thì các định nghĩa dịch vụ của tầng đó có thể yêu cầu sửa đổi nhằm cho phép các yêu cầu về các dịch vụ an ninh được truyền qua tầng thấp hơn.

CHÚ THÍCH

1 Các cơ chế an ninh thâm nhập khắp (xem điều 5.4) không được thảo luận trong điều này

2 Lựa chọn vị trí của các cơ chế mã hóa đối với các ứng dụng được thảo luận trong Phụ lục C.

7.1 Tầng vật lý

7.1.1 Các dịch vụ

Chỉ các dịch vụ an ninh được cung cấp tại tầng vật lý một cách đơn lẻ hoặc kết hợp:

a) Tính mật của kết nối; và

b) Tính mật của luồng lưu lượng.

Dịch vụ về tính mật của luồng lưu lượng chia làm hai dạng:

1) Tính mật của luồng lưu lượng đầy đủ chỉ có thể được cung cấp trong các trường hợp nhất định, ví dụ: truyền dẫn đồng thời hai chiều, đồng bộ, điểm-điểm; và

2) Tính mật của luồng lưu lượng giới hạn có thể được cung cấp các kiểu truyền dẫn khác nhau, ví dụ: truyền dẫn không đồng bộ.

Các dịch vụ an ninh này được giới hạn cho các mối đe dọa bị động và có thể được áp dụng cho truyền thông điểm nối điểm và truyền thông đa điểm.

7.1.2 Các cơ chế

Toàn bộ mã hóa dòng dữ liệu là cơ chế an ninh chủ yếu tại tầng vật lý.

Dạng mã hóa cụ thể chỉ có thể áp dụng tại tầng vật lý là an ninh truyền dẫn (nghĩa là: an ninh phổ trải rộng).

Bảo vệ tầng vật lý được cung cấp bởi thiết bị mã hóa. Mục tiêu của việc bảo vệ tầng vật lý là bảo vệ toàn bộ dòng bit dữ liệu của dịch vụ vật lý và cung cấp tính mật của luồng lưu lượng.

7.2 Tầng liên kết dữ liệu

7.2.1 Các dịch vụ

Các dịch vụ an ninh cung cấp tại tầng liên kết dữ liệu là:

a) Tính mật của chế độ kết nối; và

b) Tính mật của chế độ không-kết nối.

7.2.2 Các cơ chế

Cơ chế mã hoá được sử dụng để cung cấp các dịch vụ an ninh trong tầng liên kết dữ liệu (xem Phụ lục C).

Chức năng bảo vệ an ninh bổ sung của tầng liên kết được thực hiện trước các chức năng truyền của tầng thông thường và sau các chức năng nhận, tức là các cơ chế an ninh xây dựng và sử dụng tất cả các chức năng của tầng thông thường.

Các cơ chế mã hoá tại tầng liên kết dữ liệu bị ảnh hưởng mạnh bởi giao thức của tầng liên kết dữ liệu.

7.3 Tầng mạng

Tầng mạng được tổ chức bên trong nhằm cung cấp (các) giao thức để thức hiện các thao tác sau đây:

a) Truy cập mạng con;

b) Hội tụ phụ thuộc mạng con;

c) Hội tụ không phụ thuộc mạng con; và

d) Chuyển tiếp và định tuyến.

(xem điều 2.4)

7.3.1 Các dịch vụ

Các dịch vụ an ninh được cung cấp bởi giao thức thực hiện các chức năng truy cập mạng con kết hợp với việc cung cấp dịch vụ mạng OSI như sau:

a) Xác thực thực thể ngang hàng;

b) Xác thực nguồn gốc dữ liệu;

c) Dịch vụ điều khiển truy cập;

d) Tính mật của chế độ kết nối;

e) Tính mật của chế độ không-kết nối;

f) Tính mật của luồng lưu lượng;

g) Tính toàn vẹn của chế độ kết nối không hồi phục; và

h) Tính toàn vẹn của chế độ không-kết nối.

Các dịch vụ an ninh này có thể được cung cấp đơn lẻ hoặc kết hợp. Các dịch vụ an ninh có thể được cung cấp bởi giao thức thực hiện các thao tác chuyển tiếp và định tuyến kết hợp với việc cung cấp dịch vụ mạng OSI từ hệ thống đầu đến hệ thống cuối, giống với các dịch vụ được cung cấp bởi giao thức thực hiện các thao tác truy cập mạng con.

7.3.2 Các cơ chế

7.3.2.1 Các cơ chế an ninh đồng nhất được sử dụng bởi (các) giao thức thực hiện thao tác truy cập mạng con, thao tác chuyển tiếp và định tuyến kết hợp với việc cung cấp dịch vụ mạng OSI từ hệ thống đầu đến hệ thống cuối. Việc định tuyến được thực hiện trong tầng này, do đó điều khiển định tuyến được định vị trong tầng này. Các dịch vụ an ninh đã định danh được cung cấp như sau:

a) Dịch vụ xác thực thực thể an ninh ngang hàng được cung cấp bởi liên kết thích hợp của các trao đổi dẫn xuất mật mã hoặc các trao đổi xác thực được bảo vệ, các cơ chế trao đổi mật khẩu được bảo vệ và các cơ chế chữ ký;

b) Dịch vụ xác thực nguồn gốc của dữ liệu được cung cấp bởi các cơ chế mã hoá hoặc chữ ký;

c) Dịch vụ điều khiển truy cập được cung cấp thông qua việc sử dụng các cơ chế điều khiển truy cập cụ thể thích hợp;

d) Dịch vụ về tính mật của chế độ kết nối được cung cấp bởi cơ chế mã hoá và/hoặc điều khiển định tuyến;

e) Dịch vụ về tính mật của chế độ không-kết nối được cung cấp bởi cơ chế mã hoá và/hoặc điều khiển định tuyến;

f) Dịch vụ về tính mật của luồng lưu lượng đạt được bởi cơ chế đệm lưu lượng, cùng với dịch vụ tin cẩn tại hoặc dưới tầng mạng và/hoặc điều khiển định tuyến;

g) Dịch vụ về tính toàn vẹn của chế độ kết nối mà không có sự khôi phục được cung cấp bằng cách sử dụng cơ chế về tính toàn vẹn của dữ liệu, đôi khi liên kết với cơ chế mã hoá; và

h) Dịch vụ về tính toàn vẹn của chế độ không-kết nối được cung cấp bằng cách sử dụng cơ chế về tính toàn vẹn của dữ liệu, đôi khi liên kết với cơ chế mã hoá.

7.3.2.2 Các cơ chế trong giao thức thực hiện các thao tác truy cập mạng con kết hợp với việc cung cấp dịch vụ mạng OSI từ hệ thống đầu đến hệ thống cuối, đưa ra các dịch vụ qua mạng con đơn.

Bảo vệ mạng con bằng cách quản lý mạng con sẽ được áp dụng khi các giao thức truy cập mạng con ra lệnh nhưng thường được áp dụng trước các chức năng truyền dẫn mạng con thông thường và sau các chức năng nhận mạng con thông thường.

7.3.2.3 Các cơ chế cung cấp bởi giao thức thực hiện các thao tác chuyển tiếp và định tuyến kết hợp với việc cung cấp dịch vụ mạng OSI từ hệ thống đầu đến hệ thống cuối, đưa ra các dịch vụ qua một hoặc nhiều mạng liên kết nối.

Các cơ chế này được gọi ra trước các chức năng truyền dẫn chuyển tiếp và định tuyến và sau các chức năng nhận chuyển tiếp và định tuyến. Đối với cơ chế điều khiển định tuyến, các ràng buộc định tuyến thích hợp được dẫn xuất từ SMIB trước dữ liệu, cùng với các ràng buộc định tuyến cần được truyền đến các chức năng chuyển tiếp và định tuyến

7.3.2.4 Điều khiển truy cập trong Tầng mạng có thể đáp ứng nhiều mục đích. Ví dụ, cho phép một hệ thống cuối điều khiển việc thiết lập của các kết nối mạng và chối bỏ các cuộc gọi không mong muốn. Nó cũng cho phép một hoặc nhiều mạng con điều khiển việc sử dụng các tài nguyên của tầng mạng. Trong một số trường hợp, mục đích sau liên quan đến việc tính giá sử dụng mạng.

CHÚ THÍCH - Việc thiết lập kết nối mạng có thể dẫn đến các cách tính giá bởi ban quản trị mạng con. Sự tối thiểu hoá giá cả có thể được thực hiện bằng cách điều khiển truy cập và bằng cách lựa chọn cách tính giá ngược hoặc các thông số cụ thể về mạng.

7.3.2.5 Yêu cầu của mạng con riêng rẽ có thể áp đặt các cơ chế điều khiển truy cập trên giao thức thực hiện các thao tác truy cập mạng con kết hợp với việc cung cấp dịch vụ mạng OSI từ hệ thống đầu đến hệ thống cuối. Khi các cơ chế điều khiển truy cập được cung cấp bởi giao thức thực hiện các thao tác chuyển tiếp và định tuyến kết hợp với việc cung cấp dịch vụ mạng OSI từ hệ thống đầu đến hệ thống cuối, chúng có thể được sử dụng cả hai để điều khiển truy cập các mạng con bởi các thực thể chuyển tiếp và để điều khiển truy cập các hệ thống cuối. Rõ ràng, việc mở rộng việc cách ly điều khiển truy cập là không thực hiện được, chỉ phân biệt giữa các thực thể tầng mạng.

7.3.2.6 Nếu việc đệm lưu lượng được sử dụng cùng với cơ chế chế mã hoá trong tầng mạng (hoặc dịch vụ tin cẩn từ tầng vật lý) thì mức tin cẩn của luồng lưu lượng có thể đạt được.

7.4 Tầng giao vận

7.4.1 Các dịch vụ

Các dịch vụ an ninh có thể được cung cấp đơn lẻ hoặc kết hợp trong tầng giao vận là:

a) Xác thực thực thể ngang hàng;

b) Xác thực nguồn gốc của dữ liệu;

c) Dịch vụ điều khiển truy cập;

d) Tính mật của chế độ kết nối;

e) Tính mật của chế độ không-kết nối;

f) Tính toàn vẹn của chế độ kết nối có khôi phục;

g) Tính toàn vẹn của chế độ kết nối không khôi phục; và

h) Tính toàn vẹn của chế độ không-kết nối.

7.4.2 Các cơ chế

Các dịch vụ an ninh được cung cấp như sau:

a) Dịch vụ xác thực thực thể an ninh ngang hàng được cung cấp bởi liên kết thích hợp của các trao đổi dẫn xuất mật mã hoặc các trao đổi xác thực được bảo vệ, các cơ chế trao đổi mật khẩu được bảo vệ và các cơ chế chữ ký;

b) Dịch vụ xác thực nguồn gốc của dữ liệu được cung cấp bởi các cơ chế mã hoá hoặc chữ ký;

c) Dịch vụ điều khiển truy cập được cung cấp thông qua việc sử dụng các cơ chế điều khiển truy cập cụ thể thích hợp;

d) Dịch vụ về tính mật của chế độ kết nối được cung cấp bởi cơ chế mã hoá và/hoặc điều khiển định tuyến;

e) Dịch vụ về tính mật của chế độ không-kết nối được cung cấp bởi cơ chế mã hoá và/hoặc điều khiển định tuyến;

f) Dịch vụ về tính toàn vẹn của chế độ kết nối có khôi phục được cung cấp bằng cách sử dụng cơ chế về tính toàn vẹn của dữ liệu, đôi khi kết hợp với cơ chế mã hoá;

g) Dịch vụ về tính toàn vẹn của chế độ kết nối không khôi phục được cung cấp bằng cách sử dụng cơ chế về tính toàn vẹn của dữ liệu, đôi khi kết hợp với cơ chế mã hoá;

h) Dịch vụ về tính toàn vẹn của chế độ không-kết nối được cung cấp bằng cách sử dụng cơ chế về tính toàn vẹn của dữ liệu, đôi khi liên kết với cơ chế mã hoá.

Các cơ chế bảo vệ sẽ vận hành theo cách mà các dịch vụ an ninh có thể được gọi ra cho kết nối giao vận riêng lẻ. Việc bảo vệ theo cách mà các kết nối giao vận riêng lẻ có thể bị cô lập khỏi toàn bộ các kết nối giao vận khác.

7.5 Tầng phiên

7.5.1 Các dịch vụ

Không có dịch vụ an ninh nào được cung cấp trong tầng phiên.

7.5 Tầng trình diễn

7.6.1 Các dịch vụ

Các tiện ích được cung cấp bởi tầng phiên nhằm hỗ trợ việc cung cấp các dịch vụ an ninh sau đây bởi tầng ứng dụng của quy trình ứng dụng:

a) Tính mật của chế độ kết nối;

b) Tính mật của chế độ không-kết nối; và

c) Tính mật của trường lựa chọn.

Các tiện ích trong tầng trình diễn cũng có thể hỗ trợ việc cung cấp các dịch vụ sau đây bởi tầng ứng dụng của quy trình ứng dụng:

d) Tính mật của luồng lưu lượng;

e) Xác thực thực thể ngang hàng;

f) Xác thực nguồn gốc của dữ liệu;

g) Tính toàn vẹn của chế độ kết nối có khôi phục;

h) Tính toàn vẹn của chế độ kết nối không khôi phục;

j) Tính toàn vẹn của chế độ kết nối trường lựa chọn;

k) Tính toàn vẹn của chế độ không-kết nối;

m) Tính toàn vẹn của chế độ không-kết nối trường lựa chọn;

n) Chống chối bỏ bằng chứng xuất xứ; và

p) Chống chối bỏ bằng chứng việc gửi.

CHÚ THÍCH – Các tiện ích được cung cấp bởi tầng trình diễn sẽ là các tiện ích mà phụ thuộc vào cơ chế chỉ có thể điều hành trên cú pháp truyền mã hoá dữ liệu và bao gồm các tiện ích dựa trên kỹ thuật mật mã.

7.6.2 Các cơ chế

Đối với các cơ chế an ninh sau đây, các cơ chế hỗ trợ có thể được định vị trong tầng trình diễn, nếu như vậy, nó có thể được sử dụng cùng với các cơ chế an ninh tầng ứng dụng để cung cấp các dịch vụ an ninh tầng ứng dụng:

a) Dịch vụ xác thực thực thể ngang hàng có thể được hỗ trợ bởi các cơ chế biến đổi cú pháp (ví dụ: mã hoá);

b) Dịch vụ xác thực nguồn gốc dữ liệu có thể được hỗ trợ bởi cơ chế mã hoá hoặc cơ chế chữ ký;

c) Dịch vụ về tính mật của chế độ kết nối có thể được hỗ trợ bởi cơ chế mã hoá;

d) Dịch vụ về tính mật của chế độ không-kết nối có thể được hỗ trợ bởi cơ chế mã hoá;

e) Dịch vụ về tính mật của trường lựa chọn có thể được hỗ trợ bởi cơ chế mã hoá;

f) Dịch vụ về tính mật của luồng lưu lượng có thể được hỗ trợ bởi cơ chế mã hoá;

g) Dịch vụ về tính mật của chế độ kết nối có khôi phục có thể được hỗ trợ bởi cơ chế về tính toàn vẹn của dữ liệu, đôi khi kết hợp với cơ chế mã hoá;

h) Dịch vụ về tính mật của chế độ kết nối không khôi phục có thể được hỗ trợ bởi cơ chế về tính toàn vẹn của dữ liệu, đôi khi kết hợp với cơ chế mã hoá;

j) Dịch vụ về tính toàn vẹn của chế độ kết nối trường lựa chọn có thể được hỗ trợ bởi cơ chế về tính toàn vẹn của dữ liệu, đôi khi kết hợp với cơ chế mã hoá;

k) Dịch vụ về tính toàn vẹn của chế độ không-kết nối có thể được hỗ trợ bởi cơ chế về tính toàn vẹn của dữ liệu, đôi khi kết hợp với cơ chế mã hoá;

m) Dịch vụ về tính toàn vẹn của chế độ không-kết nối trường lựa chọn có thể được hỗ trợ bởi cơ chế về tính toàn vẹn của dữ liệu, đôi khi kết hợp với cơ chế mã hoá;

n) Dịch vụ thừa nhận bằng chứng xuất xứ có hể được hỗ trợ bởi sự kết hợp của cơ chế về tính toàn vẹn của dữ iệu, cơ chế chữ ký và cơ chế chứng thực; và

p) Dịch vụ thừa nhận bằng chứng việc gửi có thể được hỗ trợ bởi sự kết hợp của cơ chế về tính toàn vẹn của dữ liệu, cơ chế chữ ký và cơ chế chứng thực.

Các cơ chế mã hoá áp dụng cho việc truyền dữ liệu, khi được định vị trong các tầng cao hơn thì phải có trong tầng trình diễn.

Một số dịch vụ trong danh mục ở trên có thể được cung cấp bởi các cơ chế an ninh chứa trong tầng ứng dụng.

Chỉ có các dịch vụ an ninh tin cẩn mới có thể được cung cấp bởi các cơ chế an ninh chứa trong tầng trình diễn.

Các cơ chế an ninh trong tầng trình diễn vận hành như một giai đoạn biến đổi cuối cùng cú pháp truyền trên đường truyền dẫn và như giai đoạn biến đổi quy trình nhận ban đầu.

7.7 Tầng ứng dụng

7.7.1 Các dịch vụ

Tầng ứng dụng có thể cung cấp một hoặc nhiều dịch vụ an ninh cơ sở một cách đơn lẻ hoặc kết hợp sau đây:

a) Xác thực thực thể ngang hàng;

b) Xác thực nguồn gốc của dữ liệu;

c) Dịch vụ điều khiển truy cập;

d) Tính mật của chế độ kết nối;

e) Tính mật của chế độ không-kết nối;

f) Tính mật của trường lựa chọn;

g) Tính mật của luồng lưu lượng;

h) Tính toàn vẹn của chế độ kết nối có khôi phục;

j) Tính toàn vẹn của chế độ kết nối không khôi phục;

k) Tính toàn vẹn của chế độ kết nối trường lựa chọn;

m) Tính toàn vẹn của chế độ không-kết nối;

n) Tính toàn vẹn của chế độ không-kết nối trường lựa chọn;

p) Chống chối bỏ bằng chứng xuất xứ; và

q) Chống chối bỏ bằng chứng việc gửi.

Xác thực các đối tác truyền thông cung cấp việc hỗ trợ các bộ điều khiển truy cập cho cả tài nguyên OSI và tài nguyên không theo OSI (ví dụ: các tệp tin, phần mềm, thiết bị đầu cuối, máy in) trong các hệ thống mở thực.

Xác định các yêu cầu an ninh cụ thể trong trường hợp truyền thông bao gồm tính mật, tính toàn vẹn và xác thực dữ liệu do Quản lý tầng ứng dụng hoặc quản lý an ninh OSI tạo ra trên cơ sở thông tin trong SMIB công thêm các yêu cầu tạo bởi quy trình ứng dụng.

7.7.2 Các cơ chế

Các dịch vụ an ninh trong tầng ứng dụng được cung cấp bởi các cơ chế sau đây:

a) Dịch vụ xác thực thực thể ngang hàng có thể được cung cấp bằng cách sử dụng thông tin xác thực truyền giữa các thực thể ứng dụng, bảo vệ bởi các cơ chế mã hoá tầng trình diễn hoặc tầng tầng thấp hơn;

b) Dịch vụ xác thực nguồn gốc dữ liệu có thể được hỗ trợ bằng cách sử dụng các cơ chế chữ ký hoặc các cơ chế mã hoá tầng thấp hơn;

c) Dịch vụ điều khiển truy cập các khía cạnh của hệ thống mở truy cập là thích hợp với OSI, ví dụ như khả năng giao tiếp với các hệ thống hoặc thực thể ứng dụng từ xa, có thể được cung cấp bởi một tổ hợp các cơ chế điều khiển truy cập trong tầng ứng dụng và trong các tầng thấp hơn;

d) Dịch vụ về tính mật của chế độ kết nối có thể được hỗ trợ bằng cách sử dụng cơ chế mã hoá tầng thấp hơn;

e) Dịch vụ về tính mật của chế độ không-kết nối có thể được hỗ trợ bằng cách sử dụng cơ chế mã hoá tầng thấp hơn;

f) Dịch vụ về tính mật của trường lựa chọn có thể được cung cấp bằng cách sử dụng cơ chế mã hoá tại tầng trình diễn;

g) Dịch vụ về tính mật của luồng lưu lượng giới hạn có thể được hỗ trợ bằng cách sử dụng cơ chế đệm lưu lượng tại tầng ứng dụng kết hợp với dịch vụ tin cẩn tại tầng thấp hơn;

h) Dịch vụ về tính toàn vẹn của chế độ kết nối có khôi phục có thể được hỗ trợ bằng cách sử dụng cơ chế về tính toàn vẹn của dữ liệu tầng thấp hơn (đôi khi kết hợp với cơ chế mã hoá);

j) Dịch vụ về tính toàn vẹn của chế độ kết nối không khôi phục có thể được hỗ trợ bằng cách sử dụng cơ chế về tính toàn vẹn của dữ liệu tầng thấp hơn (đôi khi kết hợp với cơ chế mã hoá);

k) Dịch vụ về tính toàn vẹn của chế độ kết nối trường lựa chọn có thể được hỗ trợ bằng cách sử dụng cơ chế về tính toàn vẹn của dữ liệu (đôi khi kết hợp với cơ chế mã hoá) tại tầng trình diễn;

m) Dịch vụ về tính toàn vẹn của chế độ không-kết nối có thể được hỗ trợ bằng cách sử dụng cơ chế về tính toàn vẹn của dữ liệu tầng thấp hơn (đôi khi kết hợp với cơ chế mã hoá);

n) Dịch vụ về tính toàn vẹn của chế độ không-kết nối trường lựa chọn có thể được hỗ trợ bằng cách sử dụng cơ chế về tính toàn vẹn của dữ liệu (đôi khi kết hợp với cơ chế mã hoá) tại tầng trình diễn;

p) Dịch vụ thừa nhận bằng chứng xuất xứ có thể được hỗ trợ bởi sự kết hợp của cơ chế chữ ký và cơ chế về tính toàn vẹn của dữ liệu tầng thấp hơn cùng với bên thứ ba; và

q) Dịch vụ thừa nhận bằng chứng việc gửi có thể được hỗ trợ bởi sự kết hợp của cơ chế chữ ký và cơ chế về tính toàn vẹn của dữ liệu tầng thấp hơn cùng với bên thứ ba.

Nếu cơ chế chứng thực được sử dụng để cung cấp dịch vụ thừa nhận thì nó sẽ đóng vai trò là bên thứ ba tin cậy. Nó có thể có bản ghi các đơn vị dữ liệu chuyển tiếp theo dạng được truyền (tức là cú pháp truyền) nhằm giải quyết các khúc mắc. Có thể sử dụng các dịch vụ bảo vệ từ các tầng thấp hơn.

7.7.3 Các dịch vụ an ninh không theo OSI

Bản thân các quy trình ứng dụng có thể cung cấp tất cả các dịch vụ và sử dụng cùng loại cơ chế được mô tả trong tiêu chuẩn này khi được đặt thích hợp trong các tầng khác nhau của kiến trúc. Kiến trúc này nằm ngoài phạm vi của tiêu chuẩn và không nhất quán với dịch vụ, các định nghĩa giao thức OSI và kiến trúc OSI.

7.8 Minh hoạ mối quan hệ của dịch vụ và tầng an ninh

Bảng 2 minh hoạ các tầng của mô hình tham chiếu mà các dịch vụ an ninh riêng biệt có thể được cung cấp. Các định nghĩa dịch vụ an ninh có trong điều 5.2. Các minh chứng về sự xếp đặt dịch vụ tại tầng riêng biệt được đưa ra trong Phụ lục B.

Bảng 2

Dịch vụ	Tầng						
	1	2	3	4	5	6	7*
Xác thực thực thể ngang hàng	•	•	Y	Y	•	•	Y
Xác thực nguồn gốc của dữ liệu	•	•	Y	Y	•	•	Y
Dịch vụ điều khiển truy cập	•	•	Y	Y	•	•	Y
Tính mật của chế độ kết nối	Y	Y	Y	Y	•	•	Y
Tính mật của chế độ không kết nối	•	Y	Y	Y	•	•	Y
Tính mật của trường lựa chọn	•	•	•	•	•	•	Y
Tính mật của luồng lưu lượng		•		•	•	•	Y
Tính toàn vẹn của chế độ kết nối có khôi phục	•	•	•	Y	•	•	Y
Tính toàn vẹn của chế độ kết nối không khôi phục	•	•	Y	Y	•	•	Y
Tính toàn vẹn của chế độ kết nối trường lựa chọn	•	•	•	•	•	•	Y
Tính toàn vẹn của chế độ không-kết nối	•	•	Y	Y	•	•	Y
Tính toàn vẹn của chế độ không-kết nối trường lựa chọn	•	•	•	•	•	•	Y
Chống chối bỏ bằng chứng xuất xứ	•	•	•	•	•	•	Y
Chống chối bỏ bằng chứng việc gửi	•	•	•	•	•	•	Y

Ghi chú: Y (Yes), dịch vụ nên được hợp nhất trong các tiêu chuẩn về tầng như một lựa chọn của nhà cung cấp.

- Không được cung cấp.
- Nên được chú thích đối với tầng 7 rằng quy trình ứng dụng có thể cung cấp các dịch vụ an ninh.

CHÚ THÍCH

1. Bảng 2 không chỉ ra rằng các mục có tầm quan trọng như nhau, trái lại có một sự thay đổi về phạm vi trong các mục của bảng.
2. Việc xếp đặt các dịch vụ an ninh trong Tầng Mạng được mô tả trong điều 7.3.2. Vị trí của các dịch vụ an ninh trong tầng mạng không ảnh hưởng đến bản chất và phạm vi áp dụng của các dịch vụ sẽ được cung cấp.
3. Tầng trình diễn chứa số lượng tiện ích an ninh hỗ trợ việc cung cấp các dịch vụ an ninh bởi tầng ứng dụng.

8 Quản lý an ninh

8.1 Khái quát

8.1.1 Quản lý an ninh OSI đề cập tới các khía cạnh quản lý an ninh liên quan đến OSI và đến an ninh của quản lý OSI. Các khía cạnh quản lý an ninh OSI đề cập đến các thao tác nằm ngoài các thể hiện truyền thông nhưng yêu cầu hỗ trợ và điều khiển các khía cạnh an ninh của truyền thông.

CHÚ THÍCH – Tính sẵn có của dịch vụ truyền thông được xác định bởi thiết kế mạng và/hoặc các giao thức quản lý mạng. Các lựa chọn thích hợp được yêu cầu bảo vệ khỏi việc chối bỏ dịch vụ.

8.1.2 Có thể có nhiều chính sách an ninh được áp đặt bởi việc quản trị các hệ thống mở phân tán và các tiêu chuẩn quản lý an ninh OSI nên hỗ trợ các chính sách này. Các thực thể tuân theo chính sách an ninh đơn do thẩm quyền đơn quản lý, đôi khi được tập hợp trong "Vùng an ninh". Các vùng an ninh và các tương tác của chúng là khu vực quan trọng cho việc mở rộng trong tương lai.

8.1.3 Quản lý an ninh OSI đề cập đến việc quản lý các dịch vụ và cơ chế an ninh OSI. Việc quản lý này yêu cầu phân tán thông tin quản lý cho các dịch vụ và cơ chế này cũng như việc tập hợp thông tin liên quan đến thao tác của các dịch vụ và cơ chế này. Các ví dụ là sự phân tán các khóa mật mã, thiết lập các thông số lựa chọn an ninh quản trị, báo cáo các sự việc an ninh thông thường và bất thường (các biên bản kiểm định) và việc kích hoạt và không kích hoạt dịch vụ. Quản lý an ninh không đề cập đến việc truyền thông tin trong các giao thức gọi các dịch vụ an ninh cụ thể (ví dụ: trong các thông số tại yêu cầu kết nối).

8.1.4 Cơ sở thông tin quản lý an ninh (SMIB) là kho khái niệm về tất cả thông tin liên quan đến an ninh được yêu cầu bởi các hệ thống mở. Khái niệm này không đề xuất bất kỳ dạng lưu trữ thông tin nào hoặc việc thực hiện của nó. Tuy nhiên, mỗi hệ thống cuối phải chứa thông tin cục bộ cần thiết giúp cho chính sách an ninh thích hợp có hiệu lực. SMIB là cơ cở thông tin phân tán cho việc mở rộng, cần giúp cho chính sách an ninh trong nhóm các hệ thống cuối có hiệu lực. Thực tế, các phần của SMIB có thể hoặc không thể hợp nhất với MIB.

CHÚ THÍCH – Có thể có nhiều phép thể hiện của SMIB, ví dụ:

a) Bảng dữ liệu;

b) Ttệp tin;

c) Dữ liệu hoặc quy tắc gắn trong phần mềm hoặc phần cứng của hệ thống mở thực.

8.1.5 Các giao thức quản lý, nhất là các giao thức quản lý an ninh và các kênh truyền truyền thông mang thông tin quản lý có khả năng bị tấn công. Do đó cần đảm bảo rằng các giao thức và thông tin quản lý được bảo vệ sao cho bảo vệ an ninh được cung cấp cho các thể hiện truyền thông không bị suy yếu.

8.1.6 Quản lý an ninh có thể yêu cầu trao đổi thông tin liên quan đến an ninh giữa các quản trị hệ thống khác nhau theo trình tự mà SMIB có thể được thiết lập hoặc mở rộng. Trong một số trường hợp, thông tin liên quan đến an ninh sẽ được chuyển qua các đường truyền thông không theo OSI và các nhà quản trị hệ thống cục bộ sẽ cập nhật SMIB qua các phương pháp không được tiêu chuẩn hóa. Trong các trường hợp khác, có thể trao đổi thông tin này qua đường truyền thông OSI trong trường hợp thông tin được chuyển giữa hai ứng dụng quản lý an ninh đang chạy trong các hệ thống mở thực. Ứng dụng quản lý an ninh sử dụng thông tin giao tiếp để cập nhật SMIB. Việc cập nhật SMIB này có thể yêu cầu quyền ưu tiên của nhà quản trị an ninh thích hợp.

8.1.7 Các giao thức ứng dụng sẽ được xác định cho việc trao đổi thông tin liên quan đến an ninh thông qua các kênh truyền thông OSI.

8.2 Các hạng mục quản lý an ninh OSI

Có ba hạng mục của quản lý an ninh OSI:

a) Quản lý an ninh hệ thống;

b) Quản lý dịch vụ an ninh; và

c) Quản lý cơ chế an ninh.

Ngoài ra, phải cân nhắc an ninh quản lý OSI (xem điều 8.2.4). Các chức năng thực hiện bởi các hạng mục quản lý an ninh này được tóm tắt dưới đây.

8.2.1 Quản lý an ninh hệ thống

Quản lý an ninh hệ thống đề cập đến việc quản lý các khía cạnh an ninh của toàn bộ môi trường OSI. Danh mục sau đây tiêu biểu cho các hoạt động trong hạng mục quản lý an ninh:

a) Quản lý toàn bộ chính sách an ninh, bao gồm các cập nhật và duy trì tính nhất quán;

b) Tương tác với các chức năng quản lý OSI khác;

c) Tương tác với quản lý dịch vụ an ninh và quản lý cơ chế an ninh;

d) Quản lý việc điều khiển sự việc (xem điều 8.3.1);

e) Quản lý kiểm định an ninh (xem điều 8.3.2); và

f) Quản lý việc khôi phục an ninh (xem điều 8.3.3).

8.2.2 Quản lý dịch vụ an ninh

Quản lý dịch vụ an ninh đề cập đến việc quản lý các dịch vụ an ninh riêng biệt. Danh mục sau đây tiêu biểu cho các hoạt động có thể được thực hiện trong việc quản lý dịch vụ an ninh riêng biệt:

a) Xác định và ấn định việc bảo vệ an ninh mục tiêu cho dịch vụ;

b) Ấn định và duy trì các quy tắc về việc lựa chọn cơ chế an ninh cụ thể được sử dụng để cung cấp dịch vụ an ninh được yêu cầu;

c) Thương thảo (cục bộ và từ xa) các cơ chế an ninh sẵn có yêu cầu thỏa thuận quản lý ưu tiên;

d) Dẫn chứng các cơ chế an ninh cụ thể qua chức năng quản lý cơ chế an ninh thích hợp, ví dụ: đối với việc cung cấp các dịch vụ an ninh về hành chính; và

e) Tương tác với các chức năng quản lý dịch vụ an ninh khác và các chức năng quản lý cơ chế an ninh.

8.2.3 Quản lý cơ chế an ninh

Quản lý cơ chế an ninh đề cập đến việc quản lý các cơ chế an ninh riêng biệt. Danh mục các chức năng quản lý cơ chế an ninh sau đây là tiêu biểu nhưng không bao gồm mọi khía cạnh:

a) Quản lý khóa;

b) Quản lý mã hóa hóa;

c) Quản lý chữ ký số;

d) Quản lý điều khiển truy cập;

e) Quản lý tính toàn vẹn của dữ liệu;

f) Quản lý việc xác thực;

g) Quản lý đệm lưu lượng;

h) Quản lý điều khiển định tuyến; và

i) Quản lý việc chứng thực.

Mỗi chức năng quản lý cơ chế an ninh đã liệt kê được thảo luận chi tiết hơn trong điều 8.4.

8.2.4 An ninh quản lý OSI

An ninh của *tất cả* các chức năng quản lý OSI và của truyền thông tin quản lý OSI là các thành phần quan trọng của an ninh OSI. Hạng mục này sẽ gọi ra các lựa chọn dịch vụ và cơ chế an ninh OSI đã liệt kê để đảm bảo rằng các giao thức và thông tin quản lý OSI được bảo vệ triệt để (xem điều 8.1.5). Ví dụ, truyền thông giữa các thực thể quản lý bao gồm Cơ sở thông tin quản lý yêu cầu một số dạng bảo vệ.

8.3 Các hoạt động quản lý an ninh hệ thống cụ thể

8.3.1 Quản lý điều khiển sự việc

Các khía cạnh quản lý điều khiển sự việc trong OSI là báo cáo từ xa các thử nghiệm vi phạm an ninh hệ thống và sửa đổi các ngưỡng sử dụng để khởi động báo cáo sự việc.

8.3.2 Quản lý kiểm định an ninh

Quản lý kiểm định an ninh có thể bao gồm:

a) Lựa chọn các sự kiện được ghi lại và/hoặc tập hợp từ xa;

b) Kích hoạt và không kích hoạt bản ghi theo dõi kiểm định các sự kiện được lựa chọn;

c) Tập hợp từ xa các bản kiểm định được lựa chọn; và

d) Chuẩn bị các báo cáo kiểm định an ninh.

8.3.3 Quản lý khôi phục an ninh

Quản lý khôi phục an ninh có thể bao gồm:

a) Duy trì các quy tắc được sử dụng để phản ứng lại các vi phạm an ninh thực hoặc đáng nghi;

b) Báo cáo từ xa các vi phạm an ninh hệ thống;

c) Các tương tác của nhà quản trị an ninh.

8.4 Các chức năng quản lý cơ chế an ninh

8.4.1 Quản lý khóa

Quản lý khóa có thể bao gồm:

a) Tạo ra các khóa phù hợp xứng với mức an ninh yêu cầu;

b) Xác định theo đúng các yêu cầu về điều khiển truy cập, ở đó các thực thể nhận bản sao của mỗi khóa; và

c) Tạo sẵn hoặc phân tán các khóa theo cách an toàn cho các trường hợp thực thể trong các hệ thống mở thực.

Một số chức năng quản lý khóa sẽ được thực hiện bên ngoài môi trường OSI. Các chức năng này bao gồm việc phân tán các khóa bằng các phương tiện đáng tin cậy.

Việc trao đổi các khóa hoạt động sử dụng trong một liên kết là chức năng giao thức tầng thông thường. Lựa chọn các khóa hoạt động cũng có thể được hoàn thành bằng cách truy cập tới trung tâm phân tán khóa hoặc phân tán trước qua các giao thức quản lý.

8.4.2 Quản lý mã hóa

Quản lý mã hóa có thể bao gồm:

a) Tương tác với quản lý khóa;

b) Thiết lập các thông số mật mã;

c) Đồng bộ hóa mật mã.

Sự tồn tại của cơ chế mã hóa bao hàm việc sử dụng quản lý khóa và các cách thông thường nhằm tham chiếu các thuật toán mật mã.

Mức độ phân biệt việc bảo vệ do mã hóa tạo ra được xác định bởi các thực thể trong môi trường OSI được khóa một cách độc lập. Nhìn chung, mức độ này được xác định bởi kiến trúc an ninh và cơ chế quản lý khóa.

Tham chiếu thông thường đối với các thuật toán mật mã có thể đạt được bằng cách sử dụng một bộ đăng ký về các thuật toán mật mã hoặc bằng các thỏa thuận ưu tiên giữa các thực thể.

8.4.3 Quản lý chữ ký số

Quản lý chữ ký số có thể bao gồm:

a) Tương tác với quản lý khóa;

b) Thiết lập các thông số và thuật toán mật mã; và

c) Sử dụng giao thức giữa các thực thể giao tiếp và bên thứ ba.

CHÚ THÍCH – Nhìn chung, có sự tồn tại các tương đồng giữa quản lý chữ ký số và quản lý mã hóa.

8.4.4 Quản lý điều khiển truy cập

Quản lý điều khiển truy cập có thể bao gồm việc phân tán các thuộc tính hoặc cập nhật an ninh (bao gồm các mật khẩu) nhằm truy cập các danh mục điều khiển hoặc danh mục các khả năng. Nó cũng có thể bao gồm việc sử dụng một giao thức giữa các thực thể truyền thông và các thực thể khác cung cấp các dịch vụ điều khiển truy cập.

8.4.5 Quản lý tính toàn vẹn của dữ liệu

Quản lý tính toàn vẹn của dữ liệu có thể bao gồm:

a) Tương tác với quản lý khóa;

b) Thiết lập các thông số và thuật toán mật mã; và

c) Sử dụng giao thức giữa các thực thể truyền giao tiếp.

CHÚ THÍCH – Khi sử dụng các kỹ thuật mật mã về tính toàn vẹn của dữ liệu, có sự tồn tại các tương đồng giữa quản lý tính toàn vẹn của dữ liệu và quản lý mã hóa.

8.4.6 Quản lý xác thực

Quản lý xác thực có thể bao gồm việc phân tán thông tin mô tả, mật khẩu hoặc khóa (sử dụng quản lý khóa) cho các thực thể được yêu cầu nhằm thực hiện việc xác thực. Cũng bao gồm việc sử dụng giao thức giữa các thực thể giao tiếp và các thực thể khác cung cấp các dịch vụ xác thực.

8.4.7 Quản lý đệm lưu lượng

Quản lý đệm lưu lượng có thể bao gồm việc duy trì các quy tắc được sử dụng cho việc đệm lưu lượng. Ví dụ, điều này bao gồm:

a) Tỉ lệ dữ liệu được quy định trước;

b) Tỉ lệ dữ liệu ngẫu nhiên;

c) Các đặc điểm thông điệp như độ dài; và

d) Sự khác nhau của đặc tả, theo đúng với thời gian trong ngày và/hoặc lịch.

8.4.8 Quản lý điều khiển định tuyến

Quản lý điều khiển định tuyến có thể bao gồm việc xác định các liên kết hoặc các mạng con được xem xét là an toàn hoặc tin tưởng theo tiêu chí riêng.

8.4.9 Quản lý chứng thực

Quản lý chứng thực có thể bao gồm:

a) Phân tán thông tin về các công chứng viên;

b) Sử dụng giao thức giữa công chứng viên và các thực thể giao tiếp; và

c) Tương tác với các công chứng viên.

Phụ lục A

(Tham khảo)

Thông tin cơ bản về an ninh trong OSI

A.1 Bối cảnh

Phụ lục này cung cấp:

a) Thông tin về an ninh OSI nhằm đưa ra một số quan điểm của tiêu chuẩn này; và

b) Bối cảnh về các vấn đề liên quan đến kiến trúc của các tính năng và yêu cầu an ninh.

An ninh trong môi trường OSI chỉ là một khía cạnh của an ninh xử lý dữ liệu/an ninh truyền thông dữ liệu. Nếu chúng hiệu quả thì các biện pháp bảo vệ sử dụng trong môi trường OSI sẽ yêu cầu các biện pháp hỗ trợ nằm ngoài OSI. Ví dụ, luồng thông tin giữa các hệ thống có thể được mã hóa nhưng nếu không có các hạn chế về an ninh đặt trên truy cập các hệ thống thì việc mã hóa có thể không có kết quả. Cũng như vậy, OSI chỉ đề cập đến kết nối các hệ thống. Các biện pháp an ninh OSI hiệu quả khi chúng được sử dụng cùng với các biện pháp nằm ngoài phạm vi của OSI.

A.2 Yêu cầu đối với an ninh

A.2.1 Được định nghĩa như thế nào bởi an ninh?

Thuật ngữ "An ninh" được sử dụng theo nghĩa giảm thiểu các điểm yếu của tài sản và tài nguyên. Tài sản gồm mọi thứ có giá trị. Điểm yếu là tình trạng yếu kém mà có thể được lợi dụng để xâm nhập hệ thống hoặc thông tin. Mối đe dọa là tiềm năng vi phạm an ninh.

A.2.2 Thúc đẩy an ninh trong các hệ thống mở

ISO định danh yêu cầu cho chuỗi các tiêu chuẩn nhằm mở rộng an ninh giữa kiến trúc liên kết hệ thống mở. Điều này xuất phát từ:

a) Tăng sự phụ thuộc của xã hội vào máy tính mà được truy cập hoặc kết nối bằng truyền thông dữ liệu và yêu cầu bảo vệ chống lại các mối đe dọa khác nhau;

b) Sự xuất hiện ở một số quốc gia về luật "bảo vệ dữ liệu", luật này bắt buộc nhà cung cấp phải chứng minh tính toàn vẹn và riêng tư của hệ thống; và

c) Sự mong muốn của các tổ chức là được sử dụng các tiêu chuẩn OSI, mở rộng khi được yêu cầu đối với các hệ thống an ninh hiện có và trong tương lai.

A.2.3 Cái gì được bảo vệ?

Nhìn chung, các vấn đề sau đây yêu cầu sự bảo vệ:

a) Thông tin và dữ liệu (bao gồm phần mềm và dữ liệu tiêu cực liên quan đến các biện pháp an ninh như là các mật khẩu);

b) Các dịch vụ truyền thông và xử lý dữ liệu; và

c) Trang thiết bị và các phương tiện.

A.2.4 Các mối đe dọa

Các mối đe dọa đến hệ thống truyền thông dữ liệu bao gồm:

a) Phá hủy thông tin và/hoặc các tài nguyên khác;

b) Làm sai lạc thông tin;

c) Lấy cắp, di chuyển hoặc mất mát thông tin và/hoặc các tài nguyên khác;

d) Làm lộ thông tin; và

e) Ngắt các dịch vụ.

Các mối đe dọa có thể được phân loại một cách ngẫu nhiên hoặc cố ý và có thể là tiêu cực hoặc tích cực.

A.2.4.1 Các mối đe dọa ngẫu nhiên

Các mối đe dọa ngẫu nhiên là các mối đe dọa tồn tại mà không có dự định trước. Các ví dụ về mối đe dọa ngẫu nhiên bao gồm: sự cố về hệ thống; sai thao tác và lỗi phần mềm.

A.2.4.2 Các mối đe dọa cố ý

Các mối đe dọa cố ý có thể đi từ việc kiểm tra đột xuất sử dụng các công cụ sẵn có đến các tác động phức tạp vận dụng hiểu biết về hệ thống. Mối đe dọa cố ý nếu được thực hiện ra có thể được xem là một "tác động".

A.2.4.3 Các mối đe dọa tiêu cực

Các mối đe dọa tiêu cực là các mối đe dọa mà nếu được thực hiện sẽ không dẫn đến bất kỳ việc sửa đổi thông tin nào chứa trong (các) hệ thống và nơi mà không có thao tác hay trạng thái hệ thống bị thay đổi. Việc sử dụng thiết bị nghe trộm nhằm quan sát thông tin được phát qua đường truyền thông là một cách phát hiện ra mối đe dọa tiêu cực.

A.2.4.4 Các mối đe dọa tích cực

Các mối đe dọa tích cực đến hệ thống liên quan đến sự biến đổi thông tin chứa trong hệ thống hoặc các thay đổi đến trạng thái hoặc thao tác của hệ thống. Một thay đổi có hại cho các bảng định tuyến của hệ thống bởi việc sử dụng trái phép là ví dụ về mối đe dọa tích cực.

A.2.5 Một vài kiểu tác động cụ thể

Các nhận xét ngắn gọn về một số tác động cụ thể liên quan đến môi trường xử lý dữ liệu/truyền thông dữ liệu. Trong các phần sau đây, xuất hiện các thuật ngữ cho phép và trái phép. "Quyền hạn" có nghĩa là sự ban quyền. Hai thuật ngữ này được bao hàm bởi định nghĩa này là: các quyền thực hiện một số hoạt động (như là truy cập dữ liệu); và chúng được cấp cho một số thực

thể, tác nhân con người, hoặc quy trình. Trạng thái cho phép là việc thực hiện các hoạt động với các quyền được cấp cho (và không được thu hồi). Để biết nhiều hơn về khái niệm quyền hạn, xem điều A.2.3.1.

A.2.5.1 Sự giả mạo

Sự giả mạo là nơi mà một thực thể đóng giả một thực thể khác. Sự giả mạo thường được sử dụng với một số dạng tác động tích cực khác, nhất là phát lại và sửa đổi thông điệp. Ví dụ, các chuỗi xác thực có thể được thu thập và phát lại sau khi chuỗi xác thực hợp lệ được thực hiện. Thực thể cho phép với một ít đặc quyền có thể sử dụng sự giả mạo để đạt được thêm các đặc quyền bằng cách đóng giả một thực thể có các đặc quyền đó.

A.2.5.2 Sự phát lại

Sự phát lại xảy ra khi một thông điệp hoặc một phần thông điệp được nhắc lại nhằm tạo ra tác dụng cho phép. Ví dụ, một thông điệp hợp lệ chứa thông tin xác thực có thể được phát lại bởi thực thể khác để tự xác thực.

A.2.5.3 Sửa đổi thông điệp

Sửa đổi thông điệp xảy ra khi nội dung của việc truyền dẫn dữ liệu được biến đổi mà không bị xóa và các kết quả trong khả năng tác động trái phép, ví dụ: thông điệp 'cho phép John Smith' đọc tệp tin mật 'accounts' được thay đổi thành 'cho phép Fred Brown' đọc tệp tin mật 'Accounts'.

A.2.5.4 Chối bỏ dịch vụ

Chối bỏ dịch vụ xảy ra khi một thực thể thực hiện chức năng và hoạt động của nó nhằm ngăn ngừa các thực thể khác thực hiện các chức năng riêng của chúng. Sự tác động có thể là chung chung khi một thực thể chặn tất cả các thông điệp hoặc có thể có mục tiêu cụ thể khi một thực thể chặn tất cả các thông điệp hướng tới điểm đến riêng biệt như là dịch vụ kiểm định an ninh. Sự tác động có thể liên quan việc chặn lưu lượng như đã mô tả trong ví dụ này hoặc nó có thể tạo ra các thông điệp nhằm mục đích làm đứt đoạn thao thác mạng, nhất là nếu mạng có các thực thể chuyển tiếp quyết định việc định tuyến dựa trên các báo cáo trạng thái nhận từ các thực thể chuyển tiếp khác.

A.2.5.5 Tác động bên trong

Tác động bên trong xảy ra khi người sử dụng hệ thống theo các cách ngẫu nhiên hoặc trái phép. Hầu hết tội phạm máy tính được biết đến liên quan đến các tác động bên trong bao gồm an ninh hệ thống. Các phương pháp bảo vệ có thể được sử dụng để chống lại các tác động bên trong bao gồm:

a) Xem xét chặt chẽ lý lịch, trình độ chuyên môn của nhân viên;

b) Xem xét kỹ lưỡng phần cứng, phần mềm, chính sách an ninh và các cấu hình của hệ thống sao cho có một mức độ bảo đảm rằng chúng sẽ vận hành đúng (gọi là chức năng tin tưởng); và

c) Các biên bản kiểm định nhằm tăng khả năng phát hiện các tác động.

A.2.5.6 Các tác động bên ngoài

Các tác động bên ngoài có thể sử dụng các kỹ thuật như là:

a) Nghe trộm (tích cực và tiêu cực)

b) Hủy bỏ việc chặn thiết bị nghe trộm;

c) Giả mạo là người sử dụng hệ thống hoặc là các thành phần của hệ thống; và

d) Theo các cơ chế điều khiển truy cập hoặc xác thực.

A.2.5.7 Cửa bẫy

Khi một thực thể của hệ thống được biến đổi cho phép kẻ tấn công tạo ra tác dụng trái phép lên lệnh hoặc tại sự việc xác định trước hoặc chuỗi các sự việc, kết quả được gọi là cửa bẫy. Ví dụ, việc xác định tính hợp lệ của mật khẩu có thể được sửa đổi thêm vào tác dụng thông thường của nó sao cho nó cũng xác định tính hợp lệ của mật khẩu của kẻ tấn công.

A.2.5.8 Trojan horse

Khi giới thiệu hệ thống, thì trojan horse có chức năng trái phép thêm vào chức năng cho phép của nó. Việc chuyển tiếp sao chép các thông điệp cho kênh trái phép gọi là một trojan horse.

A.2.6 Đánh giá mối đe dọa, rủi ro và các biện pháp đếm

Các tính năng về an ninh thường làm tăng giá cả của hệ thống và có thể khiến cho việc sử dụng khó hơn. Trước khi thiết kế một hệ thống an toàn thì cần định danh các mối de dọa cụ thể và yêu cầu việc bảo vệ để chống lại chúng. Điều này được hiểu là đánh giá mối đe dọa. Hệ thống có thể bị làm hại theo nhiều cách nhưng chỉ một số là có thể khai thác được bởi vì kẻ tấn công không có nhiều cơ hội hoặc bởi vì kết quả không chứng minh được tác động và rủi ro của việc phát hiện. Mặc dù các vấn đề chi tiết về đánh giá mối de dọa không nằm trong phạm vi của Phụ lục này nhưng trong bản thảo mở rộng chúng bao gồm:

a) Định danh các điểm yếu của hệ thống;

b) Phân tích các mối đe dọa nhằm khai thác các điểm yếu này;

c) Ước lượng giá của mỗi tấn công;

d) Tính giá các biện pháp đếm tiềm năng; và

e) Lựa chọn các cơ chế an ninh (có thể bằng cách sử dụng các phân tích giá thành).

Các biện pháp phi kỹ thuật như là phạm vi bảo hiểm có thể là các phương pháp thay thế có hiệu quả đối với các biện pháp an ninh kỹ thuật. An ninh kỹ thuật hoàn hảo giống với an ninh vật lý hoàn hảo là không thể xảy ra. Do đó, mục tiêu là để tạo cho chi phí của một tác động đủ cao để giảm các mức độ rủi ro.

A.3 Chính sách an ninh

Điều này thảo luận về chính sách an ninh: yêu cầu cho một chính sách an ninh đã xác định một cách phù hợp; vai trò của nó; các phương pháp tiếp cận chính sách đang sử dụng và các phương pháp tinh vi để áp dụng các tình huống cụ thể. Do đó, các khái niệm được áp dụng cho các hệ thống truyền thông.

A.3.1 Yêu cầu và mục đích của chính sách an ninh

Toàn bộ trường an ninh đều phức tạp và có thể áp dụng rộng rãi. Mọi phân tích hoàn thiện sẽ tạo ra các chi tiết khác nhau. Chính sách an ninh phù hợp tập trung vào các khía cạnh tình huống mà mức cao nhất của quyền hạn nên nhận được sự chú ý. Về cơ bản, chính sách an ninh cho biết, trong các thuật ngữ chung, thuật ngữ được và không được phép trong trường an ninh trong quy trình đề cập đến thao tác của hệ thống. Chính sách thường không cụ thể, nó gợi ý cái gì là tầm quan trọng tối cao mà không cho biết chính xác kết quả đạt được như thế nào. Chính sách thiết lập mức cao nhất của một đặc tả an ninh.

A.3.2 Các hệ quả của định nghĩa chính sách: Quy trình lọc

Bởi vì các chính sách là quá chung nên tại lúc bắt đầu không dễ dàng để chỉ ra cách mà chính sách có thể được kết hợp với ứng dụng cho trước. Thông thường, cách tốt nhất để thực hiện điều này là đưa ra chính sách cho quy trình lọc kế tiếp bổ sung thêm chi tiết từ ứng dụng tại mỗi giai đoạn. Để biết các chi tiết nào cần nghiên cứu vùng ứng dụng chi tiết trong chính sách chung. Việc kiểm tra này xác định các vấn đề nảy sinh từ cố gắng áp đặt các điều kiện của chính sách trên ứng dụng. Quy trình lọc sinh ra chính sách chung trình bày lại trong các thuật ngữ được trực tiếp đưa ra từ ứng dụng. Chính sách này giúp xác định chi tiết thực hiện dễ dàng hơn.

A.3.3 Các thành phần chính sách an ninh

Có hai khía cạnh của chính sách an ninh hiện có. Cả hai phụ thuộc vào khái niệm về cách xử lý cho phép.

A.3.3.1 Quyền hạn

Các mối đe dọa đã thảo luận liên quan đến khái niệm về cách xử lý cho phép và trái phép. Phát biểu về quyền hạn được bao gồm trong chính sách an ninh. Chính sách an ninh chung cho biết "thông tin không thể được đưa ra, được truy cập hoặc được phép suy luận hoặc không thể là tài nguyên được sử dụng, chúng đều không được phép". Bản chất của quyền hạn là phân biệt các chính sách khác nhau. Các chính sách có thể được chia thành hai thành phần riêng rẽ, dựa trên bản chất của quyền hạn liên quan, là các chính sách dựa trên quy tắc hoặc các chính sách dựa trên định danh. Việc sử dụng các quy tắc dựa trên số lượng nhỏ các thuộc tính hoặc các lớp chung bắt buộc. Chính sách thứ hai liên quan đến tiêu chí quyền hạn dựa trên các thuộc tính riêng lẻ, cụ thể. Một số thuộc tính giả thiết được kết hợp với thực thể mà chúng áp dụng; các thuộc tính khác có thể là các quyền sở hữu (ví dụ như các khả năng) mà có thể được phát đến các thực thể khác. Một là cũng có thể phân biệt giữa dịch vụ quyền hành chính và dịch vụ quyền

hạn lựa chọn động. Chính sách an ninh xác định các phần tử của an ninh hệ thống trong đó luôn luôn được áp dụng và có hiệu lực (ví dụ: các thành phần chính sách an ninh dựa trên định danh và dựa trên quy tắc, nếu có) và các phần tử mà người sử dụng có thể lựa chọn khi họ thấy phù hợp.

A.3.3.2 Chính sách an ninh dựa trên định danh

Khía cạnh của các chính sách an ninh dựa trên thực thể tương ứng với khái niệm an ninh được hiểu là 'điều cần biết'. Mục đích là lọc truy cập dữ liệu hoặc tài nguyên. Có hai cách cơ bản về việc thực hiện các chính sách dựa trên định danh, phụ thuộc vào việc liệu thông tin về quyền truy cập có được thực hiện bởi người truy cập hoặc là một phần của dữ liệu được truy cập hay không. Cách đầu tiên được minh họa bởi các ý tưởng về các đặc quyền và khả năng cung cấp cho người sử dụng và được sử dụng bởi các quy trình đóng vai trò thay thế. Các danh mục điều khiển truy cập (ACLs) là các ví dụ về cách thứ hai. Trong cả hai trường hợp trên, kích cỡ của mục dữ liệu (từ tệp tin đầy đủ đến phần tử dữ liệu) có thể được đặt tên theo khả năng hoặc mang ACL của chính nó có thể thay đổi cao.

A.3.3.3 Chính sách an ninh dựa trên quy tắc

Quyền hạn trong chính sách an ninh dựa trên quy tắc thường dựa vào độ nhạy. Trong hệ thống an toàn, dữ liệu và/tài nguyên nên được đánh dấu với các nhãn an ninh. Các quy trình đóng vai trò thay mặt cho người sử dụng có thể thu được nhãn an ninh phù hợp với người phát dữ liệu.

A.3.4 Chính sách an ninh, truyền thông và các nhãn

Khái niệm ghi nhãn là quan trọng trong môi trường truyền thông. Nhãn mang các thuộc tính đóng các vai trò khác nhau. Có các mục dữ liệu di chuyển trong quy trình truyền thông; có các quy trình và thực thể khởi tạo việc truyền thông; và đáp lại; có các kênh và các tài nguyên khác của bản thân hệ thống được sử dụng trong quy trình truyền thông. Tất cả đều được ghi nhãn theo một cách hoặc cách khác với các thuộc tính của chúng. Các chính sách an ninh chỉ ra cách mà các thuộc tính có thể được sử dụng để cung cấp chính sách an ninh cần thiết. Việc thương thảo nhằm thiết lập tầm quan trọng của các thuộc tính an ninh riêng. Khi các nhãn an ninh được gắn với các quy trình đang truy cập và dữ liệu đã truy cập, thông tin bổ sung cần áp dụng bộ điều khiển truy cập dựa trên thực thể nên là các nhãn liên quan. Khi một chính sách an ninh được dựa trên định danh người sử dụng truy cập dữ liệu trực tiếp hoặc qua một quy trình thì các nhãn an ninh bao gồm thông tin về định danh của người sử dụng. Các quy tắc về các nhãn riêng nên được trình bày theo chính sách an ninh trong Cơ sở thông tin quản lý an ninh (SMIB) và/hoặc được thương thảo với hệ thống cuối khi có yêu cầu. Nhãn có thể được thêm hậu tố bởi các thuộc tính, các thuộc tính này làm giảm bớt độ nhạy của nhãn, quy định việc sử dụng và các nơi phân tán, quy định sự tính toán thời gian, cách sắp xếp và giải thích rõ ràng các yêu cầu đặc trưng cho hệ thống cuối.

A.3.4.1 Các nhãn quy trình

Trong quy trình xác thực, việc định danh đầy đủ các quy trình hoặc thực thể đó khởi tạo và đáp lại trường hợp truyền thông, cùng với tất cả các thuộc tính đều có tầm quan trọng cơ bản. Do đó, SMIBs sẽ chứa thông tin đầy đủ về các thuộc tính đó, các thuộc tính này có tầm quan trọng đối với mọi chính sách an ninh quản trị.

A.3.4.2 Các nhãn mục dữ liệu

Khi các mục dữ liệu di chuyển trong thời gian thực hiện việc, mỗi mục dữ liệu sẽ được gắn với nhãn của nó. (Việc gắn này là quan trọng, trong một số trường hợp của chính sách dựa trên quy tắc, cần yêu cầu rằng nhãn được tạo ra là một phần đặc biệt của mục dữ liệu trước khi nó thực hiện ứng dụng.) Các kỹ thuật nhằm bảo vệ tính toàn vẹn của mục dữ liệu cũng duy trì tính chính xác và sự kết hợp của nhãn. Các thuộc tính này có thể được sử dụng bởi các chức năng điều khiển định tuyến trong tầng liên kết dữ liệu của mô hình tham chiếu OSI.

A.4 Các cơ chế an ninh

Chính sách an ninh có thể được thực hiện bằng cách sử dụng các cơ chế khác nhau một cách đơn lẻ hoặc kết hợp, phụ thuộc vào các mục tiêu của chính sách và các cơ chế sử dụng. Nhìn chung, cơ chế sẽ phụ thuộc vào một trong ba lớp sau:

a) Ngăn chặn;

b) Phát hiện; và

c) Khôi phục.

Các cơ chế an ninh phù hợp với môi trường truyền dữ liệu được thảo luận dưới đây.

A.4.1 Các kỹ thuật mật mã và mã hóa

Mật mã làm cơ sở cho nhiều dịch vụ và cơ chế an ninh. Các chức năng mật mã có thể được sử dụng như một phần của mã hóa, giải mã, tính toàn vẹn của dữ liệu, trao đổi xác thực, kiểm tra và lưu trữ mật khẩu, v.v. nhằm đạt được tính mật, tính toàn vẹn và/hoặc tính xác thực. Mã hóa biến đổi dữ liệu nhạy cảm (tức là dữ liệu được bảo vệ) thành các dạng ít nhạy cảm hơn. Khi được sử dụng cho tính toàn vẹn và xác thực, các kỹ thuật mật mã được sử dụng để ước tính các chức năng đáng nhớ.

Mã hóa được thực hiện đầu tiên trên bản rõ nhằm tạo ra văn bản viết bằng mật mã. Kết quả của việc giải mã là bản rõ hoặc văn bản viết bằng mật mã dưới một số lớp bảo vệ. Việc sử dụng bản rõ nhằm mục đích xử lý là khả thi; nội dung ngữ nghĩa của nó có thể truy cập được. Ngoại trừ trong các cách đã quy định, (giải mã đầu tiên hoặc sự phù hợp). Sẽ không khả thi khi xử lý văn bản viết bằng mật mã khi nội dung ngữ nghĩa của nó bị giấu kín. Việc mã hóa đôi khi là phi thuận nghịch (ví dụ: bằng cách cắt bớt hoặc mất mát dữ liệu) khi việc mã hóa không muốn dẫn xuất bản rõ gốc như là các mật khẩu.

Các chức năng mật mã sử dụng các biến mật mã và điều hành qua các trường, đơn vị dữ liệu, và/hoặc các nhánh của đơn vị dữ liệu. Hai biến mật mã là khóa định hướng các phép biến đổi cụ

thể và biến khởi tạo được yêu cầu trong các giao thức mật mã nhất định nhằm bảo vệ tính ngẫu nhiên của văn bản viết bằng mật mã. Khóa phải luôn đáng tin, chức năng mật mã và biến khởi tạo có thể tăng sự tiêu thụ băng thông. Điều này làm phức tạp việc bổ sung mật mã "rõ ràng" hoặc "treo" cho các hệ thống hiện có.

Các biến mật mã có thể là đối xứng hoặc phi đối xứng thông qua việc mã hóa và giải mã. Các khóa sử dụng trong các thuật toán phi đối xứng có liên quan toán học với nhau; một khóa có thể được tính toán từ khóa khác. Các thuật toán này đôi khi được gọi là các thuật toán "khóa công khai" bởi vì một khóa có thể tạo công khai trong khi khóa khác giữ bí mật.

Văn bản viết bằng mật mã có thể được giải mã khi nó có thể khôi phục bản rõ mà không biết về khóa. Điều này có thể xảy ra nếu chức năng mật mã yếu được sử dụng. Các trạng thái bị chặn và phân tích lưu lượng có thể dẫn đến các tác động lên hệ thống mật mã bao gồm việc chèn, xóa và thay đổi thông điệp/trường, sự phát lại văn bản viết bằng mật mã hợp lệ và sự giả mạo. Do đó, các giao thức mật mã được thiết kế để chống lại các tác động và các phân tích lưu lượng. Biện pháp đếm các phân tích lưu lượng cụ thể, "tính mật của luồng lưu lượng" nhằm che đậy sự có mặt hoặc vắng mặt của dữ liệu và các đặc điểm của nó. Nếu văn bản viết bằng mật mã được chuyển tiếp thì địa chỉ phải rõ ràng tại các điểm chuyển tiếp và các cổng. Nếu dữ liệu được mã hóa trên mỗi liên kết và được giải mã trong chuyển tiếp hoặc trong cổng thì kiến trúc được cho biết là sử dụng "mã hóa từng liên kết". Nếu chỉ địa chỉ (và dữ liệu kiểm soát tương tự) là rõ ràng tại điểm chuyển tiếp và cổng thì kiến trúc được cho biết là sử dụng "mã hóa toàn trình". Mã hóa toàn trình được mong đợi hơn từ quan điểm an ninh nhưng phức tạp hơn về mặt kiến trúc, nhất là nếu phân tán khóa điện tử trong dải (quản lý chức năng khóa) được bao gồm. Mã hóa từng liên kết và mã hóa toàn trình có thể được kết hợp với nhau để đạt được nhiều mục tiêu an ninh. Tính toàn vẹn của dữ liệu thường đạt được bằng cách tính toán các giá trị kiểm tra mật mã. Giá trị kiểm tra có thể được dẫn xuất trong một hoặc nhiều bước và là chức năng toán học của các biến mật mã và dữ liệu. Các giá trị kiểm tra này liên kết với dữ liệu được bảo vệ. Các giá trị kiểm tra mật mã đôi khi được gọi là các mã phát hiện thao tác.

Các kỹ thuật mật mã có thể cung cấp việc bảo vệ chống lại:

a) Quan sát và/hoặc sửa đổi chuỗi thông điệp;

b) Phân tích lưu lượng;

c) Sự chối bỏ;

d) Sự giả mạo;

e) Kết nối trái phép; và

f) Sửa đổi thông điệp.

A.4.2 Các khía cạnh của quản lý khóa

Quản lý khóa được bao hàm bởi việc sử dụng các thuật toán mật mã. Quản lý khóa bao gồm việc tạo, phân phát và kiểm soát các khóa mật mã. Việc lựa chọn phương pháp quản lý khóa được

dựa trên đánh giá về môi trường của người tham gia mà sử dụng phương pháp đó. Các xem xét về môi trường này bao gồm việc bảo vệ khỏi các mối de dọa (cả bên trong và bên ngoài tổ chức), các công nghệ được sử dụng, cấu trúc kiến trúc và vị trí các dịch vụ mật mã được cung cấp, cấu trúc vật lý và vị trí của các nhà cung cấp dịch vụ mật mã.

Các điểm xem xét liên quan đến quản lý khóa bao gồm:

a) Việc sử dụng một "lifetime" (vòng đời) dựa trên thời gian, việc sử dụng hoặc các tiêu chí khác với mỗi khóa được xác định một cách rõ ràng và triệt để;

b) Định danh chính xác các khóa theo chức năng của nó sao cho việc sử dụng có thể được dành riêng cho chức năng của chúng, ví dụ: các khóa được sử dụng cho dịch vụ đáng tin cậy không nên được sử dụng cho dịch vụ toàn vẹn và ngược lại; và

c) Các xem xét không theo OSI, ví dụ như phân tán các khóa và lưu trữ các khóa.

Các điểm xem xét liên quan đến quản lý khóa đối với các thuật toán khóa đối xứng bao gồm:

a) Việc sử dụng dịch vụ đáng tin cậy trong giao thức quản lý khóa nhằm truyền tải các khóa;

b) Việc sử dụng hệ phân cấp khóa. Các tình huống khác nhau được cho phép như:

1) Các hệ phân cấp khóa "flat" chỉ sử dụng các khóa mã hóa dữ liệu, được lựa chọn một cách rõ ràng và triệt để từ một tập bởi định danh khóa hoặc chỉ mục;

2) Các hệ phân cấp khóa nhiều tầng; và

3) Các khóa mã hóa khóa không bao giờ được sử dụng để bảo vệ dữ liệu và các khóa mã hóa dữ liệu không bao giờ được sử dụng để bảo vệ các khóa mã hóa khóa.

c) Việc phân chia trách nhiệm để cho không người nào có quyền sao chép khóa quan trọng.

Các điểm xem xét liên quan đến quản lý khóa đối với các thuật toán khóa phi đối xứng bao gồm:

a) Việc sử dụng dịch vụ đáng tin cậy trong giao thức quản lý khóa nhằm truyền tải các khóa bí mật; và

b) Việc sử dụng dịch vụ toàn vẹn hoặc dịch vụ thừa nhận bằng chứng xuất xứ, trong giao thức quản lý khóa nhằm truyền tải các khóa công khai. Các dịch vụ này có thể được cung cấp thông qua việc sử dụng các thuật toán mật mã đối xứng và/hoặc phi đối xứng.

A.4.3 Các cơ chế chữ ký số

Thuật ngữ chữ ký số được sử dụng để chỉ ra một kỹ thuật riêng được sử dụng để cung cấp các dịch vụ an ninh ví dụ như chống chối bỏ và xác thực. Các cơ chế chữ ký số yêu cầu việc sử dụng các thuật toán mật mã phi đối xứng. Đặc điểm chủ yếu của cơ chế chữ ký số là đơn vị dữ liệu có dấu không thể được tạo ra mà không sử dụng khóa riêng tư. Điều này có nghĩa là:

a) Đơn vị dữ liệu có dấu không thể được tạo ra bởi cá nhân ngoại trừ người giữ khóa riêng tư; và

b) Người nhận không thể tạo ra đơn vị dữ liệu có dấu.

Do đó, chỉ sử dụng thông tin sẵn có một cách công khai, có khả năng định danh người đánh dấu đơn vị dữ liệu như một người sở hữu khóa riêng tư. Trong trường hợp xung đột sau đó giữa hai người tham gia, có thể chứng minh việc định danh người đánh dấu đơn vị dữ liệu cho bên thứ ba tin cậy, người này sẽ đánh giá tính xác thực của đơn vị dữ liệu có dấu. Kiểu chữ ký số này được gọi là chữ ký trực tiếp (xem Hình 1). Trong các trường hợp khác, (các) đặc tính bổ sung có thể được yêu cầu:

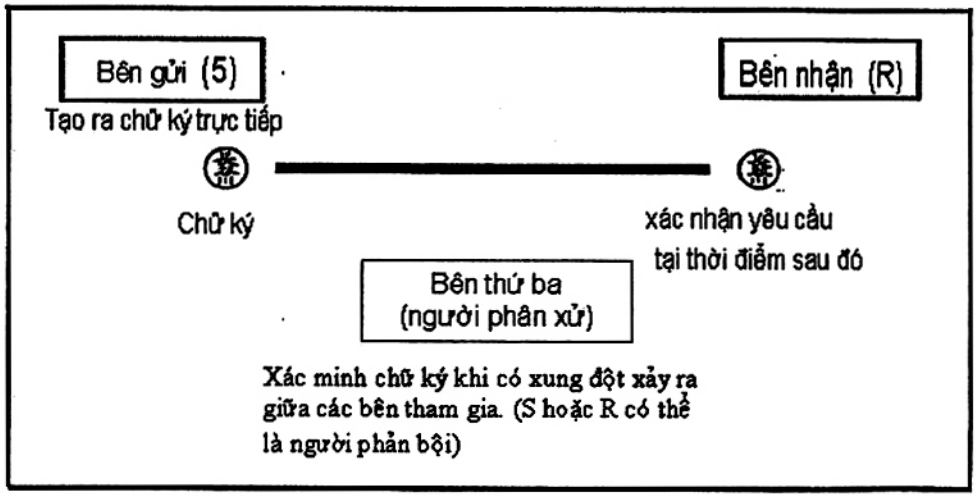
c) Người gửi không thể chối bỏ việc gửi đơn vị dữ liệu có dấu.

Bên thứ ba tin cậy chứng minh cho người nhận nguồn thông tin và tính toàn vẹn của thông tin. Kiểu chữ ký số này đôi khi được phán đoán bằng lược đồ chữ ký số (xem Hình 2).

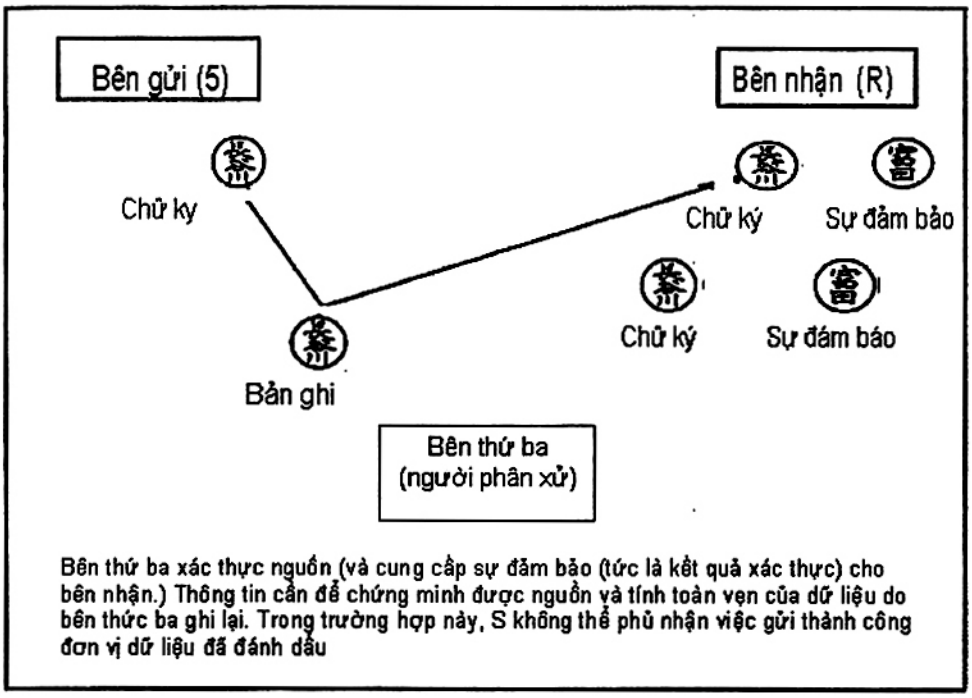
CHÚ THÍCH – Người gửi có thể yêu cầu rằng người nhận không thể chối bỏ việc nhận đơn vị dữ liệu có dấu sau đó. Điều này có thể được hoàn thành với dịch vụ thừa nhận bằng chứng xuất xứ bằng sự kết hợp của các cơ chế chữ ký số, tính toàn vẹn của dữ liệu và chứng thực.

A.4.4 Các cơ chế điều khiển truy cập

Các cơ chế điều khiển truy cập là các cơ chế đòi hỏi chính sách truy cập tài nguyên giới hạn cho người sử dụng hợp pháp. Các kỹ thuật bao gồm việc sử dụng các danh mục hoặc ma trận điều khiển truy cập (thường chứa các định danh các mục được kiểm soát và người sử dụng hợp lệ ví dụ: con người hoặc các quy trình), các mật khẩu và các khả năng, các nhãn hoặc các thẻ lệnh, việc sở hữu các kỹ thuật trên có thể được sử dụng để chỉ ra các quyền truy cập. Các khả năng được sử dụng nên dễ nhớ và được truyền tải một cách đáng tin cậy.



Hình 1 – Lược đồ chữ ký trực tiếp



Hình 2 – Lược đồ chữ ký có phân xử

A.4.5 Các cơ chế về tính toàn vẹn của dữ liệu

Các cơ chế về tính toàn vẹn của dữ liệu gồm 2 kiểu: chúng sử dụng để bảo vệ tính toàn vẹn của đơn vị dữ liệu đơn và sử dụng để bảo vệ tính toàn vẹn của các đơn vị dữ liệu đơn và trình tự toàn bộ dòng đơn vị dữ liệu trên một kết nối.

A.4.5.1 Phát hiện việc sửa đổi dòng thông điệp

Các kỹ thuật phát hiện sự sai lạc thường được kết hợp với việc phát hiện các lỗi bit, các lỗi khối, các lỗi sắp chuỗi do các mạng và các liên kết truyền thông đưa ra, cũng có thể được sử dụng để phát hiện việc sửa đổi dòng thông điệp. Tuy nhiên, phần đầu và phần cuối giao thức không được bảo vệ bởi các cơ chế toàn vẹn, một người xâm nhập am hiểu có thể bỏ qua các cản trở này. Việc phát hiện thành công việc sửa đổi dòng thông điệp chỉ có thể đạt được bằng cách sử dụng các công nghệ phát hiện sai lạc cùng với thông tin chuỗi. Điều này tuy không ngăn ngừa việc sửa đổi dòng thông điệp nhưng sẽ cung cấp một thông báo về các tác động.

A.4.6 Các cơ chế trao đổi xác thực

A.4.6.1 Lựa chọn cơ chế

Có nhiều lựa chọn và sự kết hợp của các cơ chế trao đổi xác thực phù hợp với các trường hợp khác nhau. Ví dụ:

a) Khi các thực thể ngang hàng và phương tiện truyền thông đều đáng tin cậy thì việc định danh thực thể ngang hàng có thể được xác nhận bằng mật khẩu. Mật khẩu bảo vệ khỏi lỗi, nó không phải bằng chứng chống lại các tác động xấu, (nhất là không chống lại việc phát lại). Xác thực lẫn nhau có thể được thực hiện bằng cách sử dụng mật khẩu khác biệt ở mỗi hướng.

b) Khi mỗi thực thể tin tưởng các thực thể ngang hàng mà không tin tưởng phương tiện truyền thông thì việc bảo vệ khỏi các tác động tích cực có thể được cung cấp bởi sự kết hợp của mật khẩu và mã hóa hoặc bởi phương tiện mật mã. Bảo vệ khỏi các tác động của việc phát lại yêu cầu thỏa thuận hai chiều (với các thông số bảo vệ) hoặc tem thời gian (với các sơ đồ đồng bộ hóa tin cậy). Xác thực lẫn nhau với việc bảo vệ khỏi sự phát lại có thể đạt được bằng cách sử dụng thỏa thuận ba chiều;

c) Khi các thực thể không tin tưởng các thực thể ngang hàng hoặc phương tiện truyền thông thì các dịch vụ thừa nhận có thể được sử dụng. Dịch vụ thừa nhận có thể đạt được bằng cách sử dụng các cơ chế chữ ký số và/hoặc các cơ chế chứng thực. Các cơ chế này có thể được sử dụng với các cơ chế mô tả ở mục (b).

A.4.7 Các cơ chế đệm lưu lượng

Việc tạo lưu lượng giả mạo và các đơn vị dữ liệu giao thức đệm cho một độ dài không đổi có thể cung cấp việc bảo vệ giới hạn khỏi các phân tích lưu lượng. Để thành công, mức lưu lượng giả mạo phải xấp xỉ với mức cao nhất của lưu lượng thực. Ngoài ra, các nội dung của các đơn vị dữ liệu giao thức phải được mã hóa hoặc được cải trang để lưu lượng giả mạo không thể được định danh và phân biệt từ lưu lượng thực.

A.4.8 Cơ chế điều khiển định tuyến

Đặc tả các cảnh báo định tuyến đối với việc truyền dữ liệu (bao gồm việc đặc tả toàn bộ tuyến) có thể được sử dụng nhằm đảm bảo rằng dữ liệu chỉ được truyền tải qua các tuyến an toàn về mặt vật lý hoặc để đảm bảo rằng thông tin nhạy cảm chỉ được đưa qua các tuyến với mức bảo vệ thích hợp.

A.4.9 Cơ chế chứng thực

Cơ chế chứng thực được dựa trên khái niệm bên thứ ba tin cậy để bảo đảm các đặc tính nhất định về thông tin trao đổi giữa hai thực thể, ví dụ như nguồn gốc của nó, tính toàn vẹn của nó hoặc thời gian nó được gửi hoặc nhận.

A.4.10 An ninh vật lý và an ninh nhân sự

Các biện pháp an ninh vật lý luôn cần thiết để đảm bảo việc bảo vệ hoàn toàn. An ninh vật lý thường tốn nhiều tiền của, các nỗ lực nhằm giảm thiểu yêu cầu bằng cách sử dụng các kỹ thuật khác (rẻ hơn). Các xem xét về an ninh vật lý và an ninh nhân sự nằm ngoài phạm vi của OSI, mặc dù tất cả các hệ thống dựa trên một số dạng an ninh vật lý và dựa trên tính đáng tin cậy của người điều hành hệ thống. Các thủ tục điều hành nên được xác định để đảm bảo thao tác chính xác và để vạch ra các trách nhiệm của người thực hiện.

A.4.11 Phần cứng/phần mềm đáng tin cậy

Các phương pháp sử dụng để có được độ tin cậy trong hoạt động của một thực thể bao gồm các phương pháp chứng minh chính thức, sự xác nhận và kiểm tra tính hợp lệ, sự phát hiện và ghi lại các tác động đã biết và việc xây dựng thực thể bởi một cá nhân đáng tin cậy trong môi trường an toàn. Các cảnh báo cũng được yêu cầu để đảm bảo rằng thực thể không bị sửa đổi một cách ngẫu nhiên hay cố ý bao gồm an ninh trong suốt thời gian vận hành của nó, ví dụ trong lúc duy trì hay cập nhật. Một số thực thể trong hệ thống cũng phải được tin tưởng để thực hiện chức năng chính xác nếu an ninh được duy trì. Các phương pháp sử dụng để thiết lập độ tin cậy không nằm trong phạm vi của OSI.

Phụ lục B

(Tham khảo)

Giải thích dịch vụ và các cơ chế an ninh trong Điều 7

B.1 Khái quát

Phụ lục này cung cấp một số lý do về việc cung các dịch vụ an ninh định danh trong các tầng khác nhau như đã nêu ra ở Điều 7. Các quy tắc sắp tầng an ninh định danh trong điều 6.1.1 của tiêu chuẩn chi phối quy trình lựa chọn này.

Nếu có hiệu quả thì dịch vụ an ninh riêng rẽ được cung cấp bởi nhiều tầng của an ninh truyền thông chung có thể được xem là khác nhau (ví dụ: tính mật của kết nối ở tầng 1 và 4). Việc xem xét các chức năng truyền thông dữ liệu OSI hiện có (ví dụ: các thủ tục đa liên kết, chức năng ghép kênh, các cách khác nhau nhằm nâng cao dịch vụ không kết nối đến dịch vụ kết nối) và cho phép điều hành các cơ chế truyền dẫn này, cần cho phép dịch vụ riêng rẽ được cung cấp ở tầng khác mặc dù hiệu quả an ninh không được cho là khác nhau.

B.2 Xác thực thực thể ngang hàng

Tầng 1 và 2: Không, xác thực thực thể ngang hàng không được xem là có ích trong các tầng này.

Tầng 3: Có, qua các mạng con riêng lẻ và đối với việc định tuyến và/hoặc qua mạng quốc tế.

Tầng 4: Có, xác thực hệ thống cuối đến hệ thống cuối trong tầng 4 có thể xác thực hai hay nhiều thực thể phiên, trước khi khởi đầu một kết nối và đối với thời lượng của kết nối đó.

Tầng 5: Không, không có lợi ích nào khi cung cấp dịch vụ này ở các tầng 4 và/hoặc các tầng cao hơn.

Tầng 6: Không, các cơ chế mã hóa có thể hỗ trợ dịch vụ này trong Tầng Ứng dụng.

Tầng 7: Có, xác thực thực thể ngang hàng nên được cung cấp bởi tầng ứng dụng.

B.3 Xác thực nguồn gốc dữ liệu

Các tầng 1 và 2: Không, xác thực nguồn gốc dữ liệu không được xem là có ích trong các tầng này

Các tầng 3 và 4: xác thực nguồn gốc dữ liệu có thể được cung cấp giữa hai đầu mút trong vai trò chuyển tiếp và định tuyến của tầng 3 và/hoặc tầng 4 như sau:

a) Cung cấp sự xác thực thực thể ngang hàng thời gian thiết lập kết nối cùng với xác thực liên tục dựa trên mã hóa trong suốt thời gian một kết nối cung cấp dịch vụ xác thực nguồn gốc dữ liệu; và

b) Khi không được cung cấp thì việc xác thực nguồn gốc dữ liệu có thể được cung cấp với lượng bổ sung cho các cơ chế về tính toàn vẹn của dữ liệu đặt trong các tầng này.

Tầng 5: Không, không có các lợi ích nào khi cung cấp điều này ở tầng 4 hoặc tầng 7.

Tầng 6: Không, các cơ chế mã hóa có thể hỗ trợ dịch vụ này trong tầng ứng dụng.

Tầng 7: Có, có thể kết hợp với các cơ chế trong tầng trình diễn.

Các tầng 1 và 2: các cơ chế điều khiển truy cập không thể được cung cấp tại các tầng 1 hoặc 2 trong hệ thống phù hợp với các giao thức OSI đầy đủ, bởi không có các tiện ích sẵn có cho cơ chế như vậy.

Tầng 3: Các cơ chế điều khiển truy cập có thể được áp đặt lên vai trò truy cập mạng con bởi các yêu cầu về mạng con riêng rẽ. Khi được thực hiện bởi vai trò chuyển tiếp và định tuyến, các cơ chế truy cập trong tầng mạng có thể được sử dụng để điều khiển các truy cập mạng con bởi các thực thể chuyển tiếp và để điều khiển truy cập đến các hệ thống cuối. Rõ ràng, độ chi tiết của kết nối chỉ phân biệt giữa các thực thể tầng mạng.

Việc thiết lập kết nối mạng có thể dẫn đến các cách tính giá bởi quản trị mạng con. Sự giảm thiểu giá cả có thể được thực hiện bằng cách điều khiển truy cập và lựa chọn cách tính giá ngược hoặc các thông số cụ thể của mạng con hay mạng khác.

Tầng 4: Có, các cơ chế điều khiển truy cập có thể được sử dụng trên mỗi cơ sở toàn trình của kết nối giao vận.

Tầng 5: Không, không có lợi ích nào khi cung cấp dịch vụ này ở tầng 4 và/hoặc tầng 7.

Tầng 6: Không, không phù hợp ở tầng 6.

Tầng 7: Có, các giao thức ứng dụng và/hoặc các quy trình ứng dụng có thể cung cấp các tiện ích điều khiển truy cập ứng dụng.

B.5 Tính mật của tất cả dữ liệu người sử dụng-tầng (N) trên kết nối-tầng (N)

Tầng 1: Có, nên được cung cấp bởi việc chèn các cặp thiết bị biến đổi điện có thể tin cậy hoàn toàn trên kết nối vật lý.

Tầng 2: Có, nó không cung cấp các lợi ích an ninh bổ sung qua tính mật ở tầng 1 hoặc tầng 3.

Tầng 3: Có, đối với vai trò truy cập mạng con qua các mạng con riêng lẻ và đối với các vai trò chuyển tiếp và định tuyến qua mạng quốc tế.

Tầng 4: Có, vì kết nối giao vận riêng lẻ đưa ra cơ chế giao vận giữa hai đầu mút và có thể cung cấp việc cách ly các kết nối phiên.

Tầng 5: Không, vì nó không cung cấp lợi ích bổ sung thông qua tính mật ở các tầng 3,4 và 7. Nó không thích hợp để cung cấp dịch vụ này ở tầng 5.

Tầng 6: Có, vì các cơ chế mã hóa cung cấp các phép biến đổi cú pháp.

Tầng 7: Có, cùng với các cơ chế tại các tầng thấp hơn.

B.6 Tính mật của tất cả dữ liệu người sử dụng-tầng (N) trong SDU không kết nối đơn - tầng (N)

Đối với tính mật của tất cả dữ liệu người sử dụng-tầng (N) ngoại trừ tầng 1 nơi không có dịch vụ không kết nối.

B.7 Tính mật của của trường lựa chon trong dữ liệu người sử dụng SDU-tầng (N)

Dịch vụ tin cẩn này được cung cấp bởi việc mã hóa trong tầng trình diễn và được gọi ra bởi các cơ chế trong tầng ứng dụng theo các ngữ nghĩa của dữ liệu.

B.8 Tính mật của luồng lưu lượng

Tính mật của luồng lưu lượng đầy đủ chỉ có thể thực hiện được ở tầng 1. Điều này đạt được bằng cách chèn một cặp thiết bị mã hóa vào trong đường truyền dẫn vật lý. Giả thiết rằng đường truyền dẫn là hai chiều đồng thời và đồng bộ hóa sao cho việc chèn thiết bị sẽ hoàn lại các đường truyền dẫn trên các phương tiện vật lý không nhận dạng được.

Trên tầng vật lý, không xuất hiện an ninh luồng lưu lượng. Một số hiệu quả được tạo ra bằng cách sử dụng dịch vụ tin cẩn của SDU ở một tầng và chối bỏ lưu lượng giả mạo ở tầng cao hơn. Cơ chế này có giá cao và tiêu thụ số lượng lớn vật mang và dung lượng chuyển mạch.

Nếu tính mật của luồng lưu lượng được cung cấp ở tầng 3 thì bộ điều khiển đệm lưu lượng và/hoặc định tuyến sẽ được sử dụng. Điều khiển định tuyến có thể cung cấp tính mật của luồng lưu lượng giới hạn bằng cách định tuyến các thông điệp xung quanh các kết nối và mạng con không an toàn. Tuy nhiên, sự hợp nhất của việc đệm lưu lượng trong tầng 3 giúp cho việc sử dụng mạng tốt hơn, ví dụ: bằng cách tránh sự quá tải mạng và việc làm đệm không cần thiết.

Tính mật của luồng lưu lượng giới hạn có thể được cung cấp ở tầng ứng dụng bằng cách tạo ra lưu lượng giả mạo cùng với tính mật để ngăn ngừa định danh lưu lượng giả mạo.

B.9 Tính toàn vẹn của tất cả dữ liệu người sử dụng-tầng (N) trên (Kết nối-tầng (N)(có sự khôi phục lỗi)

Các tầng 1 và 2: các tầng 1 và 2 không thể cung cấp dịch vụ này. Tầng 1 không có các cơ chế phát hiện hoặc khôi phục và tầng 2 chỉ điều hành trên cơ sở điểm-điểm, do đó không được xem là thích hợp để cung cấp dịch vụ này.

Tầng 3: Không, vì sự khôi phục lỗi không có sẵn.

Tầng 4: Có, vì dịch vụ này cung cấp kết nối giao vận giữa hai đầu mút.

Tầng 5: Không, vì sự khôi phục lỗi không phải là chức năng của tầng 5.

Tầng 6: Không, nhưng các dịch vụ mã hóa có thể hỗ tợ dịch vụ này trong tầng ứng dụng.

Tầng 7: Có, cùng với các cơ chế trong Tầng trình diễn.

B.10 Tính toàn vẹn của tất cả dữ liệu người sử dụng-tầng (N) trên kết nối-tầng (N)(không có sự khôi phục lỗi)

Các tầng 1 và 2: Các tầng 1 và 2 không thể cung cấp dịch vụ này. Tầng 1 không có các cơ chế phát hiện hoặc khôi phục và tầng 2 chỉ vận hành trên cơ sở điểm-điểm, do dó không được xem là thích hợp để cung cấp dịch vụ này.

Tầng 3: Có, đối với vai trò truy cập tầng mạng con qua các mạng con riêng lẻ và đối với việc vai trò định tuyến và chuyển tiếp qua mạng quốc tế.

Tầng 4: Có, đối với các trường hợp sử dụng ở đó nó được thừa nhận để kết thúc việc truyền thông sau khi phát hiện một tác động tích cực.

Tầng 5: Không, vì nó không cung cấp lợi ích bổ sung qua tính toàn vẹn của dữ liệu ở các tầng 3, 4 và 7.

Tầng 6: Không, nhưng các cơ chế mã hóa có thể hỗ trợ dịch vụ này trong tầng ứng dụng.

Tầng 7: Có, cùng với các cơ chế trong tầng trình diễn.

B.11 Tính toàn vẹn của cac trường lựa chọn trong dữ liệu người sử dụng-tầng (N)của SDU-tầng (N) truyền qua kết nối-tầng (N)(không có sự khôi phục)

Tính toàn vẹn của các trường lựa chọn có thể được cung cấp bởi các cơ chế mã hóa trong tầng trình diễn cùng với các cơ chế gọi ra và kiểm tra trong tầng ứng dụng.

B.12 Tính toàn vẹn của tất cả dữ liệu người sử dụng-tầng (N)trong SDU không kết nối đơn-tầng (N)

Để giảm thiểu sự nhân đôi các chức năng, tính toàn vẹn của việc truyền không kết nối được cung cấp ở các tầng giống nhau đối với tính toàn vẹn không có sự khôi phục, ví dụ các tầng giao vận và ứng dụng. Các cơ chế toàn vẹn này có tính hiệu quả giới hạn và phải được thừa nhận.

B.13 Tính toàn vẹn của các trường lựa chọn trong SDU-tầng (N) không kết nối đơn

Tính toàn vẹn của các trường lựa chọn có thể được cung cấp bởi các cơ chế mã hóa trong tầng trình diễn cùng với các cơ chế gọi ra và kiểm tra trong tầng ứng dụng.

B.14 Chống chối bỏ

Các dịch vụ thừa nhận nguồn gốc và sự gửi đi có thể được cung cấp bởi cơ chế chứng nhận liên quan đến sự chuyển tiếp ở tầng 7.

Sử dụng cơ chế chữ ký số đối với chống chối bỏ yêu cầu sự hợp tác khép kín giữa các tầng 6 và 7.

Phụ lục C

(Tham khảo)

Lựa chọn vị trí mã hóa cho các ứng dụng

C.1 Hầu hết các ứng dụng không yêu cầu mã hóa được sử dụng ở nhiều tầng. Việc lựa chọn tầng phụ thuộc vào các vấn đề chủ chốt được mô tả dưới đây:

1. Nếu tính mật của luồng lưu lượng được yêu cầu thì mã hóa tầng vật lý hoặc an ninh truyền dẫn (ví dụ: các kỹ thuật trải phổ thích hợp) sẽ được lựa chọn. An ninh vật lý tương xứng, định tuyến đáng tin cậy và chức năng tương tự tại các chuyển tiếp có thể thỏa mãn tất cả các yêu cầu về tính mật.
2. Nếu tính chi tiết của việc bảo vệ được yêu cầu (tức là một khóa riêng biệt đối với mối liên kết ứng dụng) và chống chối bỏ hoặc bảo vệ trường lựa chọn thì mã hóa tầng trình diễn được lựa chọn. Việc bảo vệ trường lựa chọn khá quan trọng bởi vì các thuật toán mã hóa tiêu thụ số lượng năng lượng lớn. Việc mã hóa trong tầng trình diễn có thể cung cấp tính toàn vẹn mà không có sự khôi phục, chống chối bỏ và tính mật.
3. Nếu việc bảo vệ hàng hóa đơn giản của các phương tiện truyền thông hệ thống cuối đến hệ thống cuối và/hoặc thiết bị mã hóa bên ngoài được yêu cầu (ví dụ: để đưa ra cách bảo vệ thuật toán và các khóa hoặc bảo vệ khỏi phần mềm hỏng hóc) thì mã hóa hóa tầng mạng sẽ được lựa chọn.

CHÚ THÍCH – Mặc dù việc khôi phục không được cung cấp trong tầng mạng nhưng các cơ chế khôi phục thông thường của tầng giao vận có thể được sử dụng để khôi phục khỏi các tác động do tầng mạng phát hiện ra.

4. Nếu tính toàn vẹn có sự khôi phục được yêu cầu cùng với tính chi tiết của việc bảo vệ cao thì mã hóa tầng giao vận sẽ được lựa chọn. Điều này có thể cung cấp tính mật và tính toàn vẹn có hoặc không có sự phục hồi.
5. Mã hóa ở tầng liên kết dữ liệu không được khuyến cáo cho các thực thi trong tương lai.

C.2 Khi có sự quan tâm đến hai hay nhiều vấn đề về khóa thì việc mã hóa sẽ được cung cấp trong nhiều tầng.