Teacher: Bùi Huy Anh

email: buiquyanh@tdtu.edu.vn

**Chương 1: Computer Security Concepts**

* **Khái niệm**

+Bảo mật máy tính: Sự bảo vệ dành cho hệ thống thông tin tự động nhằm đạt được các mục tiêu áp dụng là duy trì tính toàn vẹn, tính sẵn sàng và tính bảo mật của các tài nguyên hệ thống thông tin (bao gồm phần cứng, phần mềm, chương trình cơ sở, thông tin / dữ liệu và viễn thông).

* đảm bảo 3 yêu cầu integrity(tính toàn vẹn), availability(sẵn sàng) và confidentiality(bí mật)
* **Ba mục tiêu chính (bộ ba CIA)**
* Confidentiality(tính bảo mật) là đảm bảo thông tin đó là duy nhất, những người muốn tiếp cận phải được phân quyền truy cập
* Bảo mật dữ liệu: Đảm bảo rằng thông tin bí mật không bị tiết lộ cho những cá nhân không được phép
* Bảo mật: Đảm bảo rằng cá nhân kiểm soát hoặc ảnh hưởng đến những thông tin có thể được thu thập và lưu trữ
* Integrity(tính toàn vẹn) là bảo vệ sự hoàn chỉnh toàn diện cho hệ thống thông tin
* Tính toàn vẹn của dữ liệu: Đảm bảo rằng thông tin và chương trình chỉ được thay đổi theo cách cụ thể và được cho phép.
* Tính toàn vẹn của hệ thống: Đảm bảo rằng hệ thống thực hiện các hoạt động của mình theo cách không bị lỗi
* Availability(tính sẵn sàng)
* Đảm bảo rằng hệ thống luôn luôn phải sẵn sàng ,hoạt động nhanh chóng và dịch vụ không bị từ chối đối với người dùng được ủy quyền
* **Một số tính khác**
* Tính xác thực:
* Thuộc tính chính hãng và có thể được xác minh và tin cậy; tin tưởng vào tính hợp lệ của việc truyền tải, hoặc một thông điệp, hoặc người khởi tạo nó
* Trách nhiệm giải trình:
* Tạo ra yêu cầu đối với các hành động của một thực thể phải được truy nguyên duy nhất đối với cá nhân đó để hỗ trợ việc không từ chối, phản đối, cách ly lỗi, v.v.
* Mức độ ảnh hưởng của vi phạm an ninh( có 3 mức độ)
* Thấp: Tổn thất sẽ có tác động hạn chế
* Trung bình: Tổn thất có ảnh hưởng nghiêm trọng
* Cao: Tổn thất có tác động bất lợi nghiêm trọng hoặc thảm khốc đến hoạt động, tài sản của tổ chức hoặc cá nhân (ví dụ, mất mạng)
* Ví dụ về yêu cầu bảo mật
* Bảo mật
* Thông tin điểm của học sinh là tài sản có tính bảo mật được coi là rất cao ✓ Đạo luật FERPA của Hoa Kỳ: điểm chỉ được cung cấp cho học sinh, phụ huynh và chủ nhân của họ (khi cần thiết cho công việc)
* Thông tin tuyển sinh của học sinh: có thể có xếp hạng bảo mật vừa phải; ít thiệt hại hơn nếu kèm theo
* Thông tin danh bạ: mức độ bảo mật thấp; thường có sẵn công khai

❖ Tính toàn vẹn

* Thông tin dị ứng của bệnh nhân trong bệnh viện (dữ liệu có tính toàn vẹn cao): bác sĩ có thể tin tưởng rằng thông tin đó là chính xác và cập nhật - Nếu y tá cố tình làm sai lệch dữ liệu, cơ sở dữ liệu phải được khôi phục về cơ sở đáng tin cậy và thông tin giả mạo truy ngược lại người đã thực hiện việc đó
* Dữ liệu đăng ký nhóm tin trực tuyến: mức độ toàn vẹn vừa phải
* Một ví dụ về yêu cầu tính toàn vẹn thấp: cuộc thăm dò trực tuyến ẩn danh (mức độ không chính xác được hiểu rõ)
* Tính sẵn sàng
* Hệ thống cung cấp xác thực: yêu cầu tính khả dụng cao - Nếu khách hàng không thể truy cập tài nguyên, việc mất dịch vụ có thể dẫn đến tổn thất tài chính
* Trang web công cộng cho trường đại học: yêu cầu có sẵn vừa phải; không quan trọng nhưng gây lúng túng
* Tra cứu danh bạ điện thoại trực tuyến: yêu cầu về tính khả dụng thấp vì không có sẵn phần lớn là khó chịu (có các nguồn thay thế)
* Các thử thách của bảo mật máy tính

1. Bảo mật máy tính không đơn giản

2. Người ta phải xem xét các cuộc tấn công tiềm ẩn (bất ngờ)

3. Các thủ tục được sử dụng thường phản trực giác

4. Phải quyết định nơi triển khai các cơ chế

5. Liên quan đến các thuật toán và thông tin bí mật (khóa)

6. Trận chiến đấu trí giữa những kẻ tấn công / admin

7. Nó không được coi là lợi ích cho đến khi thất bại

8. Yêu cầu giám sát liên tục

9. Quá thường xuyên suy nghĩ sau (không phải là tích hợp)

10. Được coi là trở ngại cho việc sử dụng hệ thống

* Một mô hình cho bảo mật máy tính

❖Tài nguyên hệ thống

▪ Phần cứng, phần mềm (HĐH, ứng dụng), dữ liệu (người dùng, hệ thống, cơ sở dữ liệu),phương tiện truyền thông và mạng (LAN, cầu nối, bộ định tuyến, ...)

❖ Mối quan tâm của chúng tôi: tính dễ bị tổn thương của các tài nguyên này (bị hỏng, không có sẵn, bị rò rỉ)

❖Các mối đe dọa khai thác lỗ hổng

❖Attack là một mối đe dọa được tích tụ

▪ Chủ động hay bị động; từ bên trong hoặc từ bên ngoài

❖ Biện pháp đối phó: các hành động được thực hiện để ngăn chặn, phát hiện, khôi phục và giảm thiểu rủi ro

|  |  |
| --- | --- |
| Thuật ngữ | Khái niệm |
| Threat agent(tác nhân đe dọa) | một thực thể tấn công hoặc là mối đe dọa đối với hệ thống |
| attack | một cuộc tấn công vào an ninh hệ thống bắt nguồn từ một mối đe dọa thông minh; nghĩa là, một hành động thông minh là một nỗ lực có chủ ý (đặc biệt là theo nghĩa của một phương pháp hoặc kỹ thuật) để trốn tránh các dịch vụ bảo mật và vi phạm chính sách bảo mật của một hệ thống |
| Countermeasure( biện pháp đối phó) | một hành động, thiết bị, quy trình hoặc kỹ thuật làm giảm mối đe dọa, lỗ hổng hoặc cuộc tấn công bằng cách loại bỏ hoặc ngăn chặn nó, bằng cách giảm thiểu tác hại mà nó có thể gây ra hoặc bằng cách phát hiện và báo cáo nó để có thể thực hiện hành động khắc phục |
| Risk( rủi ro) | kỳ vọng về tổn thất được biểu thị bằng xác suất mà một mối đe dọa cụ thể sẽ khai thác một lỗ hổng cụ thể với một kết quả có hại cụ thể |
| Security policy | một tập hợp các quy tắc và thông lệ chỉ định hoặc điều chỉnh cách một hệ thống hoặc tổ chức cung cấp các dịch vụ bảo mật để bảo vệ các tài nguyên hệ thống nhạy cảm và quan trọng |

* Mối quan hệ bảo mật

Owners 🡪 coutermeasures 🡪risk 🡪assets

Threat agents 🡪threats🡪assets

* Các loại tấn công

▪ **Tấn công chủ động**: Cố gắng thay đổi tài nguyên hệ thống hoặc ảnh hưởng đến

hoạt động.

▪ **Tấn công bị động**: Cố gắng tìm hiểu hoặc sử dụng thông tin từ

hệ thống không ảnh hưởng đến tài nguyên hệ thống.

* Chúng tôi cũng có thể phân loại các cuộc tấn công dựa trên nguồn gốc của cuộc tấn công

▪ **Tấn công từ bên trong**: Được khởi xướng bởi một thực thể bên trong vành đai an ninh (một "Người trong cuộc").

▪ **Tấn công từ bên ngoài**: Bắt đầu từ bên ngoài vành đai, bởi một người không được phép

* Yêu cầu chức năng bảo mật (FIPS 200)

**Các biện pháp kỹ thuật**

* Kiểm soát truy cập; nhận dạng & xác thực; hệ thống & bảo vệ thông tin liên lạc; tính toàn vẹn của hệ thống và thông tin

**Kiểm soát và thủ tục quản lý**

* Nhận thức & đào tạo; kiểm toán & trách nhiệm giải trình; chứng nhận, đánh giá công nhận và bảo mật; kế hoạch dự phòng; Sự bảo trì; bảo vệ vật lý & môi trường; lập kế hoạch; an ninh nhân sự; đánh giá rủi ro; hệ thống & dịch vụ sự mua lại

**Chồng chéo kỹ thuật và quản lý**

* Quản lý cấu hình; ứng phó sự cố; bảo vệ phương tiện truyền thông

**Tính kinh tế của cơ chế**: thiết kế các biện pháp an ninh nên càng đơn giản càng tốt

* Đơn giản hơn để thực hiện và xác minh
* Ít lỗ hổng hơn

**Mặc định không an toàn**: quyết định truy cập phải dựa trên sự cho phép; tức là, mặc định là thiếu quyền truy cập

**Hoàn tất dàn xếp**: mọi quyền truy cập phải được kiểm tra hệ thống kiểm soát truy cập

**Thiết kế mở**: thiết kế nên cởi mở hơn là bí mật

**Sự cách ly**

* Quyền truy cập công cộng nên được cách ly khỏi các nguồn quan trọng (không kết nối giữa thông tin công khai và thông tin quan trọng)
* Các tệp người dùng phải được cách ly với nhau (ngoại trừ khi muốn)
* Cơ chế bảo mật nên được tách biệt (tức là, ngăn chặn truy cập vào các cơ chế đó)

Đóng gói:

* Tương tự với các khái niệm đối tượng (ẩn cấu trúc bên trong)

**Phân lớp (phòng thủ theo chiều sâu):** sử dụng nhiều, chồng chéo phương pháp bảo

**Ít ngạc nhiên**: một chương trình hoặc giao diện phải luôn luônphản hồi theo cách ít có khả năng làm người dùng ngạc nhiên nhất

**Tách đặc quyền**: cần nhiều đặc quyền để đạt được quyền truy cập (hoặc hoàn thành một nhiệm vụ)

**Đặc quyền ít nhất**: mọi người dùng (quy trình) nên có ít nhất đặc quyền để thực hiện một nhiệm vụ

**Cơ chế chung ít nhất**: một thiết kế nên giảm thiểu chức năng được chia sẻ bởi những người dùng khác nhau (cung cấp bảo mật lẫn nhau; giảm bế tắc)

**Khả năng chấp nhận tâm lý**: các cơ chế bảo mật không nên can thiệp quá mức vào công việc của người dùng

* Một chiến lược tổng thể để cung cấp bảo mật

**- Chính sách (thông số kỹ thuật)**: những gì các chương trình bảo mật phải làm

• Tài sản và giá trị của chúng

• Các mối đe dọa tiềm ẩn

• Dễ sử dụng và bảo mật

• Chi phí bảo mật so với chi phí hỏng hóc / phục hồi

**- Cơ chế / thực thi**: cách thức thực thi

• Phòng ngừa

• Phát hiện

• Phản ứng

• Hồi phục

**Quan trọng cho thi giữa kỳ**

Dịch vụ bảo vệ đề cập đến các khái niệm bảo mật trái với các cơ chế bảo mật bao gồm tập hợp các mật mã các công cụ hữu ích để triển khai các dịch vụ bảo mật. **X.800** **tiêu chuẩn [X800] xác định các dịch vụ bảo mật.**

▪ Tính khả dụng: Thuộc tính có thể truy cập và sử dụng được theo yêu cầu của một thực thể được ủy quyền.

▪ Kiểm soát truy cập: Ngăn chặn việc sử dụng trái phép một tài nguyên, bao gồm cả việc ngăn chặn việc sử dụng tài nguyên trong một cách trái phép

▪ Tính toàn vẹn của dữ liệu: Thuộc tính mà dữ liệu chưa được bị thay đổi hoặc phá hủy theo cách trái phép.

▪ Xác thực Nguồn gốc Dữ liệu: Chứng thực rằng nguồn dữ liệu nhận được như được xác nhận quyền sở hữu

▪ Xác thực đối tượng ngang hàng: Chứng thực rằng một đối tượng ngang hàng thực thể trong hiệp hội là thực thể được tuyên bố

▪ Tính bảo mật: Tài sản mà thông tin không được tạo ra có sẵn hoặc tiết lộ cho các cá nhân, tổ chức trái phép hoặc các quy trình

▪ Phát hiện phát lại: Phát hiện phát lại bao gồm một thực thể để phát hiện rằng dữ liệu nhận được bị trùng lặp từ trao đổi

▪ Không từ chối: Để đảm bảo rằng ai đó không thể phủ nhận điều gì đó.

**Mật mã đối xứng và không đối xứng**

▪ Mật mã đối xứng: Giải mã và giải mã hệ thống biết cùng một khóa mật mã

▪ Mật mã không đối xứng (được gọi là khóa công khai mật mã) dựa trên hai khóa bổ sung - công khai và khóa riêng

**Chương 2: Mobile and Wireless Networks**

**Kỹ thuật**

**FDMA (Frequency Division Multiple Access)** (đa truy cập phân chia theo tần số) là sự phân chia băng tần được phân bổ cho liên lạc qua điện thoại di động không dây thành 30 kênh, mỗi kênh có thể thực hiện cuộc trò chuyện thoại hoặc, với dịch vụ kỹ thuật số, truyền dữ liệu kỹ thuật số

**TDMA (Time Division Multiple Access)** Đa truy cập phân chia theo thời gian là một phương pháp truy cập kênh cho các mạng chia sẻ phương tiện. Nó cho phép một số người dùng chia sẻ cùng một kênh tần số bằng cách chia tín hiệu thành các khe thời gian khác nhau. Người dùng truyền liên tiếp nhanh chóng, lần lượt từng người sử dụng khoảng thời gian riêng của mình.

**CDMA (Code Division Multiple Access)**  đa truy nhập (đa người dùng) phân chia theo mã.

**OFDM (Orthogonal Frequency Division Multiplexing)** là một trường hợp đặc biệt của phương pháp điều chế đa sóng mang, trong đó các sóng mang phụ trực giao với nhau, nhờ vậy phổ tính hiệu ở các sóng mang phụ cho phép chồng lấn lên nhau mà phía thu vẫn có thể khôi phục lại tín hiệu ban đầu.

**Kỹ thuật giao thông**

▪ Kỹ thuật lưu lượng lần đầu tiên được phát triển để thiết kế mạng chuyển mạch kênh điện thoại. Trong bối cảnh của mạng di động, điều cần thiết là phải biết và lập kế hoạch mở rộng mạng đang chặn các nút di động tối thiểu, có nghĩa là **chấp nhận tối đa giao tiếp.**

❖**Các yếu tố của hệ thống tế bào**: Một mạng di động nói chung là bao gồm những thứ sau:

- BS: nằm ở trung tâm của tế bào

- Trung tâm chuyển mạch di động (MTSO)

|  |  |  |  |
| --- | --- | --- | --- |
| **Mạng** | **Năm ra đời** | **Mb trung bình** | **Công dụng** |
| 1G | 1980 | 14.4 Kbps | Giọng nói analog |
| 2G | 1990 | 1Mbps | Giọng nói số, dv tin nhắn ngắn |
| 3G | 2000 | 1-8 Mbps | Dữ liệu thô sơ |
| 4G | 2010 | 15 Mbps | Video internet |
| 5G | 2020 | 1-10 Gbps | Video UHD, internet vạn vật |

|  |  |  |  |
| --- | --- | --- | --- |
| PAN | LAN | MAN | WAN |
| 802.15 | 802.11 | 802.16 | 802.20 |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 802.11 | Ngày ra đời | Dải tần(GHz) | Độ rộng kênh | Speed data Mbps | Số luồng accept | Điều chế | Phạm vi trong nhà | Phạm vi ngoài trời |
| wifi | 6-1997 | 2.4 | 20 | 2 | 1 | DSSS, FHSS | 20 | 100 |
| 802.11a | 9-1999 | 5 | 20 | 54 | 1 | OFDM | 35 | 120 |
| 802.11b | 9-1999 | 2.4 | 20 | 11 | 1 | DSSS | 38 | 140 |
| 802.11g | 6-2003 | 2.4 | 20 | 54 | 1 | OFDM. DSSS | 38 | 140 |
| 802.11n | 10-2009 | 2.4/5 | 20 | 72.2 | 4 | OFDM | 70 | 250 |
| 40 | 150 |
| 802.11ac | 12-2012 | 5 | 80/160 | 866 | 8 | OFDM |  |  |

Quá trình gọi bao gồm các chức năng sau:

1. Khởi tạo điện thoại di động

2. Cuộc gọi do một nút di động bắt đầu

3. Thông báo cuộc gọi

4. Chấp nhận cuộc gọi

5. Giao tiếp tích cực

6. Chặn cuộc gọi

7. Chấm dứt cuộc gọi

8. Bỏ cuộc gọi

9. Cuộc gọi giữa một thiết bị đầu cuối cố định và một nút di động

10. Bàn giao (Handoff)

|  |  |
| --- | --- |
| Applications | Port number |
| http | 80 |
| https | 443 |
| telnet | 992 |
| ftps | 990 |
| Ftps-data | 989 |

Bảng dưới đây liệt kê các ví dụ tiêu biểu của việc Protocol nào sử dụng port number nào.

|  |  |  |
| --- | --- | --- |
| **Số port** | **Từ khóa** | **Mô tả** |
| 20 | ftp-data | File Transfer [Default Data] |
| 21 | ftp | File Transfer [Control] |
| 22 | Ssh | SSH Remote Login Protocol |
| 23 | telnet | Telnet |
| 25 | Smtp | Simple Mail Transfer |
| 53 | Domain | Domain Name Server |
| 80 | www-http | World Wide Web HTTP |
| 110 | POP3 (non-secure) | Post Office Protocol – Version 3 |
| 995 | POP3 (secure) | Post Office Protocol Secure |
| 143 | IMAP (non-secure) | Internet Message Access Protocol |
| 993 | IMAP (secure) | Internet Message Access Protocol |
| 465 | Smtp (SSL) | Simple Mail Transfer with SSL |
| 587 | Smtp (TLS) | Simple Mail Transfer with TLS |
| 443 | https | HTTP Secure |

ÔN TẬP MẠNG GIỮA KỲ

**Chương III**

* Tài sản tư nhân
* Mọi người đều có quyền được bảo vệ về tinh thần và vật chất lợi ích từ bất kỳ khoa học, văn học hoặc nghệ thuật nào sản xuất mà anh ấy là tác giả.
* Định nghĩa về bảo mật
* Bảo mật trong thời đại kỹ thuật số như một nhiệm vụ bảo vệ kỹ thuật số tài sản và bảo vệ hệ thống xử lý các tài sản đó chống lại bất kỳ hành động nào không mong muốn hoặc được coi là lạm dụng bởi chủ sở hữu tương ứng.
* Tin tưởng và chủ quan trong bảo mật
* Hai khía cạnh luôn được nhắc đến trong vấn đề bảo mật là tin tưởng và chủ quan
* Vai trò của hệ thống viễn thông
* Hệ thống viễn thông là trung tâm của thời đại kỹ thuật số
* Các mạng (quang, có dây và không dây) chính là các thành phần của hệ thống viễn thông hiện đại. Các mạng này và người dùng của họ tiếp xúc với một số rủi ro. Chúng tôi phân loại những rủi ro này bằng cách sử dụng một mô hình phân biệt vai trò của chủ sở hữu dữ liệu và chủ sở hữu của cơ sở hạ tầng xử lý dữ liệu đó.
* Các mô hình mối đe dọa trong hệ thống viễn thông
* Mô hình mối đe dọa truyền thống đối với kênh giao tiếp dựa trên giao tiếp tối thiểu mô hình tối giản liên quan đến hai người tham gia được gọi là Alice và Bob, và một kênh giao tiếp
* A có thể tấn công một trong các bên giao tiếp sử dụng các lỗ hổng trong phần mềm và các biện pháp bảo vệ được sử dụng bởi người dung B
* A có thể tấn công liên kết kênh liên lạc B đến hệ thống viễn thông
* A có thể tấn công kênh tồn tại trong hệ thống viễn thông
* Sự xâm nhập vào cơ sở hạ tầng cho phép gắn kết "Man in the middle" tấn công.
* Từ lỗ hổng đường dây đến lỗ hổng trong truyền thông không dây
* Thay đổi phương tiện
* Thiết bị đầu cuối không dây
* Dịch vụ mới

**Chương IV**

* Kiến thức cơ bản về bảo mật
* Tính khả dụng: Thuộc tính có thể truy cập và sử dụng được theo yêu cầu của một thực thể được ủy quyền.
* Kiểm soát truy cập: Ngăn chặn việc sử dụng trái phép một tài nguyên, bao gồm cả việc ngăn chặn việc sử dụng tài nguyên trong một cách trái phép
* Tính toàn vẹn của dữ liệu: Thuộc tính mà dữ liệu chưa được bị thay đổi hoặc phá hủy theo cách trái phép. ▪
* Xác thực Nguồn gốc Dữ liệu: Chứng thực rằng nguồn dữ liệu nhận được như được xác nhận quyền sở hữu
* Xác thực đối tượng ngang hàng: Chứng thực rằng một đối tượng ngang hàng thực thể trong hiệp hội là thực thể được tuyên bố
* Tính bảo mật: Tài sản mà thông tin không được tạo ra có sẵn hoặc tiết lộ cho các cá nhân, tổ chức trái phép hoặc các quy trình
* Phát hiện phát lại: Phát hiện phát lại bao gồm một thực thể để phát hiện rằng dữ liệu nhận được bị trùng lặp từ trao đổi
* Không từ chối: Để đảm bảo rằng ai đó không thể phủ nhận điều gì đó.
* Mật mã đối xứng và không đối xứng
* Mật mã đối xứng: Giải mã và giải mã hệ thống biết cùng một khóa mật mã
* Mật mã không đối xứng (được gọi là khóa công khai mật mã) dựa trên hai khóa bổ sung - công khai và khóa riêng.
* Các thuật toán đối xứng nổi tiếng nhất với mật mã không đối xứng
  + DES (Data Encryption Standard)
  + 3DES
  + AES (Advanced Encryption Standard)
  + ECB (Electronic Code Book) mode
  + CBC (Cipher Block Chaining) mode
* Các thuật toán đối xứng nổi tiếng nhất với mật mã không đối xứng
  + RSA (Rivest, Shamir, Adleman)
* Sự bổ sung giữa hai hệ thống mật mã
* Các giao thức bảo mật sử dụng cả hai giao thức bảo mật, mỗi có cách sử dụng cụ thể:
  + Mật mã đối xứng giúp bảo vệ tốc bit độ cao dữ liệu được trao đổi qua mạng
  + Mật mã không đối xứng được sử dụng để khởi tạo một kết nối an toàn giữa hai thực thể của mạng bằng cách cho phép các thực thể đó xác thực lẫn nhau và thiết lập khóa đối xứng trong một cách bí mật.
* Hàm băm
* Các hàm băm nhằm mục đích đưa ra kết quả đại diện cho nội dung của tin nhắn trên một số byte giới hạn.
* Các thuộc tính được chờ đợi của các hàm băm này là sau:
  + một kết quả trên một số byte giới hạn (thường là 16 hoặc 20 byte)
  + Không có khả năng khôi phục tin nhắn ban đầu từ kết quả của hàm
  + Hai thông báo chỉ khác nhau 1 bit tạo ra hai kết quả khác nhau ít nhất nửa bit.
* Các hàm băm phổ biến
  + MD (Message Digest) functions MD2, MD4 and MD5
  + SHA-1, SHA-256, SHA-224 and SHA-512
* Cơ sở hạ tầng khóa online (PKI) và chứng chỉ điện tử
* PKI hỗ trợ cả khía cạnh tổ chức và kỹ thuật để thực hiện các chức năng sau: tạo khóa công khai / riêng tư, phân phối cho chủ sở hữu của họ (khi khởi tạo một thực thể mới trong PKI) và việc xuất bản, xác nhận và thu hồi các khóa công khai.
* Cơ chế xác thực
* Có thể được chia thành nhiều loại theo:
  + Những gì thực thể biết, một mật khẩu chẳng hạn
  + những gì thực thể sở hữu, chẳng hạn như thẻ thông minh, khóa cá nhân hoặc Vé Kerberos
  + thực thể là gì: danh mục này bao gồm xác thực kỹ thuật dựa trên các đặc điểm sinh trắc học của người dùng (vân tay, mống mắt, hình dạng khuôn mặt, hình dạng của bàn tay, v.v.)
  + những gì đơn vị được biết là phải làm: bằng cách thể hiện khả năng tái tạo hành động tương tự như chữ ký bằng văn bản, một thực thể có thể xác thực
* Xác thực yếu
  + Đối với xác thực yếu, một thực thể được xác thực chỉ với một phần xác thực (ví dụ: mật khẩu).
* Xác thực mạnh mẽ
  + Kế hoạch xác thực mạnh mẽ để kết hợp ít nhất hai các yếu tố xác thực, thường là mật khẩu và thẻ thông minh.
* Xác thực dựa trên mật khẩu
  + Mật khẩu tĩnh
  + Mật khẩu động
* Xác thực dựa trên chứng chỉ hoặc PKI
  + Loại xác thực này dựa trên sự bất đối xứng mật mã và làm cho nó cần thiết để quản lý khóa riêng của các thực thể và thường quản lý chứng chỉ điện tử thông qua PKI
* Xác thực dựa trên Kerberos
* Xác thực dựa trên thẻ thông minh
  + Loại xác thực này là kết quả trực tiếp của xác thực được thực hiện trong GSM thế hệ thứ hai (Hệ thống toàn cầu cho Mobile Communications) mạng di động dành cho người đăng ký có thẻ thông minh trong thiết bị di động của họ được cung cấp bởi nhà điều hành.
* Xác thực Biometry
  + Xác thực của người dùng có thể dựa vào một hoặc nhiều các tính năng sinh trắc học được gọi là "phương thức sinh trắc học". Nhiều nhất các phương thức phổ biến là dấu vân tay, mống mắt, khuôn mặt, giọng nói hoặc chữ ký viết tay.
* Xác thực
* Các giao thức AAA để kiểm soát quyền truy cập vào một mạng hoặc mạng của một nhà điều hành
* RADIUS và Diameternet
* Kiểm soát truy cập
* Tường lửa:
  + Tường lửa xuất hiện vào cuối những năm 1980. Ban đầu của họ mục tiêu là tách các mạng để bảo vệ máy tính từ những kẻ tấn công.
  + Nhiệm vụ chính của tường lửa là kiểm soát giao tiếp giữa các mạng với độ tin cậy khác nhau để ngăn chặn các cuộc tấn công xảy ra.
* Hai đặc điểm chung thường được mong đợi từ một bức tường lửa:
  + Nó phải liêm khiết
  + Nó phải kiểm soát tất cả các thông tin liên lạc
* Một phân loại cho tường lửa
  + Cấp độ giao thức của phân tích được thực hiện bởi bức tường lửa:
    - Ở cấp độ mạng
    - Ở cấp độ mạch
    - Ở cấp độ ứng dụng
  + Vị trí.
    - Tường lửa mạng được đặt trong một mạng
    - Tường lửa cá nhân được gắn với hệ thống cuối
* Tính minh bạch.
  + Một chính sách trong đó chỉ các đơn vị dữ liệu được coi là két an toàn được phép vượt qua vành đai an ninh.
  + Một chính sách trong đó chỉ các đơn vị dữ liệu được coi là độc hại bị chặn.