**CHƯƠNG 1 – TỔNG QUAN BẢO MẬT MÁY TÍNH**

**I. Bảo mật máy tính**

- Là bảo vệ hệ thống thông tin tự động.

- Đảm bảo **3 yếu tố**:

+ **Confidentiality** : tính **bí mật** (bảo vệ hệ thống không bị lộ ra ngoài)

+ **Integrity** : tính **toàn vẹn** (toàn vẹn dữ liệu)

+ **Availability** : tính **sẵn sàng** (có thể thao tác, yêu cầu bất cứ lúc nào)

- Bao gồm phần cứng, phần mềm, thông tin, dữ liệu.

**II. Bộ ba CIA**

1. Confidentiality (Bí mật)

- ***Bí mật dữ liệu***: đảm bảo **thông tin bí mậ**t, **không** được **tiết lộ** và **cung cấp** cho những ai **không có quyền**.

- ***Quyền riêng tư***: **đảm bảo** cá nhân **kiểm soát hoạt động** và **thông tin** (tiết lộ khi **chủ sở hữu cấp quyền cho phép**)

1. Integrity (Toàn vẹn)

- ***Toàn vẹn dữ liệu:*** đảm bảo thông tin và chương trình **chỉ được thay đổi** theo **chỉ định** và **cho phép** theo quy định, dưới sự **ủy quyền của nhà quản lý**.

- ***Toàn vẹn hệ thống***: đảm bảo hệ thống được **thực hiện theo dự định**, **an toàn**, **không lỗi**, dưới sự **kiểm soát của chủ sở hữu**.

1. Availability (Sẵn sàng)

- Đảm bảo hoạt động **trơn tru, kịp thời**.

- Dịch vụ **không được từ chối người dùng**.

**III. Khái niệm bảo mật chính (CIA). Một số yêu cầu khác:**

1. **Authenticity : chứng thực**

- **Thông tin** **người nhận** phải được gửi đi từ **người gửi hợp pháp** (**đúng người**)

- Đảm bảo **4 yếu tố**:

+ Thông tin nguyên vẹn

+ Người gửi hợp pháp

+ Không bị tác động bởi yếu tố khác

+ Được xác thực rõ ràng và đáng tin

1. **Accountability : trách nhiệm giải trình**

- Yêu cầu hoạt động **CHỐNG TỪ CHỐI (non-repudiation**) => Chống việc từ chối các hành động (chống thoái hóa)

VD: ngân hàng không có quyền từ chối khi khách hàng yêu cầu sao kê.

**IV. Mức độ ảnh hưởng vi phạm bảo mật**

1. **Thấp (Low)**

- Tác động hạn chế

- Thiệt hại nhỏ, tổn thất ít, giảm uy tín tổ chức

1. **Trung bình (Moderate)**

- Ảnh hưởng nghiêm trọng

- Gây tổn hại cá nhân, thiệt hại, giảm yếu tố của các tổ chức

1. **Cao (High)**

- Gây hậu quả rất nghiêm trọng đối với tổ chức, cá nhân

VD: gây phá sản, tổ chức bị ảnh hưởng nghiêm trọng, thậm chí là tính mạng (đối với hồ sơ bệnh án, y tế,…)

**V. Ví dụ về yêu cầu bảo mật**

1. **Tính bí mật**

- Y tế: hồ sơ bệnh án bệnh nhận không được tự ý thay đổi bởi những người không có quyền.

- Giáo dục: chỉ có những người có quyền mới được xem, sửa những tài liệu bảo mật, riêng tư (điểm, thông tin,…)

1. **Tính toàn vẹn**

- Có chức năng restored để xem lại những tài liệu cũ.

1. **Tính sẵn sàng**

- Không được delay quá lâu

=> Nguy hiểm

=> Có thể ảnh hưởng nghiêm trọng trong một số trường hợp cấp bách.

**VI. Những thử thách với bảo mật (10 thử thách)**

1. **Không đơn giản**

\*\* *- Với những người mới, việc thực hiện không dễ dàng*

- Có những vấn đề cần phải yêu cầu những người có chuyên môn về một lĩnh vực nào đó.

\*\* *- Các yêu cầu đơn giản nhưng cơ chế để đáp ứng được yêu cầu thì phức tạp*

- Phải update việc bảo mật liên tục để phù hợp với biến động cuộc sống.

1. **Phải xem xét những cuộc tấn công bất ngờ**

- Tuy đã lên kế hoạch trong những trường hợp nhưng sẽ không tránh khỏi những tình huống bất ngờ.

=> Phải update kế hoạch liên tục

1. **Thủ tục được sử dụng thường phải trực quan**

- Không thể hình dung virus tấn công hoạt động như thế nào

VD: mất file trong máy tính,..

1. **Quyết định nơi triển khai**

- Cần phải xác định xây dựng hệ thống như thế nào, đặt ở đâu để hợp lý, phù hợp với từng trường hợp. (chi phí, tổ chức, cá nhân,…)

=> Đảm bảo tính an toàn, lợi thế cạnh tranh giá thành,…

1. **Thuật toán và thông tin bí mật (keys)**

- Thuật toán bảo mật phức tạp, khó hiểu.

- Các thông tin, khóa bí mật (đối xứng (chung khóa) >< bất đối xứng (2 khóa))

VD: khóa ngắn => dễ nhớ => dễ bị suy đoán

Khóa dài nhiều ký tự => khó nhớ => bảo đảm an toàn cao => khó khăn cho người dùng

* Biện pháp: dùng thể thông minh lưu trữ, sinh trắc học (vân tay, khuôn mặt, bóng mắt, mạch máu dưới mu bàn tay,…)

1. **Trận chiến đấu trí giữa kẻ tấn công và admin**

- Thủ phạm cố gắng tìm ra lỗ hỏng và admin cố gắng đóng lỗ hỏng lại.

1. **Không được nhìn nhận về lợi ích cho đến khi thất bại (Thuyết phục người dùng)**

- Chưa bị tấn công, mất dữ liệu thì không nhìn thấy được lợi ích của bảo mật.

- Người dùng cảm thấy khó chịu khi gặp những cảnh báo bảo mật.

1. **Yêu cầu giám sát liên tục**

- Không thể biết được hacker tấn công khi nào, phải túc trực 24/24

VD: đối với những thiết bị xách tay, cần mang theo thiết bị phần cứng để bảo vệ khi di chuyển. => Khó khăn trong môi trường ngắn hạn (di chuyển)

1. **Qúa thường xuyên là một suy nghĩ sau (giống ý 7)**

- Việc bảo mật luôn được xây dựng sau khi hệ thống hoàn thành.

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

* Gây khó chịu cho người dùng.
* Chiếm tài nguyên máy tính khiến hệ thống chậm

**VII. Mô hình cho bảo mật máy tính**

1. **Tài nguyên hệ thống**

- Phần cứng, phần mềm, dữ liệu (thông tin, hệ thống, CSDL), trao đổi thông tin, mạng LAN, bridges, router,…

=> Bảo vệ các thiết bị này

1. **Mối quan tâm**

- Tính dễ bị tổn thương của tài nguyên: hỏng, không khả dụng, rò rĩ,..

1. **Mối đe dọa khai thác các lỗ hỏng**
2. **Các tấn công hiểm nguy luôn tồn tại và tiềm ẩn**

- Chủ động hoặc bị động, bên trong hoặc bên ngoài.

1. **Các biện pháp đối phó**: ngăn ngừa, phát hiện, phục hồi và giảm thiểu rủi ro.

**VIII. Ngôn ngữ liên quan đến bảo mật**

1. **Adversary (threat agent): kẻ thù/ tác nhân đe dọa**
2. **Attack: tấn công vào an ninh mạng** (cố tình trốn tránh an ninh, chính sách bảo mật).
3. **Countermeasure: biện pháp đối phó** (hđ/thiết bị/quy trình/kỹ thuật làm giảm mối đe dọa/lỗ hỏng/cuộc tấn công bằng cách loại bỏ/ngăn chặn/giảm thiểu tác hại gây ra hoặc phát hiện/bảo vệ hđ có thể được thực hiện)
4. **Risk: rủi ro** (tổn thất/xác suất mà 1 mối đe dọa/lỗ hỏng nào đó đem lại)
5. **\*\* *Security Policy: chích sách bảo mật*** *(tập hợp quy tắc, thông lệ chỉ định/điều chỉnh cách hệ thống/tổ chức cung cấp dịch vụ bảo mật để bảo vệ các tài nguyên nhạy cảm/quan trọng)*
6. **System Resource (Asset): Tài nguyên hệ thống** (dl chứa trong HTTT/dịch vụ được cung cấp bởi hệ thống hoặc khả năng hệ thống như công suất xử lý, băng thông…)
7. **Threat: mối đe dọa** (khả năng vi phạm bảo mật tồn tại khi có các tình huống khả năng/hđ/sự kiện có thể vi phạm an ninh/gây hại, mối nguy hiểm khai thác lỗ hỏng)
8. **Vulnerability: tính dễ bị tổn thương** (lỗ hỏng/điểm yếu trong thiết kế/triển khai/vận hành/quản lý của ht có thể bị lợi dụng để vi phạm chính sách bảo mật hệ thống.

**IX. Mối quan hệ bảo mật**

- **Chủ sở hữu (owners)** luôn có những **tài nguyên/bí mật (assets)** cần được bảo vệ => Mong muốn **rủi ro** **(risks)** ít nhất => Áp đặt **biện pháp đối phó (countermeasure)** => Giảm **rủi ro (risks)**

**- Mối đe dọa (threat agent)** => Lạm dụng/gây thiệt hại đến **tài nguyên (assets)**

=> Tăng **mối đe dọa (threats)** => Tăng **rủi ro (risks)**

**X. Một số kiểu tấn công**

- **Chủ động**: cố gắng **thay đổi tài nguyên hệ thống** hoặc **ảnh hưởng** đến các tổ chức

- **Bị động:** cố gắng **tìm hiểu hoặc sử dụng HTTT** từ hệ thống **không ảnh hưởng** đến tài nguyên hệ thống (âm thầm ăn trộm, lưu vào CSDL khác)

VD: ngân hàng khi giao dịch online

- Dựa vào nguồn gốc cuộc tấn công: 2 loại

+ **Bên trong**: được khởi xướng từ bên trong vòng bảo mật, có thể là người trong hệ thống hoặc hacker vào hệ thống rồi tấn công (nội bộ)

+ **Bên ngoài (phổ biến)**

**XI. Hậu quả các mối đe dọa**

Bốn mối đe doạ

1. **Tiết lộ trái phép (Unauthorized Disclosure):** mối đe dọa với **tính bí mật**
2. **Deception (Lừa đảo):** mối đe dọa với **tính toàn vẹn** hệ thống/dữ liệu
3. **Discruption (Gián đoạn):** mối đe dọa với **tính sẵn sàng/tính toàn vẹn**
4. **Usurpation (Chiếm đoạt):** mối đe dọa với **tính toàn vẹn.**

**XII. Chiến lược tổng thể bảo mật**

1. **Chính sách**

- Tài nguyên và giá trị

- Mối đe dọa tiềm ẩn

- Chi phí bảo mật và sử dụng

- Chi phí tổn hại

1. **Quá trình thực hiện cơ chế**

- Phòng ngừa

- Phát hiện

- Phản ứng

- Phục hồi

1. **Tính đúng đắn**

- Đảm bảo thật sự hệ thống hoạt động đúng yêu cầu đưa ra.

**AN NINH MẠNG KHÔNG DÂY VÀ DI ĐỘNG**

**I. Tài sản cá nhân từ các lỗ hỏng đến rủi ro**

- Mọi người đều có quyền được bảo vệ về tinh thần và vật chất thu được từ bất kì sản phẩm khoa học, văn học hoặc nghệ thuật.

**II. Khái niệm liên quan đến bảo mật**

1. **Khái niệm bảo mật**

- Là trạng thái hiện hữu an toàn

- Sự an toàn của một trạng thái hoặc tổ chức chống lại tội phạm khủng bố và tổ chức gián điệp.

- Một thực thể được ký gửi hoặc cầm cố như một sự đảm bảo cho việc thực hiện cam kết hoặc việc hoàn trả một khoản vay sẽ bị tước bỏ trong trường hợp vỡ nợ

- Chứng chỉ chứng thực tín dụng, quyền sở hữu cổ phiếu hoặc trái phiếu

1. **Bảo mật**

- Thường được coi là nghệ thuật chia sẻ bí mật

- Bảo mật trong thời đại KTS như một nhiệm vụ bảo vệ các tài sản kỹ thuật số và bảo vệ các hệ thống xử lý tài sản đó chống lại bất kỳ hành động nào không mong muốn hoặc được các chủ sở hữu tương ứng coi là lạm dụng.

**III. Threat models**

- Mô hình của mối đe dọa sẽ giới thiệu kẻ tấn công trong hệ thống và thể hiện các năng lực của kẻ tấn công, tức là các vị trí của các cấu trúc liên quan trong tài nguyên để truy cập vào hệ thống.

- Mô hình mối đe dọa truyền thống đối với một kênh liên lạc dựa trên mô hình giao tiếp tối thiểu, tối giản liên quan đến hai người tham gia được gọi là Alice và Bob, và một kênh liên lạc.

- Mô hình này có các hình thức tấn công:

+ Trực tiếp vào các thiết bị của người dùng mà không cần nhà mạng.

* + Tấn công vào nhà mạng như là tìm ra các lỗ hổng của nhà mạng, giả mạo các thiết bị của nhà mạng.

**IV. Từ lỗ hổng trên đường dây hữu tuyến đến lỗ hổng trong truyền thông không dây**

1. **Thay đổi phương tiện (Changing a medium)**

**-** Phương tiện không dây, theo nghĩa truyền phát sóng vô tuyến, về bản chất rất dễ bị tổn thương, dễ bị tổn thương hơn nhiều so với phương tiện có dây.

1. **Thiết bị đầu cuối không dây (Wireless terminals)**

- Các thiết bị đầu cuối được sử dụng trong mạng không dây được đặc trưng bởi tính di động của chúng. Chúng nhỏ, thường được trang bị giao diện người-máy hạn chế (HMI – Human machine interface), hạn chế về sức mạnh xử lý và lưu trữ và được cung cấp bởi pin.

1. **Dịch vụ mới**

- Việc cung cấp các dịch vụ mới là nguy hiểm. Việc bổ sung các dịch vụ này sẽ thay đổi phần chức năng của IS và phải được theo sau bởi một đánh giá rủi ro mới, có tính đến các dịch vụ đã cung cấp trước đó, tác động của những thay đổi đối với các dịch vụ này và mức độ bảo mật mong muốn cho các dịch vụ mới.

**CHƯƠNG 4 - WIRELESS AND MOBILE**

**NETWORK SECURITY**

**(AN NINH MẠNG KHÔNG DÂY VÀ DI ĐỘNG)**

**2. Khái niệm cơ bản về an ninh (Security)**

**2.1 Dịch vụ bảo mật:**

Gồm tập hợp các công cụ mật mã hữu ích để triển khai các dịch vụ bảo mật như là tiêu chuẩn X.800.

Một dịch vụ bảo mật chính là một dịch vụ được cung cấp bởi 1 lớp giao thức hay là các giao tiếp, các hệ thống mới đảm bảo sự bảo mật thích hợp với các hệ thống hoặc là cho việc truyền tải dữ liệu 1 cách an toàn.

**2.2 Phân loại khái quát:**

**Tính sẵn sàng**: Tài nguyên có thể tiếp cận và sử dụng được theo yêu cầu của một tổ chức được ủy quyền.

**Kiểm soát truy cập**: Ngăn chặn được sử dụng trái phép tài nguyên bao gồm cả việc ngăn chặn việc sử dụng trái phép tài nguyên.

**Tính toàn vẹn dữ liệu**: Dữ liệu nhân được không bị thay đổi hoặc phá hủy theo cách trái phép. (Hàm băm: xác thực tính toàn vẹn dữ liệu).

**Xác thực nguồn gốc dữ liệu**: Đảm bảo dữ liệu nhận được là chính xác từ người gửi hợp lệ. ( Dữ liệu không bị sửa đổi lại từ bất cứ nguồn nào).

**Xác thực ngang hàng**: Chứng thực rằng một thực thể ngang hàng trong một liên kết là một thực thể đã được xác nhận. (Real partner)

**Tính bí mật**: Đảm bảo các thông tin tài khoản không được cung cấp hoặc tiết lộ cho cá nhân hay thực thể hoặc quy trình trái phép.

**Phát hiện phát lại**: Bao gồm một thực thể để phát hiện rằng dữ liệu nhận được bị trùng lặp từ lần trao đổi trước đó. Một số dữ liệu có thể được gửi một cách an toàn bởi một thực thể hợp pháp nhưng chúng có thể bị sao chép và đưa lại vào cùng một mục đích.(Cần phải phát hiện để tránh dữ liệu bị xử lý nhiều lần).

**Không chối cãi**: Đảm bảo bảo vệ khỏi sự phủ nhận của một bên truyền tin ( Giống chữ ký điện tử).

**2.3 Các kỹ thuật mật mã:**

**Mật mã đối xứng** : Hệ thống tạo ra và giải mã sử dụng chung một kháo bí mật (Secure Key)

**Mật mã bất đối xứng (Mã khóa công khai):** Mã hóa dữ liệu sử dụng 1 cặp khóa (pucblic key - private key)

Trong một hệ thống hay kết hợp 2 bộ mã. Xác thực tính an toàn ( mã bất đối xứng), để dữ liệu truyền tải từ A và B ( mã đối xứng). Dữ liệu nhỏ không quan tâm tới tốc độ ( Mã bất đối xứng)

**Mật mã đối xứng:** Khi dùng chung 1 khóa này quá trình tạo và giải mã nhanh hơn. Hay dùng để mã hóa dữ liệu.

Một số các hệ mật mã:

**DES (Data Encryption Standard):** Tiêu chuẩn mã hóa dữ liệu. (Phát minh vào năm **1977** tên là thuật toán mã khóa khóa công khai với khóa bí mật ban đầu là 56 bit, đầu vào là các khối dữ liệu 64 bit).

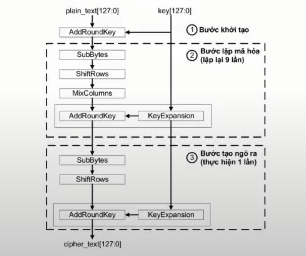
**3DES(Triple DES):** Mạnh mẽ hơn sự kế thừa của DES. **Khóa của 3DES tối đa là 168 bit và áp dụng cho cùng kích thược khối đầu vào là 64 bit).**

**AES (Advanced Encryption Standard):** Tiêu chuẩn mã hóa nâng cao. Đầu vào của các khối là 128 bit**.** Độ dài khóa là 128 , 192 hoặc là 256 bit tùy thuộc vào nhu cầu sử dụng**.** Độ dài càng dài độ an toàn càng cao. Thực hiện qua 5 qua trình chính: AddRoundKey, SubBytes, ShiftRows, MixColumns, AddRoundKey.

**Bước khời tạo: Dữ liệu (plan\_text) kết hợp với khóa bằng chức năng AddRoundKey.**

Bước 2: Lặp mã hóa và kết quả của bước 1 được sử dụng thuật hiện tuần tự các chức năng **SubBytes, ShiftRows, MixColumns, AddRoundKey** **(Thực hiện 9 lần).** Key Expension thực hiện song song với các chức năng.

Bước 3: Bước tạo ngỏ ra ( Thực hiện 1 lần) Kết quả bước 2 thực hiện tuần tự các chức năng **SubBytes, ShiftRows,AddRoundKey** để tạo ngỏ ra.



**ECB (Electonic Code Book):** Dữ liệu được phân thành các khối khác nhau.

**CBC (Cipher Block Chaining)**: Cùng khối đầu vào nhưng đầu ra khác nhau.

**Mã hóa bất đối xứng:**

**RSA (Rivest, Shamir, Adleman)**

**2.4 Sự bổ sung giữa 2 hệ thống mật mã:**

Hệ thống mật mã đối xứng: Giúp cho việc bảo vệ dữ liệu tốc độ bit cao được trao đổi qua mạng.

Hệ thống mật mã bất đối xứng: Khởi tạo các kết nối an toàn giữa 2 thực thể của mạng bằng cách cho phép các thực thể đó xác thực lẫn nhau và thiết lập khóa đối xứng 1 cách bí mật.

**2.5 Hàm băm:** (Là hàm 1 chiều)

Nhằm mục đích cung cấp kết quả đại diện cho nội dung thư trong 1 số byte nhất định (gần giống CRC)

**Thuộc tính chờ đợi của hàm băm:**

Kết quả đầu ra thường là các số giới hạn của byte (16 hoặc 20 byte)

Không có khả năng khôi phục dữ liệu gốc từ giá trị của hàm băm**.**

Hai tin nhắn chỉ khác nhau 1 bit sẽ tạo ra 2 kết quả khác nhau ít nhất nửa bit. (Đầu vào khác nhau đầu ra khác nhau)

Ứng dụng: Đảm bảo dữ liệu gửi đi không bị sửa đổi.

**Người gửi gửi giá trị hàm băm và dữ liệu cho người nhận. Người nhận nhận được dữ liệu sẽ giải nén dữ liệu cho chạy qua hàm băm nếu kết quả hàm băm = kết quả hàm băm thực hiện lại. (Tin tưởng được dữ liệu truyền đến đầy đủ)**

**Một số hàm băm:**

**MD (Message Digest): MD2, MD4 và MD5**

**SHA-1,SHA-256,SHA-224 và SHA-512**: Plantxet đưa vào đều cho ra số byte cố định. (Đầu ra)

**SHA-1 (trả lại kết quả dài 160 bit) (1 Byte = 8 bit)**

**SHA-224 (trả lại kết quả dài 224 bit)**

**SHA-256 (trả lại kết quả dài 256 bit)**

**SHA-384 (trả lại kết quả dài 384 bit)**

**SHA-512 (trả lại kết quả dài 512 bit)**

VD: SHA-1 => Đoạn mã có độ dài 20 Byte

**2.6 Cơ sở hạ tầng khóa công khai (PKI): (Đơn vị thứ 3 đảm bảo chứng thực)**

Nhiều tiêu chuẩn như là tiêu chuẩn SSL, TLL, TLS hoặc là IP Set,.. Chủ yếu dựa trên việc sử dụng khóa công khai để tạo trao đổi an toàn thông diệp điện tử , giao dịch điện tử và kết nối từ xa.

Mắc phải 1 vấn đề bảo mật cơ bản làm thế nào để tin tưởng 1 hiệp hội liên qua đến khóa công khai với chủ sở hữu của nó ràng buộc này đặc biệt quan trọng để xác thực các thực thế như là người dùng, máy chủ. Để đảm bảo tính bí mật và toàn vẹn của các trao đổi điều cần thiết là điều chỉnh quản lý các khóa công khai nhờ vào tổ chức là cơ sở hạ tầng khóa công khai.

Hỗ trợ khía cạnh tổ chức và kỹ thuật để thực hiện các chức năng tạo khóa công khai và khóa riêng tư phân phối chúng cho chủ sở hữu của chúng.

|  |  |  |  |
| --- | --- | --- | --- |
| **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 |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |  |  |

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