Tổng quan

Đầu tiên, chúng ta sẽ tìm hiểu về tam giác CIA nó ko phải là tên viết tắt của tổ chức tinh báo Mỹ :v. Nó là Confidentiality( bí mật), Integrity(toàn vẹn) and Availability(sẵn sàng).

Confidentiality (bí mật): dữ liệu cần được bí mật và riêng tư, nếu bạn không phải là chủ sở hữu bạn sẽ không xem được nó.

Integrity(toàn vẹn): dữ liệu chỉ được thay đổi bởi tác giả, trong quá trình truyền dữ liệu không được thêm vào hay xóa đi.

Availability(sẵn sàng): khi người dùng yêu cầu dữ liệu phải được đáp ứng.

Ví dụ bạn đặt password kết hợp chữ, số,ký tự đặt biệt nó sẽ tăng tính bảo mật nhưng bạn sẽ rất khó để nhớ vì vậy khi cần sử dụng bạn sẽ rất khó khăn.

Authenticity(xác thực): xác thực người dùng và xác thực đầu vào là đáng tin cậy.

Accountability (trách nhiệm): các hành động của thực thể sẽ được truy tìm khi cần thiết và khi đó kết quả là thực thể duy nhất.

Có 2 dạng tấn công:

Passive(bị động): thu thập thông tin về hệ thống nhưng không ảnh hưởng đến tài nguyên hệ thống. 2 loại thường gặp trong dạng này là: lấy cắp nội dung các tin nhắn và phân tích lưu lượng truy cập. dạng này phòng là chính.

Active(chủ động): thay đổi tài nguyên hệ thống hoặc ảnh hưởng đến hoạt động của nó. Các loại thường gặp của dạng này: (Masquerade) giả danh, (Replay)gửi lại gói tin, (Modification of mesages)thay đổi nội dung tin nhắn, (Denial of service) từ chối dịch vụ. dạng này cần phải phát hiện xâm nhập và khôi phục lại hệ thống.

Security Services (X.800)

Authentication( Xác thực): đảm bảo rằng thực thể đang giao tiếp là một điều chính xác. Trong trường hợp 1 tin nhắn duy nhất, đảm bảo rằng tin nhắn đó từ một nguồn xác thực. Trong trường hợp tương tác liên tục, đảm bảo rằng 2 thực thể là xác thực và trong kết nối không có sự can thiệp của bên thứ ba, người có thể giả mạo một trong 2 bên giao tiếp.

Access Control( kiểm soát truy cập): ngăn ngừa việc sử dụng tài nguyên trái phép. Có khả năng hạn chế và kiểm soát truy cập vào hệ thống máy chủ và ứng dụng bằng các liên kết thông tin. Vì vậy, quyển truy cập phải được xác định và xác thực, phân quyền cho cá nhân.

Data Confidentiality( Bí mật dữ liệu): bảo vệ dữ liệu không bị tiết lộ trái phép.Bảo vệ truyền dữ liệu khỏi kiểu tấn công thụ động: dịch vụ rộng bảo vệ tất cả dữ liệu truyền giữa 2 user trong 1 khoảng thời gian; dạng hẹp là bảo vệ một tin nhắn đơn hoặc 1 trường cụ thể trong tin nhắn.

Data Integrity( toàn vẹn dữ liệu): đảm bảo rằng dữ liệu nhận được là được gửi một thực thể có thẩm quyền. Áp dụng cho 1 dòng tin nhắn, 1 tin nhắn đơn, hoặc trường được chọn trong tin nhắn. Đảm bảo rằng tin nhắn được nhận không bị trùng lặp, thêm, thay đổi, sắp xếp lại, replay.

Non-Repudiation(chống chối bỏ): bảo vệ chống việc chối bỏ trong giao tiếp. Khi một thông điệp được gửi, người nhận có thể chứng minh rằng người gửi bị cáo buộc trên thực tế đã gửi tin nhắn. Khi nhận tin nhắn, người gửi có thể chứng minh rằng người nhận cáo buộc trên thực tế nhận được tin nhắn

Availability(sẵn sàng): tài nguyên có thể truy cập/ sử dụng.