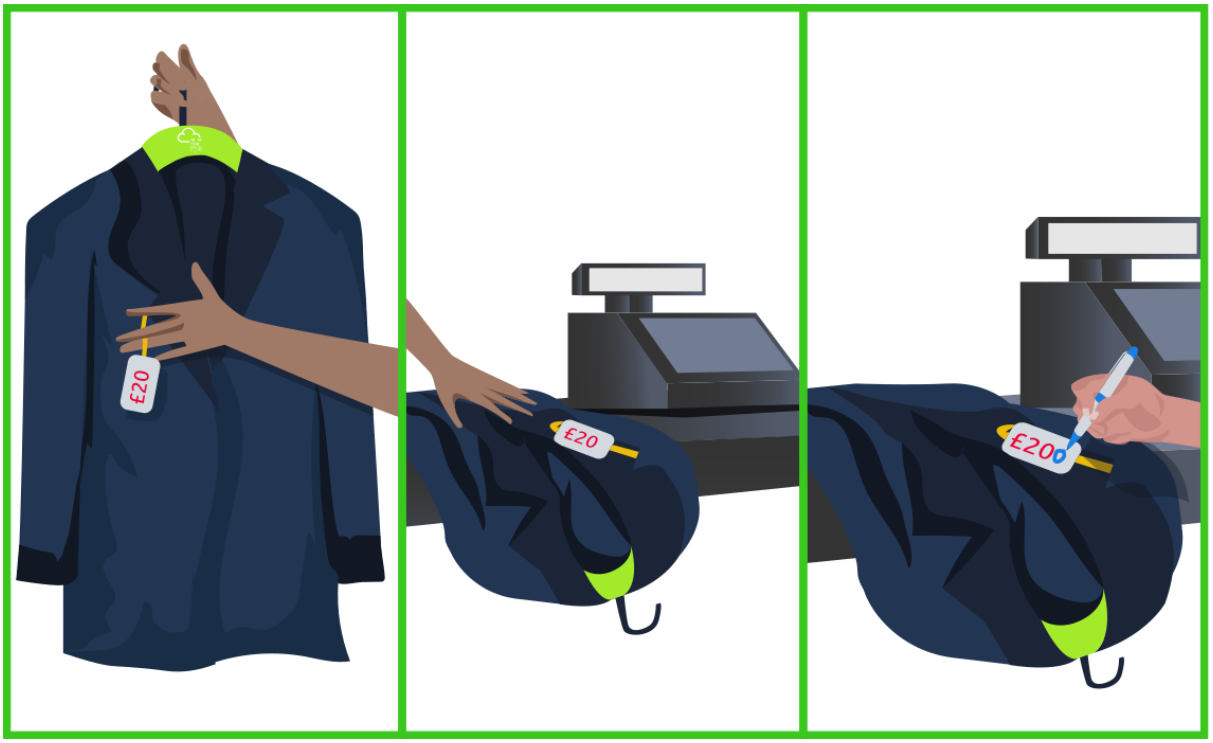
Security Principles

I. CIA

Trước khi chúng ta có thể miêu tả một cái gì đó là an toàn, chúng ta cần xem xét kỹ hơn về những gì tạo nên an ninh. Khi bạn muốn đánh giá tính bảo mật của một hệ thống, bạn cần suy nghĩ dựa trên tam giác bảo mật: bảo mật thông tin, tính toàn vẹn và tính khả dụng (CIA).

Bảo mật thông tin đảm bảo rằng chỉ những người hoặc đối tượng dự định mới có thể truy cập vào dữ liệu.
Tính toàn vẹn nhằm đảm bảo rằng dữ liệu không thể bị thay đổi; hơn nữa, chúng ta có thể phát hiện bất kỳ sự thay đổi nào nếu có.
Tính khả dụng nhằm đảm bảo rằng hệ thống hoặc dịch vụ có sẵn khi cần thiết.
Một người bán có biên lai, thêm một số 0 vào giá của một mặt hàng sau khi người mua chọn nó, từ đó nhân giá lên mười lần.



Hãy xem xét tam giác CIA trong trường hợp đặt hàng mua sắm trực tuyến:

Bảo mật thông tin: Trong quá trình mua sắm trực tuyến, bạn mong đợi số thẻ tín dụng của mình chỉ được tiết lộ cho đơn vị xử lý thanh toán. Nếu bạn nghi ngờ rằng thông tin thẻ tín dụng của mình sẽ được tiết lộ cho một bên không đáng tin cậy, bạn rất có thể không tiếp tục giao dịch. Hơn nữa, nếu xảy ra việc vi phạm dữ liệu dẫn đến tiết lộ thông tin cá nhân, bao gồm thẻ tín dụng, công ty sẽ gánh chịu tổn thất lớn ở nhiều mức độ.
Tính toàn vẹn: Sau khi điền thông tin đặt hàng, nếu một kẻ xâm nhập có thể thay đổi địa chỉ giao hàng mà bạn đã gửi, gói hàng sẽ được gửi cho người khác. Nếu không đảm bảo tính toàn vẹn dữ liệu, bạn có thể rất ngại để đặt hàng với người bán này.
Tính khả dụng: Để đặt đơn hàng trực tuyến, bạn sẽ duyệt trang web của cửa hàng hoặc sử dụng ứng dụng chính thức của nó. Nếu dịch vụ không khả dụng, bạn sẽ không thể duyệt qua sản phẩm hoặc đặt đơn hàng. Nếu bạn tiếp tục gặp các vấn đề kỹ thuật như vậy, bạn có thể cuối cùng bỏ cuộc và tìm một cửa hàng trực tuyến khác.

Hãy xem xét tam giác CIA liên quan đến hồ sơ bệnh nhân và các hệ thống liên quan:

Bảo mật thông tin: Theo các luật pháp ở các nước hiện đại, nhà cung cấp dịch vụ chăm sóc sức khỏe phải đảm bảo và duy trì tính bảo mật hồ sơ y tế. Do đó, nhà cung cấp dịch vụ chăm sóc sức khỏe có thể chịu trách nhiệm pháp lý nếu tiết lộ trái pháp luật tiết lộ trái phép hồ sơ y tế của bệnh nhân.
Tính toàn vẹn: Nếu một hồ sơ bệnh nhân bị thay đổi một cách ngẫu nhiên hoặc cố

ý, có thể dẫn đến việc áp dụng điều trị sai, điều này có thể gây ra tình huống đe dọa tính mạng. Do đó, hệ thống sẽ trở nên vô dụng và có thể gây hại nếu không đảm bảo tính toàn vẹn của hồ sơ y tế.
Tính khả dụng: Khi một bệnh nhân đến một phòng khám để theo dõi tình trạng sức khỏe của mình, hệ thống phải sẵn sàng. Một hệ thống không khả dụng sẽ có nghĩa là nhà cung cấp dịch vụ y tế không thể truy cập vào hồ sơ bệnh nhân và do đó sẽ không biết liệu các triệu chứng hiện tại có liên quan đến lịch sử y tế của bệnh nhân hay không. Tình huống này có thể làm cho quá trình chẩn đoán y tế phức tạp hơn và dễ mắc lỗi hơn.

Nhấn mạnh không cần phải như nhau trên cả ba chức năng bảo mật. Một ví dụ là thông báo của một trường đại học; mặc dù thông tin này thường không được bảo mật, tính toàn vẹn của tài liệu là quan trọng.

Vượt xa hơn CIA

Một người giao hàng với một số lượng lớn hộp pizza và một người đứng ở cửa nói: "Tôi không đặt hàng đó."

Đi một bước xa hơn tam giác bảo mật CIA, chúng ta có thể nghĩ đến:

Tính xác thực: Xác thực có nghĩa là không giả mạo hoặc là hàng giả. Tính xác thực liên quan đến việc đảm bảo rằng tài liệu/tệp tin/dữ liệu đến từ nguồn được tuyên bố.
Tính không thể chối bỏ: Chối bỏ có nghĩa là từ chối công nhận tính hợp lệ của một

cái gì đó. Tính không thể chối bỏ đảm bảo rằng nguồn gốc ban đầu không thể chối bỏ rằng họ là nguồn của một tài liệu/tệp tin/dữ liệu cụ thể. Đặc tính này là không thể thiếu đối với nhiều lĩnh vực, chẳng hạn như mua sắm, chẩn đoán bệnh nhân và ngân hàng.

Hai yêu cầu này có mối liên hệ chặt chẽ. Việc phải phân biệt giữa tệp tin/thứ tự thật và giả là không thể thiếu. Hơn nữa, đảm bảo rằng bên kia không thể chối bỏ việc là nguồn gốc là quan trọng đối với nhiều hệ thống để có thể sử dụng.

Trong mua sắm trực tuyến, tùy thuộc vào doanh nghiệp của bạn, bạn có thể chấp nhận việc cố gắng giao một chiếc áo phông kèm theo thanh toán khi nhận hàng và sau đó phát hiện rằng người nhận chưa bao giờ đặt hàng như vậy. Tuy nhiên, không có công ty nào có thể chấp nhận việc vận chuyển 1000 chiếc xe ô tô và phát hiện rằng đơn hàng là giả mạo. Trong ví dụ về đơn hàng mua sắm, bạn muốn xác nhận rằng khách hàng đã đặt hàng như đã nói; đó là tính xác thực. Hơn nữa, bạn muốn đảm bảo họ không thể phủ nhận việc đặt hàng; đó là tính không thể chối bỏ.

Là một công ty, nếu bạn nhận được đơn đặt hàng giao 1000 chiếc xe ô tô, bạn cần đảm bảo tính xác thực của đơn hàng này; hơn nữa, nguồn gốc không được phép phủ nhận việc đặt hàng như vậy. Mà không có tính xác thực và tính không thể chối bỏ, kinh doanh không thể được tiến hành.

Hệ thập lục phân *Parkerian*

Năm 1998, Donn Parker đề xuất Hexad của Parker, một tập hợp gồm sáu yếu tố bảo mật. Chúng bao gồm:

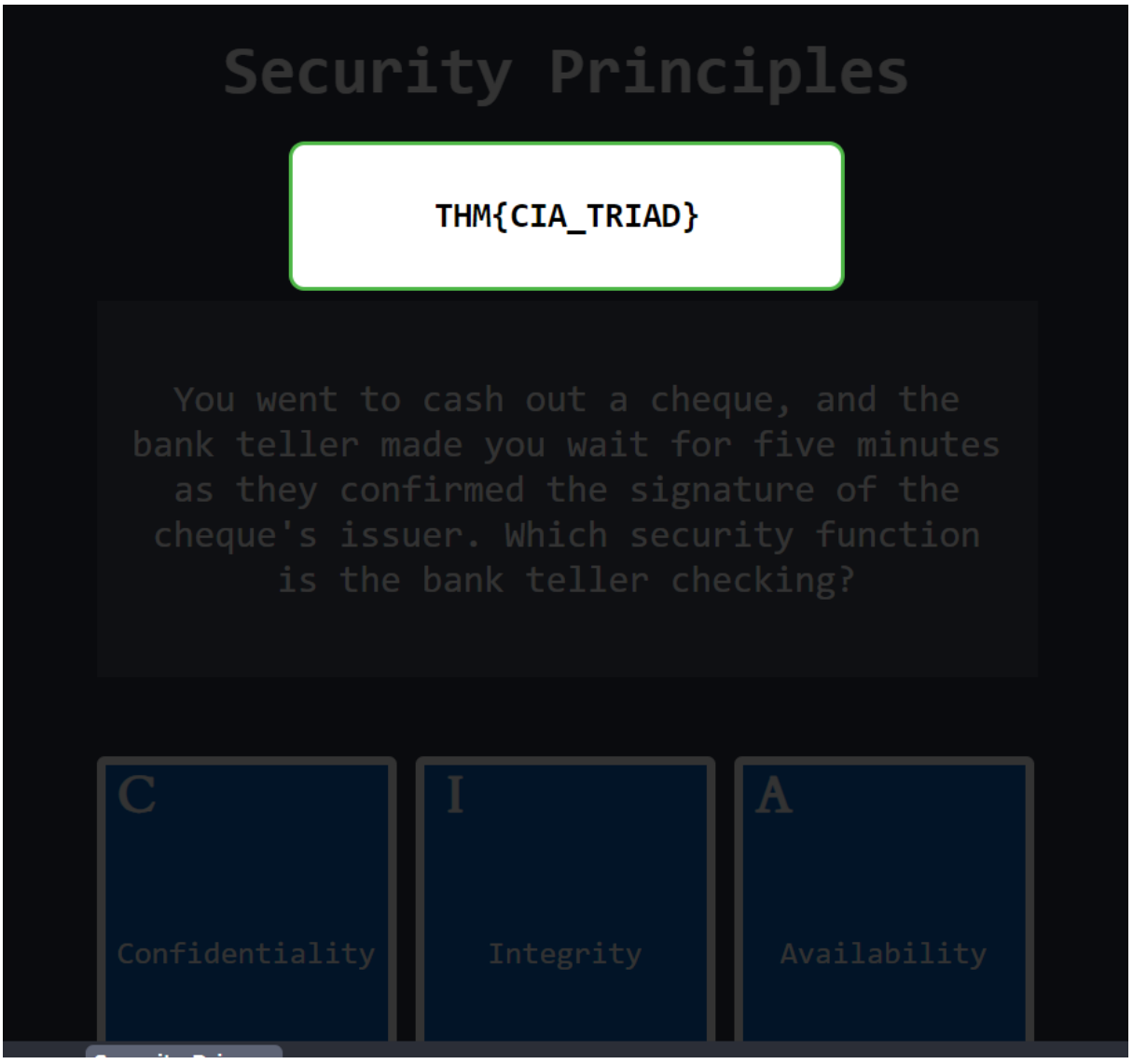
Tính khả dụng
Tính hữu ích
Tính toàn vẹn
Tính xác thực
Tính bảo mật
Tính sở hữu

Chúng tôi đã đề cập đến bốn trong số sáu yếu tố trên. Hãy thảo luận về hai yếu tố còn lại:

Tính hữu ích: Tính hữu ích tập trung vào tính hữu ích của thông tin. Ví dụ, người dùng có thể đã mất khóa giải mã để truy cập vào một máy tính xách tay với bộ nhớ được mã hóa. Mặc dù người dùng vẫn còn máy tính xách tay với các ổ đĩa của nó vẫn nguyên vẹn, họ không thể truy cập vào chúng. Nói cách khác, mặc dù thông tin vẫn có sẵn nhưng không hữu ích, tức là không có tính hữu ích.

Tính sở hữu: Yếu tố bảo mật này yêu cầu chúng ta bảo vệ thông tin khỏi việc lấy cắp, sao chép hoặc kiểm soát trái phép. Ví dụ, một kẻ thù có thể lấy đi một ổ đĩa sao

lưu, có nghĩa là chúng ta mất sở hữu thông tin miễn là họ có ổ đĩa. Hoặc, kẻ thù có thể thành công trong việc mã hóa dữ liệu của chúng ta bằng ransomware; điều này cũng dẫn đến mất sở hữu dữ liệu.



II. DAD

Bảo mật của một hệ thống có thể bị tấn công thông qua một số phương pháp khác nhau. Đó có thể là thông qua việc tiết lộ dữ liệu bí mật, thay đổi dữ liệu hoặc phá hủy dữ liệu.

Việc tiết lộ là ngược lại của tính bảo mật. Nói cách khác, việc tiết lộ dữ liệu bí mật sẽ là một cuộc tấn công vào tính bảo mật.
Thay đổi là ngược lại của tính toàn vẹn. Ví dụ, tính toàn vẹn của một séc là không thể thiếu.
Phá hủy/từ chối là ngược lại của tính khả dụng.
Ngược lại với Tam giác CIA sẽ là Tam giác DAD: Tiết lộ, Thay đổi và Phá hủy.

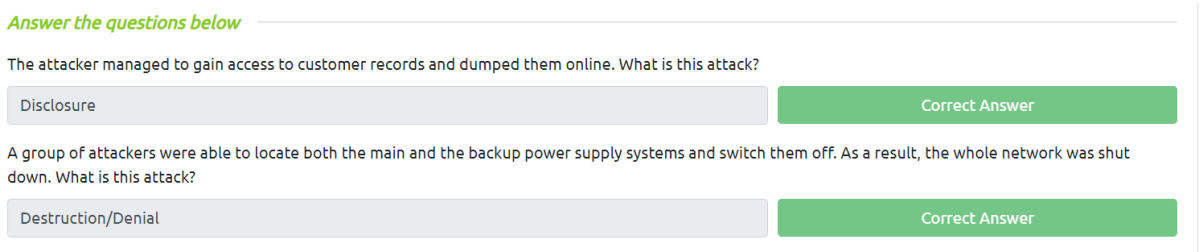
Hãy xem xét ví dụ trước về hồ sơ bệnh nhân và hệ thống liên quan:

Tiết lộ: Như trong hầu hết các nước hiện đại, nhà cung cấp dịch vụ chăm sóc sức khỏe phải duy trì tính bảo mật của hồ sơ y tế. Kết quả là, nếu một kẻ tấn công thành công lấy cắp một số hồ sơ y tế này và đăng chúng trực tuyến để công khai, nhà cung cấp dịch vụ chăm sóc sức khỏe sẽ gánh một mất mát do cuộc tấn công tiết lộ dữ liệu này.
Thay đổi: Hãy xem xét tình hình nghiêm trọng nếu kẻ tấn công thành công thay đổi hồ sơ y tế của bệnh nhân. Cuộc tấn công thay đổi này có thể dẫn đến việc áp dụng sai phương pháp điều trị và do đó, cuộc tấn công thay đổi này có thể mang tính mạng.
Phá hủy/Từ chối: Hãy xem xét trường hợp một cơ sở y tế hoàn toàn không còn sử dụng giấy. Nếu kẻ tấn công thành công làm cho hệ thống cơ sở dữ liệu không khả

dụng, cơ sở y tế sẽ không thể hoạt động bình thường. Họ có thể quay trở lại sử dụng giấy tạm thời; tuy nhiên, hồ sơ bệnh nhân sẽ không có sẵn. Cuộc tấn công từ chối này sẽ làm trì hoãn toàn bộ cơ sở.

Bảo vệ chống lại tiết lộ, thay đổi và phá hủy/từ chối là vô cùng quan trọng. Bảo vệ này tương đương với việc duy trì tính bảo mật, tính toàn vẹn và tính khả dụng.

Việc bảo vệ tính bảo mật và tính toàn vẹn đến mức cực đoan có thể hạn chế tính khả dụng, và việc tăng tính khả dụng đến mức cực đoan có thể dẫn đến mất tính bảo mật và tính toàn vẹn. Việc thực hiện nguyên tắc bảo mật tốt yêu cầu sự cân đối giữa ba yếu tố này.



III. Các khái niệm cơ bản của các mô hình bảo mật

Chúng ta đã học rằng tam giác bảo mật được đại diện bởi tính bảo mật thông tin, tính toàn vẹn và tính khả dụng (CIA). Một người có thể đặt câu hỏi, làm thế nào chúng ta có thể tạo ra một hệ thống đảm bảo một hoặc nhiều chức năng bảo mật? Câu trả lời sẽ nằm trong việc sử dụng các mô hình bảo mật. Trong nhiệm vụ này, chúng ta sẽ giới thiệu ba mô hình bảo mật cơ bản:

Mô hình Bell-LaPadula
Mô hình Integrity Biba
Mô hình Clark-Wilson

Mô hình Bell-LaPadula

Mô hình Bell-LaPadula nhằm đạt được tính bảo mật thông tin bằng cách chỉ định ba quy tắc:

Thuộc tính bảo mật đơn giản: Thuộc tính này được gọi là "không đọc lên"; nó quy định rằng một đối tượng thuộc một mức bảo mật thấp không thể đọc một đối tượng thuộc một mức bảo mật cao hơn. Quy tắc này ngăn chặn việc truy cập vào thông tin nhạy cảm ở mức bảo mật vượt quyền.

Thuộc tính bảo mật sao: Thuộc tính này được gọi là "không ghi xuống"; nó quy định rằng một chủ thể thuộc một mức bảo mật cao không thể ghi vào một đối tượng thuộc một mức bảo mật thấp hơn. Quy tắc này ngăn chặn việc tiết lộ thông tin nhạy cảm cho một chủ thể thuộc mức bảo mật thấp hơn.
Thuộc tính bảo mật theo ý muốn: Thuộc tính này sử dụng ma trận truy cập để cho phép các hoạt động đọc và ghi. Một ví dụ về ma trận truy cập được hiển thị trong bảng dưới đây và được sử dụng cùng với hai thuộc tính đầu tiên.

Chủ thể	Đối tượng A	Đối tượng B
Chủ thể 1	Ghi	Không truy cập
Chủ thể 2	Đọc/Ghi	Đọc

Hai thuộc tính đầu tiên có thể được tóm tắt là "ghi lên, đọc xuống". Bạn có thể chia sẻ thông tin bí mật với những người có cấp độ bảo mật cao hơn (ghi lên), và bạn có thể nhận thông tin bí mật từ những người có cấp độ bảo mật thấp hơn (đọc xuống).

Mô hình Bell-LaPadula có một số hạn chế. Ví dụ, nó không được thiết kế để xử lý việc chia sẻ tập tin.

Mô hình Biba

Mô hình Biba nhằm đạt được tính toàn vẹn thông qua việc quy định hai quy tắc chính:

Thuộc tính toàn vẹn đơn giản: Thuộc tính này được gọi là "không đọc xuống"; một chủ thể toàn vẹn cao hơn không nên đọc từ một đối tượng toàn vẹn thấp hơn.
Thuộc tính toàn vẹn sao: Thuộc tính này được gọi là "không ghi lên"; mộtchủ thể toàn vẹn thấp hơn không nên ghi vào một đối tượng toàn vẹn cao hơn.

Hai thuộc tính này có thể được tóm tắt là "đọc lên, ghi xuống". Quy tắc này trái ngược với mô hình Bell-LaPadula, điều này không quá bất ngờ vì mô hình này quan tâm đến tính bảo mật thông tin trong khi mô hình kia quan tâm đến tính toàn vẹn.

Mô hình Biba cũng có nhiều hạn chế. Ví dụ, nó không xử lý được các mối đe dọa từ bên trong (đe dọa từ nhân viên nội bộ).

Mô hình Clark-Wilson

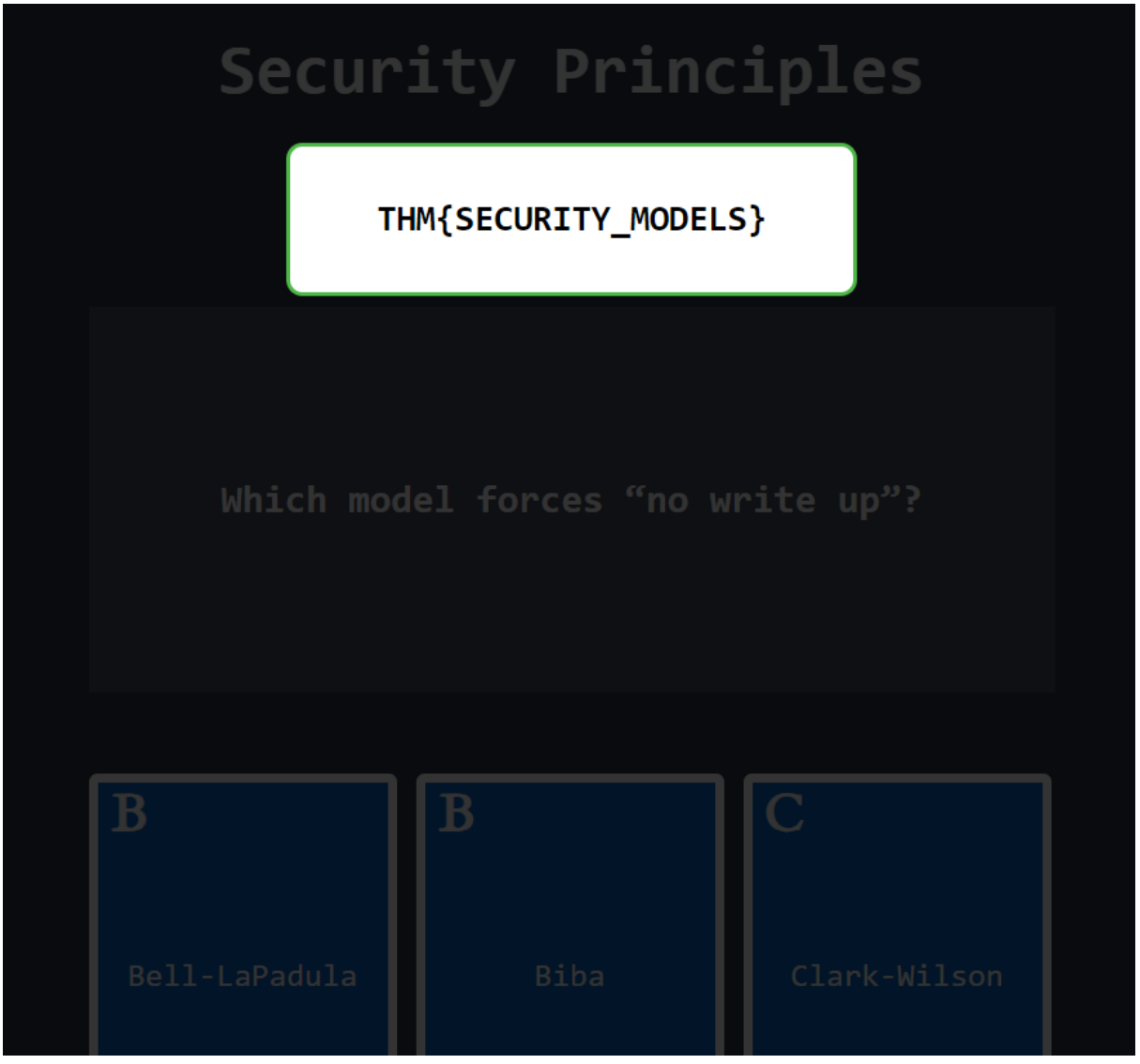
Mô hình Clark-Wilson cũng nhằm đạt được tính toàn vẹn bằng cách sử dụng các khái niệm sau:

Mục dữ liệu ràng buộc (CDI): Đây là loại dữ liệu mà chúng ta muốn bảo toàn tính toàn vẹn.
Mục dữ liệu không ràng buộc (UDI): Đây là tất cả các loại dữ liệu vượt quá CDI, chẳng hạn như dữ liệu người dùng và dữ liệu hệ thống.
Các thủ tục biến đổi (TPs): Các thủ tục này là các hoạt động được lập trình, chẳng hạn như đọc và ghi, và nên duy trì tính toàn vẹn của CDI.

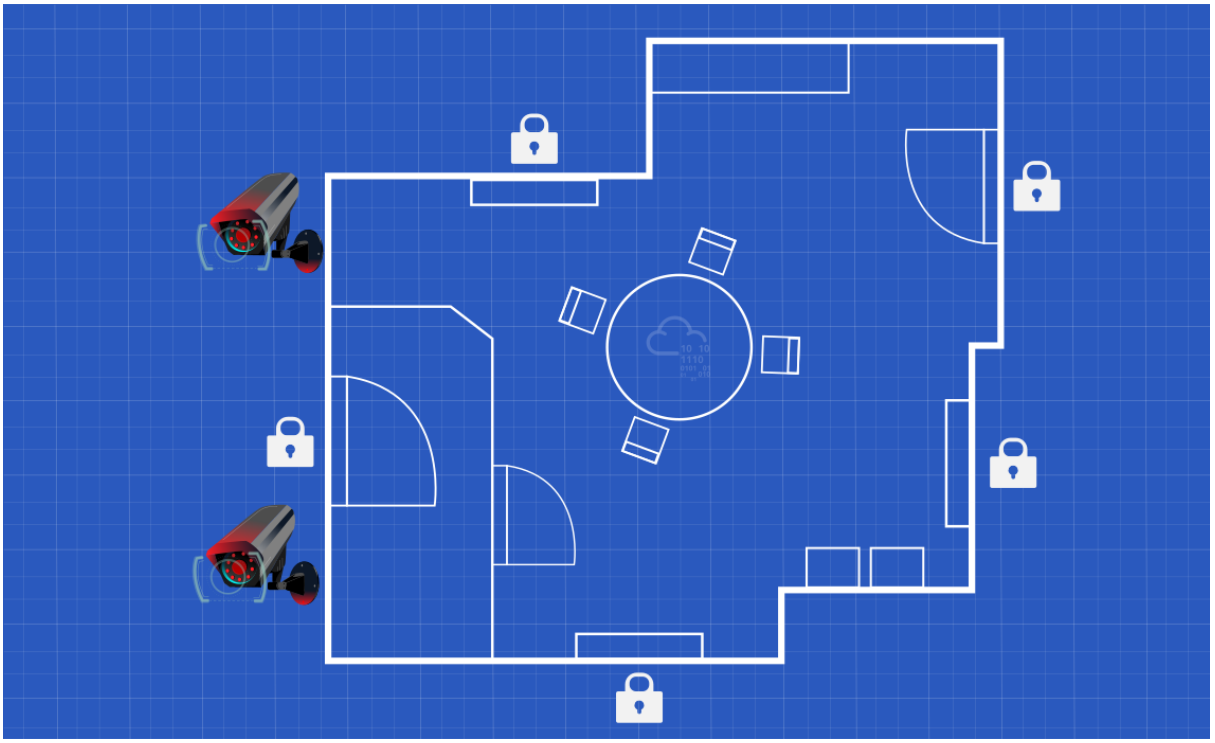
Các thủ tục xác minh tính toàn vẹn (IVPs): Các thủ tục này kiểm tra và đảm bảo tính hợp lệ của CDI.

Chúng tôi chỉ đề cập đến ba mô hình bảo mật. Người đọc có thể tìm hiểu nhiều mô hình bảo mật khác. Ví dụ bao gồm:

Mô hình Brewer và Nash
Mô hình Goguen-Meseguer
Mô hình Sutherland
Mô hình Graham-Denning
Mô hình Harrison-Ruzzo-Ullman



IV. Phòng thủ đa tầng(Defence-in-Depth)



Phòng thủ đa tầng (Defense-in-Depth) ám chỉ việc tạo ra một hệ thống bảo mật với nhiều cấp độ; vì vậy, nó còn được gọi là Bảo mật Đa Cấp.

Hãy xem ví dụ như sau: bạn có một ngăn kéo khóa nơi bạn để các tài liệu quan trọng và đồ đắt tiền. Ngăn kéo đã khóa; tuy nhiên, bạn có muốn chỉ có khóa ngăn kéo này là thứ duy nhất ngăn cản trộm đột nhập và lấy đi những vật phẩm đắt tiền của bạn? Nếu chúng ta nghĩ về bảo mật đa cấp, chúng ta sẽ muốn ngăn kéo được khóa, phòng liên quan được khóa, cửa chính căn hộ được khóa, cổng tòa nhà được khóa, và bạn cũng có thể muốn có một số camera an ninh trên đường đi. Mặc dù những cấp độ bảo mật đa tầng này không thể ngăn chặn mọi tên trộm, chúng sẽ chặn đa số và làm chậm lại những tên trộm khác.

V. ISO/IEC 19249

Tổ chức Quốc tế về Tiêu chuẩn (ISO) và Tổ chức Quốc tế về Điện kỹ thuật (IEC) đã tạo ra tiêu chuẩn ISO/IEC 19249. Trong nhiệm vụ này, chúng ta sẽ tóm tắt ngắn gọn về ISO/IEC 19249:2017 Công nghệ thông tin - Kỹ thuật bảo mật - Danh mục nguyên tắc kiến trúc và thiết kế cho các sản phẩm, hệ thống và ứng dụng an toàn. Mục đích là hiểu rõ hơn về những nguyên tắc bảo mật mà các tổ chức quốc tế giảng dạy.

ISO/IEC 19249 liệt kê năm nguyên tắc kiến trúc:

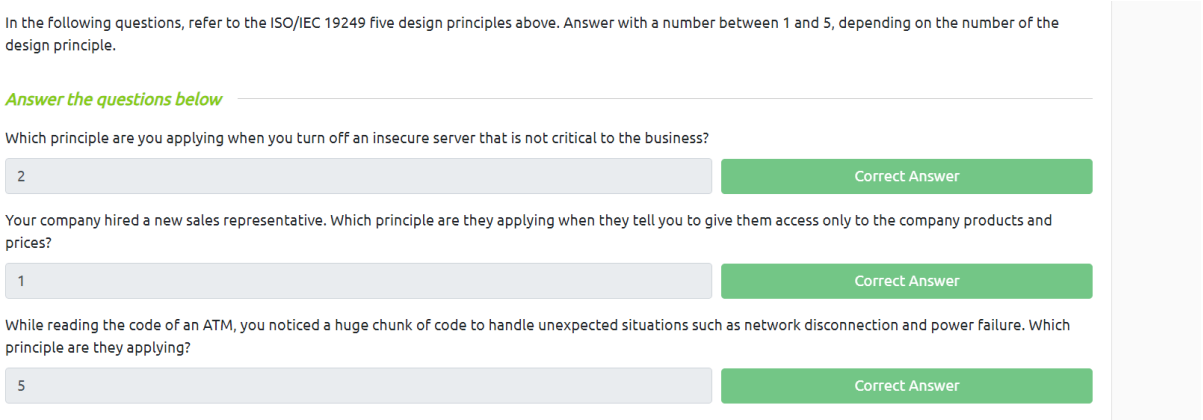
1. Tách biệt miền: Mỗi nhóm thành phần liên quan được nhóm lại thành một thực thể duy nhất; các thành phần có thể là ứng dụng, dữ liệu hoặc các tài nguyên

khác. Mỗi thực thể sẽ có miền riêng và được gán một tập hợp chung các thuộc tính bảo mật. Ví dụ, hãy xem xét cấp độ đặc quyền của bộ xử lý x86: hạt nhân hệ điều hành có thể chạy ở cấp độ vòng 0 (cấp đặc quyền cao nhất). Ngược lại, các ứng dụng chế độ người dùng có thể chạy ở cấp độ vòng 3 (cấp đặc quyền thấp nhất). Tách biệt miền được bao gồm trong Mô hình Goguen-Meseguer.

2. Lớp: Khi một hệ thống được tổ chức thành nhiều mức hoặc lớp trừu tượng, ta có thể áp dụng các chính sách bảo mật ở các mức khác nhau; hơn nữa, ta có thể xác minh hoạt động một cách dễ dàng. Hãy xem xét mô hình OSI (Open Systems Interconnection) với bảy lớp trong mạng. Mỗi lớp trong mô hình OSI cung cấp các dịch vụ cụ thể cho lớp phía trên nó. Cấu trúc lớp này cho phép áp dụng các chính sách bảo mật và kiểm tra dễ dàng xem hệ thống đang hoạt động như mong muốn. Một ví dụ khác trong thế giới lập trình là thao tác đĩa; một lập trình viên thường sử dụng các chức năng đọc và ghi đĩa được cung cấp bởi ngôn ngữ lập trình cấp cao đã chọn. Ngôn ngữ lập trình giấu đi các cuộc gọi hệ thống cấp thấp và trình bày chúng dưới dạng các phương thức dễ sử dụng hơn. Lớp liên quan đến Phòng thủ đa lớp.
3. Đóng gói: Trong lập trình hướng đối tượng (OOP), chúng ta giấu đi các cài đặt cấp thấp và ngăn chặn việc truy cập trực tiếp vào dữ liệu trong một đối tượng bằng cách cung cấp các phương thức cụ thể cho mục đích đó. Ví dụ, nếu bạn có một đối tượng đồng hồ, bạn sẽ cung cấp một phương thức tăng() thay vì cho người dùng truy cập trực tiếp vào biến giây. Mục đích là ngăn ngừa giá trị không hợp lệ cho biến của bạn. Tương tự, trong các hệ thống lớn hơn, bạn sẽ sử dụng (hoặc thậm chí thiết kế) một giao diện lập trình ứng dụng (API) đúng đắn để ứng dụng của bạn sử dụng để truy cập cơ sở dữ liệu một cách an toàn.
4. Dự phòng: Nguyên tắc này đảm bảo tính sẵn có và tính toàn vẹn. Có nhiều ví dụ liên quan đến dự phòng. Hãy xem xét trường hợp của một máy chủ phần cứng có hai nguồn cung cấp điện tích hợp sẵn: nếu một nguồn cung cấp điện hỏng, hệ thống vẫn hoạt động. Hãy xem xét một cấu hình RAID 5 với ba ổ đĩa: nếu một ổ đĩa hỏng, dữ liệu vẫn sẵn có bằng cách sử dụng hai ổ đĩa còn lại. Hơn nữa, nếu dữ liệu bị thay đổi không đúng trên một trong các đĩa, nó sẽ được phát hiện thông qua dư thừa, đảm bảo tính toàn vẹn của dữ liệu.
5. Ảo hóa: Với sự xuất hiện của dịch vụ đám mây, ảo hóa đã trở nên phổ biến và được ưa chuộng hơn. Khái niệm ảo hóa là chia sẻ một bộ phần cứng duy nhất cho nhiều hệ điều hành. Ảo hóa cung cấp khả năng tạo ra các vùng cách ly cải tiến, giới hạn an ninh, và quan sát các chương trình độc hại.

ISO/IEC 19249 giảng dạy năm nguyên tắc thiết kế:

1. Nguyên tắc đặc quyền nhỏ nhất: Bạn cũng có thể diễn đạt nó một cách không chính thức là "dựa trên nhu cầu" hoặc "dựa trên nhu cầu biết" khi bạn trả lời câu hỏi "ai có thể truy cập vào cái gì?". Nguyên tắc đặc quyền nhỏ nhất giảng dạy rằng bạn nên cung cấp ít quyền nhất có thể cho một người để thực hiện nhiệm vụ của họ và không thêm quyền khác. Ví dụ, nếu một người dùng cần có khả năng xem một tài liệu, bạn nên cấp cho họ quyền đọc mà không có quyền ghi.
2. Giảm thiểu diện tích tấn công: Mỗi hệ thống đều có các lỗ hổng mà một kẻ tấn công có thể sử dụng để xâm nhập vào hệ thống. Một số lỗ hổng đã được biết đến, trong khi những lỗ hổng khác vẫn chưa được phát hiện. Những lỗ hổng này đại diện cho các rủi ro mà chúng ta nên cố gắng giảm thiểu. Ví dụ, trong một trong các bước để tăng cường một hệ thống Linux, chúng ta sẽ tắt bất kỳ dịch vụ nào mà chúng ta không cần thiết.
3. Kiểm tra tham số tập trung: Nhiều mối đe dọa xuất phát từ hệ thống nhận đầu vào, đặc biệt là từ người dùng. Đầu vào không hợp lệ có thể được sử dụng để khai thác các lỗ hổng trong hệ thống, chẳng hạn như tấn công từ chối dịch vụ và thực thi mã từ xa. Do đó, việc kiểm tra tham số là một bước cần thiết để đảm bảo trạng thái hệ thống chính xác. Xem xét số lượng tham số mà một hệ thống xử lý, việc kiểm tra các tham số nên được tập trung trong một thư viện hoặc hệ thống duy nhất.
4. Các dịch vụ bảo mật chung tập trung: Là một nguyên tắc bảo mật, chúng ta nên cố gắng tập trung tất cả các dịch vụ bảo mật. Ví dụ, chúng ta sẽ tạo ra một máy chủ tập trung cho xác thực. Tất nhiên, bạn có thể thực hiện các biện pháp thích hợp để đảm bảo tính sẵn có và ngăn chặn việc tạo ra một điểm thất bại duy nhất.
5. Chuẩn bị xử lý lỗi và ngoại lệ: Khi xây dựng một hệ thống, chúng ta nên lưu ý rằng lỗi và ngoại lệ xảy ra và sẽ xảy ra. Ví dụ, trong một ứng dụng mua sắm, một khách hàng có thể cố gắng đặt hàng cho một mặt hàng hết hàng. Một cơ sở dữ liệu có thể quá tải và ngừng phản hồi cho ứng dụng web. Nguyên tắc này giảng dạy rằng hệ thống nên được thiết kế để đảm bảo an toàn khi xảy ra lỗi; ví dụ, nếu một tường lửa bị hỏng, nó nên chặn tất cả lưu lượng thay vì cho phép tất cả lưu lượng. Hơn nữa, chúng ta nên cẩn thận để thông báo lỗi không rò rỉ thông tin mà chúng ta coi là bí mật, chẳng hạn như trích xuất nội dung bộ nhớ chứa thông tin liên quan đến khách hàng khác.



VI. Không tin tưởng vs Tin tưởng nhưng xác minh

Tin tưởng là một chủ đề rất phức tạp; trong thực tế, chúng ta không thể hoạt động mà không có sự tin tưởng. Nếu ai đó nghĩ rằng nhà cung cấp máy tính xách tay đã cài đặt phần mềm gián điệp trên máy tính, họ có thể kết thúc việc xây dựng lại hệ thống. Nếu ai đó không tin tưởng nhà cung cấp phần cứng, họ sẽ ngừng sử dụng hoàn toàn nó. Nếu chúng ta nghĩ về sự tin tưởng ở mức doanh nghiệp, mọi thứ chỉ trở nên phức tạp hơn; tuy nhiên, chúng ta cần một số nguyên tắc bảo mật hướng dẫn. Hai nguyên tắc bảo mật liên quan đến sự tin tưởng mà chúng ta quan tâm:

Tin tưởng nhưng xác minh
Không tin tưởng

Tin tưởng nhưng xác minh: Nguyên tắc này dạy rằng chúng ta nên luôn luôn xác minh ngay cả khi chúng ta tin tưởng một đối tượng và hành vi của nó. Một đối tượng có thể là người dùng hoặc một hệ thống. Việc xác minh thường yêu cầu thiết lập các cơ chế ghi nhật ký thích hợp; việc xác minh chỉ ra việc kiểm tra qua các nhật ký để đảm bảo mọi thứ bình thường. Trong thực tế, việc xác minh mọi thứ không khả thi; hãy nghĩ về công việc cần thực hiện để xem xét tất cả các hành động của một đối tượng duy nhất, chẳng hạn như các trang web truy cập bởi một người dùng duy nhất. Điều này đòi hỏi các cơ chế bảo mật tự động, chẳng hạn như proxy, hệ thống phát hiện xâm nhập và hệ thống ngăn chặn xâm nhập.

Không tin tưởng: Nguyên tắc này coi sự tin tưởng như một điểm yếu, và do đó, nó chú trọng đến các mối đe dọa liên quan đến nhân viên bên trong. Sau khi xem xét sự tin tưởng như một điểm yếu, nguyên tắc không tin tưởng cố gắng loại bỏ nó. Nó giảng dạy gián tiếp rằng "không bao giờ tin tưởng, luôn luôn xác minh". Nói cách khác, mọi đối tượng được coi là đối địch cho đến khi chứng minh ngược lại. Nguyên tắc không tin tưởng không trao quyền tin tưởng cho một thiết bị dựa trên vị trí hoặc

sở hữu. Xác thực và ủy quyền được yêu cầu trước khi truy cập vào bất kỳ tài nguyên nào. Kết quả là, nếu xảy ra bất kỳ vi phạm nào, thiệt hại sẽ được giới hạn hơn nếu một kiến trúc không tin tưởng đã được triển khai.

Microsegmentation là một trong những cách triển khai được sử dụng cho nguyên tắc không tin tưởng. Nó áMicrosegmentation là một trong những cách triển khai được sử dụng cho nguyên tắc Không tin tưởng. Nó đề cập đến thiết kế mạng trong đó một phân đoạn mạng có thể nhỏ đến mức chỉ chứa một máy chủ duy nhất. Hơn nữa, giao tiếp giữa các phân đoạn yêu cầu xác thực, kiểm tra danh sách điều khiển truy cập và các yêu cầu bảo mật khác.

Tuy nhiên, có giới hạn về mức độ chúng ta có thể áp dụng nguyên tắc Không tin tưởng mà không ảnh hưởng tiêu cực đến doanh nghiệp. Tuy nhiên, điều này không có nghĩa là chúng ta không nên áp dụng nó miễn là khả thi.

VII. Mối đe dọa vs Rủi ro

Có ba thuật ngữ mà chúng ta cần lưu ý để tránh bất kỳ sự nhầm lẫn nào.

Vulnerability (Lỗ hổng): Vulnerable có nghĩa là dễ bị tấn công hoặc hư hại. Trong bảo mật thông tin, một lỗ hổng là một điểm yếu.
Threat (Mối đe dọa): Một mối đe dọa là một nguy cơ tiềm tàng liên quan đến điểm yếu hoặc lỗ hổng này.
Risk (Rủi ro): Rủi ro liên quan đến khả năng một đối tác mối đe dọa khai thác một lỗ hổng và tác động kết quả lên doanh nghiệp.

Rời xa các hệ thống thông tin, một showroom có cửa và cửa sổ bằng kính tiêu chuẩn gặp một điểm yếu hoặc lỗ hổng do tính chất của kính. Do đó, có một mối đe dọa là cửa và cửa sổ kính có thể bị vỡ. Chủ cửa hàng showroom nên xem xét rủi ro, tức là khả năng một cửa hoặc cửa sổ kính bị vỡ và tác động kết quả lên doanh nghiệp.

Hãy xem một ví dụ khác liên quan trực tiếp đến hệ thống thông tin. Bạn làm việc cho một bệnh viện sử dụng một hệ thống cơ sở dữ liệu cụ thể để lưu trữ tất cả hồ sơ y tế. Một ngày nọ, bạn đang theo dõi tin tức bảo mật mới nhất và bạn biết rằng hệ thống cơ sở dữ liệu đã sử dụng không chỉ có lỗ hổng mà còn có một mã khai thác thực nghiệm đã được phát hành; mã khai thác đã phát hành cho thấy rằng mối đe dọa là có thật. Với kiến thức này, bạn phải xem xét rủi ro kết quả và quyết định các bước tiếp theo.