Trường Đại học Công nghệ Thông tin (UIT)
Đại Học Quốc Gia Tp. HCM

Assignment 02

Môn học: Lập trình an toàn & Khai thác lỗ hổng phần mềm

Tên chủ đề: **Quy trình phát triển phần mềm an toàn - Secure SDLC**

Mã môn học: NT521 – Năm học 2023-2024

1. NỘI DUNG THỰC HIỆN

Mô hình hóa mối đe dọa – Threat modeling

Mục đích của bài tập này là để tạo cơ hội cho người học thực hành kỹ thuật mô hình hóa mối đe dọa (threat modeling) trong giai đoạn thiết kế phần mềm an toàn, và làm quen với một trong những mô hình hóa mối đe dọa phổ biến – mô hình STRIDE.

Yêu cầu:

*Đọc mô tả hệ thống phần mềm Hỗ trợ Bảo dưỡng Phi cơ cần được phát triển **của hãng hàng không A** như bên dưới. Vì lí do an toàn trong hoạt động bay, ứng dụng này cần được quan tâm tới độ an toàn, bảo mật nghiêm ngặt. Thực hiện các yêu cầu:*

1) *Tìm và xác định các tác nhân đe dọa cho phần mềm sắp được phát triển theo **mô hình STRIDE** cho ngữ cảnh được chỉ định.*
2) *Sử dụng công cụ "Microsoft Threat Modeling Tool" để vẽ bản thiết kế phần mềm và hiển thị các danh sách tác nhân đe dọa.*

Ngữ cảnh:

Việc bảo dưỡng máy bay là vô cùng quan trọng để tránh máy bay gặp sự cố trong hành trình bay. Do đó, trong lĩnh vực hàng không, có nhiều thủ tục và qui định liên quan đến cách bảo dưỡng máy bay.

Trong ngữ cảnh này, tổ chức **hãng hàng không A** cần phát triển một ứng dụng chạy trên các thiết bị Apple iPad để tạo và quản lý-duy trì các dữ liệu liên quan tới hoạt động bảo dưỡng máy bay. Ứng dụng này có tên là "**Bảo Dưỡng Phi Cơ"**, sẽ thay thế các hệ thống cũ đang vận hành vốn tồn tại nhiều lỗi, và chi phí vận hành khá đắt.

Các hồ sơ dữ liệu bảo trì cho máy bay bao gồm nhiều thông tin: bao gồm kiểu máy và số sê-ri của khung máy bay, từng động cơ, từng cánh quạt, v.v. Hồ sơ bao gồm thời điểm từng bộ phận này được lắp đặt, kiểm tra hoặc được bảo dưỡng và người đã chứng nhận rằng công việc được thực hiện đúng cách.

Khi bảo dưỡng máy bay, những người thực hiện công việc được cung cấp danh sách kiểm tra (checklist) các công việc phải hoàn thành. Người giám sát công việc phải có chứng chỉ thích hợp để thực hiện nhiệm vụ cụ thể đó, và phải ký tên ở cuối ghi rằng công việc đã được thực hiện một cách chính xác.

Ngoài ra, nhiều tổ chức, hay hãng hàng không coi hồ sơ máy bay của họ là bí mật. Họ có thể cung cấp các tài liệu sẵn có cho các cơ quan quản lý, nhưng vì nhiều lý do, họ không muốn đối thủ cạnh tranh của mình hoặc công chúng biết chi tiết về các chính sách và quy trình bảo dưỡng của họ hoặc chi tiết về máy bay cá nhân của họ.

Định kỳ, các cập nhật trong danh sách kiểm tra hoặc chính sách bảo trì thiết bị của máy bay được xem xét và điều chỉnh thích hợp bởi tổ chức, hãng hàng không. Đây là công việc thường xuyên để phòng các tai nạn có thể xảy ra – ví dụ như những người có trách nhiệm sẽ đưa ra quyết định một cách thích hợp để ngăn chặn một tai nạn tương tự tái diễn.

Trường hợp sử dụng điển hình (Use case):

- Đội bảo dưỡng của hãng hàng không nhận một hoặc nhiều thiết bị iPad vào lúc bắt đầu mỗi ca làm việc.
- Họ sẽ tham khảo Ứng dụng "Bảo Dưỡng Phi Cơ" cho ca làm việc của mình, ứng dụng này sẽ hiển thị danh sách các công việc cần được thực hiện. Chú ý rằng, họ sẽ không cần phải hoàn thành tất cả các nhiệm vụ công việc trong ca làm việc của mình - thời gian thực hiện để bảo trì có thể khác nhau và vì vậy họ sẽ làm hết sức có thể trong ca làm việc của mình, sau đó, ca sau sẽ đảm nhận.
- Khi thực hiện một nhiệm vụ bảo trì, Ứng dụng "Bảo Dưỡng Phi Cơ" sẽ hiển thị cho đội bảo dưỡng các hồ sơ bảo trì cho chiếc máy bay đó, hướng dẫn sử dụng để thực hiện tác vụ cụ thể đó và danh sách kiểm tra chính xác.
- Khi một thành viên của đội bảo dưỡng hoàn thành một mục trong danh sách kiểm tra, họ phải thực hiện một số hành động (chẳng hạn như nhấn đúng nút trên màn hình) để kiểm tra, xác nhận lại rằng qui trình đã được hoàn thành. Đôi khi các mục trong danh sách kiểm tra sẽ yêu cầu điền thông tin như số sê-ri của một bộ phận thay thế cho một bộ phận cũ.
- Các thành viên đội bảo dưỡng có thể chụp ảnh công việc của họ bằng máy ảnh trên iPad và đính kèm chúng vào hồ sơ dịch vụ bảo trì phụ tùng máy bay.
- Khi một nhiệm vụ hoàn thành, Ứng dụng "Bảo Dưỡng Phi Cơ" sẽ có người chịu trách nhiệm về nhiệm vụ đó (người phải được chứng nhận hợp lệ) ký tên rằng nhiệm vụ đã được thực hiện đúng quy trình chuẩn.
- Đôi khi thực hiện một nhiệm vụ bảo dưỡng thiết bị máy bay sẽ dẫn đến việc tạo ra một nhiệm vụ mới. Ví dụ, một cuộc kiểm tra tình trạng thiết bị sẽ đưa ra kết luận rằng một bộ phận của máy bay cần được thay thế. Ứng dụng cũng sẽ hỗ trợ tính năng tạo mới nhiệm vụ bảo dưỡng này.
- Khi ca làm việc của họ kết thúc, đội bảo trì sẽ trả lại iPad mà họ đã sử dụng.

Cơ sở dữ liệu chính của tổ chức/hãng hàng không về hồ sơ của máy bay sẽ được cập nhật chính xác khi dịch vụ bảo dưỡng được thực hiện.

Đặc tả hệ thống:

Trung tâm dữ liệu (data center) của tổ chức/hãng hàng không sẽ đảm nhận lưu trữ:

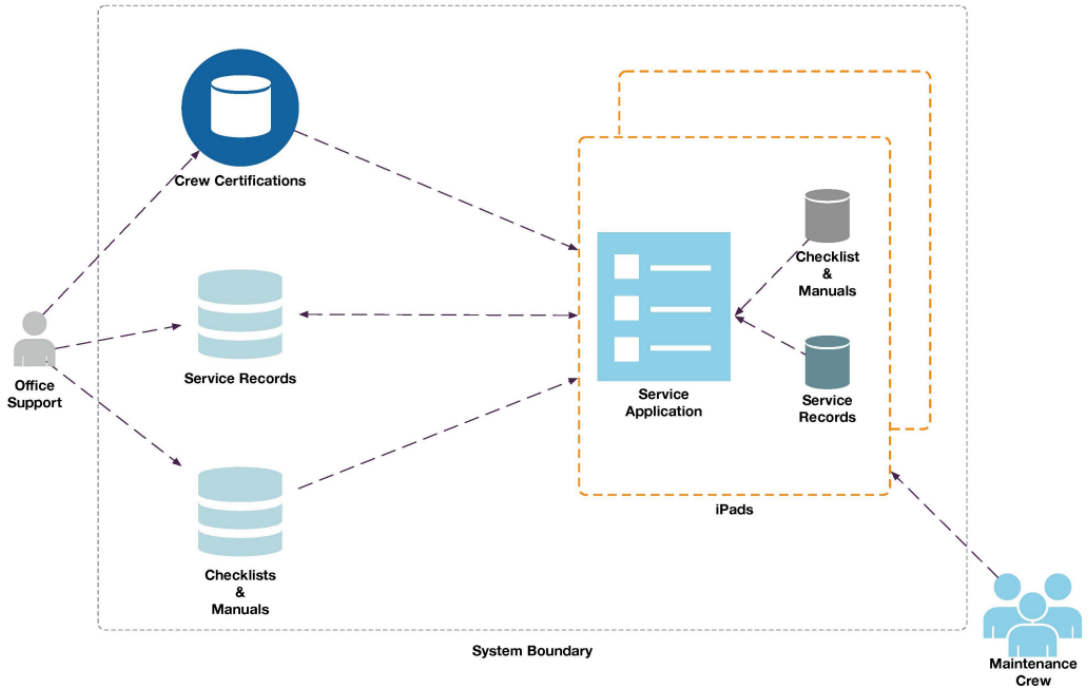
- Cơ sở dữ liệu chứa tất cả các hồ sơ dịch vụ cho máy bay của hãng. Cơ sở dữ liệu này đã tồn tại: Ứng dụng "Bảo Dưỡng Phi Cơ" sẽ phải xử lý các bản ghi được tạo bởi các hệ thống đã phát triển trước đó. Ngoài ra, hãng hàng không sẽ không thể thay thế đồng thời hệ thống bảo trì máy bay hiện có của mình, vì vậy ngay cả khi Ứng dụng "Bảo Dưỡng Phi Cơ" được đưa vào sử dụng, một số người trong tổ chức vẫn sẽ sử dụng các hệ thống cũ hơn.
- Cơ sở dữ liệu tổng thể của tất cả các hướng dẫn sử dụng dịch vụ và danh sách kiểm tra cho tất cả các thiết bị, phụ tùng máy bay được hãng A sử dụng.
- Cơ sở dữ liệu về các chứng chỉ do nhân viên dịch vụ của hãng A nắm giữ.

Lưu ý:

Thiết bị iPad sẽ được kích hoạt wifi và wifi sẽ có sẵn trong văn phòng của tổ chức/hãng hàng không. Tuy nhiên, ở ngoài sân bay (hoặc bên trong khu vực động cơ của máy bay) tính khả dụng của wifi sẽ không được đảm bảo.

Ứng dụng "Bảo Dưỡng Phi Cơ" sẽ được cài đặt trên iPad. Tuy vậy, do có quá nhiều hướng dẫn sử dụng dịch vụ và danh sách kiểm tra trong hãng bay để tất cả chúng được tải xuống sang iPad. Do đó, Ứng dụng "Bảo Dưỡng Phi Cơ" sẽ có những hồ sơ/thông tin cần thiết, tuy nhiên không phải tất cả chúng. Tương tự, iPad không thể chứa tất cả hồ sơ dịch vụ cho tất cả các máy bay của hãng hàng không này.

Kiến trúc tổng thể của ứng dụng được mô tả như hình bên dưới.



2. GỢI Ý – THAM KHẢO

Một số gợi ý thực hiện:

- Tham khảo bài giảng môn học.
- Threat Modeling, Step by Step: https://akademie.dw.com/docs/Handbook_Threat_Modeling_Guide.pdf
- Threat modeling: Technical walkthrough and tutorial: https://resources.infosecinstitute.com/topic/threat-modeling-technical-walkthrough-and-tutorial/
- "Tactical Threat Modeling" – SAFECode: https://safecode.org/wp-content/uploads/2017/05/SAFECode_TM_Whitepaper.pdf
- The Microsoft Threat Modeling Tool: https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling
- Microsoft Threat Modeling Tool threats: https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats

---

Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này

YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hiện bài tập theo yêu cầu, hướng dẫn.
- Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).

Báo cáo:

- File **.PDF**. Tập trung vào nội dung thực hiện, không mô tả lý thuyết.
- Đặt tên theo định dạng: **[Mã lớp]-AssignmentX_NhomY**. (trong đó X là Thứ tự Bài tập, Y là mã số thứ tự nhóm trong danh sách đăng ký đồ án môn học).
- Ví dụ: [NT521.O11.ATCL]-Assignment02_Nhom03.pdf.
- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Đánh giá:

- Hoàn thành tốt yêu cầu được giao.
- Có nội dung mở rộng, ứng dụng.

Bài sao chép, trễ, … sẽ được xử lý tùy mức độ vi phạm.

HẾT