Auxilio para frequência

Guia de desenvolvimento

Security Development Lifecycle

O plano do SDL é composto pelas seguintes fases:

1. **Education and awareness**: Planeamento de formação e sensibilização para a segurança;
2. **Project inception**: Planeamento da implementação e manutenção de um programa de segurança;
3. **Analysis and requirements**: Definição do controlo de segurança da aplicação;
4. **Architectural and detailed design**: Design da aplicação;
5. **Implementation and Testing**: Práticas de programação segura e testes de segurança;
6. **Release, deployment and support**: reposta a incidentes e atualizações de segurança.

Security Requirements

Existem dois tipos de requisitos de segurança:

- **Funcionais**: descrevem o comportamento do sistema em relação à segurança (foca-se no "o que");
- **Não funcionais**: descrevem as propriedades do sistema em relação à segurança (foca-se no "como");

Em relação aos requisitos de segurança, estes podem ser:

- **Confidencialidade**: garante que a informação só é acessível a utilizadores autorizados;
- **Integridade**: garante que a informação não é alterada por utilizadores não autorizados;
- **Disponibilidade**: garante que a informação está disponível para utilizadores autorizados quando necessário.
- **Responsabilidade**: não repudiação de ações realizadas por utilizadores autorizados;

Security Test Plan

O plano de testes de segurança é composto pelas seguintes fases:

1. **Penetration Testing**: Aqui é especificado o tipo de teste de penetração a ser realizado. Estes testes são realizados simulando um atacante externo à organização;
2. **Fuzzy Testing**: Aqui é especificado o tipo de teste de fuzzing a ser realizado. Envolve a introdução de dados inválidos para avaliar a robustez e estabilidade do sistema em condições adversas;
3. **Test Especifications for Each Requirement**: Especificação dos testes para cada requisito de segurança;

Test Especifications for Each Requirement

Estes testes têm de:

- **Serem objetivos**: os resultados dos testes devem ser claros e não ambíguos;
- **Serem quantificáveis**: os resultados dos testes devem ser mensuráveis;
- **Serem repetíveis**: os testes devem ser repetíveis para que os resultados possam ser verificados;

Resolução do "Eletric Charge system"

Considere uma aplicação/solução para sistemas de carregamento de veículos elétricos (quiosque com monitor tátil).

Antes de iniciar o carregamento, o utilizador deve autenticar-se (no ponto, por meio de ligação wifi ou Bluetooth, por uma aplicação específica) e o acesso é permitido mediante registo prévio e com login e password.

Na sua conta, o utilizador pode ver e alterar: Nome, Email, número de telefone, morada, dados do veículo, dados do CC, número de contribuinte, histórico de consumos histórico de consumos, histórico de faturas (mensal), cartão de crédito associado para pagamento direto, e outras configurações da conta (tipo de pagamento, código de desconto, etc.)

Security Development Lifecycle

Education and awareness

No desenvolvimento desta solução, é necessário que os programadores tenham conhecimento das tecnologias de comunicação utilizadas (wifi, bluetooth, nfc, etc), dos protocolos de comunicação usados e de criptografia para que a troca de informação tenha um bom balanceamento entre usabilidade e segurança. Para isso, os programadores deverão ter formação em redes de computadores e em telecomunicações, de modo a que possam fazer uma implementação tendo em conta as possíveis vulnerabilidades que possam existir nestes meios de comunicação. Além disso, devem ser bem estipuladas políticas de segurança e devem ser feitos testes de segurança com regularidade (pelo menos semanalmente).

Project inception

O projeto do Sistema de Carregamento para Veículos Elétricos tem como objetivo desenvolver uma solução segura e fácil de usar para o carregamento de veículos elétricos. O sistema incluirá um kiosk com um monitor *touchscreen* que permitirá aos utilizadores autenticarem-se e iniciar o processo de carregamento por meio de uma aplicação móvel dedicada.

O sistema de carregamento para veículos elétricos irá permitir aos utilizadores autenticarem-se e iniciar o processo de carregamento por meio de uma aplicação móvel dedicada. Este sistema irá permitir aos utilizadores monitorizar o seu consumo e histórico de faturação, e também permitirá o pagamento direto por meio de um cartão de crédito associado à conta do utilizador. Também irá permitir a utilização de códigos de desconto, que poderão ser obtidos através de campanhas de marketing ou de parcerias com empresas de serviços públicos.

Analysis and requirements

Nenhum utilizador de sistemas de carregamento de carros elétricos gostaria de ver a sua privacidade invadida por um atacante. Por conseguinte, ao aceder ao software subjacente a um quiosque, um atacante pode controlar o sistema de carregamento de carros elétricos e obter acesso a dados confidenciais, como o histórico de faturação, o número de cartão de crédito, o número de identificação fiscal, etc. De modo a evitar isso, todos os dados transmitidos entre o quiosque e a aplicação móvel, bem como aqueles armazenados no sistema, devem ser protegidos através de técnicas robustas de cifragem, em conformidade com o Regulamento Geral sobre a Proteção de Dados (RGPD). Além disso, o sistema deve ser capaz de detetar e prevenir ataques de negação de serviço (DoS) e ataques de força bruta, de modo a evitar que um atacante bloqueie o sistema ou obtenha acesso a uma conta de utilizador.

Architectural and detailed design

A autenticação do utilizador poderá ser feita usando MFA/2FA, onde após cada operação de login e transação, o utilizador terá de inserir um código de segurança que será enviado para o seu telemóvel. O quiosque irá comunicar com a aplicação móvel através de uma ligação Wi-Fi ou Bluetooth. A aplicação móvel irá comunicar com o servidor através de protocolos de comunicação seguros, como TLS. O servidor irá armazenar os dados dos utilizadores e irá comunicar com o sistema de pagamento para processar os pagamentos dos utilizadores.

Implementation and Testing

A fase de implementação e testes do sistema de carregamento de carros elétricos é crítica para garantir que as medidas de segurança propostas são eficazes.

Implementation

Os desenvolvedores seguirão práticas de programação segura, evitando vulnerabilidades comuns, como injeção de SQL e Cross-Site Scripting (XSS). Revisões de código serão realizadas para garantir a qualidade e segurança do código-fonte. Os sistemas terão limitação de privilégios para garantir que apenas as funções necessárias para o funcionamento correto do sistema tenham acesso a recursos específicos. O sistema irá conter um mecanismo de atualizações automáticas para garantir que quaisquer vulnerabilidades identificadas sejam corrigidas rapidamente. Isso incluirá patches de segurança e atualizações do sistema operacional.

Testing

Serão realizadas simulações de ataques controlados para avaliar a resiliência do sistema em face de possíveis ameaças, isto ajudará a identificar e corrigir potenciais falhas de segurança. Serão realizados testes de penetração para avaliar a segurança do sistema e identificar possíveis vulnerabilidades, testes como *Dynamic Analysis Security Testing* (DAST) e *Static Analysis Security Testing* (SAST) serão realizados. Além disso, serão realizados testes de carga para avaliar a capacidade do sistema de lidar com um grande número de utilizadores.

Release, deployment and support

Na etapa de lançamento, implementação e suporte do sistema de carregamento de carros elétricos, foi adotada uma abordagem gradual com um lançamento controlado e uma implementação piloto inicial. A comunicação transparente com os utilizadores e a monitorização contínua garantiram uma transição suave. Canais de suporte eficazes e atualizações regulares contribuíram para a estabilidade operacional. Além disso, foi incentivado o feedback dos utilizadores para melhorias contínuas. Em paralelo, vai ser mantido um Plano de Resposta a Incidentes atualizado, garantindo respostas rápidas e eficazes em casos de potenciais violações de segurança, salvaguardando assim os dados dos utilizadores.

Security Requirements

Confidentiality

- REQ-1: O sistema deve armazenar os dados dos utilizadores de forma segura, com acesso restrito a utilizadores autorizados.

- REQ-2: O sistema deve garantir que todas as comunicações entre o quiosque e a aplicação móvel, bem como entre a aplicação móvel e o servidor, são feitas usando END-TO-END encryption.
- REQ-3: O sistema deve proteger de mudanças na base de dados (intencionais ou não) de utilizadores não autorizados.

Integrity

- REQ-4: O sistema deve permitir verificar a integridade do histórico de faturação, usando assinaturas digitais RSA para verificar a autenticidade de cada fatura.
- REQ-5: O sistema deve permitir que os utilizadores visualizem o seu histórico de faturação, bem como o seu consumo de energia.
- REQ-6: O sistema deve garantir que os dados mais sensiveis serão regularmente copiados para um local seguro (backup).

Availability

- REQ-7: O sistema deve ser capaz de detetar e prevenir ataques de negação de serviço (DoS), de modo a evitar que um atacante bloqueie o sistema ou obtenha acesso a uma conta de utilizador.
- REQ-8: O sistema deve garantir que o processo de backup não afeta a eficiência do mesmo.
- REQ-9: O sistema irá suportar não mais que 1000 quiosques de carregamento.

Test Especifications for Each Requirement

Confidentiality

- TST-1: O requisito será testado fazendo uma tentativa de acesso aos dados de registos do dispositivo com um utilizador não privilegiado.
- TST-2: O requisito será testado usando um sniffer de rede para verificar se as comunicações entre o quiosque e a aplicação móvel, bem como entre a aplicação móvel e o servidor, e tentar extrair informação sensível.
- TST-3: O requisito será testado fazendo uma tentativa de manipulação (eliminar e criar) à base de dados com um utilizador não privilegiado.

Integrity

- TST-4: O requisito será testado adicionando uma fatura falsa à base de dados e verificando se o sistema deteta a fatura como inválida.
- TST-5: O requisito será testado verificando se o utilizador consegue visualizar o seu histórico de faturação e o seu consumo de energia.
- TST-6: O requisito será testado fazendo uma monitorização ao sistema de backup e verificando se o mesmo não afeta o tempo de resposta do sistema em pelo menos 20%.

Availability

- TST-7: O requisito será testado simulando um ataque de negação de serviço (DoS), fazendo 100 mil pedidos ao sistema em 1 minuto e verificando se o sistema continua a funcionar corretamente. Para o medir, verificar se a percentagem de pedidos com sucesso é superior a 95%.

- TST-8: O requisito será testado adicionando 1000 quiosques ao sistema e verificando se o sistema continua a funcionar corretamente. Para o medir, verificar se o tempo de resposta do sistema é inferior a 2 segundos.
- TST-9: O requisito será testado fazendo uma tentativa de adicionar um novo quiosque ao sistema e verificando se o sistema invalida a adição do mesmo.