Universidade do Minho

Mestrado Integrado em Engenharia Informática

Engenharia de Segurança

OWASP - Mobile Application Security Verification Standard (MASVS)

Grupo 8

João de Macedo
A76268

João Aloísio
A77953

Nelson Gonçalves
A78173

23 de Março de 2020

Conteúdo

1 Introdução

As revoluções tecnológicas podem acontecer rapidamente. Em menos de uma década passamos de ter telemóveis com pequenos teclados para smartphones que hoje em dia são uma parte essencial das nossas vidas confiando-lhes informações e dados privados do nosso dia a dia.

A cada nova tecnologia são introduzidos novos riscos de segurança e acompanhar essas mudanças é um dos principais desafios que o setor de segurança enfrenta. Os smartphones são como pequenos computadores e as aplicações móveis são como softwares clássicos, no entanto, os requisitos de segurança não são semelhantes.

A segurança móvel tem tudo a ver com proteção de dados: as aplicações armazenam as nossas informações pessoais, fotos, gravações, anotações, dados da conta, informações comerciais, localização e muito mais. A necessidade de segurança de dados torna-se ainda mais evidente à medida que nos apercebemos que os dispositivos móveis são muito mais facilmente perdidos ou roubados.

Um padrão de segurança para aplicações móveis deve, portanto, focar em como as aplicações manipulam, armazenam e protegem informações confidenciais. Embora os sistemas operativos móveis modernos, como *iOS* e *Android*, ofereçam boas *APIs* para armazenamento e comunicação segura de dados, precisam de ser implementados e usados corretamente para serem eficazes. Armazenamento de dados, comunicação entre aplicações, uso adequado de *APIs* criptográficas e comunicação de rede segura são apenas alguns dos aspectos que requerem consideração cuidadosa.

O objetivo geral do *MASVS* é oferecer uma linha de base para segurança de aplicações móveis *(MASVS-L1)*, além de permitir a inclusão de medidas de defesa em profundidade *(MASVS-L2)* e proteções contra ameaças do lado do cliente *(MASVS-R)*. O *MASVS* deve atingir o seguinte:

• Fornecer requisitos para arquitetos e implementadores de software que desejam desenvolver aplicações móveis seguros;

• Oferecer um padrão do setor que possa ser testado nas análises de segurança de aplicações móveis;

• Fornecer recomendações específicas sobre o nível de segurança recomendado para diferentes casos de uso.

É impossível alcançar 100% de consenso no setor da segurança, no entanto a *MASVS* espera ser útil para fornecer orientação em todas as fases do desenvolvimento e teste de aplicações móveis.

2 Mobile Application Security Verification Standard

O MASVS pode ser usado para estabelecer o nível de confiança na segurança das aplicações, cobrindo apenas a segurança do lado do cliente e a comunicação entre a aplicação e o controlo remoto. Esses requisitos foram desenvolvidos com certos aspetos em mente, sendo eles:

- **Usar uma métrica :** Ter um termo de comparação padrão para que os implementadores e os utilizadores de aplicações possam comparar uma aplicação;
- **Uso de um guia:** Orientar durante todas as fases de implementação e teste de uma aplicação;
- **Base na aquisição:** Fornecer uma *baseline* para verificar a segurança de uma aplicação;

2.1 Modelo

É definido dois níveis de segurança rigorosos (L1 e L2), bem como um conjunto de requisitos de resiliência de engenharia reversa (MASVS-R) que é flexível, ou seja, dependendo da aplicação em questão, é adaptável. MASVS-L1 e MASVS-L2 contêm requisitos de segurança genéricos e são recomendados para todas as aplicações no caso de L1 e para aplicações que geram dados sensíveis L2. MASVS-R fornece controlos protetores que podem ser aplicados caso seja para prevenir as ameaças do lado do cliente o desejado. Assim sendo, preenchendo todos os requisitos MASVS-L1 resulta numa aplicação segura e que não sofre com as vulnerabilidades mais comuns. Já MASVS-L2 adiciona medidas de segurança que resulta numa aplicação segura contra ataques mais sofisticados. O MASVS-R ajuda a impedir que específicas ameaças do lado do cliente, onde o utilizador tem más intenções ou o SO do smartphone está comprometido, afetem a segurança da mesma.

2.2 Os níveis de verificação

2.2.1 MASVS-L1: Standard Security

Qualquer aplicação que consiga cumprir todos os requisitos de MASVS-L1 é considerada uma aplicação com práticas seguras, onde cumpre os requisitos mínimos da qualidade de código, manipulação de dados sensíveis e as interações com o ambiente do smartphone. Este nível é recomendado para todas as aplicações do smartphone.

2.2.2 MASVS-L2: Defense-in-Depth

Este nível já apresenta controlos de segurança mais avançados que os requisitos padronizados. Para que isto seja cumprido, a ameaça tem de ser conhecida e o mecanismo de

segurança tem de fazer parte da arquitetura e implementação da aplicação. O nível é usado mais em aplicações que manipulem muitos dados sensíveis, tal como uma aplicação de um banco.

2.2.3 MASVS-R: Resiliency Against Reverse Engineering and Tampering

Este nível é um complemento aos outros níveis em que é definido especificamente para ataques do lado do cliente, tais como, modificação de dados ou engenharia reversa para extrair código ou dados sensíveis que não deviam ser partilhados. É aplicado quando a aplicação manipula dados sensíveis e é necessário proteger a sua propriedade intelectual.

2.3 Tipos de verificação

- **MASVS-L1:**pode ser usado todas as aplicações;
- **MASVS-L1 +R:** é usado onde o objetivo é proteger o IP ou aplicações de jogos;
- **MASVS-L2:** pode ser usado nos serviços de saúde e financeiros onde seja necessário métodos de pagamento;
- **MASVS-L2-R:** pode ser usado em aplicações bancária para gerir as contas pessoais;

As diferentes combinações refletem nos diferentes níveis de segurança e resiliência, em que o objetivo é permitir a flexibilidade, por exemplo, um jogo para smartphone não necessita de um MASVS-L2, como autenticação de dois factores em termos de usabilidade, mas por termos comerciais para prevenir a modificação de dados.

A escolha do tipo de verificação a escolher deve-se começar por uma avaliação dos riscos que aplicação pode ter e posteriormente aplicar o MASVS, tendo em conta que MASVS-L2 aumenta o nível de segurança mas também aumenta o custo de implementação. Sendo assim, só deve ser usada quando o risco compensa o custo.

3 Categorias de requisitos

Os requisitos foram divididos em oito categorias tendo em conta o objetivo técnico que se pretende:

3.1 Requisitos de arquitetura, design e modelação de ameaças

Estes requisitos tem com objetivo assegurar a segurança da aplicação na fase de planeamento da arquitetura, e que as funções funcionais e de segurança de todas as componente são

conhecidas. Dado que maioria das aplicações móveis remetem para clientes de serviços remotos, é necessário garantir a segurança desses mesmos serviços, ou seja, testar isoladamente a aplicação do smartphone não é suficiente.

Sendo assim, alguns exemplos de requisitos desta categoria temos: todas as componentes da aplicação têm de estar identificadas e conhecidas caso necessárias, os controles de segurança nunca são aplicados apenas no lado do cliente mas também no ponto remoto do serviço, os dados sensíveis da aplicação do smartphone devem ser devidamente identificados, entre outros.

3.2 Requisitos de armazenamento e privacidade de dados

A protecão dos dados sensíveis, tais como as credenciais e informação privada de um utilizador, são o objetivo da segurança do smartphone. Visto que os dados numa cloud, por exemplo, podem ser acedidos indevidamente ou sendo um smartphone um objeto mais fácil de se perder ou ser roubado, deve ser implementado proteções adicionais para que dificulte o acesso a estes dados.

Os dados sensíveis no contexto da MASVS são considerados as credenciais do utilizador, números de cartões de crédito e também informções que estão protegidas por lei.

Alguns exemplos de requisitos desta categoria temos: nenhum dado sensível é guardado em *logs* do aplicativo, a cache do teclado está desativada quando são entradas de texto que processam dados confidencias, a área de transferência está desativa em campos que processam informações confidenciais, entre outros.

3.3 Requisitos de criptografia

Á prática de uma boa criptografia é essencial quando se trata de proteger dados armazenados no smartphone. Sendo assim, o objetivo deste requisitos nesta categoria é garantir que a aplicação pratica as melhores práticas criptográficas do setor, tais como, o uso de bibliotecas criptográficas comprovadas, a escolha adequada de primitivas criptográficas e um gerador de números aleatórios adequado sempre que foi necessário.

Alguns exemplo de requisitos desta categoria temos: a aplicação tem de usar criptografias primitivas comprovadas, a aplicação não pode só conter criptografia simétrica como único método de criptografia, entre outros.

3.4 Requisitos de autenticação e gestão de sessões

O login do utilizador num dispositivo remoto é, na maioria dos casos, uma parte importante da arquitetura geral das aplicações móveis. Enquanto grande parte do raciocínio reside no terminal, o *MASVS* estabelece alguns critérios específicos para a gestão de contas e sessões dos utilizadores.

Alguns exemplos dos requisitos de verificação de segurança são: o terminal remoto termina a sessão existente quando o utilizador efetua o logout, uma política de password existe e é aplicada no terminal remoto, a aplicação informa o utilizador de todas as atividades de login com sua conta, entre outros.

3.5 Requisitos de comunicação de rede

O objetivo dos requisitos de comunicação é garantir que as informações compartilhadas entre a aplicação móvel e os terminais do serviço remoto sejam confidenciais e que mantenham a sua integridade. No mínimo, um dispositivo móvel precisa de configurar um canal criptografado e seguro com as configurações corretas para comunicação em rede usando o protocolo *TLS*. Medidas adicionais de defesa em profundidade, como a fixação de *SSL*, são necessárias para o nível dois ou superior.

Alguns exemplos dos requisitos de comunicação de rede são: os dados são criptografados na rede usando *TLS*, o canal seguro é usado de forma consistente em todo a aplicação, esta não depende de um único canal de comunicação inseguro (email ou SMS) para operações críticas, como inscrições e recuperação de contas, entre outros.

3.6 Requisitos de interação entre ambientes

O objetivo destes requisitos é garantir que a aplicação use *APIs* da plataforma e componentes padrão de maneira segura. Além disso, os controlos abrangem a comunicação entre aplicações (IPC). Alguns exemplos destes requisitos de interação entre ambientes são: a aplicação solicita apenas o conjunto mínimo de permissões necessárias, o *JavaScript* está desativado em *WebViews*, a menos que seja explicitamente necessário, a serialização de objetos, se houver, é implementada usando *APIs* de serialização segura, entre outros.

3.7 Qualidade do código e requisitos de configuração de compilação

3.7.1 Controlo

O objectivo deste controlo é assegurar que as condutas básicas de programação a nível de segurança são cumpridas durante a fase de desenvolvimento da aplicação e que os recursos de segurança oferecidos pelo compilador estejam ativados.

3.7.2 Requisitos de verificação de segurança

A aplicação tem de seguir os seguintes requisitos caso seja aplicado o nível **L1** como o **L2**

- A app é assinada com um certificado válido
- A app foi construída/desenvolvida em "release mode", ou seja, com settings apropriados para este modo, como por exemplo, não ser capaz de fazer debugg
- Símbolos de debugg foram removidos do "native binaries"
- Código de debugg foi removido, ou seja, a app não apresenta mensagens de erros para efeito de debugg
- A app apanha e lida com possíveis exceções
- Por default nega acesso a controlos de segurança quando estes lidam com erros de lógica
- O código não pode ser modificado, ou seja, a memória é alocada,libertada e usada de modo seguro.
- Recursos de segurança oferecidos pelo compilador tem de estar ativados, como por exemplo, stack protection, PIE support e reference counting.
- O Java bytecode tem de estar minified

3.7.3 Processo de verificação

O OWASP Mobile Security Testing Guide providencia detalhadamente instruções para verificação de todos os requisitos listados previamente assim como boas praticas para sistemas operativos mobile. Deste modo podemos comprovar que a qualidade do código, a nível de segurança, está a ser tido em conta e utilizar boas práticas para desenvolver uma melhor e mais segura aplicação.

3.8 Resiliência contra requisitos de engenharia reversa

3.8.1 Objetivos de controlo

Os requisitos que serão apresentados a seguir são medidas de protecção de software que são recomendadas a aplicações que trabalham com dados sensíveis ou funcionalidades e que caso exista algum leak destes dados possa pôr em risco os utilizadores e a reputação da aplicação.

Ter em conta que a falta de qualquer requisito não cria nenhuma vulnerabilidade à app, o objectivo dos requisitos será dificultar um atacante de conseguir fazer engenharia reversa à aplicação, não conseguindo obter dados ou modo de funcionamento da mesma.

Ao contrário de parâmetros anteriores estes não devem ser aplicados a qualquer app, devem sim ser aplicados consoante a sua necessitada. Para isso deve ser feito um estudo

que descreva qual o risco associado caso alguma modificação e/ou engenharia reversa seja executada sem autorização.

O MASVR-R tem o objectivo de adicionar protecção conta ameaças especificas, este tipo de controlo **não substitui** outro tipo de controlo (L1 e L2)

Para isto também aconselha-se um Threat model deve ser feito de modo a identificar o objectivo dos atacantes. .

Para os requisitos/medidas sejam eficientes a aplicação deve **pelo menos** obedecer/implementar todas as medidas associadas ao nível **MASVS-L1**

App Isolation

- A app providencia um teclado personalizado sempre que dados sensíveis sejam inseridos
- Uma UI personalizada para que seja apresentada dados sensíveis. A UI não deve depender de estruturas de dados imutáveis.

Impede Dynamic Analysi and Tampering

- A app implementa dois ou mais métodos de deteção de root e responde,caso detecte um root device, alertando o utilizador ou terminar a app
- A app detecta e reponde a *tampering*
- A app detecta a presença de ferramentas utilizadas para engenharia reversa, como por exemplo, code injection tools.
- A app detecta e responde caso seja executada num emulador
- A app detecta e responde caso exista alguma modificação da memoria do processo.

Device Binding

- A app deve implementar uma funcionalidade de "device binding"como por exemplo impressão digital de forma a tornar única no dispositivo

Impede Comprehension

- Se a arquitectura exigir que informações confidenciais sejam armazenadas no dispositivo, a app será executada apenas nas versões do sistema operativo e nos dispositivos que oferecem armazenamento de chaves suportadas por hardware

4 Conclusão

Em suma este trabalho permitiu obter o conhecimento, à qual o grupo desconhecia, sobre Mobile Application Security Verification Standard(MASVS).

Hoje em dia os smartphone tem um grande impacto na vida das pessoas, as aplicações utilizadas guardam, gerem e/ou tem/podem ter acesso a informações pessoais e sensíveis (e.x cartões de créditos), isto quer dizer que comprometer um smatphone implica ter livre acesso a esses dados/informações de uma pessoa, existe então uma necessidade de implementar sistema de proteção de Software.

Os objectivos das Mobile Application Security Verification Standard(MASVS) é oferecer guidlines e standarizar boas práticas e requisitos para desenvolver aplicações seguras.

Após ler sobre as MASVS o grupo obteve uma sensibilidade mais critica no âmbito de desenvolver código seguro, aprendendo que existem diferentes níveis de segurança para o desenvolvimento de uma app mobile (L1,L2 e R) e que estes devem ser implementados consoante a nossa aplicação e o tipo de dados que ela utiliza, além disto, o grupo tem agora conhecimento de que tipo de requisitos uma aplicação deve obedecer para poder por em prática o nível de segurança pretendido.

Para finalizar o grupo tem em conta que a protecção de software **nunca deve ser implementado com o objectivo de substituir técnicas de segurança** , o MASVR tem o intuito de acrescentar segurança à aplicação não substitui-la.