OWASP - Mobile Application Security Verification Standard (MASVS)

Engenharia de Segurança

João de Macedo - a76268
Nelson Gonçalves - a78173
João Aloísio - a77953

Introdução

- Evolução tecnológica
- Mais e novos riscos de segurança
- Proteção de dados
- Objetivo geral do *MASVS*

Mobile Application Security Verification Standard

- Uso de uma métrica
- Uso de um guia
- Base na aquisição

Modelo

- MASVS-L1
- MASVS-L2
- MASVS-R

MASVS-L1: Standard Security

- Requisitos mínimos de qualidade de código
- Interações com o ambiente do smartphone

MASVS-L2: Defense-in-Depth

- Segurança mais avançada
- Usado em aplicações que manipulam vários dados confidenciais

MASVS-R: Resiliency Against Reverse Engineering and Tampering

- Complemento para os outros níveis
- Específico para ataques do lado cliente

Tipos de verificação

- MASVS-L1: Todas as aplicações;
- MASVS-L1 + R: Aplicações de jogos;
- MASVS-L2: Aplicações de serviços;
- MASVS-L2 + R: Aplicações bancárias;

Categorias e requisitos

1. Requisitos de arquitetura, design e modelação de ameaças

Exemplos:

- Os dados confidenciais da aplicação do smartphone devem ser devidamente identificados
- Controlos de segurança devem ser aplicados no lado do cliente e no ponto remoto do serviço

2. Requisitos de armazenamento e privacidade de dados

Exemplos:

- Nenhum dado confidencial é guardado em logs do aplicativo
- A cache do teclado está desativada quando são entradas de texto que processam dados confidenciais

3. Requisitos de criptografia

Exemplos:

- A aplicação tem de usar criptografias primitivas comprovadas
- A aplicação não pode só conter criptografia simétrica como único método de criptografía

4. Requisitos de autenticação e gestão de sessões

Exemplos:

- A sessão existente é encerrada quando o utilizador faz o logout.
- Política de password.
- O utilizador é informado sobre toda a atividade de login com a sua conta.

5. Requisitos de comunicação de rede

Exemplos:

- Dados encriptados usando *TLS*.
- Certificado *X.509*.
- Autoridade de certificação.

6. Requisitos de interação entre ambientes

Exemplos:

- Solicitação de permissões necessárias.
- *JavaScript* desativado em *WebViews*.
- Serialização de objetos.

7. Qualidade do código e requisitos de configuração de compilação

Exemplos:

- A app é assinada com um certificado válido
- Código de debugg foi removido, ou seja, a app não apresenta mensagens de erros para e efeitos de debugg
- A app apanha e lida com possíveis exceções
- O código não pode ser modificado, ou seja, a memória é alocada, é 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

8. Resiliência contra requisitos de engenharia reversa (MASVR-R)

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.

Impedir Dynamic Analysi and Tampering:

- App implementa dois ou mais métodos de detecção de root
- 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 memória do processo.

8. Resiliência contra requisitos de engenharia reversa (MASVR-R)

Device Binding:

- A app deve implementar uma funcionalidade de "device binding"como por exemplo impressão digital

Impedir Comprehension:

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

Conclusão

- Smartphones armazenam muita informação sensível
- Mobile Application Security Verification Standard(MASVS) oferece guidelines e standariza boas práticas e requisitos para desenvolver aplicações segura
- Ter em conta que o MASVS não substitui técnicas de segurança

OWASP Mobile Application Security Verification Standard (MASVS)

Engenharia de Segurança

João de Macedo - a76268
Nelson Gonçalves - a78173
João Aloísio - a77953