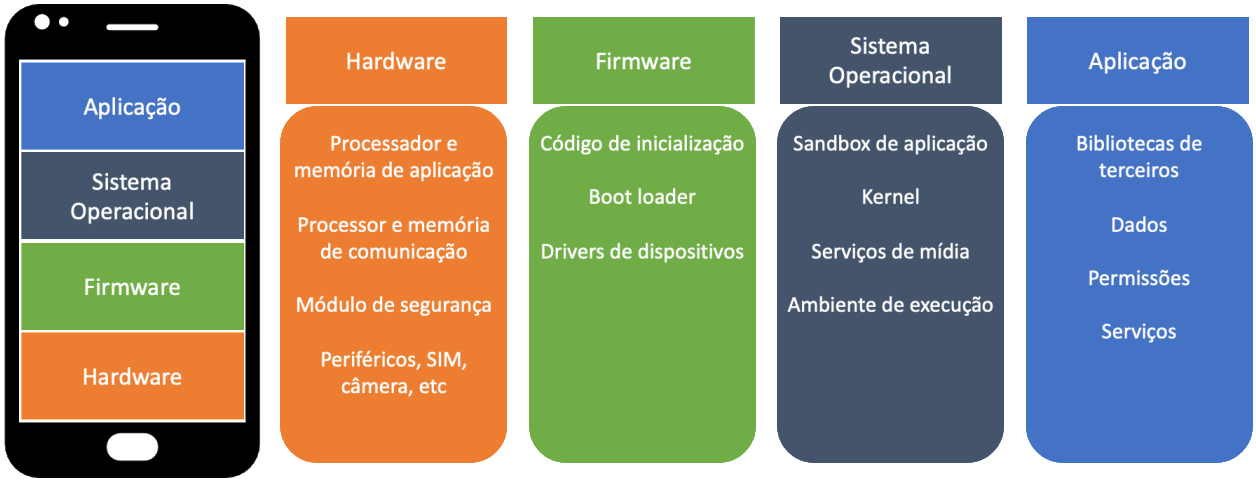
Ataques em dispositivos móveis

Em um dispositivo móvel há camadas e componentes que podem ser explorados em ataques: *hardware*, *firmware*, sistema operacional e aplicação

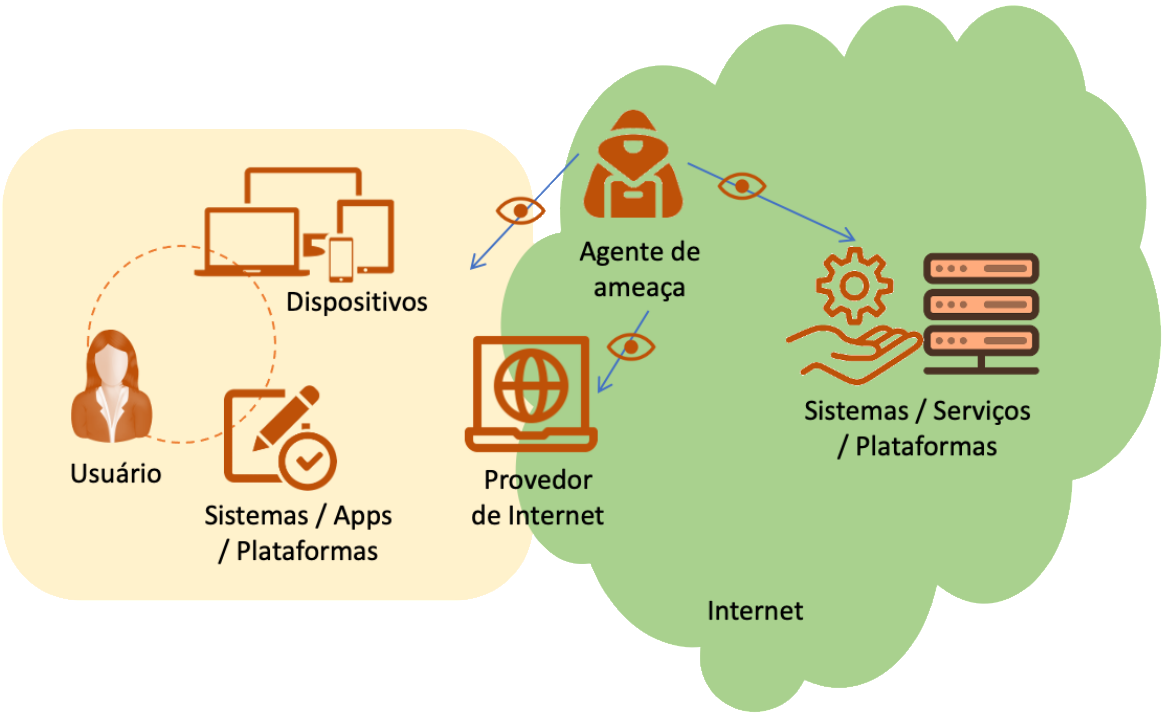
Componentes de dispositivos móveis



Fonte: adaptada de Franklin *et al.* (2020).

O foco aqui é na camada de aplicação, no desenvolvimento seguro dos aplicativos. Mas, pensando em um ambiente corporativo, o ataque pode acontecer em mais pontos.
No ambiente do usuário, há aquele usuário que pode sofrer ataques de *phishing*, além de ataques aos dispositivos (que podem ser roubados) e aos aplicativos, sistemas ou plataformas. Além desse ambiente do usuário, podem ser atacados os dados que trafegam pelo provedor de internet e a própria internet, além do ambiente da empresa, que se comunica com o usuário.

Pontos de ataques em um acesso a empresas



Fonte: elaborada pelo autor.

As 10 maiores vulnerabilidades em aplicativos móveis

Segundo a *Open Web Application Security Project* (OWASP), as 10 maiores vulnerabilidades em aplicativos móveis são as que são demonstradas a seguir e devem ser conhecidas pelos desenvolvedores para que não sejam incluídas em seus próprios aplicativos (OWASP, 2016) (KRIISTINA, 2019):

1. **Uso impróprio de plataforma**: uso incorreto de característica da plataforma ou falha no uso de controles de segurança da plataforma, como as permissões ou biometria:

Exemplo: devido a uma implementação equivocada de como um segredo era armazenado após o uso do *Touch* ID do iOS, era possível passar pela autenticação do aplicativo Citrix Worx. Com a implementação, bastava seguir os passos: reboot do dispositivo móvel; abrir o aplicativo; iniciar a autenticação, mas cancelar o *Touch* ID; fechar o aplicativo e abri-lo novamente; a autenticação estava feita. O aplicativo assumia que o usuário estava autenticado quando o processo era cancelado e o aplicativo reiniciado.

2. **Armazenamento de dados inseguro**: a proteção deve considerar um agente de ameaça que tem a posse física do dispositivo móvel, ou um *malware* ou outro aplicativo que é executado no dispositivo:

A proteção de arquivos pode ser insuficiente e o acesso a recursos de privacidade quando os dados são usados podem estar implementados incorretamente. É o que aconteceu com o Tinder no passado, que na primeira implementação, ao mostrar as pessoas próximas ao usuário, possibilitava a descoberta da exata localização. Na segunda implementação, o desenvolvedor mudou para o envio de distância ao invés de localização, mas ainda era possível descobrir a localização com a triangulação e uso de localização falsa.

3. **Comunicação insegura**: dados que trafegam em um modelo cliente-servidor podem ser interceptados em diferentes pontos, tais como uma rede de acesso comprometido, dispositivos do provedor de internet atacados ou por um *malware* no dispositivo móvel:

Exemplo: um relógio inteligente para crianças implementou incorretamente a comunicação e era possível o acesso ao dispositivo, com os resultados: descoberta da localização, chamada para a criança, criação de um canal de escuta sem o conhecimento da criança, envio da mensagem de áudio sem consentimento, acesso a dados da criança (foto, data de nascimento, nome, peso, altura).

4. **Autenticação insegura**: ataques que exploram vulnerabilidades de forma automatizada em busca de acessos:

Exemplo: um aplicativo implementou incorretamente a autenticação de dois fatores, permitindo o ataque de força bruta.

5. **Criptografia insuficiente**: a proteção deve considerar um agente de ameaça que tem a posse física do dispositivo móvel, ou um *malware* ou outro aplicativo que é executado no dispositivo:

Exemplo: “PRODKEYPRODKEY12” era a chave criptográfica utilizada em um aplicativo, que estava no próprio código-fonte, em formato decimal. Descoberta a chave, que era utilizada também para cifrar as senhas dos usuários, era possível acessar contas de qualquer usuário. Havia problemas também na forma como a segurança da camada de transporte era implementada, bem como a verificação de certificados digitais SSL.

6. **Autorização insegura:** ataques que exploram vulnerabilidades de forma automatizada em busca de acessos:

Exemplo: Um carro inteligente teve o seu acesso remoto implementado com autorização insegura, que permitia que, após o acesso ao servidor, a identificação do usuário pudesse ser modificada e outro carro pudesse ser acessado.

7. **Má qualidade de código**: a proteção deve considerar agentes de ameaça que podem utilizar entradas não confiáveis para as chamadas do código, que podem levar à execução de códigos arbitrários:

As vulnerabilidades 0-*day* surgem muitas vezes da má qualidade de código. O *buffer overflow* é um exemplo em que o uso da memória não é gerenciado e permite a execução de códigos arbitrários. É o que aconteceu com o WhatsApp, onde códigos arbitrários podiam ser executados a partir do envio de um conjunto de pacotes junto com uma ligação.

8. **Modificação de código**: a exploração pode ser pelo uso de fontes de aplicativos de terceiros que hospedam os códigos modificados, ou pela instalação pelo usuário vítima de *phishing:*

Envolvem também a modificação do binário, modificação dinâmica de memória ou *hooking* de métodos. É o que foi explorado para burlar algumas regras do jogo Pokemon Go.

9. **Engenharia reversa**: o atacante analisa o aplicativo com a ajuda de diversas ferramentas para entender e explorar as funções:

É a técnica utilizada para analisar o código-fonte, bibliotecas e algoritmos, podendo levar à descoberta de propriedade intelectual, uso de criptografia e suas chaves, e informações sobre servidores e *backend*.

10. **Funcionalidade exposta**: a exposição em aplicativos pode relevar funcionalidades de sistemas de *backend*, que pode então ser explorada diretamente:

Mesmo *backdoors* podem ser inseridas sem intenção, como ocorreu com um aplicativo de troca de arquivos, que permitia conexões remotas sem nenhuma autenticação.

Referências

- KRISTIINA. **OWASP mobile top 10 security risks explained with real world examples**. The Startup, 17 maio 2019.
- OWASP. **OWASP Mobile Top 10**.