TRAINNING
EDUCATION CENTER

Curso:

(C|EH) V12

CERTIFIED ETHICAL HACKER - SECURITY IMPLEMENTATION

Progresso do curso

Módulo 16. Hacking Wireless Networks

Módulo 17. Hacking Mobile Applications

Módulo 18. IoT & OT Hacking

Módulo 19. Cloud Computing

Módulo 20. Cryptography

Conceitos de Aplicações Mobile:

As aplicações mobile lidaram com muitas ameaças de segurança internas e externas nos últimos anos.

Até certo ponto, estudos e pesquisas de organizações empresariais desenvolveram e promoveram as melhores práticas para lidar com este problema crescente. A maioria dos dispositivos móveis tem mensagens baseadas na Internet, URL, e-mail e opções de download de aplicativos. Apesar dos avanços na tecnologia, os hackers continuam a utilizá-los para fins maliciosos.

CEHv12 (ANSI)

17.Hacking Mobile Applications

Vetores de ataques

Malware:

- Vírus e rootkit
- Modificação de aplicativo
- Modificação de SO

Exfiltração de Dados:

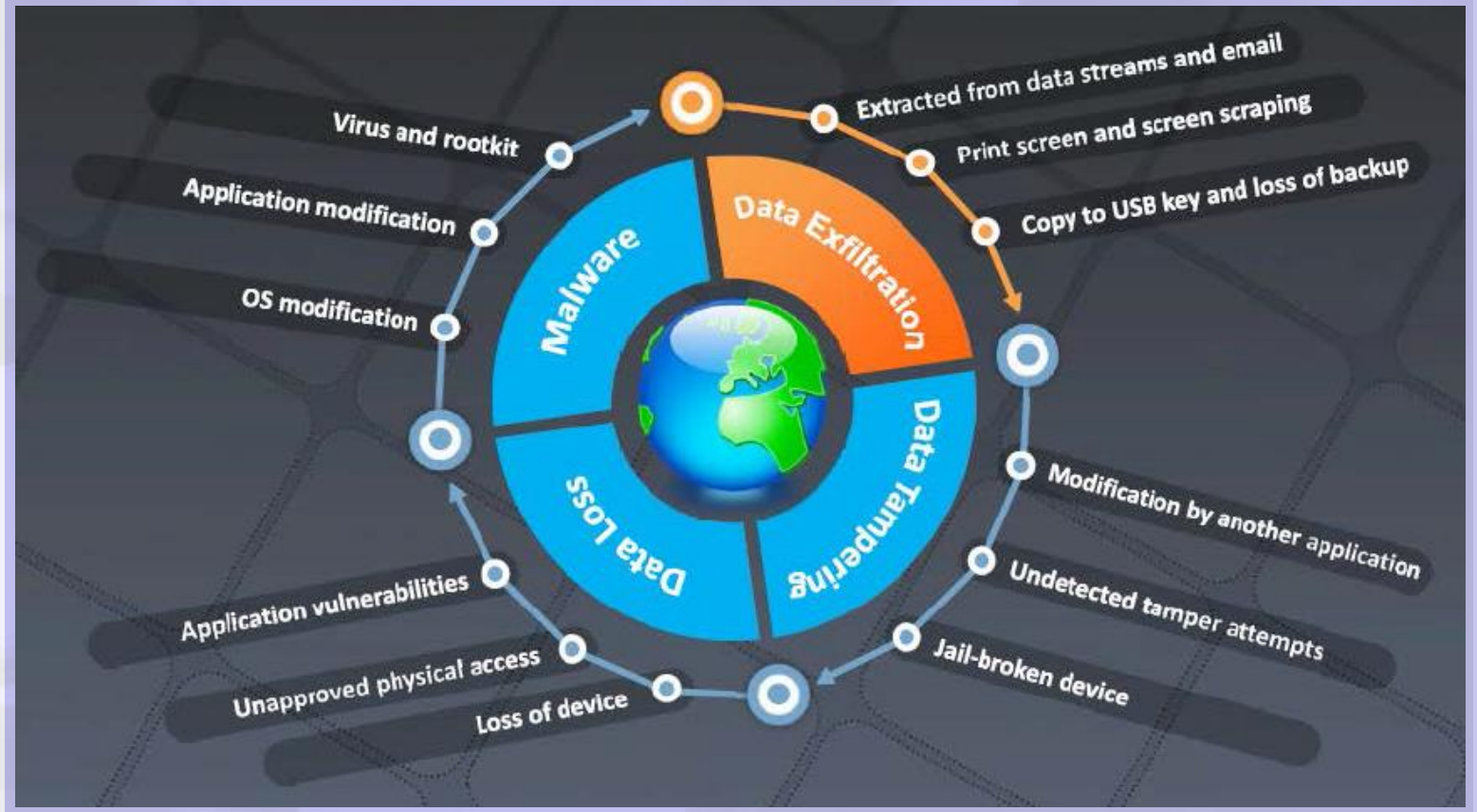
- E-mail
- Print screen
- Copia para USB e perda de backup

Adulteração de dados:

- Modificação por outro aplicativo
- Tentativas de adulteração não detectadas
- Dispositivo Jail-broken

Perda de dados:

- Vulnerabilidades de aplicativos
- Acesso físico não autorizado
- Perda de dispositivo



Resumo da tecnologia

Todos nós vimos como o rápido aumento de usuários de telefones celulares, a flexibilidade de funções e o avanço na execução de tarefas trouxeram uma mudança dramática na tecnologia.

Os smartphones atualmente disponíveis são executados em sistemas operacionais populares, como iOS, Blackberry OS, Android, Symbian e Windows, etc.

Eles também oferecem lojas de aplicativos, por exemplo, App Store da Apple e Play Store do Android - onde os usuários podem baixar aplicativos compatíveis e confiáveis para serem executados em seus respectivos sistemas operacionais.

Embora os telefones celulares sejam uma fonte de entretenimento e tenham se tornado uma ferramenta para realizar tarefas pessoais e profissionais, eles também são vulneráveis.

Um smartphone infectado com um aplicativo malicioso pode causar problemas para uma rede segura.

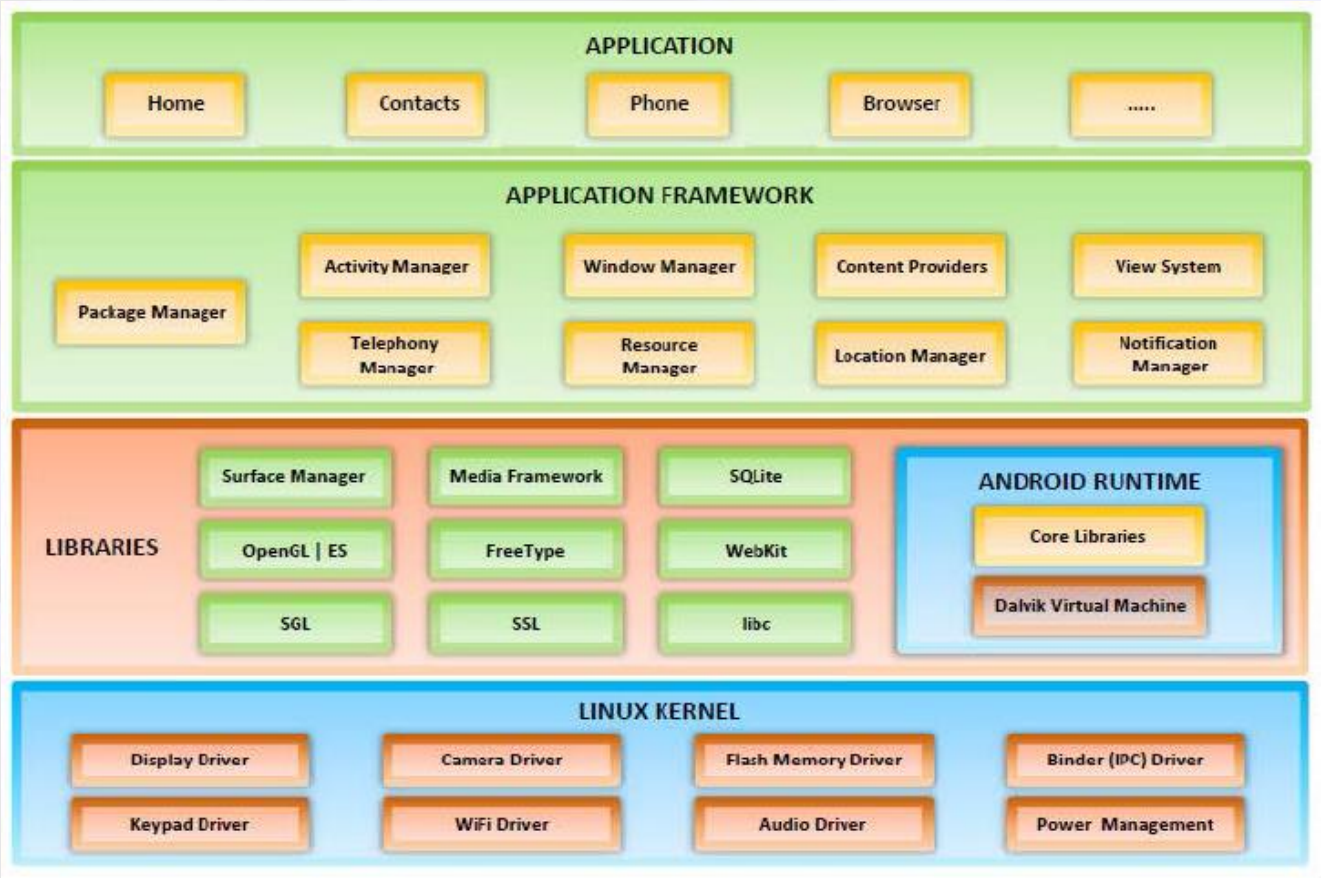
Como os telefones celulares agora são utilizados regularmente para transações financeiras on-line (através de aplicativos bancários, por exemplo), os dispositivos devem ter segurança forte, garantindo que as transações permaneçam seguras e confidenciais.

Da mesma forma, os celulares contêm dados importantes, como contatos, mensagens, e-mails, credenciais de login e arquivos que podem ser roubados facilmente quando o telefone é comprometido.

Android OS

Android é uma pilha de software desenvolvida pelo Google especificamente para dispositivos móveis, como smartphones e tablets. Ele é constituído por um sistema operacional, middleware e aplicações. O sistema operacional móvel Android é baseado no kernel do Linux. O aplicativo Android é executado em uma sandbox.

Software antivírus como o Lookout Mobile Security, AVG Technologies e McAfee são liberados por empresas de segurança para dispositivos Android. No entanto, a sandbox é também aplicável ao software antivírus. Como resultado, embora este software antivírus tem a capacidade de fazer a varredura do sistema completo, é limitado a escanear um determinado ambiente.



*** middleware** é o software que serve como ponte de comunicação entre o sistema operacional e as funções de um aplicativo. Servidores de aplicativos, softwares de mensagem, bancos de dados e monitores de processamento de transação são alguns exemplos de middlewares.

Android Rooting

Rooting é o processo de remoção das limitações e permite acesso total. Ele permite que os usuários do Android atinjam o controle privilegiado (conhecido como "acesso root") e a permissão dentro do subsistema do Android. Após o rooting do Android, um usuário terá controle sobre configurações, recursos e desempenho do seu telefone e pode até mesmo instalar um software que não é suportado pelo dispositivo.

O Rooting é basicamente hackear dispositivos Android e é equivalente ao "jailbreaking" no iPhone. O Rooting explora uma vulnerabilidade de segurança no firmware do dispositivo, e copia o binário su para um local no caminho atual do processo (/system/xbin/su) e concede permissões de execução com o comando chmod.

O Rooting permite que todos os aplicativos instalados pelo usuário executem comandos privilegiados, tais como:

- Modificar ou excluir arquivos de sistema, módulos, ROMs e kernels
- Remoção de aplicativos instalados pelo fabricante
- Acesso de baixo nível ao hardware que são tipicamente indisponíveis para os dispositivos em sua configuração padrão
- Desempenho melhorado
- Instalar aplicativos no cartão SD
- Melhor interface de utilizador e teclado

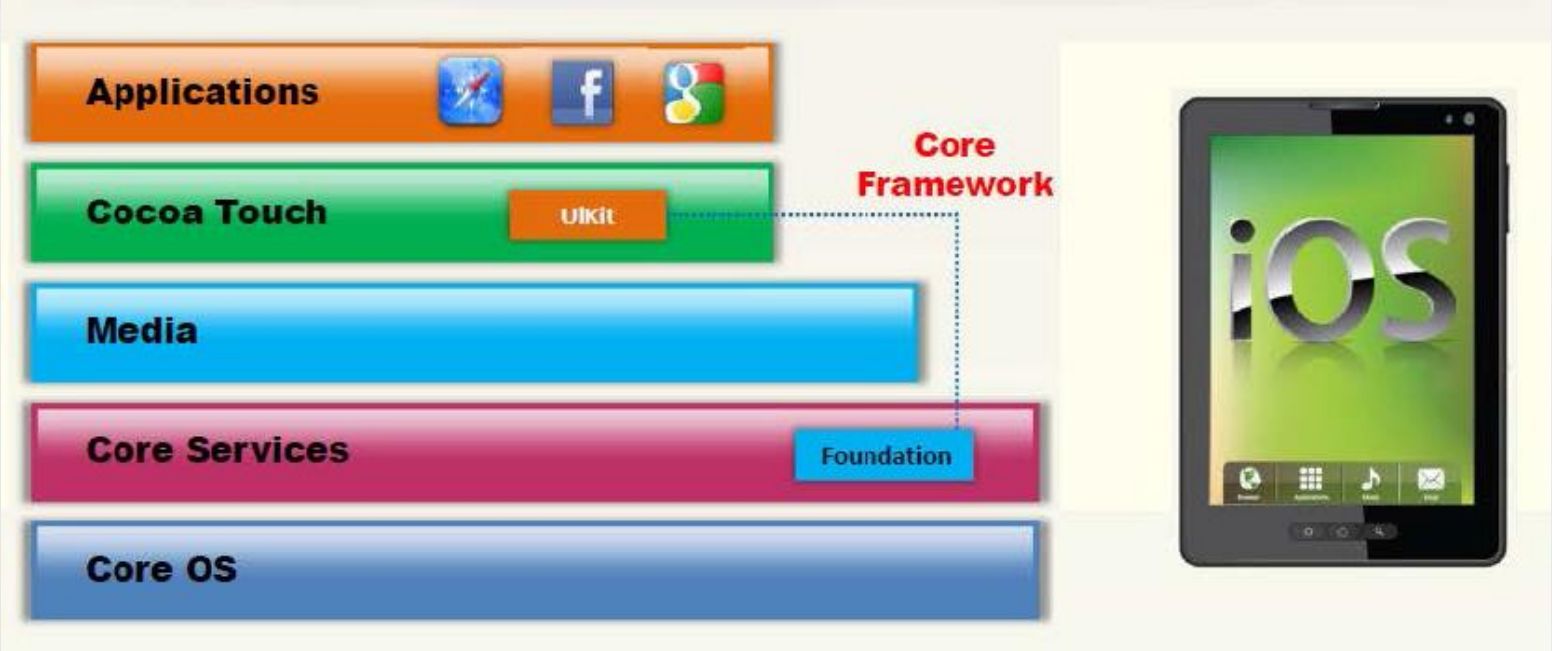
O Rooting também vem com muitos problemas de segurança e outros riscos para o dispositivo, incluindo:

- Anula a garantia do seu telefone
- Desempenho fraco
- Infecção de malware

Jailbreaking iOS

Jailbreaking, como o rooting, também vem junto com problemas de segurança e outros riscos para o seu dispositivo, incluindo:

- Anula a garantia do seu telefone
- Enfraquece o desempenho
- Infecção por malware



Windows Phone 8

Ele permite dispositivos com telas maiores e processadores multi-core até 64 núcleos.

Núcleo de compartilhamento Windows confiável e suporte melhorado para armazenamento removível.

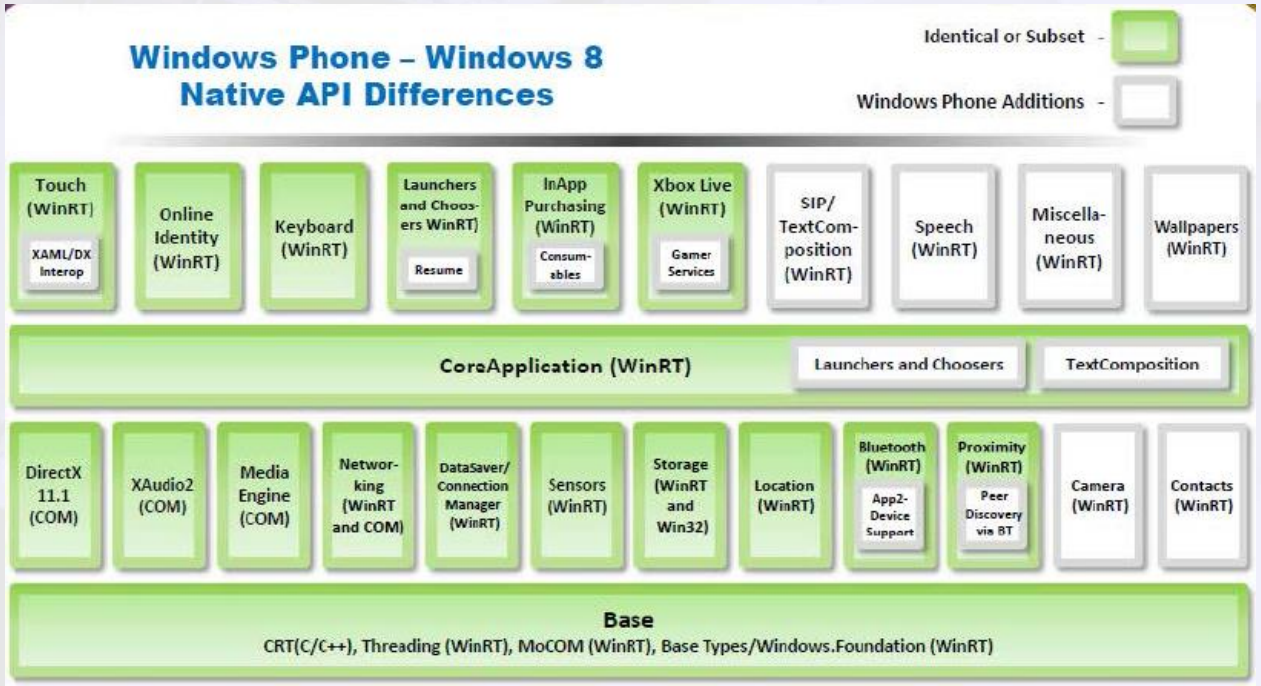
Principais componentes do Windows 8, incluindo kernel, sistema de arquivos, driver's, pilha de rede, componentes de segurança, de mídia e suporte a gráficos.

Internet Explorer 10, tecnologia Nokia mapa e fundo multitarefa.

Suporta Near Field Communication (NFC), incluindo o pagamento e compartilhamento de conteúdo com o Windows Phone 8 e máquinas Windows 8.

Suporta código nativo (C e C ++), simplificou a portabilidade de plataformas como o Android, Symbian e iOS.

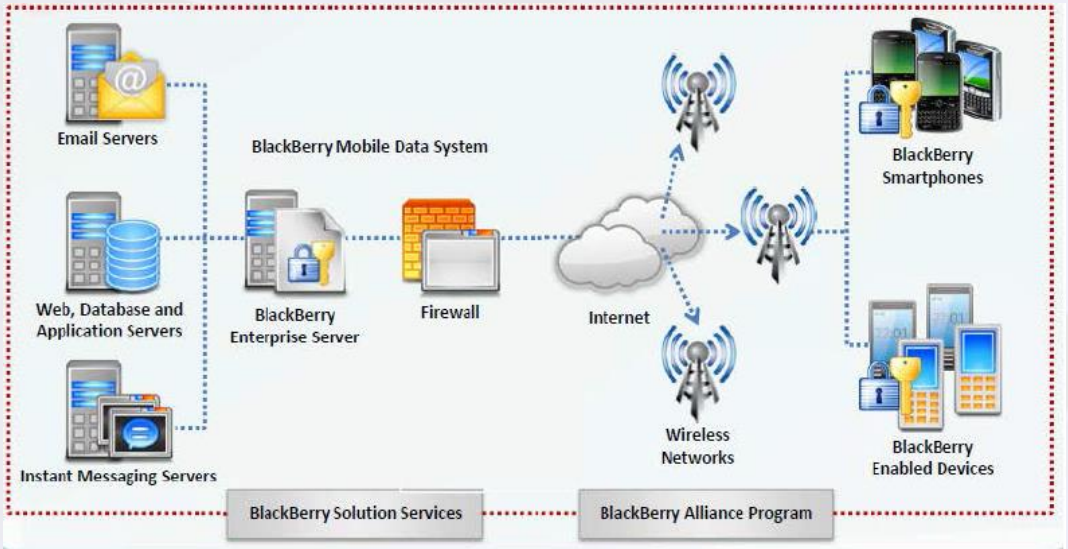
Criptografia nativa Bitlocker de 128 bits e gerenciamento remoto de dispositivos do Windows Phone.



BlackBerry

BlackBerry OS é um sistema operacional móvel proprietário desenvolvido pela Research In Motion (RIM) para sua linha BlackBerry de smartphones e dispositivos portáteis. Ele inclui um quadro baseado em Java que implementa o J2ME Mobile Information Device Profile v2 (MIDPZ) e Connected Limited Device Configuration (CLDC), bem como uma série de APIs RIM. Algumas das características de BlackBerry incluem:

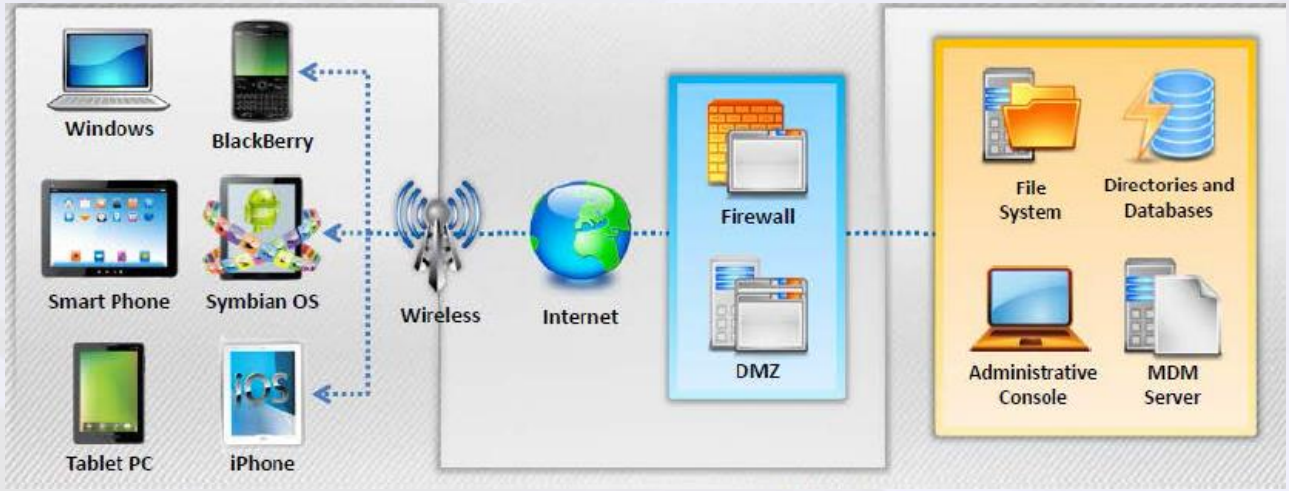
- O suporte nativo para e-mail corporativo
- BlackBerry Enterprise Server
- Mensageiro BlackBerry
- Serviço de Internet BlackBerry
- Cliente de e-mail BlackBerry



Mobile Device Management - MDM

Mobile Device Management é um componente vital que monitora, guarda, gerencia e oferece suporte a diferentes tipos de dispositivos e tablets móveis, incluindo iPhone, iPad, Android e BlackBerry, junto com as aplicações que rodam sobre eles. Ele monitora todos os dispositivos móveis com sistema operacional diferente, como o Android, Windows e Symbian móvel.

Com a ajuda do MDM, as políticas da empresa podem ser facilmente implementadas para reduzir os custos de suporte, tempo e ameaças comerciais e de segurança. O MDM pode reduzir custos de suporte e pode minimizar as ameaças de negócio controlando todo o ambiente de dados e configuração de todos os dispositivos móveis na rede.



Top 10 Mobile Risks

M1: Uso Indevido da Plataforma

Esta categoria abrange o uso indevido de um recurso da plataforma ou a falha no uso dos controles de segurança da plataforma. Pode incluir intenções do Android, permissões de plataforma, uso indevido do TouchID, do Keychain ou algum outro controle de segurança que faça parte do sistema operacional móvel.

Os vetores de ataque correspondem aos mesmos vetores de ataque disponíveis através do tradicional OWASP Top Ten. Qualquer chamada de API exposta pode servir como vetor de ataque aqui.

Para que essa vulnerabilidade seja explorada, a organização deve expor um serviço da Web ou uma chamada de API consumida pelo aplicativo móvel. O serviço exposto ou chamada de API é implementado utilizando técnicas de codificação inseguras que produzem uma vulnerabilidade OWASP Top Ten dentro do servidor. Por meio da interface móvel, um adversário pode enviar entradas maliciosas ou sequências inesperadas de eventos para o endpoint vulnerável. Portanto, o adversário percebe a vulnerabilidade OWASP Top Ten original no servidor.

M2: Armazenamento de dados inseguro

No caso de um adversário atingir fisicamente o dispositivo móvel, o adversário conecta o dispositivo móvel a um computador com software disponível gratuitamente. Essas ferramentas permitem que o adversário veja todos os diretórios de aplicativos de terceiros que geralmente contêm informações de identificação pessoal (PII) armazenadas ou outros ativos de informações confidenciais. Um adversário pode construir malware ou modificar um aplicativo legítimo para roubar tais ativos de informação.

As vulnerabilidades de armazenamento de dados inseguros ocorrem quando as equipes de desenvolvimento assumem que os usuários ou o malware não terão acesso ao sistema de arquivos de um dispositivo móvel e às informações confidenciais subsequentes nos armazenamentos de dados do dispositivo. Os sistemas de arquivos são facilmente acessíveis. As organizações devem esperar que um usuário mal-intencionado ou malware inspecione os armazenamentos de dados confidenciais. O uso de bibliotecas de criptografia ruins deve ser evitado.

Top 10 Mobile Risks

M3: Comunicação Insegura

Ao projetar um aplicativo móvel, os dados geralmente são trocados de maneira cliente-servidor. Quando a solução transmite seus dados, ela deve passar pela rede da operadora do dispositivo móvel e pela internet. Os agentes de ameaças podem explorar vulnerabilidades para interceptar dados confidenciais enquanto eles trafegam pela rede. Existem os seguintes agentes de ameaça:

- Um adversário que compartilha sua rede local (Wi-Fi comprometido ou monitorado);
- Operadora ou dispositivos de rede (roteadores, torres de celular, proxy's, etc); ou
- Malware em seu dispositivo móvel.

M4: autenticação insegura

Agentes de ameaças que exploram vulnerabilidades de autenticação normalmente o fazem por meio de ataques automatizados que usam ferramentas disponíveis ou personalizadas.

Depois que o adversário entende como o esquema de autenticação é vulnerável, ele falsifica ou ignora a autenticação enviando solicitações de serviço ao servidor de back-end do aplicativo móvel e ignora qualquer interação direta com o aplicativo móvel. Esse processo de envio geralmente é feito por meio de malware móvel no dispositivo ou botnets pertencentes ao invasor.

Top 10 Mobile Risks

M5: Criptografia insuficiente

Os agentes de ameaça incluem o seguinte: qualquer pessoa com acesso físico a dados criptografados incorretamente ou malware móvel agindo em nome de um adversário.

Os vetores de ataque correspondem aos mesmos vetores de ataque disponíveis através do tradicional OWASP Top Ten. Qualquer chamada de API exposta pode servir como vetor de ataque aqui.

M6: Autorização insegura

Agentes de ameaças que exploram vulnerabilidades de autorização geralmente o fazem por meio de ataques automatizados que usam ferramentas disponíveis ou personalizadas.

Assim que o adversário entender como o esquema de autorização é vulnerável, ele fará login no aplicativo como um usuário legítimo. Eles passam com sucesso no controle de autenticação. Após a autenticação, eles normalmente forçam a navegação para um ponto de extremidade vulnerável para executar a funcionalidade administrativa. Esse processo de envio geralmente é feito por meio de malware móvel no dispositivo ou botnets pertencentes ao invasor.

Top 10 Mobile Risks

M7: Qualidade de código ruim

Agentes de ameaças incluem entidades que podem passar entradas não confiáveis para chamadas de método feitas no código móvel. Esses tipos de problemas não são necessariamente problemas de segurança em si, mas levam a vulnerabilidades de segurança. Por exemplo, estouros de buffer em versões mais antigas do Safari (uma vulnerabilidade de baixa qualidade de código) levaram a ataques Jailbreak drive-by de alto risco. Problemas de baixa qualidade de código são normalmente explorados por meio de golpes de malware ou phishing.

Um invasor normalmente explorará as vulnerabilidades nessa categoria fornecendo entradas cuidadosamente elaboradas para a vítima. Essas entradas são passadas para o código que reside no dispositivo móvel onde ocorre a exploração. Tipos típicos de ataques exploram vazamentos de memória e estouros de buffer.

M8: Adulteração de código

Normalmente, um invasor explora a modificação de código por meio de formas maliciosas dos aplicativos hospedados em lojas de aplicativos de terceiros. O invasor também pode induzir o usuário a instalar o aplicativo por meio de ataques de phishing.

Normalmente, um invasor fará o seguinte para explorar essa categoria:

- Realizar alterações diretas no binário principal do pacote do aplicativo
- Realizar alterações diretas nos recursos dentro do pacote do aplicativo
- Redirecionar ou substituir APIs do sistema para interceptar e executar códigos estrangeiros maliciosos.

Top 10 Mobile Risks

M9: Engenharia Reversa

Um invasor normalmente baixa o aplicativo de destino de uma loja de aplicativos e o analisa em seu próprio ambiente local utilizando um conjunto de ferramentas diferentes.

Um invasor deve realizar uma análise do binário principal final para determinar sua tabela de string original, código-fonte, bibliotecas, algoritmos e recursos incorporados ao aplicativo. Os invasores usarão ferramentas relativamente acessíveis e bem compreendidas, como IDA Pro, Hopper, otool, strings e outras ferramentas de inspeção binária de dentro do ambiente do invasor.

M10: Funcionalidade Estranha

Normalmente, um invasor procura entender a funcionalidade estranha em um aplicativo móvel para descobrir a funcionalidade oculta nos sistemas de back-end. O invasor normalmente explora funcionalidades estranhas diretamente de seus próprios sistemas, sem qualquer envolvimento dos usuários finais.

Um invasor fará o download e examinará o aplicativo móvel em seu próprio ambiente local. Eles examinarão arquivos de log, arquivos de configuração e talvez o próprio binário para descobrir quaisquer opções ocultas ou código de teste que foi deixado para trás pelos desenvolvedores. Eles explorarão essas opções e funcionalidades ocultas no sistema de back-end para realizar um ataque.

Obrigado!

“QUEM NÃO SABE O QUE PROCURA, NÃO PERCEBE QUANDO ENCONTRA”.