SoK: Lessons Learned From Android Security Research For Appified Software Platforms

Rodrigo de Lima (rlo)
Valdemiro Vieira (vrvs)

Roteiro

1. Introdução
2. Metodologia
3. Problema e Áreas de Pesquisa
4. Android / Ecossistemas baseados em Aplicativos
5. Sistematização das Áreas de Pesquisa em Ecossistemas baseados em Apps
6. Conclusão

1. Introdução

- Ascensão de aplicativos mobile
- Barreira de mercado baixa
- Literatura mostra desafios e soluções para área
- Esforços fragmentados

2. Metodologia

- Contribuições feitas em diferentes áreas
- Criar um entendimento comum
- Interação entre agentes
- Áreas que tem recebido atenção e sub representadas
- Tanto trabalhos atacantes como defensivos
- Excluído trabalhos com hardware

2. Metodologia

Critérios para selecionar trabalhos:

- Unicidade/Pioneirismo
- Agravados
- Atenção
- Impacto
- Escopo
- Desafios abertos

3. Problemas e Áreas de Pesquisa

Sistemas tradicionais de software vs. plataformas baseadas em apps

- Acesso a recursos
  - Protagonistas do sistema de segurança
  - Monitor de referência
  - Política de segurança

3. Problemas e Áreas de Pesquisa

Sistemas tradicionais de software vs. plataformas baseadas em apps

- Compartilhamento de funcionalidades
  - ICC
- Distribuição do software
  - Descentralizado vs. centralizado
- Engenharia de Software
  - Processo de desenvolvimento
  - Ambiente de programação

3. Problemas e Áreas de Pesquisa

Sistemas tradicionais de software vs. plataformas baseadas em apps

- Erros de programação
  - Mau uso das APIs de programação
- Webficação
  - Alto uso
- Atualização de software
  - Apps vs. S.O.

4. Android / Ecossistemas baseados em Apps

Visão global do sistema

- Número de desenvolvedores Android grande
  - 460.000 diferentes contas
- Muitos apps se conectam a serviços web
- Monetização
  - Vender apps
  - Redes de anúncios
  - Compras no app
- ICC
  - Android permite e encoraja

4. Android / Ecossistemas baseados em Apps

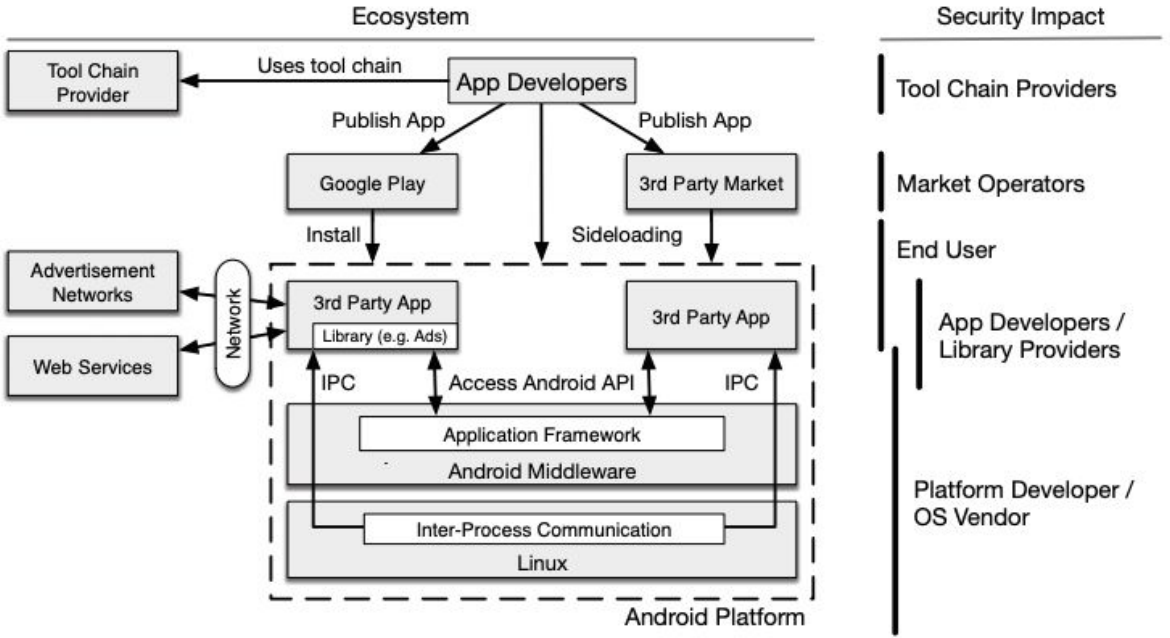

Fig. 1. The Android ecosystem: Actors and their impact on the ecosystem's security.

4. Android / Ecossistemas baseados em Apps

Agentes envolvidos

- Desenvolvedores da plataforma
  - Fornece o Android
  - Tomam decisões básicas de sistema e segurança
- Fabricantes de dispositivos
  - Customização do Android
  - Podem adotar decisões de segurança ou adotar próprias

4. Android / Ecossistemas baseados em Apps

Agentes envolvidos

- Fornecedores de Bibliotecas
  - Fornecer novas features
  - Facilitar o uso das existentes
- Desenvolvedores de Apps
  - Poderiam fazer contribuições essenciais para segurança
  - Fazem escolhas não seguras

4. Android / Ecossistemas baseados em Apps

Agentes envolvidos

- Fornecedores de ferramentas
  - Análise de código
  - Corrigir fraquezas
- Publicadores de Aplicativos
  - Ajudam desenvolvedores a publicar apps
  - Podem rodar análises de código e reportar bugs

4. Android / Ecossistemas baseados em Apps

Agentes envolvidos

- Lojas de Aplicativos
  - Podem rodar diferentes técnicas de análise de segurança
  - Não rodam análises profundas
- Usuários
  - Podem tomar decisões seguras
  - Impacto de único usuário é negligenciável

4. Android / Ecossistemas baseados em Apps

TABLE I
ALL ACTORS IN THE ECOSYSTEM AND THE IMPACT OF THEIR SECURITY DECISIONS ON THE REMAINING ACTORS.

Actor	OS Developer	Hardware Vendor	Library Provider	Software Developer	Toolchain Provider	Software Publisher	Software Market	End User
OS Developer	■	◐	●	●	◐	●	●	●
Hardware Vendor	○	■	●	●	○	○	○	●
Library Provider	○	○	■	●	○	○	○	●
Software Developer	○	○	◐	■	○	○	○	●
Toolchain Provider	○	○	○	●	■	○	○	◐
Software Publisher	○	○	◐	◐	○	■	◐	●
Software Market	○	○	◐	◐	○	○	■	●
End User	○	○	○	○	○	○	○	■

● = fully applies; ◐ = partly applies, ○ = does not apply at all.

4. Android / Ecossistemas baseados em Apps

Modelo de ataque global

- Permissões perigosas
  - Acesso a dados sensíveis, controlar o dispositivo
  - Permissões normais apresentam baixo risco
- Múltiplos aplicativos
  - Dois aplicativos ou mais apresentam alto risco
  - Um só apresenta risco mais baixo

4. Android / Ecossistemas baseados em Apps

Modelo de ataque global

- Piggybacking apps
  - Reempacotamento de apps
  - Código que é injetado nos apps (bibliotecas)
- Carregamento dinâmico de código
  - Carregar código em tempo de execução
  - Injetar código em outro

4. Android / Ecossistemas baseados em Apps

Modelo de ataque global

- Ataques de Rede
  - Modificar/interromper/forjar a comunicação wi-fi ou de rede móvel
  - Escutar o canal de comunicação

5. Sistematização das áreas de pesquisa

- Permissões (permission evaluation)
  - Compreensão das permissões
    - Por parte do usuário
    - Por parte dos desenvolvedores

5. Sistematização das áreas de pesquisa

- Revolução das permissões(permission revolution)
  - Separação das permissões ausentes
  - Aplicativos de segurança ineficazes
  - Falta de suporte ao controle de acesso obrigatório

5. Sistematização das áreas de pesquisa

- Vazamentos induzidos por programação(programming-induced Leaks)
  - APIs complexas e com fraca documentação
  - Falta de empenho (técnico e tempo)

5. Sistematização das áreas de pesquisa

- Webfication
  - Tendência para os desenvolvimento
  - Vulnerabilidades herdadas

5. Sistematização das áreas de pesquisa

- Mecanismo de atualização (Software Update Mechanism
  - 20.400 dispositivos - 87% apresenta vulnerabilidades
  - Complexidade -> Problemas com permissões

6. Conclusão

- Historia de vitorias e derrotas
- Muito já foi feito

Obrigado
Perguntas?

Rodrigo de Lima (rlo)
Valdemiro Vieira (vrvs)