Universidade Federal de Pernambuco
Graduação em Ciência da Computação
Centro de Informática
2016.1

Detecção incremental de comunicação entre componentes Android com base em informação imprecisa

---

Proposta de Trabalho de Graduação

Aluno: João Paulo Tenório Trindade (jptt@cin.ufpe.br)
Orientador: Leopoldo Motta Teixeira (lmt@cin.ufpe.br)

Recife, 15 de Abril de 2016

Sumário

1. Contextualização

No último trimestre de 2015 o Android alcançou 80.7% das vendas no mercado de dispositivos móveis, segundo pesquisa realizada pela Gartner [1]. E boa parte desse percentual pode ser atribuída a enorme variedade encontrada na Google Play Store, que alcançou a marca dos 2 milhões aplicativos disponíveis no começo de 2016 [2].

Os aplicativos nessa plataforma são compostos por blocos básicos chamados de componentes [3]. São eles: *Activity, Service, Content Provider e Broadcast Receiver*. Essa estrutura com base em componentes provê flexibilidade, reuso, compartilhamento de dados e funcionalidades, possibilitando assim a comunicação entre eles e, por fim, entre aplicações. A comunicação entre *Activities, Services e Broadcast Receivers* de aplicações diferentes, ou não, acontece por meio do envio e recebimento de mensagens assíncronas [3], chamadas de *Intents*.

As *Intents* são usadas para ativar componentes e isso acontece, basicamente, de duas formas: explicitamente ou implicitamente. Uma *Intent* explícita deve especificar qual componente será o recipiente da mensagem, isto é, ela declara o nome do componente alvo. Enquanto que uma *Intent* implícita não declara o nome do seu receptor, mas define uma ação a ser executada, e desta forma permite que componentes desconhecidos a trate [4].

Com o fluxo de dados entre componentes de aplicações diferentes surge a possibilidade de vazamento de informações. Isso acontece quando aplicativos maliciosos expõem intencionalmente alguma informação ou se aproveitam de um outro aplicativo “ingênuo” que envia informações sensíveis através de *Intents* implícitas. O vazamento de informações sensíveis em aplicações Android na comunicação entre componentes é também conhecida por *Component Hijacking* [5].

Algumas ferramentas, como Epicc [6] e IC3 [7], foram desenvolvidas para detecção de comunicação entre componentes (ou ICC, do inglês *inter-component communication*). Entretanto, elas possuem limitações quanto a escalabilidade [8] e, em particular, no contexto de Android onde nem sempre o fluxo de comunicação é definido explicitamente e, como já citado anteriormente, acontece com envio e recebimento de *Intents* implícitas, que em alguns casos podem ser resolvidas apenas em tempo de execução.

Portanto, com as soluções atuais, quando um usuário instala novos aplicativos e remove outros, é necessário executar uma nova análise, muitas vezes bastante custosa, incluindo todos os aplicativos anteriormente checados, a cada nova verificação.

No entanto, existem casos onde há interesse de se realizar analises de aplicativos individualmente e também na possibilidade de combinar incrementalmente os resultados para identificação da comunicação entre componentes de fontes distintas, sendo este um primeiro passo para futura análises de fluxo de dados entre aplicativos no Android.

2. Objetivos

O objetivo deste trabalho é desenvolver um ambiente que seja capaz de identificar de forma incremental a comunicação entre componentes de aplicações na plataforma Android. Incremental neste caso significa combinar os resultados individuais de cada aplicativo sem a necessidade de realizar nova análise quando se deseja testar uma nova aplicação.

Serão consideradas informações extraídas a partir de coletas de dados de *Intents* e para tais coletas serão utilizadas algumas ferramentas específicas [5-7] disponíveis atualmente.

3. Cronograma

Atividade	Março	Abril	Maio	Junho	Julho
Revisão da literatura e Elaboração da proposta	x	x			
Implementação da ferramenta		x	x	x	
Análise de resultados			x	x	
Elaboração de relatório final			x	x	x
Defesa					x

Tabela1 - Cronograma de Trabalho de Graduação

4. Possíveis Avaliadores

- Paulo Borba (phmb@cin.ufpe.br)
- Fernando Castor (castor@cin.ufpe.br)

5. Referências

[1] **Gartner Says Worldwide Smartphone Sales Grew 9.7 Percent in Fourth Quarter of 2015**. Disponível em: <http://www.gartner.com/newsroom/id/3215217> Acesso em 16 de Abril.
[2] **Number of available applications in the Google Play Store from December 2009 to February 2016**. Disponível em: <http://www.statista.com/statistics/266210/number-of-available-applications-in-the-google-play-store/> Acesso em 16 de Abril de 2016.
[3] **Application Fundamentals**. Disponível em: <http://developer.android.com/intl/pt-br/guide/components/fundamentals.html> Acesso em 14 de Abril de 2016.
[4] **Intents and Intent Filters**. Disponível em: <http://developer.android.com/intl/pt-br/guide/components/intents-filters.html> Acesso em 14 de Abril de 2016.
[5] LU, Long; LI, Zhichun; WU, Zhenyu; LEE, Wenke; JIANG, Guofei. **CHEX: statically vetting android apps for component hijacking vulnerabilities**. ACM CCS, Oct 2012. New York, USA.
[6] OCTEAU, Damien; MCDANIEL, Patrick; JHA, Someshet et al. **Effective Inter-Component Communication Mapping in Android with Epicc: An Essential Step Towards Holistic Security Analysis** . USENIX, 2013. Washington, D.C., EUA.
[7] OCTEAU, Damien; LUCHAUP, Daniel; DERING, Matthew et al. **Composite Constant Propagation: Application to Android Inter-Component Communication Analysis**. ICSE, 2015. Florence, Itália.
[8] SOUZA, Vinícius C. P. **Uma ferramenta leve de análise para descoberta estática de comunicações entre componentes de aplicações Android**. Trabalho de Graduação - Centro de Informática, Universidade Federal de Pernambuco, 2016. Recife, Brasil.

6. Assinaturas

_____

João Paulo Tenório Trindade
Orientando

_____

Leopoldo Motta Teixeira
Orientador

_____

Data