안전한 디지털 콘텐츠 거래를 위한 안드로이드 바인더 연구

민연아*, 민보연**, 백영태O
*가천대학교 소프트웨어학과
**전북대학교 무역학과
O김포대학교 멀티미디어과
e-mail: yah0612@gachon.ac.kr*, bonnieee@hanmail.net**, hannae@kimpo.ac.krO

Study on android binder for secure digital content transactions

Youna Min*, Beyoun Min**, Yeong tae BaekO
*Dept. of SW Engineering, Gachon University
**Dept. of trade, chonbok University
ODept. of Multmedia, Kimpo University

● 요 약 ●

스마트 디바이스를 이용한 거래가 증가함에 따라 거래 시 발생할 수 있는 다양한 정보보안의 위협이 발생되고 있다. 본 논문에서는 스마트 디바이스를 이용한 디지털 콘텐츠 거래 시 발생할 수 있는 보안상의 위협을 감소시키기 위하여 안드로이드 바인더를 활용한 데이터 관리 방법을 제안하였다.

키워드: 스마트 디바이스, 안드로이드, 바인더

I. Introduction

전 세계적으로 스마트 디바이스가 빠르게 보급되고 있으며 이에 따라 스마트 디바이스를 활용한 구매행위가 증가하고 있다.

특히 다양한 디지털 콘텐츠의 경우 스마트 디바이스에 의한 구매율이 더욱 빠르게 증가하고 있다.

2017년 content matters 2017에 의하면 구매정보를 위해 선호하는 디바이스는 스마트폰으로 조사되었다. 2015년만 해도 PC에 의한 구매정보 및 구매가 72%로 높은 편이었으나 2016년에는 스마트폰이 62%로 PC 26% 대비 매우 높은 것으로 조사되었다[1].

본 논문에서는 향후 더욱 증가할 스마트 디바이스를 통한 거래를 위하여 안드로이드 OS기반 스마트 디바이스의 데이터 안정성을 높이기 위한 방법을 연구하였다.

II. Preliminaries

1. Related works

Gartner의 2018년 글로벌 스마트폰 운영체제 점유율에 의하면 안드로이드는 전체 85.9%이고 iOS는 14%의 점유율로 조사되었다[2].

안드로이드 OS를 적용한 스마트 디바이스가 증가함에 따라 안드로이드OS에서 안전하게 거래에 대한 transaction을 처리할 수 있는 방법이 연구되고 있다.

안드로이드 OS에서 바인더의 역할은 크다.

객체지향 가능한 운영체제 환경을 제공하기도 하고 애플리케이션보다는 서비스중심의 시스템을 제공하기도 한다.

커널에서 바인더는 misc device로 등록되며 바인더의 기본 데이터를 다루는 프로세스는 다음과 같은 자료구조로 나타낼 수 있다.[3]

Table 1. binder data structure

```
struct binder_proc{
struct hlist_node proc_node;
struct rb_root threads;
struct rb_root nodes;
...
long default_priority;
struct dentry *debugfs_entry;
}
```

다음은 안드로이드 바인딩 중 언바운드 서비스와 바운드 서비스의 사례를 그림으로 보여준 것이다[4].

Table 2. unbound and bound process

unbount : call to startService() -> onCreate() -> onStartCommand() -> onDestroy -> Service shut down **bound :** call to bindService() -> onCreate() -> onBind() -> Clints are bound to service -> onUnbind()-> onDistroy() -> Service shut down

본 논문에서는 바인터 인텐트와 AndroidManifest.xml 에 선언된 permission 중 service manager가 관리하는 데이터에 대한 지속적인 검색과 보안 위협을 탐지하여 다양한 거래에 대한 안정성을 제공할 수 있다.

III. The Proposed Scheme

본 논문에서는 안드로이드 OS의 바인더에 대한 관리를 통하여 다양한 환경에서의 거래데이터를 보호하고 transaction이 일관성 있게 처리될 수 있도록 다음과 같은 프로세스를 제안하였다.

Table 3. process

①content provider 체크 ② binder ipc call 체크 ③ service_manager실행 및 바인더 드라이버를 통한 데이터 검색 ④ 데이터 체크 및 오류 탐지

위의 프로세스 각 과정별 세부적으로 메타데이터에 대한 조정과 검색을 통하여 스마트 디바이스를 통한 다양한 거래 및 악성 데이터에 대한 모니터링이 가능하다.

이를 통하여 데이터의 오류 추적과 보안성을 높일 수 있다.

IV. Conclusions

스마트 디바이스를 통한 거래가 증가하고 있다. 특히 디지털 콘텐츠에 대한 거래는 60% 이상 스마트 디바이스를 통한 것으로 보고되었다.

거래의 안정성을 높이고 개인정보 보호를 위하여 본 논문에서는 안드로이드 OS 바인더의 구조에 대한 관리를 제시하였다.

본 연구를 통하여 스마트 디바이스상의 거래시 안정성을 높일 수 있을 것이라 사료된다.

REFERENCES

[1] http://hahmshout.com/contentmatters/

[2] http://www.gartner.com

[3] Felt, Adrienne Porter, et al. “Android permissions demystified.” Proceedings of the 18th ACM conference on Computer and communications security. ACM, 2011.

[4] https://www.oss.kr/info_techtip