The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 14, No. 2, pp.87-92, Apr. 30, 2014. pISSN 2289-0238, eISSN 2289-0246

http://dx.doi.org/10.7236/JIIBC.2014.14.2.87
JIIBC 2014-2-12

가상화 런처에서 암호화를 적용한 어플리케이션 연구

Application Study applied to the Encryption at Virtualization Launcher

임승철*

Seung-Cheol Lim*

요 약 스마트폰은 여러 가지 편의기능 제공뿐 아니라 개인의 개성까지 표현하는 등 그 범위가 점차 증가되고 있다. 사람이 서로 만났을 때 바뀌게 되는 외향의 변화와 같이 스마트폰의 변화에도 개인들이 즉각적으로 반응하게 되었다. 서로의 스마트폰을 관찰하는 것이 보편화된 지금 스마트폰 공유로 인한 정보의 유출이 심각한 문제가 되고 있다. 따라서 본 논문에서는 스마트폰을 공유할 때 스마트폰에서 사용자의 영역을 구분하며, 개인정보의 제약과 암호화를 적용함으로써 필요이상의 정보의 유출을 막고 특정 어플리케이션으로 추가된 정보는 암호화되어 저장되어 다른 유사 어플리케이션에서는 접근이 불가능하게 하여 개인정보를 보호할 수 있었다. 이를 통하여 스마트폰을 공유할 때에도 개인정보 유출을 개선하였다.

Abstract Smartphones, as well as providing a number of convenience features such as an individual's personality to express the range is gradually increasing. Changed when we met another person, such as a change of outward change in the smartphone became responsive individuals. Each other, it is common to observe smartphones smartphones. Smartphone now due to the common use of information leakage has become a serious problem. In this paper, when sharing smart phone, smartphones to separate the user's area, and the constraints of privacy and the need to apply encryption to prevent information leakage or add application-specific information is encrypted and stored in other similar applications it is not accessible to protect the personal information was through this smartphone to share your private information even improved.

Key Words : Smartphone, Mobile Visualization, Encryption, Security, Launcher

Ⅰ. 서 론

스마트폰은 여러 가지 편의기능 제공뿐 아니라 개인의 개성까지 표현하는 등 그 범위가 점차 증가되고 있다. 사람이 서로 만났을 때 바뀌게 되는 외향의 변화와 같이 스마트폰의 변화에도 개인들이 즉각적으로 반응하게 되었다. 서로의 스마트폰을 관찰하는 것이 관례가 된 지금 스마트폰 공유로 정보의 유출이 문제가 되고 있다. 가까운 관계일수록 서로의 생활에 간섭하는 감시의 새로운 대상이 된 것이다. 이처럼 스마트폰은 공공장소에서 쉽게 노출되어있고, 도난에도 취약하다. 그래서 일반적으로 스마트폰에 비밀번호 또는 패턴을 적용하여 개인정보를

*정회원, 우송대학교 컴퓨터정보학과 (교신저자)
접수일자 : 2014년 2월 11일, 수정완료 : 2014년 3월 31일
게재확정일자 : 2014년 4월 11일

Received: 11 February, 2014/ Reviced: 31 March, 2014 /
Accepted: 11 April, 2014
*Corresponding Author: sclim@wsu.ac.kr
Dept. of Computer Information Science, Woosong University, Korea

보호하고 있다. 그 이외에도 보안 어플리케이션을 설치하여 악성코드를 제한하는 방법 이외에 사용자의 영역 나누어 개인 정보의 유출을 막는 방법 등의 적용이 시급하다.[1][2]

따라서 본 논문에서는 먼저 기존의 로컬 데스크탑 기반의 어플리케이션 가상화 방식을 모바일 환경에서 구현 및 개선을 하고 기존 방식의 문제점이었던 로컬기반의 독립된 가상화 환경 구성 시 계층구성의 한계점과 이로 인한 보안성의 하락을 보완하여 사용자 영역을 나누고 어플리케이션을 암호화하는 두 가지 기능을 적용하였다.

본 논문의 2장에서는 모의 어플리케이션 보안에 대해 서술하고, 3장에서는 구현한 프로토타입과 개선결과를 서술하고 마지막으로 결론을 통해 마무리 지었다.

Ⅱ. 제안한 모의 어플리케이션 보안

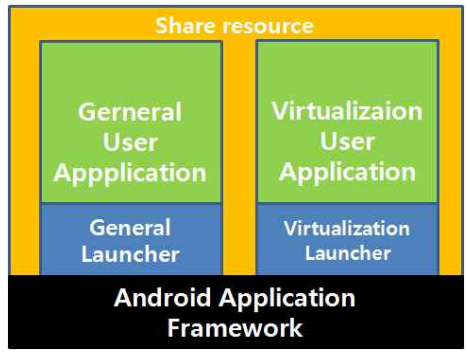
본 논문에서는 사용자 영역의 분리 측면, 어플리케이션의 보안적 측면에 대해 다루었다.

먼저 사용자 영역적인 측면에서는 하나의 OS, 하나의 사용자를 갖게 되는 모바일OS 즉, 안드로이드 상에서 어플리케이션 가상화 런처를 구현하여 일반 영역과 가상화 영역을 시각, 공간적으로 나누는 구조를 가져 이를 개선하고자 한다.

1. 사용자 작업환경의 영역 분리 개선점

가상화 환경에서의 가장 큰 특징은 작업환경을 공간적, 시각적으로 분리한 것이다. 그림 1에서 먼저 런처가 구동되면, 안드로이드의 특성상 OS에 유저가 어플리케이션을 실행시킬 수 있는 UI환경을 갖추게 되며, 이는 가상화 환경에서도 같은 기능을 가지게 된다. 먼저 일반모드 상에서는 어플리케이션 가상화가 되어있는 런처를 앱으로 등록하여 실행할 경우 가상화 런처 환경에 접근하게 되며, 두 런처는 서로 개별적인 앱을 등록하게 된다.[3][4]

서로간의 앱이 같을 수도 다를 수도 있으며, 만일 같은 앱이라 해도 공유자원에 저장되어 시각적으로 분리되어 있다. 이럴 경우에는 같은 어플이 중복되어 저장되는 일이 없는 것이다. 기존의 방식에 비해 로컬 환경에서 사용자 영역이 일반 런처모드와 가상화 런처모드로 좀 더 확고히 구분되는 특성을 가질 수 있게 된다.[5]



1. 어플리케이션 가상화 런처 설계
Fig. 1. Design of application virtualization launcher

2. 보안적 측면의 개선점

그림 2에서는 보안적인 측면에서 보면 별도의 영역을 갖고 있기 때문에 개인 환경과 보안환경 두 가지 측면에서 개선점이라 할 수 있다.

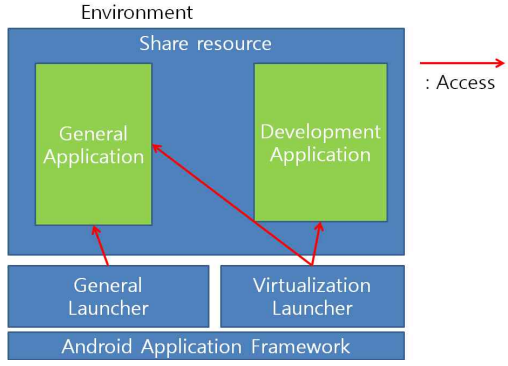


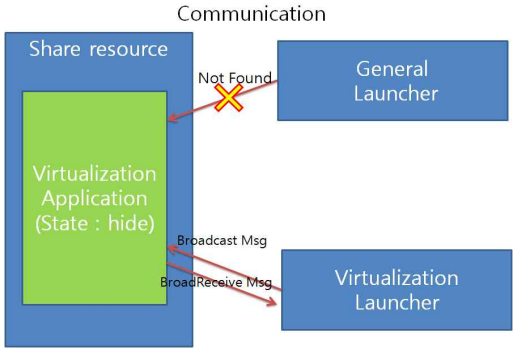
그림 2. 가상화 런처의 보안환경과 개인환경의 분리
Fig. 2. Separation of the personal environment and security environment through virtualization launcher

시각적으로 볼 때, 한 화면에 하나의 런처만이 구동되어 보여 지기 때문에, 다른 런처가 구동중일 경우 서로간에 작업환경을 알 수 없고 별도의 앱을 가지고 있기 때문이다. 공간적인 측면에서는 굳이 저장 공간까지 나누어 낭비하지 않고, 공유자원안에서 저장 공간은 공유하여 함께 사용하지만 접근권한을 따로 주어 별도의 앱을 가지게 하는 것이다.

가상화 런처에서는 별도의 앱 말고도 일반 런처의 앱에도 접근이 가능하도록 설정하는 것이 가능해지며 게스트와 주 사용자의 이용할 수 있는 서비스에 차이를 줄 수

있다. 이 경우에 게스트 사용자가 주 사용자의 중요 앱에 접근이 불가능하기 때문에 정보의 삭제라던가 접근을 할 수가 없어 오프라인상의 보안이 된다.

기존에 보안 방식으로는 사회공학적 기법을 막아 낼 수 없다는 측면에서 주소록에 특정한 암호화 알고리즘을 적용시켜 타 사용자들이 기존에 있는 주소록에는 이름은 물론 전화번호, 이메일, 주소와 같은 개인정보들을 일반 주소록에서는 알아보지 못하게 하여 사회공학적 기법에도 안전할 수 있는 어플리케이션을 구현하여 정보보안적인 측면을 개선하였다.



3. 런처 별 어플리케이션의 접근
Fig. 3. Access of applications due to launcher

그림 3에서 통신하는 모습을 보면 공유자원안에 가상화 어플리케이션은 상태가 숨김으로 되어있어 일반 런처에서는 접근 할 수 없기 때문에 메시지를 보낼 수도 통신을 할 수도 없다. 하지만 가상화 런처에서는 접근이 가능하여 메시지 송수신 등 정보 교환이 가능하다.

일반 런처와 가상화 런처는 완전히 개별적이며, 별도의 관리를 할 수 있어 보안적인 측면이 기존의 방식보다 강화되었다.

그림 4은 어플리케이션과 런처들 사이의 전체프로그램의 구조 나타낸다.

그림 4에서와 같이 런처 별로 접근할 수 있는 어플리케이션이 다르다. 가상화 런처에서의 어플리케이션일 경우 해당 어플리케이션은 DB에 저장할 때 암호화를 사용하여 저장한다. 비록 같은 DB를 사용했다 하더라도 일반적인 어플리케이션에서는 그 정보에 접근이 불가능하며 볼 수도 없고 수정도 불가능 하다. 반면 가상화 어플리케이션에서는 복호화기능을 수행하기 때문에 암호화 된 것뿐 아니라 모든 DB의 정보를 볼 수 있고 접근가능하며 수정 또한 가능하다는 이점이 있다.[6]

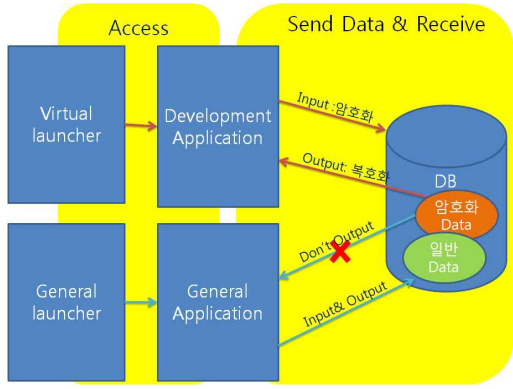


그림 4. 전체 프로그램 구조도
Fig. 4. Program architecture

DB에 저장할 때 사용한 암호화 기술을 DES를 세 번 사용하여 DES보다 안전한 Triple-DES를 사용하였다.

그림 5. 기존 문자열 암호화 프로그램
Fig. 5. Encrytion program on typical text

Triple-DES나 AES 알고리즘 같이 특정한 암호화를 적용하여 주소록에 저장하게 되면 일반 주소록에서는 알아보지 못하지만 보안 기술이 적용된 어플리케이션에서는 복호화 된 주소록 정보를 읽어, 올 수 있게 개선하고자 한다.

그림 6. Triple-DES 암호화
Fig. 6. Triple-DES encryption

그림 6에 보는 것처럼 Triple-DES 암호화 방식은 첫 번째에 암호화 와 두 번째의 복호화 과정 세 번째에 암호화 과정을 거친다.

7. Triple-DES 복호화
Fig. 7. Triple-DES de-encryption

그림 7은 DB에서 주소록으로 읽어 올 때에는 암호화와 비슷한 방식으로 복호화를 진행한다.

Triple-DES를 사용한 것은 현재 금융권 등에서의 전자지불시스템에서 Triple-DES의 종류인 DES-EDE2가 사용되고 있는 것으로 보아 상당기간 Triple-DES가 쓰일 것이라는 신뢰성이 있다고 판단된다.

Ⅲ. 구현된 프로토타입

개발환경은 안드로이드 2.3 (Gingerbread)과 4.2.2 (Jelly bean)을 기준으로 eclipse와 안드로이드 SDK를 통해 데스크탑, 4.2.1 안드로이드폰, 4.2.2 안드로이드폰 환경에서 제작하였으며, 가상화 런처는 안드로이드의 진저브레드라는 베이직 런처의 기능을 활용해 일반 런처의 모든 기능을 사용할 수 있다.

가상화 런처에서는 카테고리와 스택의 분리를 통해 공유자원을 제외한 일반 모드와 완전히 영역을 분리하여 앱 설치영역을 나누어 서로 다른 환경에서 폰을 사용하는 것처럼 가상화 환경을 구현하였다.[7][8]

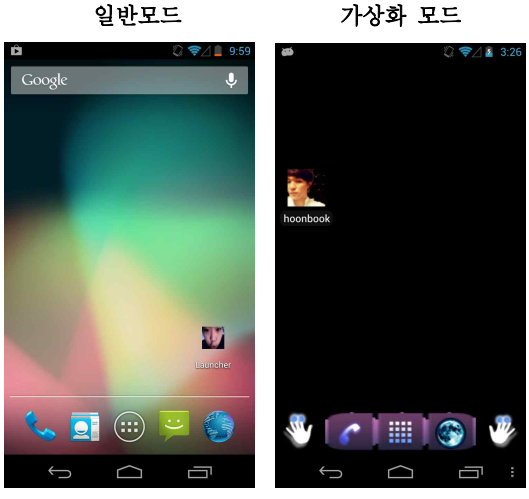


그림 8. 일반 모드 런처와 가상화 모드 런처 비교
Fig. 8. Comparison of general mode launcher and virtualization mode launcher

그림 8은 안드로이드 일반 모드 런처 화면과 가상화 모드 런처의 화면 비교이다. 일반모드에는 어플리케이션 가상화 런처가 설치되어 있고, 안드로이드에 처음 설치 시에 기본적으로 주어지는 어플리케이션들이 설치되어 있다. 가상화 모드의 hoonbook이라는 어플리케이션은 일반 런처에서는 볼 수 없으며, 실행 시킬 수 없다. 실행 방법은 일반 모드 런처에서 Launcher 아이콘을 클릭하거나, 메뉴화면상에서 Launcher 아이콘을 이용하여 가상화 환경으로 새로운 런처를 띄우도록 처리하였다.[9][10]

그림 8의 오른쪽 가상화 모드 런처는 어플리케이션 가상화를 통해 구현된 가상화 런처로 왼쪽 일반모드 런처와는 다르게 전혀 다른 구성으로 런처가 작동중이며, 두 런처 간의 설치되어있는 어플은 서로 다른 영역에서 존재하고 있다.

사용자의 영역이 구분되어있어 사용자에 따라 서로 다른 모드로 적용되어 정보의 유출을 막을 수 있다.

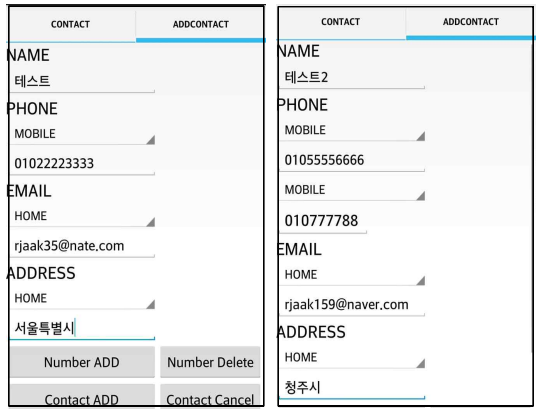


그림 9. 어플리케이션의 주소록 등록
Fig. 9. Address book registration of an application

그림 9의 가상화 모드에서 개발 어플리케이션으로 주소록에 데이터를 저장하면 스마트 폰의 주소록 저장소에 암호화된 데이터가 저장되기 때문에 복호화를 시켜주지 못하면 일반 모드의 주소록에서는 데이터를 읽어 와도 암호화가 되어 있기 때문에 시각적 보안성을 확보 할 수 있다.

10. 일반 모드와 가상화 모드의 주소록 표현
Fig. 10. Address book figure on general mode and virtualization mode

가상화 모드의 개발 어플리케이션에서는 암호화 된 데이터를 그림 10의 일반 모드에서 확인 할 수 있다.

프로토타입 어플리케이션은 Triple-Des 알고리즘이지만 문자열을 화면에 나타낼 때 문자열이 깨지기 때문에 Base64 인코딩 과정을 하여 주소록을 저장할 때에 데이터 가변이 일어나지 않도록 하였다.

Ⅳ. 결 론

본 논문에서 제안하는 어플리케이션 가상화 런처 방식과 적용플랫폼의 변경을 통해 기존에 제안되었던 방식에 비해 작업환경을 분리가 확실히 이루어져 같은 OS라 할지라도 전혀 다른 작업환경을 갖추도록 작업 영역을 일반 환경과 가상화 환경과의 분리를 하였다. 보안적인 측면에서는 서로 같은 공간의 DB를 쓰지만 일반 환경에서 볼 수 없는 Triple-DES 암호화 적용하여 데이터가 가상화 환경으로 작업환경이 변경 되었을 경우 Triple-DES로 암호화 되어 있는 주소록의 데이터를 읽어 올 수 있다는 점으로 DB공간을 효율적으로 사용하였다. 또한 로컬 데스크탑 기반의 어플리케이션 가상화 방식을 모바일 환경에서 구현 및 개선을 하고 기존 방식의 문제점이었던 로컬기반의 독립된 가상화 환경 구성 시 계층구성의 한계점과 이로 인한 보안성의 하락을 보완하여 사용자 영역을 나누고 어플리케이션을 암호화하는 두 가지 기능을 적용하여 보안적인 측면을 개선하였다.

최근 모바일 시장에서 안드로이드는 많은 발전을 하고 있으며, 구글에서는 사용자 계정의 추가 등을 통해 작업영역을 분리하는 보안 기능을 새 버전에 추가하는 등 가상화가 아니라도 작업영역의 분리와 보안성을 염두에 두는 업데이트를 이루고 있다.[11][12][13]

향후 연구 과제는 가상화 런처 진입 시에 비밀번호나 보안패드 등의 기능을 추가하여 그 보안성 강화 등의 연구를 할 예정이다.

References

[1] Sun-Hyang Jang., Su-ji Hwang, Young-Hyun Chang, Min-jeong Koo "Study on the Enhancement of the Credibility of Android OS based Applications“, Journal of IWIT, Vol.11, No.3, pp.382~384, fall 2012.

[2] Nelson Ruest, Danielle Ruest "Virtualization, A Beginner's Guide", McGraw-Hill 2009

[3] Se-jung Lim, Gwang-jun Kim, Tae-geun Kang "Application Program Virtualization based on Desktop Virtualization", The korea institute of electronic communication sciences, Vol.5, No.6, 2010

[4] SILBERSCHATZ "Operating System Principles 7/E“, Wiley 2005

[5] VMware, Inc. "Understanding Full Virtu-alization, Paravirtualization, and Hardware Assist“, White Paper, Nov. 2007

[6] Mark Murphy "Beginning Android3", Apress 2012

[7] Barret Rhoden, Kevin Klus, David Zhu, Eric Brewer "Improving Per-Node Efficiency in the Datacenter with New OS Abstractions“, ACM 2011

[8] B Weinberg, L Pundit "Designing and Deploying with Mobile Virtualization“, Whitepaper. Linux Pundit 2009

[9] Mohammad Nauman, Sohail Khan "Design and implementation of a fine-grained resource usage model for the android platform“, The International Arab Journal of Information Technology 2011

[10] Eun-Sook Cho, Chul-Jin Kim, and Sook-Hee Lee, “A Modeling Technique for Development of Mobile

App. based on Android", Journal of the Korea Academia-Industrial cooperation Society, vol. 14 No. 8, pp.3999-4005, Auguest 2013.

[11] Google, Inc. "Android 4.2 API: Multiple Users", http://developer.android.com/about/versions/android-4.2.html 2012

[12] S.J. OH, "Design of a Middleware for Android-based Smart Phone Applications", Journal of Korean Institute of Information Technology, vol. 12, issue 2, pp. 111-117, Apr 2012.

[13] Jae-Man You, In-Kyoo Park "Android Storage Access Control for Personal Information Security", Journal of The Institute of Internet, Broadcasting and Communication, vol. 13 No. 6, pp.123-129, December 2013.

소개

승 철(정회원)

- 1985년 : 한양대학교 전자공학과 학사
- 1994년 : 전북대학교 정보통신과 석사
- 2003년 : 전북대학교 영상공학과 박사
- 2006년 ~ 현재 : 우송대학교 컴퓨터정보학과 교수
- 주관심분야 : 이동통신, 컴퓨터네트워크, 임베디드시스템소프트웨어