안드로이드 루팅의 과정과 목표

글 : 변동삼(zxh)

admin@zxh.co.kr

Ver 1.0

목차

안드로이드, 그리고 루팅이란?

안드로이드는 구글에서 인수해 개발하여 2007년 OHA(Open Handset Aliance)가 공개한 스마트폰 운영체제이다. 리눅스(Linux)2.6커널을 기반으로 하며, 오픈소스로 개방한 플랫폼이기 때문에 풍부한 라이브러리와 익숙한 명령어들을 지원하며, 누구나 쉽게 개발에 뛰어들 수 있다는 장점이 있다. 여타 스마트폰이 그렇듯이 모바일 환경을 중점으로 개발된 플랫폼이지만 하나의 컴퓨터와 다름이 없다.

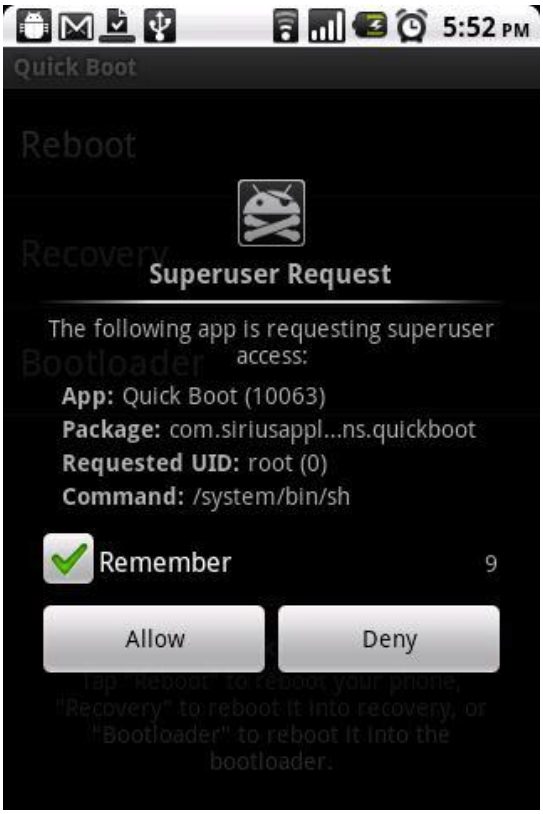
그렇다며 루팅(rooting)은 무엇일까?

루팅을 한문장으로 정리하자면 안드로이드 내 리눅스 커널의 최고관리자인 root계정의 권한을 획득(탈취)하는 행위이다. 자세히 알아보도록 하자. 리눅스는 멀티유저를 대상으로 운영하는 시스템이다. 따라서 여러 유저들에게 각각에 맞는 권한(Permission)을 주고, 해당 유저는 자신이 할당 받은 권한 내에서만 시스템을 컨트롤 할 수 있게 된다. 그 중 유저들과 그 권한을 관리하고 모든 권한을 가지고 있는 최고관리자인 root 계정이 존재한다.

일반적으로 안드로이드에서는 사용자, 개발자들의 무분별한 시스템수정, 오 남용, 보안문제 등을 막기 위해 root의 권한을 제한한 상태로 배포되었다. 제조사의 입장에선 자신들이 만든 제품을 유저들이 맘대로 변경하는 것을 꺼려하는 건 당연한 것이다. 이러한 이유에서 제한해 둔 root 의 권한을 취득하여, 정상적으로는 제어할 수 없었던 시스템파일이나, OS단의 접근할 수 없던 부분까지 커스터마이징 할 수 있게 하는 것을 루팅이라 할 수 있다.

루팅의 원리와 과정

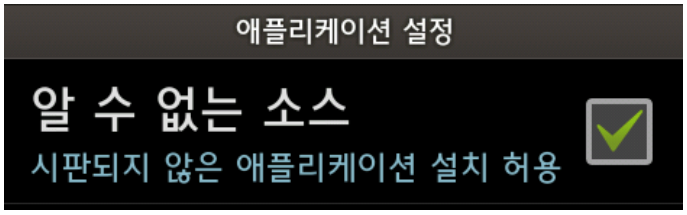
안드로이드, 리눅스 또한 사람이 만든 것이다 보니 100%완벽할 수는 없고, 취약점이 존재하기 마련이다. 레이스컨디션, 포맷 스트링, 버퍼 오버플로우 등을 시작으로 수많은 exploit들이 공개되어있다. 이러한 취약점들을 이용해 비정상적인 방법으로 root권한을 일시적으로 얻게 되고, 안드로이드의 경우 루팅 후 깔리는 SuperUser 어플리케이션을 통해 필요 시에 루트권한을 부여, 지속, 관리할 수 있다.

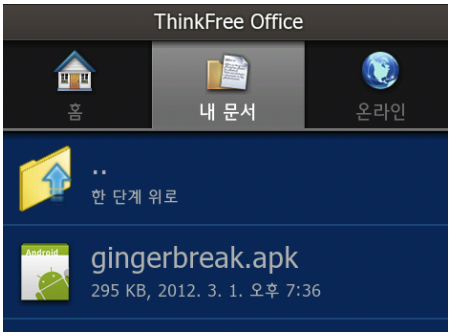


이러한 과정을 일반유저들도 손쉽게 클릭 몇 번으로 할 수 있도록 GingerBreak , Super One Click, z4root 등 여러 프로그램, 어플리케이션들이 제작, 배포되고 있다. 본 문서에서는 테이크1(2.2) 환경에서 GingerBreak어플리케이션을 통한 탈옥 과정을 보여주려 한다.

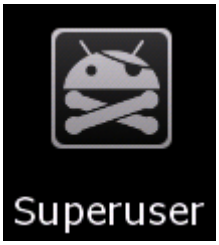
1. 배터리가 충분한 상태의 안드로이드폰에 GingerBreak의 APK파일을 다운로드 혹은 SD카드에 전송한다 (이때 해당 폰, 해당 안드로이드버전에 맞는 루팅 도구를 이용하길 바란다. 각 기종 별 카페 등 커뮤니티에 보면 가능한 툴들을 찾을 수 있을 것 이다.)

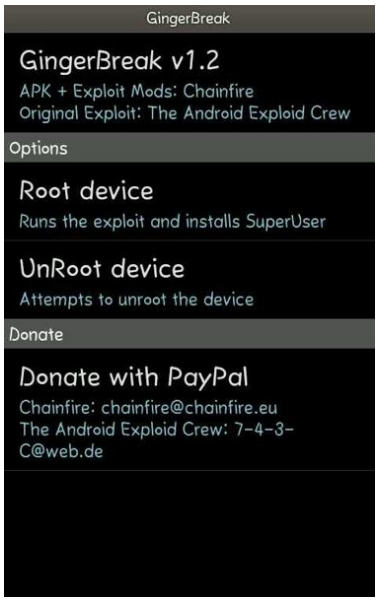
2. 그 후 PC와 USB연결을 모두 해제한 상태에서 아스트로나 ThinkFree 등 탐색기 기능이 있는 어플리케이션을 통해 GingerBreak의 APK파일이 있는 경로로 이동하여 실행하면 설치할 수 있다.(이때 설정->애플리케이션 설정->알 수 없는 소스 시판되지 않은 애플리케이션 설치 허용에 체크되어있어야 된다.)





3. 설치 후 GingerBreak를 실행하여 Root device를 누르고 재부팅(10~20분소요)이 자동으로 진행 되면 바탕화면에서 SuperUser 어플리케이션이 설치되어있는 것을 확인 할 수 있을 것 이다. 이렇게 루팅의 기본적인 과정은 끝이났다.

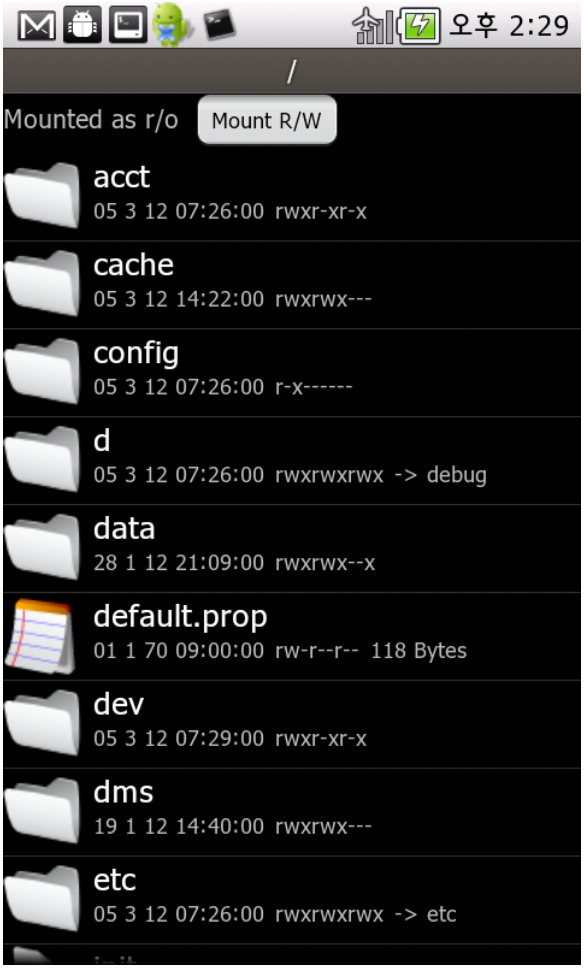




루팅 후 필수 어플 소개

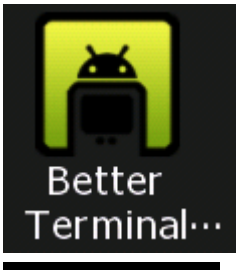
1. RootExplorer

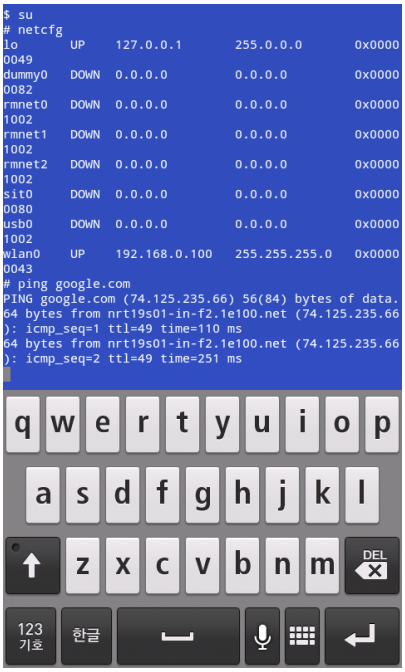
루팅 전에 파일탐색기로 많이 쓰던 아스트로의 경우 SD카드 내부의 파일들까지밖에 접근을 못하였지만 루팅 후 root권한을 부여 받은(최초 실행시 SuperUser 어플에서 권한 수락 거절 여부 확인) Root Explorer의 경우 오른쪽 캡쳐화면에서 보듯이 최상위 / 디렉토리부터 시작하여 모든 디렉토리에 접근할 수 있게 된다.



2. 터미널 어플리케이션 (Terminal Emulator, Better Terminal Emulator 등)

터미널에 접근하여 여러 명령을 내릴 수 있다. Busybox Installer를 통해 여러 명령어를 추가로 설치하면 보다 폭넓은 제어가 가능하다.(몇몇 루팅용 어플은 Busybox설치를 통한 추가명령어를 필요로 하는 경우도 있기때문에 필수로 깔아두는 것을 추천한다.)





3. Titanium Backup

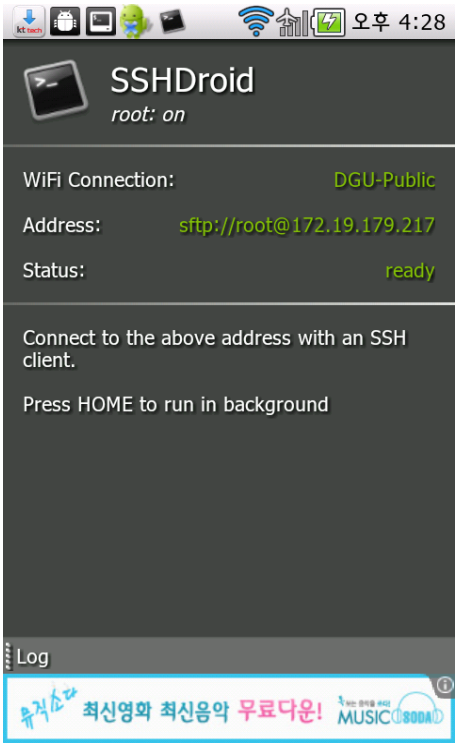
루팅 후 대표적인 백업어플이다. 루팅을 한 후 시스템을 건들이다보면 의도치않게 벽돌이 될 가능성이 항상 존재한다. 이를 러한 상황이 일어났을 때 를 대비해 자주 백업을 해두는 것이 좋은데 이 티타늄백업 어플리케이션은 어플리케이션의 내부 데이터, 설정값까지 백업, 복원이 가능하다. (루팅 후에만 가능)

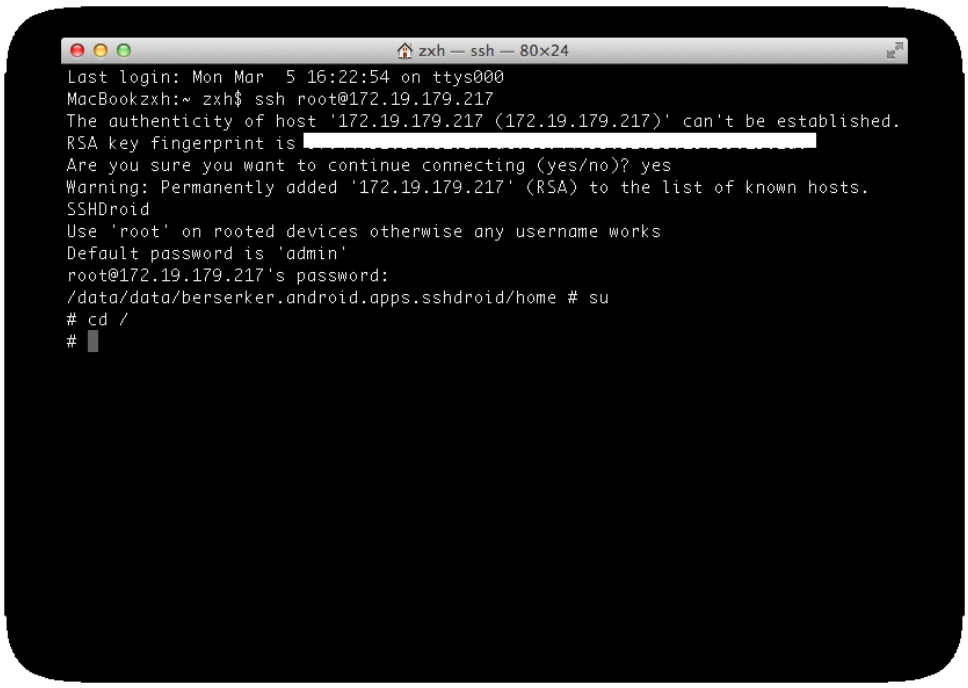
번외로 이 티타늄 백업어플로 A폰에서 카톡을 백업 한 다음, 백업파일을 B폰으로 옮긴 후 B폰에 복원시, 카톡을 1계정 멀티 디바이스로 이용할 수 있다는 사례가 있었다. 카톡 규정상 1인 1계정 1디바이스이지만 이를 우회하게 되는 것이다.

겔럭시탭 공식 사용자모임의 어느 유저의 경험담에 따르면 겔탭7에서 백업한 카톡을 넥서스S에 복원하자, 인증없이 실행이되고, 친구목록까지 유지된상태로 동일한 환경의 카톡을 두개의 디바이스에서 사용가능하다고 전했다. 댓글에 성공했다는 사례가 보여 필자 또한 시도를 해봤지만 실패하였다. 특정 환경에서만 성공하고, 알지못할 실패의 변수가 존재하는 것으로 추측된다 .

4. SSHDroid

조금전에 소개한 Terminal Emulator어플리케이션을 통해 터미널에 접속 가능한 것을 확인하였다. 하지만 작은 휴대폰의 키패드로 영타를 치며 긴 명령을 내리기란 쉽지않다. 그럴 땐 SSHDroid 를 통해 ssh포트를 열어두고, 동일 무선랜, 혹은 IP대역에 있는 PC를 통해 SSH접속을 하여 명령을 내리면 키보드로 신속하고 편리하게 명령을 내릴 수 있다.





이외에도 루팅 후에만 사용할 수 있는 여러 실속 어플들이 많다.

그럼 다음으론 루팅 후 무엇이 가능한지? 루팅의 목적, 달성 등에 대해 알아보겠다.

루팅 done, 이제 뭘 할수있지?

일반적으로 알려진 루팅 후 얻게되는 효과로는

CPU오버클럭, 세세한 테마수정, 부팅화면 수정, 제작, 통신사의 기본어플 제거를 통한 가용램 용량 확보 등이 있다.

그렇다면 그 이상으로 어디까지 가능한지 몇 가지 사례를 소개하고자 한다.

(해당 부분의 악용 시 법적 책임은 당사자 에게 있으며, 이렇게 까지 가능하다는 것을 보여주기 위한 예제일 뿐이다.)

1. MAC-Address 조작

앞 전에 소개했듯이 터미널에 접속이 가능해진다.

그렇다면 리눅스 환경과 크게 다를 바가 없다는 것이다.

따라서 터미널을 통해

ifconfig wlan0 down

ifconfig wlan0 hw ether 00:00:00:00:00:00

ifconfig wlan0 up

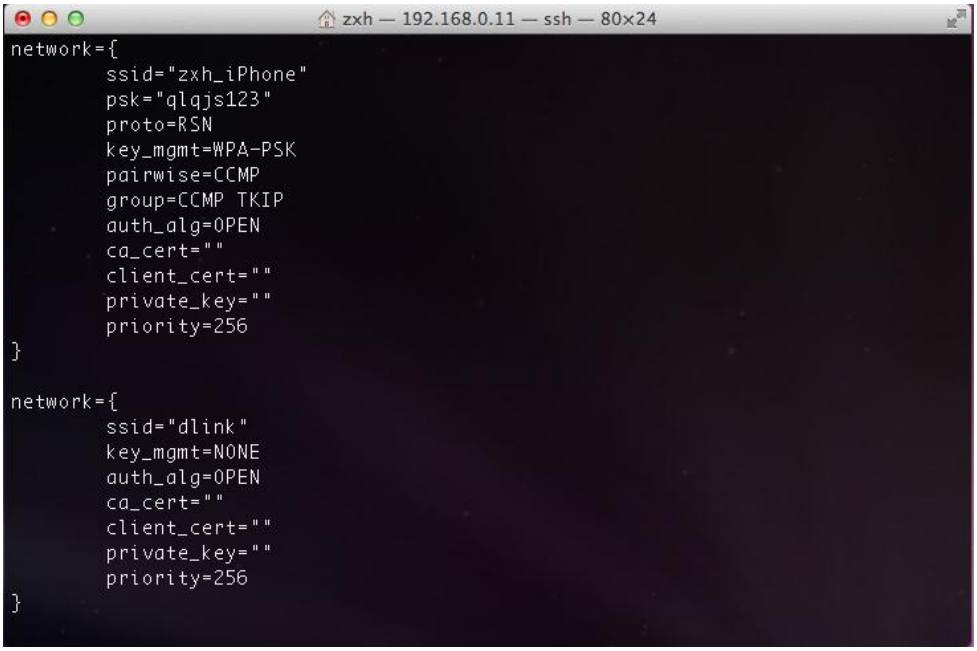
등의 명령을 통해 맥어드레스를 조작 할 수 있게된다. 하지만 디바이스에 따라 터미널 상으로 불가능 한 경우도 있다. TAKE폰의 경우 Root Explorer나 터미널 등을 통해

/data/misc/wifi/softmac 파일을 텍스트 편집기나, vi 등으로 수정 시 맥 어드레스 변경이 가능하다 (폰 마다 경로나 파일이 다를 수 있음)

이로 인하여 맥어드레스 인증을 하는 무선랜에 조작된 맥어드레스를 통해 접근할 수 있을 뿐더러, 최근 통신사별로 시행중인 WiFi존에 타 통신사가 접근하는 등의 악용 우려가 있다.

또한 같은 경로에 있는 /data/misc/wifi/wpa_supplicant.conf 파일을 열어보면 충격을 금할 수 없다. 접속했던 무선랜의 정보 뿐만 아니라, 해당 무선랜의 암호까지 plane text로 저장되어 있는 것을 볼 수 있다.

첫 번째에 위치하는 무선랜 기록은 아이폰을 통해 만든 무선랜 핫스팟이다. WPA-PSK로 암호화된 무선랜이였지만 암호가 고스란이 기록되어 있다.



만약 사내의 중요 무선랜의 암호를 알아내고자 한다면 직원의 안드로이드 폰에 악성 어플리케이션을 통해 쉽게 빼낼 수 있는 위험한 상태이다.

이것은 하나의 예제일 뿐이며 우리 주변에서 모두가 사용하는 안드로이드폰은 생각보다 위험한 요소가 많이 존재한다. 최근 특정 어플리케이션을 설치하거나 웹사이트에 접속하는 것 만으로도 루팅이 되고, 정보가 빠져나가는 등 여러 위험이 있다. 루팅, 그 자체를 나쁘다 라고 정의하기 보단, 루팅 통하여 직접 그 위험을 알고, 예방을 할 수 있는 기회가 된다면 공부도 되고 좋지 않을까 생각해 본다.