휴대폰 메시지 위·변조 위험성 연구

안중호*, 이승용**, 김민수***, 노봉남****
*전남대학교대학원 정보보호협동과정
**전남대학교 시스템보안연구센터
***목포대학교 정보보호학과
****전남대학교 전자컴퓨터공학부

A Study of the Dangers of Forgery and Modulation on Cell Phone Messages

Joong-Ho Ahn*, Seungyoung Lee**, Minsoo Kim***, Bong-Nam Noh****
*Interdisciplinary Program of Information Security, Chonnam National Univ.
**System Security Research Center, Chonnam National Univ.
***Division of Information Security, Mokpo National Univ.
****Division of Electronics Computer Engineering, Chonnam National Univ.

요 약

최근 모바일 환경의 기술 발전과 더불어 그 활용분야는 더욱 확대되고 있다. 하지만 그에 따른 역기능에 대한 문제는 나날이 심각해지고 있으며, 뚜렷한 대책 마련이 미비한 실정이다. 대표적 모바일 기기인 휴대폰도 각종 범죄의 도구로 사용되고 있으며, 그에 따라 범죄수사 과정에서 법적 증거자료 획득을 위한 중요도가 높아지고 있다. 하지만 휴대폰으로부터 획득한 증거자료의 신뢰성이 결여된다면, 법적인 증거능력의 상실로 큰 혼란을 유발시키게 된다. 본 논문에서는 법적인 증거능력을 상실시킬 수 있는 휴대폰 내부 메시지에 대한 위·변조 가능성에 대해 실험적으로 증명하고, 그 위험성을 고찰하는 것에 그 목적이 있다. 또한 이를 보완하기 위해서 해쉬함수를 휴대폰 내부 시스템에 적용하는 방법을 제시하고자 한다.

1. 서론

현재 대부분의 사람들은 다양한 모바일 기기를 소유하고 있으며, 이를 사용하여 다양한 서비스를 이용하고 있다. 대표적인 모바일 기기로 대부분의 사람들이 사용하는 휴대폰의 다양한 기능들은 휴대폰을 없어서는 안 될 가장 중요한 모바일 기기의 하나로 만들었다. 하지만 그에 따른 역기능에 대한 관심과 대응은 미흡한 실정이다. 문제가 될 수 있는 것은 공개된 특정 소프트웨어나 기술들의 오용에서 오는 정보화의 역기능일 것이다. 이것들은 인터넷상에서 어렵지 않게 구할 수 있고, 보안문제를 일으키는 원인이 될 수 있다. 더욱 문제시 되는 것은 컴퓨터 전문가, 프로그래머, 해커(크래커) 등 하드웨어나 소프트웨어에 대한 이해가 깊은 전문가들에 의한 휴대폰 내부시스템의 분석을 통해서, 더욱 심각한 수준의 휴대폰 내부정보의 변조가 가능하다. 그래서 휴대폰 내부 정보로부터 범죄 수사 과정에서 적법한 증거자료를 획득하였지만, 그 정보가 위·변조됐다면 그 증거자료는 법적 효력을 상실할 것이다. 미리 지능적으로 본인에게 유리하도록 삭제된 메시지에 대해 위·변조를 해 둘 수도 있는 문제이다. 단지 가정이였지만 법적 증거의 효력을 얻기 위해서 충분히 고려되어야 할 부분이다.

본 논문은 모바일 상에서 발생할 수 있는 휴대폰 메시지들의 위·변조의 위험성을 실험을 통해 증명하고, 그 보완 대책에 대한 필요성과 방법을 제시하고자 한다. 그 위험성은 경찰청에서 공표한 '디지털증거 처리 표준 가이드라인'에 소개된 증거수집 전 단계에서 사전에 증거자료를 위·변조함으로써 증거처리를 위한 모바일 포렌식스 과정에서 수사에 혼란을 초래하고, 잘못된 증거를 추출함으로써 범죄사실에 대한 증거의 은닉과 법적인 증거능력의 상실을 유발시키게 된다. 결국 용의자는 휴대폰 내부 정보에 대해 위·변조가 가능하고 올바른 범죄수사를 방해하는 결과를 가져온다. 이런 점에서 휴대폰의 대표적인 서비스이며 유효한 증거자료가 되는 SMS (Short Message Service) 메시지에 대해 삭제된 메시지 복원 방법과 정상적인 메시지 위·변조 방법에 대해 기술한다. 실제로 실험을 통해 그 결과로 휴대폰에 나타나는 변화를 확인함으로써 그 위험성을 고찰한다.

이 논문 각 장의 내용은 다음과 같다. 관련연구로 2장 SMS 메시지 획득 및 분석에서는 실험을 위한 메시지 획득 및 분석 방법에 대해서 소개한다. 3장 SMS 메시지 위·변조에서는 획득한 메시지에 대한 분석을 바탕으로 실제로 위·변조 작업을 실험하고 결과를 살펴본다. 그리고 이것에 대한 보완 방법에 대해 살펴본다. 4장 결론 및 향후 연구방향에서는 실험 결과에 대한 결론을 도출하여 그 위험성을 논하고, 끝으로 향후 연구를 제시한다.

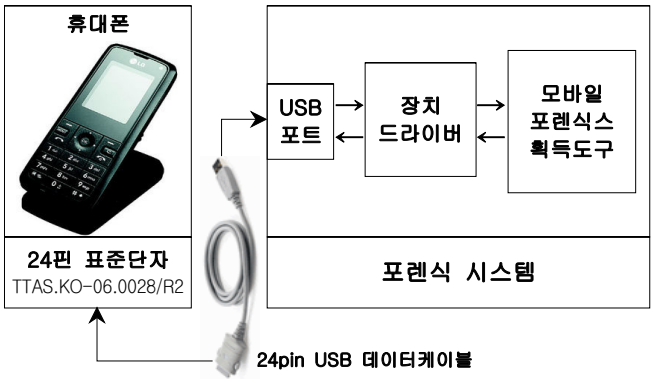
2. SMS 메시지 획득 및 분석

현재 국내에는 공식적으로 검증된 모바일 포렌식스 도구가 없는 상태이며, 휴대폰의 디지털 증거를 획득하기 위해서 휴대폰 제조사에서 제공하는 도구를 활용하거나 본 논문에서 실험을 위해 사용된 모바일 포렌식스 활용도구인 Qualcomm 사의 QPST, 오픈소스인 Bitpim, Plinksoft 사의 EasyCDMA 등의 도구를 사용할 수 있다. 각 도구들에 대한 특징과 사용법은 참고문헌이나 해당회사의 웹사이트를 참고한다[1][2][3][9][10][11].

2.1 SMS 메시지 획득 방법

2.1.1 실험환경

SMS 메시지 분석을 위해서 증거 획득을 위한 실험 환경은 (그림 1)과 같은 하드웨어적인 구성도이다[2][3][8].

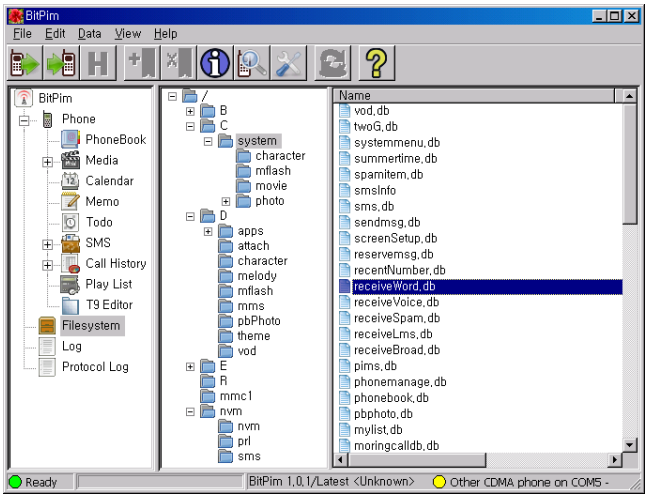


(그림 1) 데이터 획득 시스템 구성도

실험환경을 구성하기 위해서 먼저 포렌식 시스템을 준비한다. 그 후에 휴대폰의 전원을 공급한 후 포렌식 시스템과 USB를 이용한 데이터 통신을 위해서 휴대폰에 적합한 드라이버를 설치한다. 그 후에 실험 휴대폰에서 모바일 포렌식스 활용도구를 설치한다. 설치 후에 휴대폰과 모바일 포렌식스 도구의 USB 통신을 위한 연결 포트를 확인하여 도구의 사용 전 설정을 맞춘 후 실행한다. 적절한 획득도구를 이용해서 얻어온 휴대폰 파일 시스템에서 보내거나 받는 SMS 메시지 파일을 포렌식 시스템으로 다운로드 하여 분석도구를 적절히 사용하여 메시지의 바이너리 구조를 분석한다.

2.1.2 데이터 획득

실험에 사용된 휴대폰의 내부 디렉터리 구조는 (그림 2)와 같다. 그림의 가운데 창이 주요 디렉터리의 하부 목록이고, 실험에 이용되는 SMS 관련 메시지들은 '/C/system' 디렉터리 밑에 존재하고 있고, 오른쪽 창은 그 디렉터리 밑에 포함하고 있는 파일들의 목록이다. 실험을 통한 확인결과 'receiveWord.db'는 받은 휴대폰 단말기의 메뉴 중에서 문자메시지의 수신함이다. 수신된 SMS 메시지들은 모두 이 파일에 기록이 남게 된다. 이 디렉터리 밑에 있는 몇몇 파일들의 내용들은 휴대폰의 메뉴 항



(그림 2) Bitpim을 이용한 파일시스템 획득

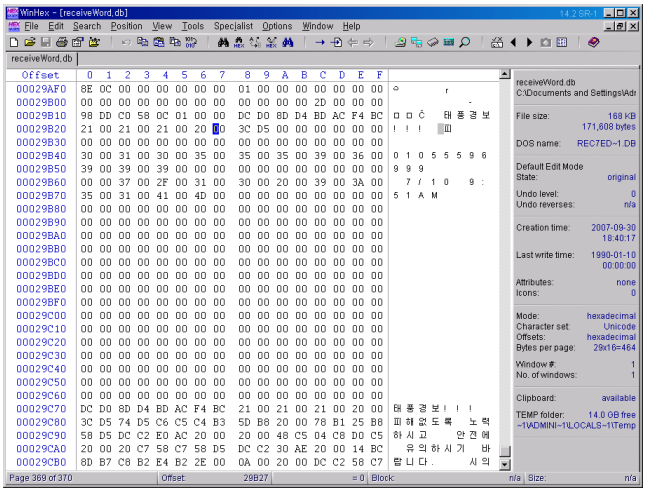
목들의 내용들과 대응된다.

하지만 이렇게 획득할 수 있는 파일시스템의 디렉터리 구조는 휴대폰별로 각기 다르다는 것을 주의한다. 제조사나 이동통신사별로 지원하는 플랫폼이나 휴대폰 내의 EFS 파일시스템 구성의 상이함 때문이다.

2.2 SMS 메시지 분석 방법

2.2.1 실험환경

데이터 획득을 통해 구성된 디렉터리 구조에서 선택한 수신함 파일을 도구에서 지원하는 저장 기능을 사용해서 포렌식 시스템에 복사본을 생성한다. 생성된 복사본을 WinHex나 UltraEdit 같은 분석도구를 활용해서 실험에 사용된 휴대폰의 메시지 구조를 분석한다[12][13].



(그림 3) 메시지 수신함 파일 내용

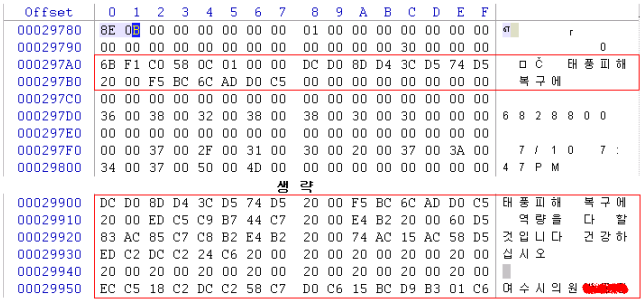
(그림 3)은 메시지 수신함 파일 내부의 내용 중 일부이다. 그림의 내용은 하나의 메시지에 대한 수신함 리스트상의 내용과 전체 원본 메시지 내용이 저장되어 있는 바이너리의 구조이다.

여러 번에 걸쳐 다양한 파일들을 실험한 결과 휴대폰의 전화번호, 패스워드, SPC 코드, 다양한 메시지, 통화기록

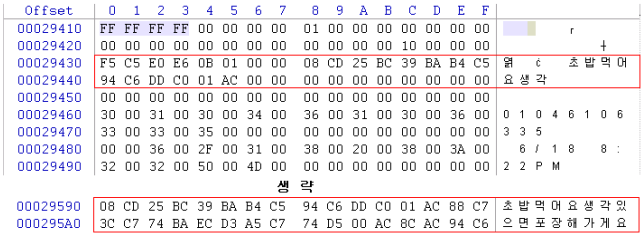
등 유용한 정보를 쉽게 얻어낼 수 있다. 하지만 하드웨어적인 상이함으로 얻기 힘든 정보들도 있다. S사의 제품의 경우는 휴대폰 메시지 정보가 자체 포맷으로 형성되어 분석도구를 사용해서 바로 SMS 메시지의 식별이 불가능 하다. 이런 경우 '디지털증거 처리 표준 가이드라인'에서도 권고하듯이 암호화된 파일에 대한 증거분석을 위해 응용 프로그램 및 암호화 증거를 암호화 패턴 검사, 역공학 기법 등의 방법으로 분석해야 된다[4]. S사 제품의 경우도 SMS 메시지의 자체 포맷의 패턴이 분석되고, 도구들을 이용하여 확인 가능한 정보를 획득할 수 있다. 이런 점들로 미루어 보아, 암호화나 특정 포맷의 사용은 메시지 파일의 분석을 어렵게 할뿐 메시지 자체의 위·변조를 완벽하게 방지하지 못한다.

2.2.2 메시지 구조

실험에 사용된 휴대폰의 문자 수신 메시지는 다운받은 파일 하나에 모두 저장되어 있고, 그 파일은 휴대폰 단말기 상에서 삭제된 수신 메시지들의 정보를 그대로 보존하고 있다.



(그림 4) 정상적인 SMS 수신 메시지



(그림 5) 삭제된 SMS 수신 메시지

(그림 4)와 (그림 5)는 정상적인 것과 삭제된 메시지의 구조를 비교한 화면이다. 두 그림을 비교함으로써 메시지 파일의 바이너리 구조가 간단한 휴대폰 시스템은 분석이 쉽게 되고, 바이너리 조작을 통해 쉽게 원하는 정보를 변경할 수 있다. 분석한 결과로는 처음 4바이트는 파일의 내부 인덱스를 나타내고 삭제된 파일의 경우 'FF FF FF FF'로 표시된다. 그리고 첫 번째 네모 상자의 내용은 휴대폰 단말기의 문자 수신함 리스트 화면에 보이는 내용을 나타내고, 두 번째 네모 상자의 내용이 원래 수신 메시지의 내용이 된다. 첫 번째 네모 상자 뒤에 오는 일련의 내용들은 발신자 번호와 수신 시간이 된다.

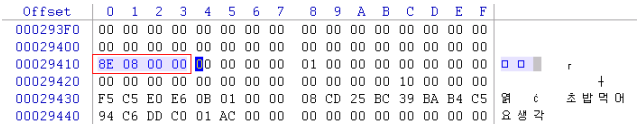
3. SMS 메시지 위·변조

삭제된 메시지를 실제 휴대폰 내에 저장하고 있는 것처럼 복원하는 것 또한 메시지 위조라고 하고, 우선 실험을 통해서 삭제된 메시지를 복원한다. 그리고 그 복원된 메시지의 일부나 전부를 수정하는 것을 변조라고 하고, 실험을 진행한다. 실험을 통한 위·변조 결과를 통해서 위·변조의 위험성을 고찰한다.

3.1 삭제된 메시지 복원

3.1.1 삭제된 메시지의 바이너리 조작

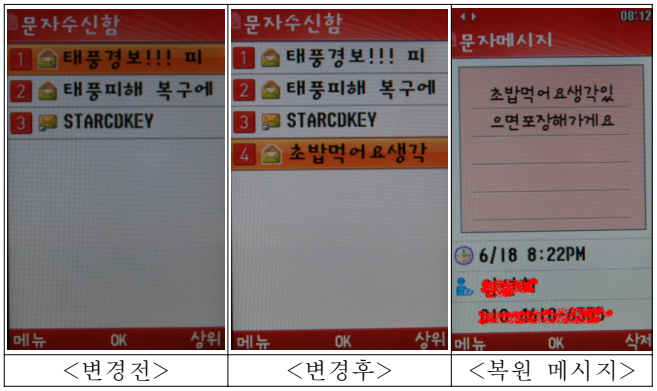
메시지 구조 분석을 통해 비교했던 메시지의 삭제된 상태를 'FF FF FF FF' 값의 위치를 찾아 분석을 토대로 내부 형식에 맞게 (그림 6)과 같이 4byte의 값을 변경한다. 바이너리 조작을 마친 문자 수신함 파일을 획득도구의 파일 업로드 기능을 이용해서 휴대폰 내부에 원본 파일로 대체시킨다.



(그림 6) 삭제 메시지 바이너리 조작 후

3.1.2 복원된 메시지 확인

휴대폰에 파일을 업로드 한 이후 휴대폰을 재부팅시켜서 변경작업 전·후에 대한 휴대폰 단말기 상에서 복원 메시지를 확인한다. (그림 7)에서와 같이 변경 전에 없었던 삭제된 파일이 변경 후에 새로 복원되어 있다.



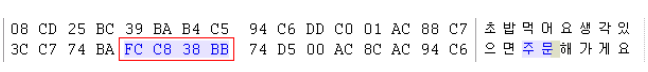
<변경전> <변경후> <복원 메시지>

(그림 7) 삭제된 파일의 복원 전/후 비교

3.2 정상적인 메시지 변조

3.2.1 정상적인 메시지 바이너리 조작

정상적인 수신메시지에 대해 변조과정을 실험하기 위해 앞에서 복원한 메시지를 그대로 사용한다. 복원된 정상적

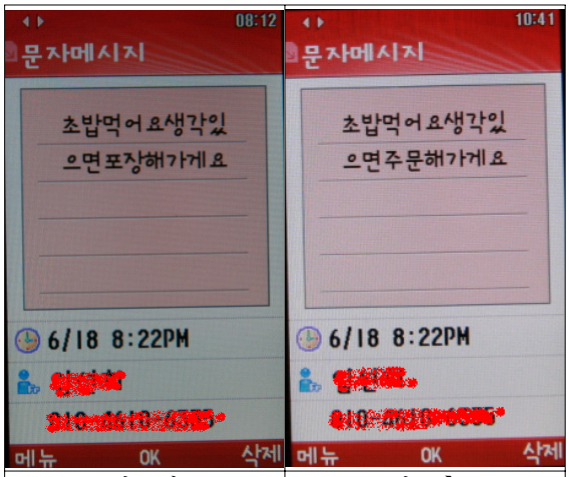


(그림 8) 정상 메시지의 바이너리 편집

인 메시지로 보이는 바이너리 값에서 변조할 부분을 (그림 8)과 같이 수정하여 앞에서와 동일한 방법을 사용해서 휴대폰에 업로드 시킨다.

4.2.2 변조된 메시지 확인

(그림 9)와 같이 휴대폰 단말기의 스크린을 통해서 정상적인 메시지에 대한 변조 전·후의 상태를 확인할 수 있다.



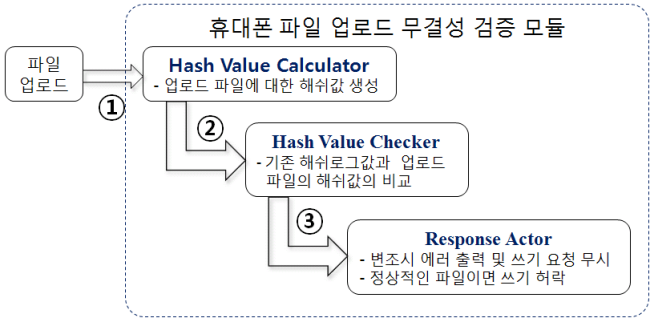
<변조전> <변조후>

(그림 9) 정상 메시지의 변조 전/후 비교

4.3 위·변조 보완 방법

본 논문에서는 휴대폰 메시지의 위·변조를 보완하는 방법으로 해쉬함수의 특징을 사용하여 (그림 10)과 같은 휴대폰 시스템 상에서의 무결성 검증 모듈을 제시한다. 모바일 플랫폼 설계시 EFS (Embedded File System)상의 중요 시스템 파일이나 모바일 포렌식스에서 유효한 증거자료라고 판단되는 부분에 대해 해쉬값을 생성하여 휴대폰 시스템의 접근이 불가능한 곳에 로그를 남기고, 그 부분에 대한 쓰기요청이 들어오면 무결성 검증 모듈에 의해서 처리된다.

(그림 10)과 같이 파일 업로드 요청이 휴대폰 단말기로 들어오면, 중요 파일에 대한 위·변조 방지를 위한 파일 업로드 무결성 검증 모듈에서 먼저 처리를 하게 된다. 요청된 파일에 대해서 해쉬값을 생성한다. 그 후에 생성된 해쉬값과 휴대폰 단말기 내의 로그로 남긴 해쉬값을 비교한다. 비교 후 처리단계에서 변조의 유·무를 파악하여 변조



(그림 10) 휴대폰 파일 업로드 무결성 검증 모듈

된 경우 에러 메시지를 보내고, 쓰기 요청을 거부하도록 한다.

5. 결론 및 향후 연구방향

본 논문에서는 모바일 상에서 발생할 수 있는 휴대폰 메시지의 위·변조의 위험성을 실험을 통해 증명하였고, 그로 인한 법적 증거 데이터의 무결성이 저해될 수 있음을 고찰하였다. 휴대폰 메시지에 대한 위·변조 위험성은 법적 증거로써의 데이터의 무결성을 입증하는 것이 무엇보다 중요한 포렌식스 분야에서 상당한 문제가 야기된다. 범인은 사전에 불리한 증거자료로 생각되는 데이터에 대해 위·변조가 가능하게 된다.

또한 휴대폰 메시지의 위·변조를 보완하는 방법에 대한 해결책을 제시하였으며, 앞으로 변화하는 모바일 환경에서 여러 가지 기술적인 어려움과 파생될 수 있는 역기능의 문제들에 대해 심각히 고민해야 한다.

실험을 진행하면서 발생하는 장애요소가 많으며, 앞으로 풀어야할 숙제로 남아있다. 개인적인 연구의 한계를 느끼며 앞으로 국내에 모바일 포렌식스 연구에 관련 교류와 협력을 기대한다. 끝으로 휴대폰 내부 정보에 대한 법적 증명력을 높일 수 있는 다양한 연구 개발과 그에 따른 안티 포렌식스에 대한 대처 방안 연구들이 향후 연구 과제로 적절할 것 같다.

참고문헌

[1] 김기환외, “모바일 포렌식에서의 무결성 입증방안 연구”, 한국컴퓨터정보학회지, 6. 2007, 제15권제1호

[2] 안중호외, “휴대폰에 대한 디지털 정보 수집 기술 연구”, 전남대학교 시스템보안연구센터, 4. 2007

[3] 안중호외, “휴대전화 단말기로 부터의 데이터 획득 기법”, 한국정보보호학회 호남제주지부학술대회, 4. 2007, pp.40-48

[4] 한국디지털포렌식학회, “디지털증거 처리 표준 가이드라인”, 경찰청사이버테러대응센터, 12. 2006

[5] 김현상외, “무결성을 보장하는 디지털 증거 수집 절차”, 한국정보보호 학회 하계 학술대회, 6.2005, CISC05

[6] 김형성외, “Computer Forensics의 법적 문제 연구”, The Institute for Comparative Legal Studies Vol.18 No. 3 December. 2006

[7] 홍석형외, “디지털 증거의 무결성 유지를 위한 절차에 관한 연구”, 한국정보처리학회 추계학술발표대회 논문집 제13권 제2호 11. 2006

[8] 파이널데이터, “국내 최고의 모바일 디지털 증거 분석 솔루션”

[9] QPST, http://www.qualcomm.com

[10] Bitpim, http://www.bitpim.org

[11] EasyCDMA, http://www.plinksoft.com

[12] WinHex, http://www.x-ways.net

[13] UltraEdit, http://www.ultraedit.com