제36회 한국정보처리학회 추계학술발표대회 논문집 제18권 제2호 (2011. 11)

스마트폰 분실 방지를 위한 보안 원격제어 관리 시스템의 설계 및 구현

이재용, 박지수, 박종혁
서울과학기술대학교 컴퓨터공학과
{lastiverse, jisoo08, jhpark1}@seoultech.ac.kr

Design and Implementation of Security Remote Control and Management System for Preventing Smartphone Lost

Jae Yong Lee, Ji Soo Park, Jong Hyuk Park
Dept of Computer Science & Engineering, Seoul National University of Science & Technology

요 약

전체 모바일 시장에서의 스마트폰의 시장점유율이 빠른 속도로 증가하고 있는 가운데 스마트폰 보안 이슈에 대한 관심도 같이 증가되고 있으며, 스마트폰의 분실 및 도난으로 인한 피해의 대응책이 필요하다. 스마트폰의 특성상 휴대성 때문에 분실 및 도난시에 개인정보 유출 등의 2차적 피해가 커질 수 있다. 이러한 피해들을 최소화하기 위해 원격 동기화, 개인정보 접근 차단, 위치정보 송/수신, 원격 카메라 제어, 이벤트 로그 전송 등의 기능을 통해 스마트폰 내부에 저장되는 사용자의 개인정보의 유출을 방지하고 분실 및 도난된 스마트폰의 재습득 가능성을 증대시킬 수 있다. 본 논문에서는 이러한 스마트폰의 분실 및 도난에 대비하는 보안 원격제어 관리 시스템을 제안, 설계하고 구현한다.

1. 서론

정보통신 기술의 발달과 더불어 모바일 시장내의 스마트폰의 점유율도 빠른 속도로 증대되고 있다. 일반적으로 사용되어 오던 피처 폰(Feature Phone)과 달리 스마트폰은 보다 진보되어 PC와 유사한 기능을 탑재한 범용 OS를 내재한 휴대폰이며, 기존의 피처 폰이 제공하는 통신 기능과 PDA를 통해 제공되어 오던 개인 정보관리 기능을 결합한 범용 모바일 기기로 볼 수 있다.

이러한 스마트폰은 통화 및 문자의 송수신을 목적으로 하는 통신 외에 데이터가 송수신되는 네트워크에 항상 접속되어 있고, 스마트폰이 가지는 광범위한 활용성으로 인해 악성 코드에 의한 공격이나 분실 및 도난으로 인해 유출되는 개인정보의 양이 방대해질 수 있다. Gartner는 스마트폰의 성능이 향상될수록 보안사고는 계속해서 늘어날 것으로 예측하고 있으며, 증가되는 보안위협 대비 일반 사용자의 스마트폰 사용의 부주의 및 안전불감증이 크게 부족한 것으로 예측하고 있다.인터넷 보안업체 Trusteer가 개인정보를 불법적으로 알아내어 활용하는 '피싱 사이트'를 조사한 결과 스마트폰 이용자가 데스크톱 PC 이용자보다 세비나 더 쉽게 자신의 민감한 개인정보를 유출시키는 것으로 나타났다 [1,2].

본 논문에서는 스마트폰의 여러가지 보안 위협 요소에 대해 살펴보고, 스마트폰의 도난이나 분실시에 발생할 수 있는 개인정보 유출을 방지하기 위한 원격제어를 할 수 있는 시스템을 제안 및 설계하고 프로토 타입을 구현한다.

2. 관련 연구 및 연구동향

2.1. 스마트폰의 개인정보

'개인정보'의 정의에 대해 '정보통신망 이용촉진 및 정보보호 등에 관한 법률'에서는 "개인정보라 함은 생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 당해 개인을 알아볼 수 있는 부호·문자·음성 및 영상 등의 정보(당해 정보만으로는 특정 개인을 식별할 수 없더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 것을 포함한다)"라고 정의하고 있다. 따라서 스마트폰 상에서의 "전화번호, 주소록, 문자메세지 목록, 스케쥴, 사진, 동영상, 통화기록, 인터넷 접속기록" 등 스마트폰의 내부에 저장되는 대부분의 정보가 개인정보로 정의된다 [3,6].

2.2. 스마트폰 분실 및 도난에 따른 위협요소

예상 가능한 보안 위협요소는 다음과 같다 [4,5].

- 기록(History) 유출 : 스마트폰 내에 저장된 동영상/사진 재생 기록, 검색 기록, 패스워드 기록 등의 유출
- 저장된 정보 유출 : 사진, 동영상, 음악 등의 자료, 저장된 문서나 사용자의 E-mail 계정, 저장된 쿠키 · 세션정보 등의 유출
- 통화, 문자정보 유출 · 조작 : 통화기록과 문자 전

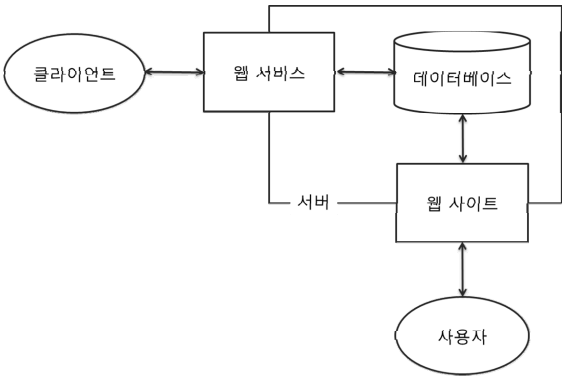
송 기록을 유출되거나 조작을 통해 또다른 2차 피해를 유발

- 과금 유발 : 지속적인 SMS 전송이나 통화 연결을 시도하거나 인가되지 않은 결재 요청을 통한 금전적 피해 유발

3. 시스템 설계 및 구현

3.1 서버 설계 및 구현

본 보안 기법 내에서의 서버의 클라이언트와 주기적으로 통신하면서 사용자로부터 임의의 요청이 들어올 경우 그 요청을 클라이언트에게 전달하는 역할을 한다. 따라서 클라이언트와 통신을 주고 받을 수 있는 웹 서비스, 사용자로부터 임의의 요청을 입력받을 수 있는 웹 사이트, 입력받은 정보를 저장할 데이터베이스로 구성된다.



(그림 1) 서버 흐름도

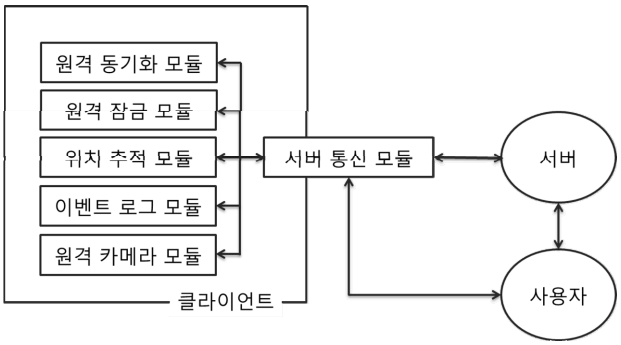
웹 서비스는 클라이언트에서 주기적으로 들어오는 통신 요청을 받아 서버 내의 데이터베이스에 쿼리를 보내 결과를 반환한다. 클라이언트와의 통신 내용은 서버상의 데이터베이스 내에 사용자로부터 새롭게 요청된 내역이 있는지 확인하는 메서드와 클라이언트의 위치정보를 저장하는 메서드, 클라이언트의 이벤트 로그를 저장하는 메서드로 이루어진다.

웹 사이트는 사용자의 스마트폰 분실 시에 사용자가 직접 웹 상에서 원격제어를 실행할 수 있도록 인터페이스를 제공한다. 그 구성 내역으로는 원격 동기화 기능, 원격 잠금 기능, 위치 추적 기능, 이벤트 로그 기능, 원격 카메라 기능 등의 실행 등 5가지로 이루어진다.

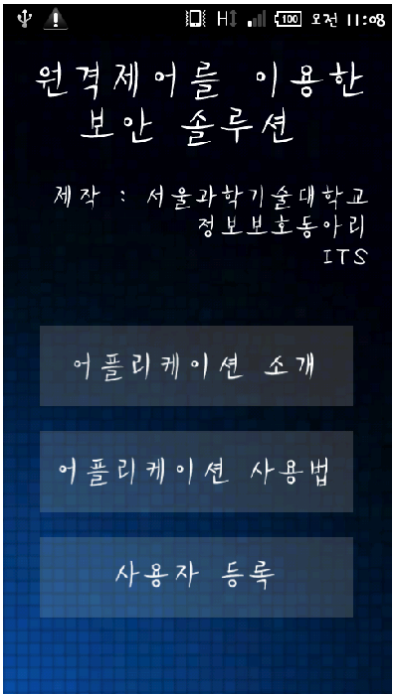
데이터베이스는 분실 및 도난된 스마트폰에 대해 사용자가 요청한 명령을 저장하는 테이블과 스마트폰의 위치정보를 저장하는 테이블, 스마트폰의 이벤트 로그를 저장하는 테이블, 계정정보를 저장하는 테이블로 구성된다.

3.2 클라이언트 설계 및 구현

본 보안기법 내에서의 클라이언트는 주기적으로 서버와의 통신을 통해 사용자로부터의 임의의 요청이 발생할 경우 그 요청에 대응되는 명령을 실행하고 경우에 따라 그 결과를 서버로 반환한다. 클라이언트 내의 모듈은 서버와의 통신을 담당하는 통신 모듈과 사용자로부터 요청된 명령을 실행하는 세부 모듈로 구성된다.



(그림 2) 클라이언트 흐름도



(그림 3) 클라이언트 어플리케이션

3.3 세부 기능 모듈

- **원격동기화**

안드로이드 기반 스마트폰은 사용자의 Google 계정으로 연락처 및 스케쥴 등의 동기화 기능을 제공한다. 이 동기화 기능은 사용자에 의해 수동으로 실행되기 때문에 스마트폰의 분실 및 도난 시에 미처 동기화하지 못한 정보를 확인할 수 있는 방법이 없다. 이를 보완하기 위해 웹상에서 원격으로 동기화하는 기능을 제공하여 사용자가 미처 동기화하지 못했던 주요 개인정보들을 확인 가능하도록 한다.

- **원격 잠금**

분실 및 도난된 스마트폰 내의 개인정보를 임의의 습득자가 접근할 수 없도록 터치패널을 통한 접근을 차단시킨다. 습득자가 Hold 버튼을 눌러 스마트폰 내부의 개인정보에 접근하려 할 경우 자동으로 스마트폰을 Sleep모드로 진입시킴으로써 원격 잠금 기능을 수행한다.

- **위치 추적**

분실 및 도난된 스마트폰의 위치정보를 웹상에서 원격제어를 통해 확인하는 기능을 제공한다. 이 때 GPS위성 기반의 위치추적이 그 활용도나 정확성이 가장 높지만 실내에서는 그 수신률이 급격히 떨어지므로 3G 통신망과 wifi를 이용한 위치정보의 도출 또한 가능하도록 한다.

- **원격 카메라 제어**

현재 출시되는 대부분의 안드로이드 스마트폰의 경우 카메라를 내장하고 있기 때문에 이 카메라 모듈을 웹상에서 원격으로 제어하여 촬영하고 그 결과물을 사용자의 E-mail로 전송함으로써 분실 및 도난된 스마트폰의 재습득 가능성을 증대시킨다.

- **이벤트 로그 전송**

안드로이드 스마트폰은 시스템 내부에서 일어나는 모든 작업들에 대한 로그를 확인할 수 있다. 이러한 특성을 이용하여 스마트폰이 분실이나 도난되었을 때 사용자의 개인정보에 접근할 수 있는 기능들의 이벤트의 로그들을 필터링하고 일반 사용자가 식별 가능한 형태로 가공하여 사용자의 E-mail로 전송함으로써 스마트폰이 분실 및 도난된 상태에서도 자신의 스마트폰에서 어떠한 작업들이 이루어지고 있는지 사용자가 직접 확인이 가능하도록 한다.

4. 결론

본 논문은 스마트폰의 광범위한 활용성과 휴대성으로 인해 분실과 그로 인한 2차적 피해를 줄이고 사용자의 개인정보 유출 방지 및 스마트폰의 재 습득 가능성을 증가시킬 수 있는 방안으로 보안 원격제어 관리 시스템을 제안 및 프로토 타입을 구현하였다.

분실이나 도난으로 인해 발생할 수 있는 보안 위협들에 대해 원격제어를 이용해 사용자가 능동적으로 대처가 가능하도록 하는 본 기법을 통하여 미처 백업해놓지 못한 스마트폰 내의 개인정보를 편리하게 확인할 수 있는 동시에 분실된 스마트폰의 습득자가 임의로 스마트폰 내의 정보들을 열어볼 수 없도록 한다. 또한 분실된 기간 동안의 이벤트 로그들을 사용자가 원격으로 확인이 가능하도록 함과 동시에 스마폰의 위치정보를 송수신하고 원격으로 내장 카메라를 작동시킴으로써 스마트폰의 재 습득 가능성을 증가시키고 사용자의 금전적인 피해를 최소화한다.

향후 연구방안으로 제한적인 사양의 스마트폰의 특성에 맞게 시스템을 경량화시키고 안드로이드 OS를 사용하는 다양한 플랫폼에 대해 서비스를 제공함으로써 증가되는 보안위협에 대비한다. 또한 타인에 의해 고의로 악용되었을 때 되려 사용자에게 커다란 피해를 가져다 줄 수 있는 기능들이기 때문에 어플리케이션 및 서버에서의 관리 기술 및 취약점 분석을 병행하고 사용자의 본인 인증절차가 철저하게 이루어져야 할 것이다.

감사의 글

이 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임 (2011-0024052).

참고문헌

[1] Gartner, "Security risks rise as smart phones get smarter", Computerworld, 2008. 09

[2] Trusteer, "Cell Phone Users Are Gullible, Report Says", PCWorld, 2011. 01

[3] 최정열, "인터넷과 개인정보의 보호," 제6차 학술심포지엄 자료집, 한국정보법학회, 2002. 7

[4] 주세홍, "컨버전스 환경에서 스마트폰 보안위협과 대응전략", A3 Security, 2010. 8

[5] 강동호, 한진희, 이윤경, 조영섭, 한승완, 김정녀, 조현숙, "스마트폰 보안 위협 및 대응 기술", 전자통신동향분석 제25권 제3호, 2010. 6

[6] 남기효, 박상중, 강형석, 길지호, "스마트폰 보안 기술 및 솔루션 동향", 정보통신산업진흥원, 2010. 10