송신자 자가인증 기법 기반의 스팸 SMS 필터링 안드로이드 애플리케이션 구현

양인식[O], 추문박[*], 백전성[*], 강경태[*]
[O*]한양대학교 컴퓨터공학과
e-mail: inshik@hanyang.ac.kr[O], {munbak, jsbaik, ktkang}@hanyang.ac.kr[*]

Implementation of Anti-spam SMS Android Application Using Self-authentication Mechanism

Inshik Yang[O], Wenbo Zou[*], Jeanseong Baik[*], Kyungtae Kang[*]
[O*]Dept. of Computer Science & Engineering, Hanyang University

● 요 약 ●

스팸·스미싱 SMS의 차단을 위하여 지금까지 다양한 차단기법이 개발되어 사용되고 있다. 그 중에서도 대부분을 차지하는 방법들이 기계학습을 통한 내용 기반의 차단과 사용자의 스팸신고를 통한 송신자 차단 방법이다. 그러나 이러한 방법들은 공통적으로 스팸·스미싱을 식별하기 위해 학습 데이터가 필요하다는 문제점을 갖고 있기 때문에, 신종 스팸 공격들은 차단이 불가능하여 차단율의 한계를 보인다. 본 논문에서는 오늘날 사용되고 있는 스팸·스미싱 차단 기법들의 근본적인 문제점들을 규명하고, 이를 해결할 수 있는 스팸차단 기법 중 하나인 송신자 자가인증 기법을 소개한다. 그리고 송신자 자가인증 기법을 적용한 안드로이드 애플리케이션의 구현 및 동작과정을 설명한다.

키워드: 산업구조분석(Industrial Structural Analysis), 경쟁분석(Competitive Analysis), 차별성(Differentiation)

I. Introduction

오늘날 많은 스마트폰 사용자들이 무분별하게 발송되는 불법 광고성 스팸 SMS에 의하여 적지 않은 불편함을 느끼고 있다. 또한 SMS를 이용해 공공기관이나 금융기관 등을 사칭하거나 피해자의 스마트폰을 해킹하여 피해자의 개인정보를 탈취하는 스미싱 범죄 또한 매년 꾸준히 일어나고 있다[1]. 이동통신사 및 개인 스마트폰 사용자들은 이러한 스팸·스미싱 SMS 피해를 방지하기 위하여 여러 가지 차단기법들을 사용하고 있지만, 신종 스팸공격과 오차단 방지를 위한 차단수위 조절 등의 문제로 인하여 높은 차단율을 보이지 못하고 있다.

본 논문에서는 현재 사용되고 있는 스팸·스미싱 차단 기법들의 한계점을 규명하고, 이를 해결하기 위한 방법인 송신자 자가인증 기법을 소개한다. 또한 송신자 자가인증 기법을 적용한 안드로이드 애플리케이션의 구현과 동작을 소개한다.

II. Preliminaries

1. SMS 공격 방법

1.1. 스팸 SMS

스팸 SMS는 수신자의 동의를 받지 않고 불특정 다수의 사람들에게 전송하는 영리 목적의 광고성 SMS를 말한다. 이는 많은 스마트폰 사용자들에게 불편함을 주며 이를 처리하기 위한 시간적·금전적 비용을 발생시킨다. 또한 SMS의 특성상 그 내용이 쉽게 사용자에게 노출되기 때문에, 불법 도박 및 성인 광고 SMS가 스팸 메일에 비하여 청소년들에게 더 큰 악영향을 끼칠 수 있다.

1.2. 스미싱

스미싱(SMiShing)은 문자메시지 서비스(SMS)와 피싱(Phishing)의 합성어로, 피싱 중에서도 SMS를 이용한 피싱 공격을 특정한 말이다. 피싱이란 전자우편이나 SMS, 메신저 등을 통해 신뢰할 만한 사람 또는 기업을 사칭하여 피해자의 비밀번호나 금융정보와 같은 개인정보를 불법적으로 습득하는 행위를 말한다. 또한 가짜 인터넷 사이트를 만들어 피해자에게 개인정보를 입력하도록 유도하는 행위도 피싱이라고 할 수 있다. 이러한 개인정보 유출은 곧 현금인출, 소액결제 등의 경제적 피해로 이어진다.

피싱 중에서도 스미싱의 대표적인 공격 유형으로는, 공공기관이나 은행 등을 사칭하여 피해자의 계좌번호나 비밀번호와 같은 개인정보를 요구하는 유형이 있다. 또한 피해자의 관심을 끄는 문구와 함께 URL을 전송하고 클릭하도록 유도하여 해당 URL을 클릭할 경우 피해자

몰래 악성 애플리케이션을 설치하는 수법을 사용한다. 설치된 악성 애플리케이션은 스마트폰 소액결제 기능을 해킹하여 돈을 탈취하거나, 모바일 뱅킹에 사용되는 은행 애플리케이션들을 삭제한 뒤 가짜 은행 애플리케이션으로 바꿔치기하여 피해자의 모바일 뱅킹 정보를 탈취하는 등의 공격을 수행한다. 이와 같이, 스미싱은 단지 클릭 한 번으로 인해 상당한 규모의 금전적 손실을 일으킬 수 있는 스마트폰 해킹 수법으로 스마트폰 사용자에게 상당한 위협이 된다.

2. 기존 스팸 · 스미싱 SMS 차단 방식

2.1. 내용 기반 차단

내용 기반 차단 방식은 SMS의 내용을 기반으로 스팸·스미싱을 식별하고 차단하는 방법들로, 기본적인 방법으로는 금칙어를 지정하고 내용에 해당 금칙어가 포함되어 있는 경우 차단하는 금칙어 필터를 사용하는 방법이 있다. 더 발전된 방식으로, 기계학습을 통해 스팸 데이터베이스를 학습하고 SMS의 내용을 분석하여 스팸·스미싱 SMS의 가능성이 높은 내용이라고 판단되는 SMS을 차단하는 방법이 있다[2,3]. 그러나 이러한 방법들은 스팸 데이터베이스의 지속적인 업데이트가 필요하며, 업데이트를 하더라도 아래와 같은 이유들로 인하여 완벽한 차단이 불가능하다.

- **희생양이 필요하다** 스패머들은 스팸 데이터베이스에 걸리지 않도록 지속적으로 내용을 바꿔 발송하기 때문에, 학습에 필요한 데이터를 제공할 피해자가 필연적으로 발생한다.
- **학습 데이터가 필요하다** 기계학습을 위해서는 유사한 패턴의 스팸·스미싱 데이터가 일정량 필요하다.
- **학습기간이 필요하다** 높은 스팸·스미싱 식별율을 갖기 위해서는 어느 정도 학습기간이 필요하다.

2.2. 스팸 · 스미싱 신고 송신자 기반 차단

사용자들의 스팸·스미싱 신고와 상호 명 제보 등의 정보를 수집하고, 이를 분석하여 해당 송신자가 스패머인지 혹은 신뢰할만한 송신자인지를 판단하는 방법을 말한다. SMS의 내용에 상관없이 송신자를 차단하는 방법이기 때문에 확인 된 스패머에 대해서는 확실한 차단이 가능하다. 그러나 신고 정보가 부족한 스팸·스미싱 송신자에 대해서는 차단이 불가능하며, 스패머들은 보통 타인의 명의로 가입된 휴대전화를 사용하여 불법 스팸 SMS를 전송하고, 적발 시 전화번호를 계속 바꿔가며 범행을 계속하기 때문에 차단에 한계가 있다.

2.3. 옵트인 & 옵트아웃 제도

옵트인(Opt-in)은 수신자가 사전에 수신을 동의한 SMS만 받도록 하는 법적 제도로, 수신자가 동의하지 않은 그 밖의 SMS 발송은 불법이다. 반대로 옵트아웃(Opt-out)은 기본적으로는 모든 SMS를 수신하지만 수신자가 수신 거부를 표시할 경우 SMS를 전송하면 안 된다는 제도이다. 현재 우리나라에서는 광고 및 홍보 목적의 SMS에 대해서 옵트인 제도를 적용하고 있기 때문에 수신자가 동의하지 않으면 광고성 SMS를 전송해서는 안 된다. 하지만 불법적인 SMS 발송이 만연하기 때문에 추가적으로 스팸 필터링 기법들을 사용해야 하며, 수신자가 의도치 않게 수신을 동의하는 경우도 많아 이상적인 스팸 차단 효과는 갖고 있지 못하다.

3. 송신자 자가인증 기법

송신자 자가인증 기법은 SMS의 정상적인 수신을 위하여 송신자가 직접 인증을 해야 하는 기법이다. 송신자가 SMS를 전송하면 수신자는 해당 송신자가 자신의 화이트리스트에 존재하는지 확인한다. 만약 송신자가 수신자의 화이트리스트에 존재하지 않으면 송신자에게 인증을 요청하는 인증 SMS를 전송한다. 송신자는 이 인증 SMS를 통해 인증을 시도하게 되고, 인증에 성공하면 송신자는 수신자의 화이트리스트에 등록되어 이후에는 인증절차 없이 정상적으로 SMS를 전송할 수 있게 된다.

송신자 자가인증 기법은 화이트리스트를 기반으로 SMS를 처리한다는 점에서 2.3절에서 언급한 옵트인 방식과 거의 동일하게 동작하는 것처럼 보일 수 있다. 하지만 화이트리스트의 갱신이 수신자 측에서 뿐만 아니라 송신자 측에서도 인증을 통하여 이뤄질 수 있기 때문에 옵트인 방식은 아니며, 옵트아웃 방식도 아닌 새로운 별개의 방식이라고 할 수 있다. 이와 같은 방식을 사용하면 악성 SMS임에도 불구하고 정상적인 SMS로 판단해버리는 제2종 오류(False-negative)를 최소화 하면서도 사용자의 편의성은 최대화 하는 것이 가능하다.

III. Implementation

1. 서버 구현

안드로이드 애플리케이션과 상호작용하며 송신자 자가인증 기능을 수행할 리눅스 서버를 구성하였다. 서버는 애플리케이션에서의 송신자 자가인증 처리를 돕기 위해 크게 두 가지 기능을 제공한다.

1.1. 공공 화이트 · 블랙리스트 학습 및 제공

송신자 자가인증 기법을 사용하는 사용자들은 SMS의 송신자를 분류할 때 개개인의 화이트리스트를 사용하게 된다. 여기에 사용자의 편의성을 제공하고 스팸·스미싱 차단율을 높이기 위하여, 서버는 사용자에게 추가적인 공공 화이트·블랙리스트를 제공한다. 서버는 주기적으로 애플리케이션 사용자들에 의해 생성되는 차단 및 인증 전화번호 정보를 수집하고, 수집된 정보를 이용하여 빅데이터 분석을 수행한다. 이를 통해 다수의 사용자들이 공통적으로 등록하고 차단한 전화번호 리스트들을 각각 공공 화이트리스트와 블랙리스트로 생성하고 보관한다. 애플리케이션 사용자들은 서버로부터 이 리스트들을 다운로드하여 내부 데이터베이스에 저장하고, SMS의 송신자 분류 시 개인 화이트리스트와 공공 리스트들을 모두 사용할 수 있게 된다.

1.2. 인증문항 관리 및 제공

구현한 애플리케이션에서는 인증 방법으로 송신자에게 간단한 문제를 전송하고 이에 대한 답을 작성하여 회신하도록 한다. 이 때

사용되는 문항들은 애플리케이션이 아닌 서버에서 관리하며, 애플리케이션은 필요시에 서버로부터 무작위의 인증문항 하나를 다운로드하여 사용한다. 이러한 관리 방식을 통해 인증문항에 대한 보안성을 강화하였다.

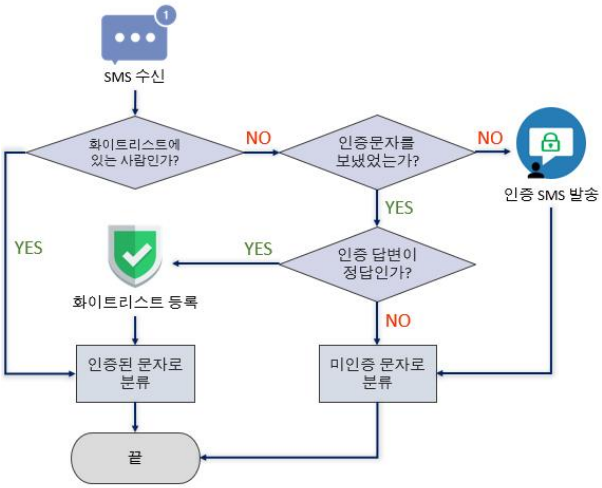

Fig. 1. Flowchart of SMS self-authentication in android application

2. 안드로이드 애플리케이션 구현

송신자 자가인증 기법을 적용한 스팸·스미싱 SMS 차단 안드로이드 애플리케이션을 구현하였다. SMS 수신 시 수신 이벤트가 발생함을 알려주는 안드로이드 브로드캐스트 리시버를 이용하여 SMS를 처리한다. SMS를 수신하게 되면 브로드캐스트 리시버를 통해 수신 이벤트를 전달받아 해당 SMS에 대한 수신자 식별 및 분류를 수행한다. 백그라운드에서 대기하며 SMS의 수신을 기다리는 방식이 아닌 SMS 수신 이벤트가 발생하는 경우에만 동작하는 방식으로 구현하여, 동시 다발적으로 수신되어 수행되는 SMS 핸들링 쓰레드에 대한 동기화 문제와 관련된 데이터 손실 문제를 방지하였다.

Fig. 1은 SMS의 송신자 자가인증을 처리하는 과정을 나타낸 순서도이다. 송신자 자가인증 절차는 크게 송신자 분류, 인증요청, 인증처리의 세 과정으로 나눌 수 있다. SMS를 수신하면 송신자의 인증 여부와 인증의 필요성을 판단하고, 필요하다면 인증절차를 처리하게 된다.

```
CREATE TABLE IF NOT EXISTS pending_table
    (address VARCHAR NOT NULL UNIQUE, qid INT, saflag INT, aflag INT);

CREATE TRIGGER sync_address AFTER DELETE ON pending_table
BEGIN
    INSERT OR IGNORE INTO contact_table (address) VALUES (new.address);
END;
```

Fig. 2. SQLite queries using trigger for integrity of database table

2.1. 송신자 분류

구현한 애플리케이션에서는 사용자의 전화번호부 목록을 송신자 자가인증 방식의 화이트리스트 개념으로써 사용한다. 사용자 스마트폰의 내부 데이터베이스에 저장되어 있는 전화번호부 정보를 바탕으로 데이터베이스 테이블을 생성하여 화이트리스트로 사용한다. 일반적인 컴퓨팅 환경에서는 데이터베이스에서 기존 테이블을 참조하는 외래키 테이블을 사용하여 다수의 테이블 간 동기화 작업을 수행하는 방법을 사용한다. 하지만 스마트폰 환경에서는 이러한 방법을 사용할 수 없기 때문에 Fig. 2와 같이 데이터베이스 트리거를 사용하여 데이터의 무결성을 유지하고, 기존의 테이블에서 필요한 최소한의 정보만 추출하도록 하여 데이터베이스 접근으로 인한 오버헤드를 최소화하였다.

SMS를 수신하면 애플리케이션은 우선 송신자가 수신자의 화이트리스트에 있는 지의 여부를 확인한다. 만약 송신자가 화이트리스트에 있으면 해당 송신자는 인증된 송신자로 취급하여 별도의 인증절차를 거치지 않고 정상적으로 SMS을 수신한다. 반대로 송신자가 화이트리스트에 없으면 해당 송신자는 미인증 송신자로 취급되어 자가인증 절차를 거치게 된다.

2.2. 인증요청

송신자 분류 시 송신자가 화이트리스트에 존재하지 않아 미인증 송신자로 분류된 경우, 이전에 해당 송신자에게 인증요청 SMS를 전송했었는지의 여부를 확인한다. 만약 인증 SMS를 전송한 적이 없다면 애플리케이션은 서버와의 통신을 통해 준비된 다수의 인증문항 중에 무작위로 하나의 문항을 다운로드하여 인증 SMS에 실어 해당 송신자에게 전송한다. 그리고 추후 답변의 정답 여부를 판단할 때 사용할 목적으로 해당 문항에 대한 정보를 내부 데이터베이스에 저장한다. 외부의 서버에서 인증 SMS를 보내지 않고 사용자 애플리케이션에서 보냄으로써 서버의 부하를 줄이고 서버로의 개인정보 노출을 최소화하였다. 만약 송신자에게 인증 SMS를 전송한 적이 있다면 수신한 SMS는 인증 SMS에 대한 답변으로 취급되어 인증처리 절차를 거치게 된다.

2.3. 인증처리

수신한 SMS의 송신자가 미인증 송신자로 분류되고, 인증 SMS를 전송한 적이 있다면 해당 SMS는 그 내용과는 상관없이 인증 SMS에 대한 답변으로 취급된다. 애플리케이션은 인증 SMS을 전송했을 때 저장해두었던 인증문항에 관한 정보를 불러와서 그 문항의 정답과 SMS의 내용이 서로 일치하는지 비교한다. 만약 SMS의 내용이 정답과 일치하면 애플리케이션은 해당 송신자를 화이트리스트에 추가하여 이후 해당 송신자로부터의 SMS는 인증과정 없이 정상적으로 수신하도록 한다. 반대로 SMS의 내용이 정답과 일치하지 않으면 애플리케이션은 송신자에게 인증에 대한 답변이 틀렸다는 SMS를 전송한 후 작업을 마친다.

```
private static DatabaseManager uniqueInstance;
private DatabaseManager(Context _context) {
    context = _context;
}

public static DatabaseManager getInstance(Context context) {
    if(uniqueInstance == null)
        uniqueInstance = new DatabaseManager(context);
    return uniqueInstance;
}
```

Fig. 3. Singleton pattern of database manager fragment in android application source code

3. 싱글턴 패턴

구현한 안드로이드 애플리케이션은 메인 액티비티를 제외한 모든 액티비티 및 프래그먼트가 싱글턴 패턴(Singleton pattern)을 따른다. 싱글턴 패턴이란 어떤 클래스의 객체를 오직 하나만 생성하고 사용하는 디자인 패턴을 말한다. 적용하고자 하는 클래스를 정적 클래스로 만들어 사용하면 생성자가 여러 차례 호출되더라도 처음 생성된 단일 객체만을 재사용할 수 있다. 구현한 애플리케이션은 기능 수행 시 메인 컨트롤 플로우 진행, 데이터베이스 사용 등의 여러 작업을 수행하기 때문에 데이터베이스와 같은 자원의 동기화 문제가 발생한다. 모든 작업들을 하나의 메인 컨트롤 플로우에 구현하는 직관적인 방법으로 동기화 문제를 해결할 수도 있지만, 이는 코드의 가독성을 떨어뜨리며 객체지향 접근법이 갖는 높은 확장성 및 유지·보수의 효율성 등의 장점을 얻을 수 없다. 따라서 구현한 애플리케이션에서는 Fig. 3과 같이 정적 클래스를 사용하여 싱글턴 패턴을 따름으로써 이와 같은 문제를 해결하였다.

IV. Discussion

오늘날 사용되고 있는 스팸·스미싱 SMS 차단 애플리케이션들은 대부분 사용자의 신고정보를 이용하는 데이터베이스 기반의 방법이나 기계학습을 통한 식별 방법들을 사용하기 때문에 지속적으로 데이터베이스 업데이트를 수행한다. 하지만 이러한 방법들은 이전에 수집된 SMS 데이터를 기반으로 악성 여부를 식별하기 때문에 신종 스팸·스미싱은 차단이 불가능하다.

송신자 자가인증 방식을 이용한 스팸·스미싱 차단 애플리케이션은 기존의 데이터베이스 기반의 식별이 아니라 송신자의 유효성을 검증하는 방법을 사용하기 때문에 신종 스팸·스미싱도 차단이 가능하다. 또한 수신자가 아닌 송신자 측에서 인증이 이루어지므로 수신자의 입장에서 별다른 조치나 데이터베이스의 업데이트 없이도 스팸·스미싱 차단 효과를 얻을 수 있다.

물론 정상적인 송신자의 입장에서는 인증 절차를 거쳐야 하는 추가 작업이 발생하여 조금 번거로울 수 있다. 그래도 송신자의 전화번호를 알고 있지 않은 수신자에 대해 최초 한 번의 인증절차만 거치면 되므로 일반적인 상황에서는 큰 불편함 없이 사용 가능할 것으로 보인다.

간혹 스패머임에도 불구하고 인증 SMS를 통해 인증을 하는 악용 사례가 발생할 수 있다. 대부분의 스패머들은 대량문자 발송서비스를 통해 대량으로 스팸 SMS를 발송하기 때문에 이런 사례는 극히 드물게 발생하지만, 이를 대비하기 위하여 추후 다른 상용 스팸·스미싱 차단 애플리케이션들과 같이 기계학습 기반 URL 검사기법 등의 내용 기반 차단 기법의 추가를 고려하고 있다.

REFERENCES

[1] Yeboah-Boateng and Ezer Osei, *"Phishing, SMiShing & Vishing: An Assessment of Threats Against Mobile Devices,"* Journal of Emerging Trends in Computing and Information Sciences, Vol. 5, No. 4, pp. 297-307, 2014.

[2] Jae Woong Joo, Seo Yeon Moon, Saurabh Singh, and Jong Hyuk Park, *"S-Detector: An Enhanced Security Model for Detecting Smishing Attack for Mobile Computing,"* Telecommunication Systems (TCS), Vol. 66, No. 1, pp. 29-38, Sep. 2017.

[3] Gaurav Sethi and Vijender Bhootna, *"SMS Spam Filtering Application Using Android,"* International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 5, No. 3, pp. 4624-4626, 2014.