공학석사학위논문

허위 사용자 정보를 이용한 피싱 웹사이트의 공통 동작 기반 스미싱 공격 방지 기법

Preventing SMishing Attack Using Fake User Information Based on Common Behavior of Phishing Websites

2014 년 2 월

서울대학교 대학원

전기.컴퓨터 공학부

한 승 환

허위 사용자 정보를 이용한 피싱 웹사이트의 공통 동작 기반 스미싱 공격 방지 기법

Preventing SMishing Attack
Using Fake User Information
Based on Common Behavior of Phishing Websites

지도교수 조 유 근

이 논문을 공학석사학위논문으로 제출함

2013 년 12 월

서울대학교 대학원

전기.컴퓨터 공학부

한 승 환

한승환의 석사학위논문을 인준함

2013 년 12 월

위 원 장 : _____민 상 렬_____ (인)
부위원장 : _____조 유 근_____ (인)
위 원 : _____김 지 홍_____ (인)

요약

스미싱 공격은 모바일 피싱 공격의 한 유형으로 스마트폰 사용자의 개인정보를 탈취하거나 소액결제 등으로 금전적 피해를 입히는 것을 목적으로 한다. URL이 포함된 메시지로 사용자를 속여 악의적인 웹사이트에 접속을 유도하는 방법으로 최근 피해 사례가 크게 증가하고 있다.

본 논문에서는 스마트폰의 스미싱 공격 방지 기법으로 몇 가지 기법을 합쳐 'Phishing URL Detector'를 제안한다. 첫 단계에서는 접속할 URL을 분석하여 알려진 피싱 URL 패턴이 포함된 경우 접속을 차단한다. 두 번째 단계로 모바일 웹 브라우저의 북마크와 접속 이력을 기반으로 한 whitelist를 검색해 접속할 URL이 포함돼 있으면 안전한 것으로 간주하고 접속을 허용한다. 세 번째 단계에서는 blacklist를 검색하여 접속할 URL이 포함되어 있으면 위험한 URL로 간주하고 접속을 차단한다. 마지막은 URL의 안전성을 판단할 수 없는 단계이므로 우선 URL에 접속한 뒤 허위 사용자 정보를 입력한 뒤 웹사이트의 동작을 분석하고 피싱 웹사이트인지 판별한다. 이 기법은 입력하는 정보의 유효성을 실시간으로 확인할 수 없고, 모두 입력 되었는지 확인만 가능하다는 피싱 웹사이트의 특징을 이용한다. 따라서, 허위 사용자 정보에도 유효성 검사 후 재입력 요구 없이 다른 동작이 진행된다면 피싱 웹사이트로 판별할 수 있다.

URL에 접속해 보기 전에는 피싱 URL 판별이 어렵다는 기존의 문제점을 해결할 수 있는 본 기법은 스미싱 공격을 효과적으로 방지할 수 있는 첫 번째 방어막이 될 수 있다.

주요어 : 스미싱, 모바일 피싱, 허위 사용자 정보, 피싱 웹사이트 공통 동작

학 번 : 2012-20883

목차

그림 목차

표 목차

제 1 장 서론

스마트폰이 생활 필수품으로 자리잡으면서 인터넷과 함께 생활에 필요한 많은 일을 처리할 수 있는 세상이 되었다. 이에 따라 자연스럽게 스마트폰에는 사용자의 중요한 정보들이 많이 저장되고 있다. 사용자 개인 별로 특화된 사용 환경을 제공하고 신용카드나 소액 결제 등 생활에 매우 밀접한 기능을 장소에 관계 없이 다양하게 이용할 수 있기 때문에 PC 보다 중요한 개인정보들이 더 많이 저장된다. 거기에 더해, 스마트폰은 증권 거래 및 금융 관련 업무를 처리할 수 있으며 사용자 인증 등 각종 중요 정보를 저장하고 전달함과 동시에 많은 사람들의 연락처 정보도 저장할 수 있다. 기술의 발전으로 스마트폰의 성능이 빠르게 향상되어 PC 와 비교되는 수준까지 도달 하였으며, 스마트폰으로 할 수 있는 일이 계속 늘어나면서 점점 더 많은 수의 스마트폰이 보급되고 더 많은 개인정보가 저장되고 있다.

가트너(Gartner) 등 여러 시장조사기관의 조사를 토대로 한 자료에 따르면, 전세계 스마트폰의 출하량이 2009 년 이후 급격히 성장하기 시작하여 2012 년을 기점으로 데스크탑(desktop)과 랩탑(laptop)을 포함한 PC 의 출하량을 앞지르기 시작했으며, 그 격차는 점점 더 벌어지게 될 것이라고 한다 (그림 1.1 참조)[1]. 이와 같은 경향은 국내도 마찬가지여서, 미국의 시장조사기관인 스트래티지 애널리틱스(Strategy Analytics)에서 발표한 2012 년

기준 주요 국가의 스마트폰 보급률 추이를 보면, 한국이 67.6%의 가장 높은 스마트폰 보급률을 보이고 있다 (그림 1.2 참조)

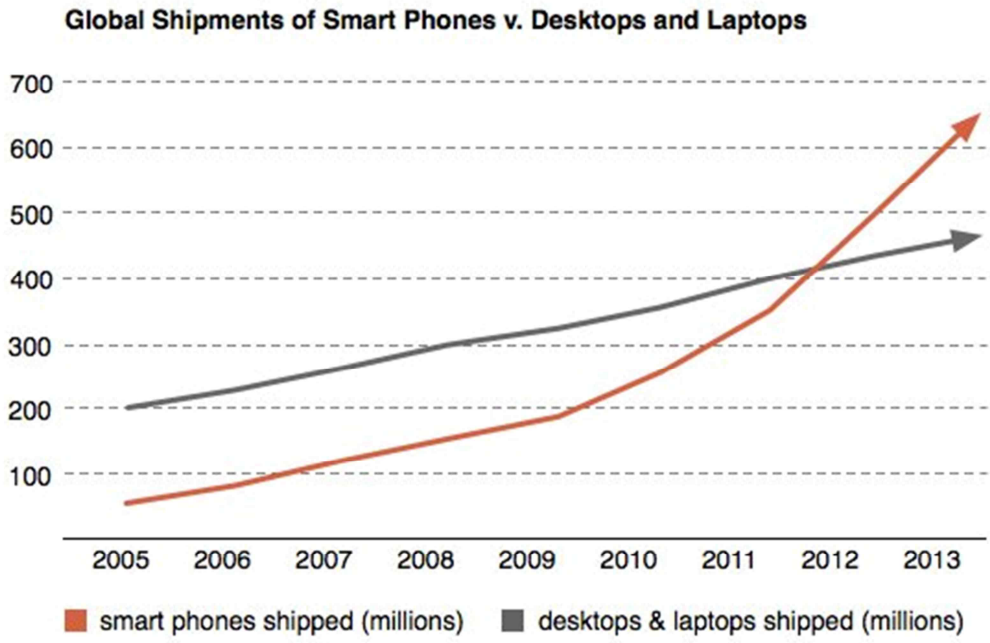

그림 1.1 전세계 스마트폰과 PC 출하량 비교 추이[1]

따라서, 이와 같은 스마트폰의 증가세를 따라 스마트폰을 대상으로 하는, 다시 말해 스마트폰에 저장된 개인정보를 노리는 범죄 역시 증가하게 될 것임을 어렵지 않게 짐작할 수 있다. 실제로 다양한 형태로 스마트폰 사용자의 개인정보를 노리는 모바일 피싱(mobile phishing) 공격들이 지속적으로 보고되고 있으며, 피해사례도 꾸준히 증가하고 있다. 특히, 본 논문에서 중점적으로 다루고 있는 스미싱 공격의 경우를 예로 들어보면, 그림 1.3 과 같이 보안전문기업 안랩(AhnLab)에 접수된 모바일 피싱용 악성코드 샘플의 수가

[1] 출처 : [1]

2013 년 상반기에 매우 큰 증가세를 보이고 있으며, 특히 8 월에는 전월 대비 2 배 이상 급증하고 있음을 확인할 수 있다 [2].

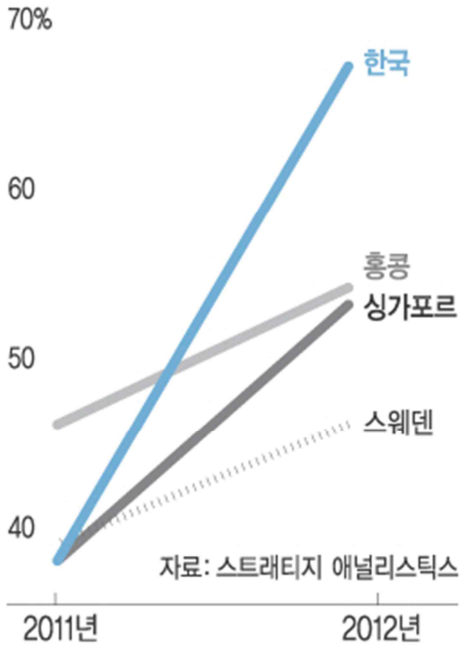

그림 1.2 주요국 스마트폰 보급률 추이[2]

피싱(phishing) 공격은 진짜와 유사하게 위조되거나 복제된 가짜 웹사이트(website)로 사용자를 유도하여 직접 개인정보를 입력하도록 속이거나 악성코드를 유포시키는 계기를 만든다. 즉, 일정 부분 사용자의 직접적인 개입을 필요로 한다는 점에서 기술적인 방법을 이용해 시스템(system)에 침입하거나 악성코드를 침투시키는 일반적인 크래킹(cracking) 공격과는 차이를 보인다. 따라서, 어느 정도 자동화된 하드웨어(hardware) 또는 소프트웨어(software)적인

[2] 출처 : http://www.connectinglab.net/wordpress/?p=6411

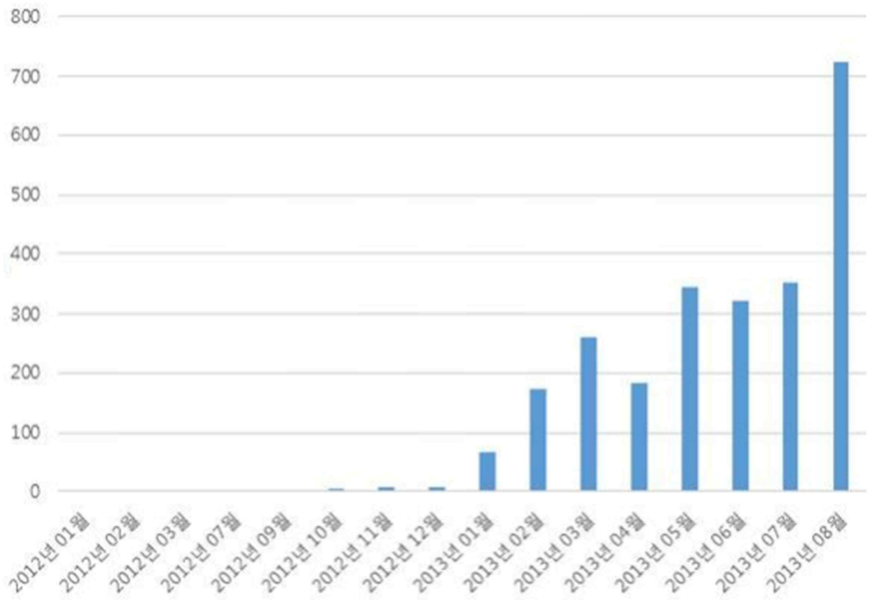

그림 1.3 월별 스미싱 악성코드 접수량 추이[3]

도구를 이용해 침입을 탐지하고 방어할 수 있는 크래킹 공격과 달리 피싱 공격은 사용자의 주의와 직접적인 회피 노력을 필요로 한다는 특징이 있다. 사용자에게 무의식적으로 형성되어 있는 대상에 대한 신뢰를 이용하여 사용자를 속이고 필요한 정보를 직접 입력하도록 유도하기 때문에 자동화된 도구만으로는 공격을 탐지하고 방어하는데 한계가 있기 때문이다. 또한, 피싱 공격의 형태는 매우 다양하고 교묘하게 변형되고 있기 때문에 사용자가 공격 시도 자체를 알아채기 어려운 경우도 많이 있다. 실제로 그림 1.3 에서 보는 것처럼 최근 피해 사례가 급증하고 있는 것은 다양한 공격 유형을 사전에 탐지하기도 어려울 뿐만 아니라 사용자가 공격에 속아 넘어가는 경우도 그만큼 많이 발생하고 있음을 의미하는 것으로 볼 수 있다.

[3] 출처 : [2]

본 논문에서는 위와 같이 사용자가 피싱 공격에 노출될 위험이 큰 환경에서 사용자를 안전하게 보호하고 미처 알아채지 못한 채로 스미싱 공격의 피해를 입는 경우를 방지하기 위한 기법을 제안한다.

피싱 웹사이트가 사용자를 속여 개인정보를 입력하도록 유도하지만 입력된 개인정보의 유효성은 실시간으로 확인할 수 없다는 공통적인 특징을 이용하여 의심스러운 웹사이트에 허위 사용자 정보를 입력한 뒤 보이는 동작을 분석하여 피싱 웹사이트를 판별한다. 이를 위해 피싱 웹사이트들이 목적으로 하는 정보를 입력 받은 후 나타내는 공통적인 동작 패턴을 분석하고 분류하였으며, 알려진 실제 피싱 웹사이트에 접속해 허위 개인정보를 입력하고 동작을 확인해 보는 방법으로 제안 기법이 실제로 효과가 있는지 확인 하였다. 아울러 전달 받은 URL(Uniform Resource Locator)의 위험성을 사전에 검사하고 접속을 차단하기 위한 기법과 whitelist 와 blacklist 를 함께 운영하는 기법까지 포함하여 안드로이드 플랫폼(platform)에서 제안된 모든 기법을 구현하기 위한 프로토타입(prototype)을 제안한다.

이를 위해 본 논문은 먼저 2 장에서 모바일 피싱과 스미싱 공격에 대해 알아보고 관련 연구 동향을 살펴보는 순서를 갖는다. 3 장에서는 스미싱 공격 방지 기법 연구 과정으로 스미싱 공격의 특성을 분석한 내용과 ‘Phishing URL Detector’의 구체적인 제안 내용을 서술한다. 그리고, 4 장에서 기법의 효용성 확인을 위해 수행한 실험의 내용과 제안 기법을 실제로 구현하기 위한 프로토타입을 제시하고 구현 시 고려해야 할 사항 등에 대해 살펴본 뒤, 마지막으로 5 장에서 결론을 맺는다.

제 2 장 스미싱 공격

본 장에서는 모바일 피싱과 스미싱 공격에 대해 자세히 살펴본다. 또한, 스미싱 공격을 비롯한 여러 모바일 피싱 공격법과 방지법들을 분석하고 분류한 관련 연구들에 대해서도 살펴본다.

2.1 모바일 피싱 공격

모바일 피싱 공격은 스마트폰과 같은 모바일 기기를 대상으로 한 피싱 공격을 통칭한다. 먼저 피싱 공격에 대해 알아본다. 피싱 공격은 사용자를 속여 사용자의 계정 정보나 암호와 같은 개인정보 또는 신용카드나 은행 계좌와 같은 금융정보를 탈취한 뒤 이를 악용하여 금전적인 이익을 도모하는 것을 목적으로 한다. 신뢰할 수 있는 지인이나 기관 등을 사칭한 이메일(e-mail) 또는 메신저(messenger)를 사용자에게 보내 유명 웹사이트를 복제한 가짜 웹사이트에 접속하도록 유도한 뒤 목적으로 하는 정보를 입력하도록 유도하거나 악성코드를 몰래 설치해 중요 정보를 탈취하는 공격 형태를 보인다 [3].

피싱에 사용되는 가짜 웹사이트 다양하게 위조된다. 보통 카드사나 은행 또는 페이팔(PayPal)과 같은 유명 웹사이트의 로그인(log-in) 페이지나 결제 정보 입력 페이지와 같이 사용자에게 익숙하면서 중요한 정보를 입력할 것을 요청하는 웹 페이지를 모방하거나 페이스북(Facebook)과 같은 유명 소셜 네트워크 서비스(SNS, Social Network Services)의 로그인 페이지 등을 모방한다. 사용자는 주의 깊게 살펴보지 않는 한 복제된 가짜 웹사이트임을 알아채기 쉽지 않

다. 그리고 공격자가 목적으로 하는 정보를 취득한 뒤에는 정상 웹사이트로 연결을 전환시키는 경우가 많기 때문에 사용자는 미처 알지 못하는 사이에 중요 정보를 직접 유출시키고도 이 사실을 알아채지도 못한 채 피해를 입게 된다.

피싱이란 용어는 낚시를 의미하는 'fishing'에서 유래하여 보통 해커(hacker)들이 단어에 포함된 'f'를 'ph'로 바꾸는 습성에 따라 변형되었을 것으로 보고 있으며, 복잡한 미끼들을 사용해서 사용자의 중요한 정보를 '낚는다'는 의미로 사용되고 있다 [4][5]. 피싱 공격의 수법은 교묘하고 다양하게 진화하고 있으며, 피해 사례도 꾸준히 증가하고 있다. 따라서, 이로 인한 피해를 미연에 방지하기 위해 피싱 공격을 탐지하고 방어하기 위한 기법들도 역시 꾸준히 연구되고 있다.

모바일 피싱은 최근 스마트폰의 보급이 급속도로 진행됨에 따라 발생 비율도 함께 증가하고 있다. 비약적으로 향상된 스마트폰의 성능에 비해 여전히 보안과 관련된 기능은 PC보다 부족하기 때문에 스마트폰에서는 사용자들을 속일 방법을 보다 쉽게 찾을 수 있는 반면, 스마트폰의 제약으로 공격을 탐지하는 것은 더 어렵다. 또한, 위에 언급한 것처럼 많은 개인정보가 저장되기 때문에 공격에 노출되었을 경우 더 큰 피해를 입을 수 있다. 스마트폰에서는 아래 세 가지 이유로 인해 사용자들이 피싱 공격에 노출되기 쉽다 [6].

시큐리티 인디케이터의 제약. 기본적으로 PC보다 훨씬 작은 크기의 화면을 가진 스마트폰은 화면에 표시할 수 있는 내용에 제약이 따를 수 밖에 없다. 때문에 스마트폰용 모바일 웹 브라우저(mobile web browser)는 PC용 웹 브라우저와 달리 신뢰할 수 있는 웹사이트나 보안 접속 여부와 같은 시큐리티 인디케이터(security indicator)를

화면에 표시하기 어렵다. 이로 인해 사용자는 신뢰할 수 없는 웹사이트에 접속했거나, 보안 접속이 지원되지 않는 악의적인 웹사이트로 강제 접속되는 경우에도 이를 인지하기 어렵기 때문에 모바일 피싱 공격에 보다 쉽게 노출되는 경우가 발생한다.

응용 프로그램과 웹의 상호 연동. 스마트폰은 인터넷에 항상 연결되어 있는 것을 전제로 동작하기 때문에 응용 프로그램(application. 이하 'app')에서 웹 브라우저를 호출해 웹(web)에 접속하거나 반대로 웹에서 app을 호출하는 동작이 자연스럽게 발생한다. 따라서, 개인정보를 입력하도록 유도하거나 악성코드를 설치하기 위해 사용자가 악의적인 웹사이트에 접속하도록 유도하는 동작도 정상적인 동작으로 인식하기 때문에 피싱 공격에 노출된 사실을 인지하지 못하게 된다.

단순한 모바일 웹 페이지. 화면의 크기가 작고 PC에 비해 제약이 많은 스마트폰에서는 모바일 웹 브라우저를 위해 따로 구현된 모바일 웹 페이지에 접속한다. 보통의 웹 페이지는 모바일 웹 브라우저에서는 일부분만 표시되거나 정상적으로 동작하지 않는 경우가 발생할 수 있기 때문이다. 대부분의 모바일 웹 페이지들은 비교적 단순하게 디자인 되는데, 이 점이 공격자가 손쉽게 해당 웹사이트를 복제해 악의적인 웹 페이지를 만들 수 있는 요인이 된다. 그리고 사용자는 이렇게 위조된 가짜 웹 페이지를 매우 주의 깊게 살피지 않는 한 쉽게 구별할 수 없기 때문에 피싱 공격에 쉽게 노출될 수 있다.

따라서, 최근에는 모바일 피싱 공격이 심각한 문제로 대두되고 있는데 이 중에서도 스미싱 공격은 모바일 피싱 공격의 가장 많은 형태로 이용되고 있어 큰 문제가 되고 있다.

2.2 스미싱 공격

스미싱 공격은 'SMS'와 'Phishing' 두 단어를 조합한 것으로, 모바일 피싱 공격의 한 유형에 해당한다. 사용자를 유혹하는 단문 메시지(Short Message Service. 이하 'SMS')에 URL을 첨부하여 전송해 악의적인 가짜 웹사이트에 접속하도록 유도한 뒤 악성코드를 몰래 설치하거나 개인정보를 입력하도록 유도하여 가로챈 다음 금전적인 피해를 입히거나 2차 공격의 도구로 활용한다. 최근에는 SMS 뿐만 아니라 다양한 메신저 app을 이용해 URL이 포함된 메시지를 전달하는 경우도 등장하고 있다. 스마트폰에서는 URL이 포함된 SMS를 이용해 광고를 하거나 인터넷 상의 내용을 공유하는 경우가 많기 때문에 사용자의 의심을 피하기 쉬워 모바일 피싱 공격 유형의 다수를 스미싱 공격이 차지하고 있다. 수신된 URL에 접속할 때 사용되는 모바일 웹 브라우저는 앞서 언급한 바와 같이 PC용 웹 브라우저만큼 강력한 보안 성능을 갖추고 있지 않고 구성이 간단한 모바일 웹 페이지는 쉽게 위조될 수 있기 때문에 사용자가 스미싱 공격으로 피해를 입을 확률은 더 올라가게 된다.

스미싱 공격이 행해지면 사용자에게 특정 웹사이트의 계정이 만료되었다거나 비밀번호를 변경하라는 권고 메시지 등과 함께 URL이 전달되어 가짜 웹사이트로 접속을 유도한다. 또는, 요즘 인터넷을 통해 파티나 행사의 초대장을 전송하는 서비스를 사칭해 지인의 초대장으로 위장하거나, 연락처가 변경된 지인의 안내문으로 위장하는 등 다양한 방법으로 사용자를 유혹한다. 진짜와 거의 동일해 쉽게 구별이 어려운 가짜 웹사이트에 접속한 사용자는 이를 알아채지 못하고 제시된 안내에 따라 자신의 계정 정보 또는 결제 정보 등 공격자가 목적

으로 하는 정보를 입력하게 된다. 입력이 완료되면 가짜 웹사이트는 사용자의 접속을 다시 진짜 웹사이트로 전환 시키고, 사용자는 가짜 웹사이트에서 스스로 정보를 유출한 사실도 모른 채 지나간다. 이후 공격자는 취득한 정보를 이용해 소액 결제 등 금전적인 피해를 입히거나 2, 3차 공격을 위한 자료로 활용한다.

위와 같은 방식 외에도 사용자가 가짜 웹사이트에 접속했을 때 보안 프로그램 등으로 위장한 악성코드를 스마트폰에 다운로드 하여 설치하도록 유도하거나 몰래 설치되게 한 뒤 스마트폰에 저장된 개인정보를 유출시키는 유형도 존재한다. 또한, 최근에는 설치된 악성코드가 개인정보를 유출한 뒤 스마트폰을 동작 불능 상태로 만들고, 그 사이 공격자는 본인 인증 문자 등을 가로채 사용자 본인으로 위장해 개인정보를 추가로 탈취하거나 소액 결제를 진행하는 등 여러 형태로 변형된 공격 유형들이 보고되고 있다 [7].

위와 같이 스미싱 메시지는 대부분 사용자가 신뢰할 수 있는 기관이나 지인, 친근한 형태의 광고 등을 사칭하고 있으며, 모바일 웹 브라우저를 이용해 전달된 URL에 쉽게 접속할 수 있기 때문에 사용자는 각별히 주의하지 않을 경우 매우 쉽게 스미싱 공격에 노출될 수 있다. 더군다나, 스마트폰은 PC에 비해 여러 제약이 있어 PC를 위한 피싱 공격 방지법이 그대로 적용될 수 없기 때문에 위험에 노출될 확률은 더욱 커진다. 상대적으로 작은 화면으로 인해 표시할 수 있는 정보의 양이 제한되어 있다는 점, 모바일 웹사이트를 비롯해 스마트폰의 사용자 인터페이스(user interface)가 PC에 비해 구조적으로 단순하다는 점 등이 대표적인 요인이 된다. 모바일 웹 브라우저 역시 상대적으로 PC용 웹 브라우저만큼 강력한 보안 기능을 지원하지 않기 때문에 스스로 악의적인 웹사이트를 탐지하고 접속을 차단하는 기

능을 제공할 것을 기대하기 어렵다. 또한, 구조가 단순한 모바일 웹사이트는 공격자가 위조하기 쉽다는 문제점도 있다. 알려진 연구에 의하면 스마트폰 사용자는 PC 사용자에 비해 약 3배 가량 더 피싱 공격의 위험에 노출되고 있는 것으로 보고 있다 [8].

2.3 관련 연구

다양한 형태의 피싱 공격이 보고되고 있는 만큼, 피싱 공격 방지법에 대한 연구도 다양하게 진행되고 있다.

일반적으로 PC의 피싱 공격은 브라우저와 이메일을 통해 이루어지는 경우가 많다 [9]. 하지만 모바일 피싱의 경우에는 블루투스(Bluetooth. 이하 'BT')와 SMS, 음성 인터넷 프로토콜(Voice over Internet Protocol. 이하 'VoIP') 및 app과 모바일 웹 브라우저 등을 통해 공격이 이루어질 수 있다. 이에 대해 K. Dunham은 그의 저서에서 모바일 기기의 피싱 공격을 'BT 피싱'과 'SMS 피싱(스미싱)', 'vishing'으로 알려진 'VoIP 피싱' 등으로 구분하고 있다 [10].

모바일 피싱에 대한 탐지 기법 중 가장 대표적인 것은 content-based filtering 기법이다. 전송 받은 메시지의 내용을 분석하여 피싱 공격의 위험이 있을 경우 이를 차단하거나 사용자에게 경고해 준다. 피싱 공격뿐만 아니라 불법 스팸(spam) 메시지나 이메일을 탐지하는 데도 널리 사용된다. 하지만 분석 대상이 되는 메시지의 내용이 너무 광범위하고 위험성 여부를 판단하기 위한 단어나 표현도 상황에 따라 다르게 해석될 수 있기 때문에 단독으로는 큰 탐지 효과를 거두기 어렵다는 단점이 있다 [11].

이 외에도 blacklist와 whitelist, heuristic과 같은 기법들이 모바일 피싱을 방지하기 위한 기법으로 연구되고 있으며, blacklist와

feature-based와 같은 두 가지 피싱 탐지 기법을 함께 사용하는 방법, blacklist, whitelist와 graylist를 기반으로 하는 이메일 피싱 탐지 기법 등이 다양하게 제안되고 있다 [12][13][14][15].

일반적으로 스마트폰과 같은 무선 모바일 기기는 처리 능력이나 저장 공간, 전력 등의 제약으로 인해 PC의 피싱 공격 방지법이 동일하게 적용될 수 없다. 따라서, 모바일 피싱에 대한 방지법은 좀 더 간단하면서도 정확도를 높일 수 있어야 한다 [16].

여러 연구에서 제안되고 있는 모바일 피싱 방지 기법들을 정리해 보면 공통적으로 스미싱 탐지, 보이스 피싱 탐지, 모바일 웹 브라우저 피싱 탐지 등으로 나눌 수 있다. 이에 따라, [16]에서는 모바일 기기를 대상으로 한 공통적인 탐지 기법을 분류하여 Content-based filtering, Blacklist 및 Whitelist 기법 등으로 정리하고 있으며, 그림 2.1과 같은 분류표를 보여주고 있다. 그림에 따르면, 모바일 기기에 대한 피싱 공격의 형태는 유형별로 BT와 SMS, VoIP와 모바일 웹 app을 이용한 형태로 나누어진다. 그리고, 각 공격 유형별로 다양한 탐지 기법이 제안되고 있음을 확인할 수 있다. 특히, 본 논문의 주제인 스미싱의 경우는 content-based Filtering과 blacklist, whitelist 기법이 공통적인 탐지 기법으로 제안되고 있다.

Content-based filtering 기법의 대표적 사례는 [11]에서 찾아볼 수 있다. 앞서 언급된 content-based filtering 기법의 단점을 보완하기 위해 challenge-response protocol이라 명명된 기법을 결합한 것으로, 스팸 가능성이 있는 메시지에 대해 발신자의 신분을 인증하기 위한 challenge 메시지를 보여주고 발신자가 올바른 response 메시지를 보낼 때만 요청된 메시지의 전송을 허용한다. 이는 대부분의 스팸 메시지나 이메일이 컴퓨터를 이용해 자동으로 대량 전송되는 경

우가 많다는 특징을 이용한 것으로, 발신자가 컴퓨터일 경우에는 challenge-response protocol에 올바르게 응답할 수 없어 발신이 차단된다.

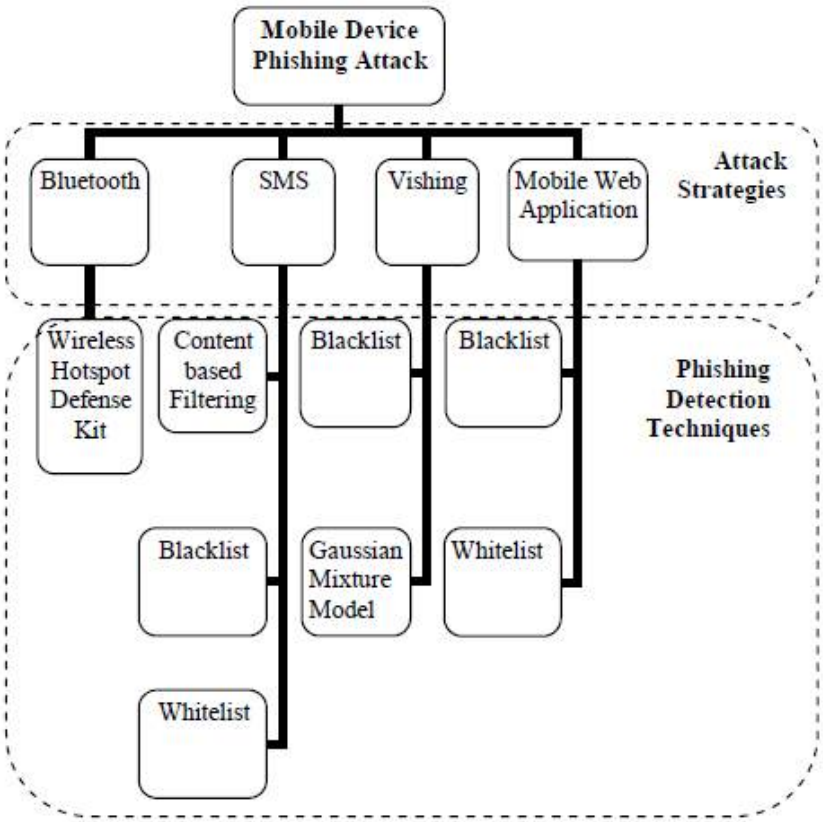

그림 2.1 모바일 피싱 공격&탐지 유형 구분도[4]

Blacklist는 폭넓게 피싱 방지 분야에 사용되고 있는 기법으로 모든 피싱 URL 및 관련 내용을 보관하므로 blacklist에 포함된 URL을 전달 받았을 경우에는 정확하게 피싱 URL임을 탐지해 낼 수 있다. 오탐률(false positive)이 매우 낮고 비교적 구조가 간단하다는 특징

[4] 출처 : [16]

이 있지만, 목록에 들어 있지 않은 새로운 공격 유형에 대해서는 효율적으로 대처할 수 없다는 단점이 있다.

마지막으로 whitelist 기법은 blacklist 기법과는 달리 접속해도 안전한 것으로 여겨지는 거의 모든 웹사이트를 목록으로 보관하고 비교하여 목록에 포함된 웹사이트에 대해서만 접속을 허용한다. 따라서, 목록에 포함된 웹사이트들의 안전성을 보장 받음과 동시에 새로운 피싱 URL에 대처할 수 없는 blacklist의 단점을 보완할 수 있다. 하지만, 실제로는 방대한 양의 웹사이트 목록을 모두 저장하고 관리하는 작업이 매우 큰 부담이 되므로 완벽한 whitelist는 사실상 구현이 어렵다는 제약이 있다.

PC용 웹 브라우저에서는 피싱 공격에 의한 사용자의 로그인 정보 유출을 차단하기 위해 'LoginInspector'가 제안되었다 [17]. 'LoginInspector'는 브라우저 익스텐션(extension)으로 구현되어 사용자의 로그인 활동을 감시한다. 감시 중에 사용자가 성공적으로 로그인 한 웹사이트의 URL 및 관련 로그인 정보를 별도로 안전하게 저장하여 whitelist를 구성하고, 차후 저장된 URL과 로그인 정보가 일치되는 경우에만 접속을 허용한다. 사용자는 본의 아니게 피싱 공격에 노출되어 접속한 가짜 웹사이트가 아무리 친숙한 곳과 유사하더라도 접속된 URL이 다르므로 주의를 요하는 경고를 받을 수 있어 웹 브라우저의 부족한 피싱 탐지 기능을 보완한다.

Whitelist를 기반으로 하는 'LoginInspector'는 위와 같이 비교적 간단한 개념을 바탕으로 긍정적인 피싱 방지 효과를 보이고 있어 본 논문에서 제안하는 'Phishing URL Detector'의 whitelist 관련 개념을 정립하는데 참고가 되었다. 다만, 안드로이드 스마트폰의 모바일

웹 브라우저는 PC 웹 브라우저와 같은 익스텐션을 추가할 수 없기 때문에 웹 브라우저를 직접 수정해야 'LoginInspector'와 같이 직접 브라우저가 접속한 URL과 사용자의 로그인 활동을 관찰하고 저장할 수 있다. 따라서, 본 논문의 'Phishing URL Detector'는 웹 브라우저의 웹사이트 접속 이력(history)과 북마크(bookmark)를 이용해 whitelist를 구성하고, 모바일 웹 브라우저로 전달되는 URL의 피싱 위험도를 판단하는 것으로 개념을 다시 정의 하였다. 또한, 사용자의 로그인 정보를 직접 수집하는 대신 피싱 위험도가 있는 것으로 판단된 URL들을 별도의 blacklist에 저장하고 전달 받은 URL과 알려진 피싱 URL의 패턴(pattern)을 비교하여 위험성을 분석하여 방지 효율을 높이는 방안을 제안 하고 있다.

제 3 장 스미싱 공격 방지 기법

스미싱 공격의 방지 기법을 연구하는 과정으로 스미싱 공격의 특성을 분석한 내용을 자세히 살펴본다. 또한, 피싱 웹사이트의 공통적인 동작 패턴을 분석한 과정과 'Phishing URL Detector'의 제안 내용을 자세히 서술한다.

3.1 스미싱 공격 특성 분석

3.1.1 스미싱 공격 흐름 분석

스미싱 공격의 특성을 분석하는 과정으로 먼저 스미싱 공격의 흐름을 분석해 본다. 이 과정을 통해 스미싱 공격의 방지는 결국 각 단계별 공격의 흐름을 차단하는 것임을 확인할 수 있었다. 또한, 좀 더 좋은 방지 효과를 얻을 수 있는 차단 단계와 많은 관련 연구들이 고려하고 있는 차단 단계에 대해서도 확인해볼 수 있었다.

스미싱 공격에 대한 2.2절의 설명을 바탕으로 스미싱 공격의 흐름과 각 단계별 구분을 그림 3.1로 정리 하였다. 그림에서 보는 바와 같이, 스미싱 공격은 크게 공격자에 의해 이루어지는 부분과 사용자에 의해 이루어지는 부분으로 나눠진다. 또한, 취해지는 행위를 기준으로 사용자가 수신한 URL을 선택하기 전과 선택한 후의 단계 및 공격자가 목적으로 하는 정보를 취득한 이후 단계로도 나눠진다. 스미싱 공격뿐만 아니라 다른 피싱 공격도 세부적인 내용에서 차이는 있지만 대략적인 흐름은 그림과 유사하다.

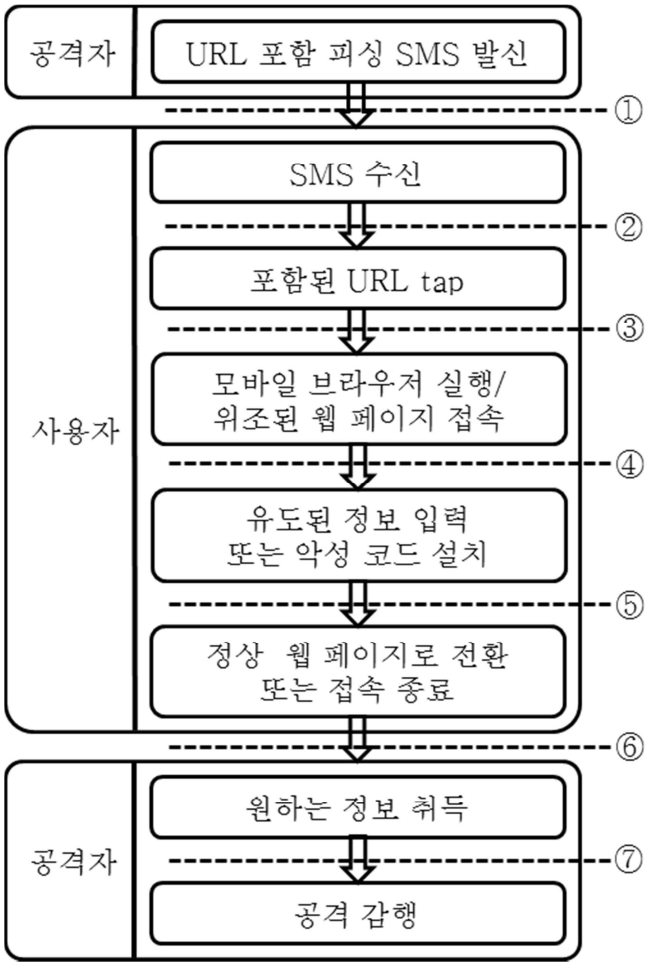

그림 3.1 스미싱 공격 흐름도 및 단계 구분

위 그림을 통해 스미싱 공격의 방지 기법은 공격의 흐름 중 어느 단계를 차단할 것인가가 중요함을 알 수 있다. 즉, 다음 단계로 진행하기 위해 필요한 조건들을 파악하고 그 중 하나 또는 모든 조건을 차단하거나 조건 자체를 없애 버림으로써 다음 단계로 진행하지 못하게 하여 공격자가 중요 정보를 탈취하지 못하도록 해야 한다. 2.3 절에서 언급된 여러 관련 연구들뿐만 아니라 널리 사용되고 있는 상용 피싱 방지 솔루션 제품들의 경우도 대부분 위와 같은 개념에 초점을

맞춘 방지 기법을 제안하고 있다.

그림 3.1에서 각 단계별로 취해질 수 있는 대략적인 방지 기법을 아래와 같이 정리 하였다.

① 단계 : 스팸 SMS의 발신/수신 차단. 스미싱 공격의 주요 수단이 되는 가짜 웹사이트의 URL을 포함한 SMS의 발신을 차단하거나 사용자에게 수신되지 않도록 하면 스미싱 공격을 비교적 원천적으로 방지할 수 있다.

② 단계 : URL 선택 차단. 스미싱 SMS가 수신되었어도 사용자가 포함된 URL을 선택하지 못하게 차단하면 공격을 방지할 수 있다. 이 때 중요한 것은 사용자가 정상 URL과 위험 URL을 확실히 구분 지을 수 있도록 도와주는 것이다.

③ 단계 : URL 접속 차단. 사용자가 스미싱 SMS의 URL을 선택해도 선택된 URL에 대한 접속을 자동으로 차단할 수 있다면 공격을 방지할 수 있다. 피싱 URL을 사전에 판별해 내는 능력이 매우 중요하다.

④ 단계 : 피싱 웹 페이지 분석 및 차단. URL에 접속한 경우에도 접속한 웹 페이지를 분석해 피싱 위험이 있으면 사용자의 정보 입력을 차단하거나 악성코드가 자동으로 설치되는 것을 차단하면 공격을 방지하고 사용자를 보호할 수 있다. 다양한 형태의 피싱 웹 페이지를 자동으로 분석해낼 수 있는 기법이 중요하다.

⑤ 단계 : 접속 전환 차단. 사용자가 이미 중요 정보를 입력한 후에도 웹 페이지 전환을 차단하고 이후 단계의 진행을 차단 하면 유출된 정보를 보호하고 공격을 방지할 수 있다. 하지만, 기술적 관점으로는 사실상 방지가 어려운 단계에 해당한다.

⑥ 단계 : 적용 가능한 방지법 없음. 피싱 웹사이트를 벗어나게 되면 유출된 정보가 이미 공격자에게 전달되었다고 볼 수 밖에

없다. 따라서, 스미싱 공격은 더 이상 방지할 수 없다. 다만, 이론적으로는 웹 페이지 전환 내역을 분석하여 피싱 웹사이트에 접속했던 사실을 탐지할 수 있으면, 사용자에게 가능한 한 빨리 이 사실을 경고하고 유출된 정보를 변경하여 공격자가 취득한 정보가 무의미 해지면 피해를 예방할 수 있다.

⑦ 단계 : 사실상 적용 가능한 방지법이 없는 단계에 해당한다.

위 내용에 따르면, 공격 흐름의 초반에는 메시지 전송을 차단하거나 URL 접속을 차단하는 등 비교적 간단한 방지법을 적용할 수 있고, 기대할 수 있는 방지 효과도 큰 편에 해당한다. 반면, 흐름의 후반으로 갈수록 방지법을 적용하기 위해 고려해야 할 사항이 더 복잡해지고 방지법을 실제 적용하기도 어려워지는 것을 확인할 수 있다. 결국 공격의 흐름은 초반에 차단하는 것이 상대적으로 간단하면서도 좋은 결과를 기대할 수 있다.

이와 같은 경향은 앞서 2.3 절에서 언급된 관련 연구 및 상용 피싱 방지 솔루션 제품에서도 확인할 수 있다. 예를 들어, [16]의 content-based filtering 기법은 수신된 메시지의 내용을 기반으로 피싱 여부를 판단하여 차단하므로, 그림 3.1의 ①단계에 적용될 기법으로 볼 수 있다. 또한, blacklist와 whitelist 기법은 각각 수신 받은 메시지에 포함된 URL의 피싱 여부를 판단하여 차단하는 기법이므로 그림 3.1의 ②와 ③ 단계에 적용될 수 있는 방지 기법으로 볼 수 있다. 상용 피싱 방지 솔루션 제품들도 대부분 자체적으로 피싱 URL의 정보를 보관하고 있는 서버(server)를 이용해 URL의 피싱 여부를 판단하는 blacklist 기반 기법을 사용하고 있으므로 그림 3.1의 ②와 ③ 단계에 해당한다. 마지막으로 content-based filtering 기법과 함께 challenge-response protocol을 결합하여 피싱 위험이 있는 메

시지가 자동으로 전송되지 못하도록 차단하는 기법[11]도 위험성이 있는 메시지의 전송 자체를 차단하고 있으므로 그림 3.1의 ① 단계에 적용될 수 있는 기법으로 볼 수 있다.

결국 대부분의 방지 기법은 스미싱 공격 흐름 상 초기에 적용되어 공격의 흐름을 비교적 초반에 차단하는 것을 목적으로 하고 있음을 알 수 있다. 하지만, 앞서 살펴본 바와 같이 스미싱 공격에 의한 피해가 지속적으로 증가하고 있는 상황에 비춰볼 때 단순히 공격의 흐름을 초반에 차단하는 기법만으로는 만족할 만한 방지 효과를 얻기는 어려운 것으로 여겨진다. 이와 같은 이유로 본 논문에서는 'Phishing URL Detector'의 주요 기법으로 오히려 공격의 후반부인 ④, ⑤단계에 적용되어 허위 정보를 이용해 웹사이트의 동작 내용을 근거로 피싱 웹사이트인지 판별하는 기법을 제안하고 있다.

3.1.2 스미싱 공격 특징 분석

스미싱과 같은 피싱 공격은 사회 공학(social engineering) 기법에 기반을 두고 있다. 즉, 사람들간에 상호 작용 시 형성되는 기본적인 신뢰를 이용해 사용자를 속여 정상적인 보안 절차를 깨트리기 위한 비기술적인 수단을 바탕으로 하고 있다 [18]. 이것은 다시 말해 피싱 공격을 방지하는데 있어 시스템 자체의 자동화된 보안 못지 않게 인간적인 차원의 보안 역시 매우 중요함을 의미하고 있다.

실제로 피싱 공격은 사용자가 착각할 수 있는 친숙한 조건을 다양하게 설정해 놓고 여기에 속아 넘어간 사용자가 공격자가 목적으로 하는 정보를 직접 입력하거나 악성코드의 설치를 허용하도록 유도하는 형태를 취하고 있다. 사용자가 신뢰할 수 있는 기관이나 유명 웹

서비스 등을 위조의 대상으로 삼기 때문에 사용자가 무의식적으로 지니고 있는 대상에 대한 기본적인 신뢰가 오히려 피싱 공격의 위험에 사용자를 쉽게 노출 시키는 약점이 된다. 그리고 사용자가 공격에 노출되었다는 사실을 깨닫지 못하거나 오랜 시간이 걸리도록 만드는 원인이 되기도 한다. 피싱 공격은 이와 같이 사용자의 신뢰라는 비기술적 특징에 기반하여 사용자의 직접적인 행동을 유발하는 공격 형태를 취하고 있기 때문에 기술적인 접근 만으로는 공격을 탐지하고 방어하는데 한계가 있을 수 밖에 없으며 일정 부분 이상 인간적인 주의와 방어 대책이 필요할 수 밖에 없다는 특징을 가진다.

스미싱 공격은 또한 공격 진행 과정이 매우 간단하다는 특징을 지니고 있다. 위에서 살펴본 바와 같이 스미싱 공격은 미끼 URL이 담긴 SMS를 수신한 뒤 포함된 URL을 선택하면 스마트폰의 모바일 웹 브라우저를 이용해 곧바로 악의적인 웹사이트에 접속하는 과정을 따른다. 이와 같은 스미싱 공격이 이루어지는 동안 관계되는 app은 SMS를 수신하는 '메시지 app'과 URL 선택 후 실행되는 '모바일 웹 브라우저'가 전부로 스마트폰의 다른 기능이나 사양 등에 큰 영향을 받지 않는 부분으로 이루어져 있다. 또한, 공격의 진행과 관련된 동작도 'SMS의 수신'과 'URL의 선택' 및 '웹 페이지 접속'이라는 매우 간단한 단계로 이루어지기 때문에 스마트폰 전체의 성능에 큰 영향을 받지 않고, 스마트폰의 전체 동작에 미치는 영향 역시 매우 적다. 그리고 접속 이후에 개인정보의 입력이나 악성코드의 다운로드 같은 부분도 모바일 웹 브라우저 내에서 이루어지는 동작이 대부분이다.

결과적으로 스미싱 공격의 진행이 실제로 스마트폰의 기능이나 사양, 전체 동작 등에 영향을 끼치거나 받는 부분은 미미한 편이며, 이와 같은 특징은 스마트폰에서 스미싱 공격을 감지하고 방어하기 위한

기법을 적용하는데 있어 기술적으로 큰 어려움을 겪게 만드는 요인이 된다. 기술적인 관점에서 보면 스미싱 SMS를 수신할 때와 정상 SMS를 수신할 때 스마트폰에서 특정 동작이나 app 사용의 차이점이 발생한다거나, 피싱 URL에 접속할 때 기술적인 특성의 변화가 관찰되지 않기 때문이다. 즉, 어떤 형태로든 스마트폰 고유의 특성을 이용한 기술적인 접근으로 스미싱 공격을 차단하기 위한 기법을 개발하는 것은 어려움이 있을 수밖에 없다.

다음으로 스미싱 공격은 매우 빠른 속도로 공격 형태와 패턴이 진화하고 있으며 다양한 변종이 존재한다는 특징이 있다. 전형적인 스미싱 공격은 사용자를 속이기 위해 꾸며진 SMS에 URL을 포함시켜 전송하고 사용자의 접속을 유도하는 형태로 시작되었지만, 최근에는 2.2 절에서 언급한 바와 같이 메신저 app 등으로 URL 전송 매개체를 다양화하고 있다. 메신저 app의 사용자 계정을 취득하여 피싱 URL을 배포하는 형태의 스미싱 공격은 메신저 app이 SMS app보다 친구나 친숙한 지인들만 메시지를 주고 받는 폐쇄성이 더 높다는 특성으로 인해 사용자가 보다 쉽게 스미싱 메시지에 속게 된다. 이 외에도 사용자를 유도하기 위한 메시지의 내용도 점점 더 교묘해지고, 위조되는 웹사이트 역시 진짜와 더 구별하기 어렵게 정교해지고 있어 기존의 방지 기법들이 신속히 대처하지 못하는 경우가 많이 발생하고 있다. 따라서, 지속적인 주의를 기울이지 않으면 예기치 못한 순간에 쉽게 공격에 노출될 수 있다.

마지막으로 스미싱 공격에 사용되는 피싱 URL은 실제로 직접 접속해 보기 전에는 위험한 URL인지 명확히 판별하기 어렵다는 특징이 있다. 이는 스미싱 공격뿐만 아니라 피싱 공격 자체의 특징이기도 한

데, 피싱 공격에 사용되는 URL은 공격자가 임의로 만들어낼 수 있는 부분이고 공격자의 의도에 따라 어떤 형태로든 변형 및 조작이 가능하기 때문에 URL만을 가지고 위험도를 분석하거나 피싱 여부를 판별하는 것은 한계가 있을 수 밖에 없다. 물론 [9]와 같이 피싱 URL의 공통적인 패턴을 분석하는 등 위험도를 예측하기 위한 연구가 많이 진행되고 있지만, 이러한 분석만으로 판별해낼 수 있는 피싱 URL의 비율은 그렇게 높지 않기 때문에 큰 공격 방지 효과를 기대하기는 어렵다. 실제로 본 논문에서 제안하고 있는 'Phishing URL Detector' 역시 [9]를 참조해 URL에서 피싱 URL 패턴을 분석해 내는 기능을 포함하고 있지만, 실제 피싱 URL 조차 패턴 분석을 통해 피싱 URL로 판별되는 비율이 높지 않은 것을 확인할 수 있었다.

정리하면, 스미싱 공격은 사용자의 신뢰를 기반으로 하는 비기술적인 공격 형태를 취하고 공격 진행 과정이 매우 간단해 공격 방지를 위해 스마트폰의 특성이나 기술적인 측면을 이용한 접근이 어렵다는 특징이 있다. 또한, 빠른 속도로 공격 형태와 패턴이 변형되고 있다는 점과 피싱 URL에 직접 접속하지 않고는 명확한 판별이 어렵다는 특징이 더해져 신속히 공격 유형을 분석하고 대응하는데 어려움이 있다.

3.1.3 스미싱 SMS 특징 분석

스미싱 SMS는 다음과 같은 특징을 갖고 있다.

첫 번째는 거의 모든 스미싱 SMS가 URL을 포함하고 있다는 점이다. 이는 공격자가 꾸며놓은 악의적인 웹사이트로 사용자를 유도하기 위한 미끼의 역할로 SMS를 전송하는 것이기 때문에 당연한 공통점에 해당한다. 하지만, 이러한 특징은 반대로 스미싱 SMS를 색출해

내기 위한 좋은 단서가 될 수 있다. 즉, SMS와 MMS를 포함해 전송되는 메시지에 대해 URL을 포함한 경우와 URL이 포함되지 않은 경우에 서로 다른 보안적인 관심을 기울이는 기법을 적용한다면 스미싱 메시지가 전송되는 비율을 크게 낮출 수 있는 효과를 기대할 수 있다.

예를 들어, [11]에서 제안하고 있는 challenge-response protocol 기법과 같이 content-based filtering 기법과 함께 의심되는 메시지에 challenge-response protocol을 적용하면, 단순히 URL이 포함되어 있는 메시지에 대해서만 전송 중 인증 과정을 추가하는 것 만으로도 스미싱 메시지의 자동 전송을 제한할 수 있다.

다음으로 스미싱 SMS 뿐만 아니라 대부분의 스팸 메시지는 공격자가 소량을 직접 전송하기 보다는 자동화된 방식을 이용해 다수의 사용자들에게 대량으로 전송한다는 특징을 가지고 있다. 공격자는 조금이라도 더 많은 수의 사용자가 공격에 노출되기를 원하기 때문이다. 따라서, 메시지를 전송하는 과정에서 컴퓨터나 웹 서비스 등을 이용해 자동으로 대량 전송되는 메시지에 대해 위와 같은 challenge-response protocol 기반의 추가 보안 기법을 적용하거나 수신자에게 메시지의 전송이 컴퓨터나 웹 서비스를 통해 이루어졌음을 알려줄 수 있다면 스미싱 메시지의 전송을 제한하고 사용자의 주의를 환기시키는 효과를 기대할 수 있다.

마지막으로 스미싱 SMS는 발신 번호가 사용자의 전화번호부에 저장되어 있지 않은 경우가 많다는 점과 동일한 발신 번호로 여러 번 수신되지 않는다는 점을 특징으로 들 수 있다.

스미싱 SMS의 발신 번호가 사용자의 전화번호부에 저장되어 있는 경우는 발신 번호로 이용된 번호의 사용자가 이미 스미싱 또는 피싱

공격에 노출되어 개인정보에 해당하는 전화번호부를 탈취당한 뒤 2차 공격이 진행되고 있음을 의미한다. 이 경우는 저장된 지인들을 대상으로 스미싱 SMS를 전송하기 때문에 수신자가 더 쉽게 공격에 속을 수 있다는 위험이 있다. 하지만, 대부분의 경우는 공격자가 불특정 다수의 사용자들에게 스미싱 SMS를 유포하기 때문에 스미싱 SMS의 발신 번호는 전화번호부에 저장되어 있지 않을 확률이 훨씬 높다.

또한, 스미싱 SMS는 사용자의 호기심을 자극하고 의심을 피하기 위해 대개 1~2회 정도만 발신될 뿐 같은 내용이 주기적으로 반복해서 발신되지 않는다. 이는 반복해서 전송되는 광고용 메시지와 차별되는 점으로 인터넷 상에서 피싱 웹사이트들이 짧은 시간 동안만 존재하다 사라진다는 점을 반영한 특징이라 볼 수 있다. 따라서, 스마트폰에서 동일 발신 번호 또는 동일 메시지 내용을 기준으로 수신 패턴 등을 정리해서 보여줄 수 있다면 사용자가 보다 쉽게 광고용 SMS와 스미싱 SMS를 구별해낼 수 있을 것이다.

위와 같은 스미싱 SMS의 특징을 이용하여 본 논문은 'Phishing URL Detector' 기법 외에 추가 제안으로 'Challenge-Response Authentication' 기능을 메시지 센터 (Message Center. 이하 'MC')에 적용하여 URL이 포함된 메시지의 전송을 관리하는 내용을 포함하고 있다. 통신사에서 직접 관리하고 있는 MC에 제안 내용과 같은 추가 보안 기법들이 적용되면 자동으로 전송되는 스미싱 메시지들을 차단하고 피해를 상당수 감소시킬 수 있을 것으로 기대된다.

3.2 Phishing URL Detector 제안

본 논문에서 제안하는 'Phishing URL Detector'는 몇 가지 기법을

하나로 묶어 완전한 스미싱 방지 솔루션으로 제안되고 있다. 그 중 본 논문에서 주요하게 다루는 기법은 중요 정보의 입력을 유도하는 형태의 피싱이 의심되는 웹사이트에 허위 사용자 정보를 보내고 웹사이트의 동작이 피싱 웹사이트의 공통 패턴에 해당하는지 확인함으로써 피싱 웹사이트를 판별하고 개인정보의 유출을 막는 기법이다.

앞에서 살펴본 스미싱 공격의 여러 특성을 통해 스미싱 공격은 자동화된 기술적인 접근으로는 완벽하게 차단하기 어렵다는 것을 확인할 수 있었다. 다양한 형태로 진행되고 있는 관련 연구에서도 스미싱과 모바일 피싱의 여러 특징을 모두 고려할 수 있는 근본적인 방지 기법은 아직 제안되지 못하고 있다. 이에 따라 본 논문에서는 3.1.1 절에서 언급한 바와 같이 단순히 스미싱 공격의 진행을 차단하는 기법으로는 효율적인 방지 효과를 거두기 어렵다고 판단하고 다른 형태의 방지 기법을 제안하는데 집중하였다.

본 연구에서는 피싱 웹사이트를 효율적으로 판별하는 기법을 도출하는 것에 집중하였다. 그리고 이것은 전달된 피싱 URL의 위험도는 직접 접속해 보기 전에는 확실히 판별할 수 없다는 스미싱 공격의 주요 특징이자 문제점 중 하나를 해결하기 위한 것에 해당한다. 많은 기존 연구들이 직접 접속 없이 전달된 URL의 위험도를 분석하고 예측하는 방법으로 방지 기법을 제안하려는 것과는 방식을 달리한다.

이에 따라 본 논문의 제안 기법은 피싱 웹사이트들이 목적으로 하는 중요 정보를 입력 받은 뒤에 공통적으로 보이는 동작 패턴을 분석하고, 피싱 웹사이트가 의심되는 경우 전달된 URL에 직접 접속하여 허위 사용자 정보를 입력하고, 입력된 정보에 대해 접속한 웹사이트가 보이는 동작을 분석하여 피싱 웹사이트인지를 판별하는 것을 기본 내용으로 제시하고 있다. 중요 정보를 입력할 것을 요구하는 형태의

피싱 웹사이트는 입력되는 정보의 유효성을 실시간으로 검사할 수 없기 때문에, 허위 정보가 입력된 경우에도 이 점을 알아차리고 재입력을 요구하는 동작을 보이지 않는다. 따라서, 허위 정보를 입력했을 때 유효성 검사를 진행하고 재입력을 반복해서 요구하는 웹사이트는 진짜 웹사이트로 간주할 수 있지만, 허위 정보 입력 후에도 유효성 검사 없이 정해진 동작을 실행한다면 접속 웹사이트는 피싱 웹사이트로 판별할 수 있는 근거가 된다. 결국 사용자를 속이기 위한 피싱 웹사이트를 역으로 속이는 동작을 통해 접속한 웹사이트가 피싱 웹사이트인지 판별해 낼 수 있는 것이다. 이와 같은 기법을 도출하기 위해 먼저 알려진 피싱 웹사이트들의 공통적인 동작 패턴을 분석하는 작업을 진행 하였다.

3.2.1 피싱 웹사이트 공통 동작 패턴 분석

피싱 웹사이트는 알려진 바와 같이 공격자가 필요로 하는 사용자의 개인정보를 취득하기 위해 사용자가 속기 쉬운 형태로 꾸며진 가짜 웹사이트를 의미한다. 피싱 웹사이트는 공격자의 의도에 따라 중요 정보를 입력할 것을 요구하는 형태와 자동으로 악성코드를 설치하는 형태로 크게 나눌 수 있다. 이 중 본 논문에서는 중요 정보를 입력할 것을 유도하는 형태의 피싱 웹사이트를 판별하는 것에 집중하고 있다. 악성코드를 몰래 설치하는 형태는 기존의 방지법이나 모바일 웹 브라우저 자체에서 허가되지 않는 파일 다운로드를 자동으로 차단하는 기능을 이미 많이 제공하고 있기 때문에 본 논문의 논의 대상에서는 제외한다.

위와 같은 피싱 웹사이트들이 가지는 가장 공통적이면서 큰 약점이 될 수 있는 속성은 입력된 정보의 유효성은 검사하지 못한다는 점이

다. 본 논문의 제안 기법은 바로 이점을 역으로 이용하고 있다. 즉, 진짜 사용자의 정보 대신 허위 정보를 전송했을 때 접속한 웹사이트가 나타내는 동작을 분석하여 피싱 웹사이트인지를 판별한다.

예를 들어, 사용자의 금융 정보를 탈취하기 위해 특정 은행을 사칭해 꾸며진 가짜 웹사이트로 유도한 경우, 사용자가 가짜 웹사이트임을 구분하지 못하고 요구되는 계좌 정보와 보안카드 정보 등을 입력하면 해당 정보는 그대로 공격자에게 전달된다. 그리고, 접속했던 웹사이트는 정보가 입력된 것을 확인하고 본래 계획됐던 동작을 실행한다. 입력 확인 후 본인 인증을 위해 다시 로그인 하라는 안내와 함께 진짜 은행의 웹사이트로 접속을 전환하는 것을 예로 들 수 있다. 하지만 이 과정에서 피싱 웹사이트는 사용자가 입력한 정보가 진짜 정보인지 확인할 수 있는 방법은 없다. 사용자의 진짜 금융 정보를 사전에 갖고 있어 비교해 보거나, 사용자의 정보 입력과 동시에 진짜 웹사이트에서 정보의 유효성을 확인하지 못하기 때문이다. 결국, 피싱 웹사이트는 사용자가 요구하는 항목을 입력 하기만 하면 입력이 완료된 것으로 간주할 수 밖에 없고, 입력이 완료된 정보는 보관해 놓을 수밖에 없다. 이것은 다시 말해 피싱 웹사이트가 사용자의 기본적인 신뢰를 이용해 중요 정보를 탈취하는 만큼 반대로 사용자가 올바른 정보를 입력할 것이라는 신뢰를 바탕으로 하고 있음을 의미한다. 따라서, 사용자의 입장에서는 피싱 웹사이트가 전제하고 있는 이러한 신뢰를 역으로 이용하여 의심스러운 웹사이트에 허위 개인정보를 보낸 후 나타내는 동작을 분석하면 확실하게 피싱 웹사이트를 판별해낼 수 있는 근거가 된다.

일반적으로 피싱 웹사이트에서 요구하는 개인정보의 유형은 몇 가지로 분류될 수 있다. 첫 번째는 사용자의 로그인 정보 즉, 아이디

(ID)와 비밀번호이다. 이용자의 수가 많은 페이스북과 같은 웹 서비스의 경우 사용자가 계정을 갖고 있을 확률이 높기 때문에 가짜 로그인 페이지나 계정 정보 갱신 페이지 등을 위조해 사용자를 유도하고 로그인 정보를 탈취한다. 이렇게 탈취된 로그인 정보를 이용해 사용자의 친구들에게 다시 피싱 메시지를 전송하거나 유료 서비스 결제를 통해 요금을 청구 받게 만드는 등의 공격을 감행한다.

두 번째는 사용자의 결제 관련 정보 즉, 신용카드나 모바일 소액결제 등과 관련된 정보이다. 최근에는 PC뿐만 아니라 스마트폰을 이용해서도 인터넷상에서 결제가 가능하기 때문에 사용자의 결제 정보를 저장해 두고 사용할 수 있는 서비스가 많이 등장하고 있다. 앞서 예를 들었던 페이팔과 같은 서비스가 대표적인 경우로 사용자의 신용카드 정보를 등록해 두면 다른 웹 서비스에서 간편하게 인터넷 결제가 가능하므로, 페이팔 등의 결제 정보 입력 페이지를 위조한 피싱 웹사이트를 통해 사용자의 신용카드 정보를 탈취한 뒤 금전적인 피해를 입히는 경우가 많이 발생하고 있다.

세 번째는 사용자의 금융 관련 정보이다. 우리나라는 금융기관의 인터넷뱅킹 서비스를 이용 시 공인 인증서와 보안카드 등을 이용한 보안 단계를 거치도록 의무화 되어 있다. 피싱 웹사이트는 이점을 악용하여 유명 금융기관과 동일한 웹사이트를 구축하고 사용자에게 개인정보 보호를 위한 정보 갱신 등의 이유 또는 본인 인증 등의 이유를 들어 공인 인증서의 암호와 보안카드의 내용을 입력할 것을 유도한다. 그리고 입력된 정보를 이용해 사용자의 계좌에서 금액을 인출하거나 계좌를 불법적인 목적으로 이용하는 등의 피해를 발생 시킨다.

마지막은 사용자의 세부 개인정보가 해당된다. 회원가입이나 본인확인 또는 사용자의 이메일이나 전화번호 등을 ID로 사용하는 웹 서비스를 위조해 사용자의 세부 개인정보 입력을 유도한다. 이렇게 유

출된 개인정보는 보이스 피싱과 같은 또 다른 형태의 피싱 공격의 대상으로 사용되거나 사용자의 신분으로 위장해 인터넷 상에서 금전적 피해를 입힐 수 있는 서비스를 이용하는 방법 등으로 악용될 수 있다.

이 외에도 인터넷에서 입력할 수 있는 사용자 정보는 모두 피싱 공격의 대상이 된다고 볼 수 있다. 하지만, 여러 피해 사례와 공격 유형 등을 종합해 볼 때 위의 정보를 대상으로 한 피싱 공격이 가장 많이 발생하고 있다.

위와 같은 개인정보를 입력 받은 뒤 피싱 웹사이트가 취하는 동작은 아래와 같이 분류가 가능하다. 아래 분류 외에도 피싱 웹사이트는 다양한 형태로 동작할 수 있지만, 본 논문이 스미싱 공격을 대상으로 삼고 있는 만큼 스마트폰에서 접속했을 때 관찰할 수 있는 동작 패턴만을 대상으로 분류하였다.

첫 째, 고의적인 오류 화면을 보여주고 접속을 차단한다. 주로 로그인 정보를 탈취하기 위한 피싱 웹사이트에서 많이 발생하는 경우로 사용자가 정보를 입력하고 나면 'HTTP 404 Page Not Found'나 'HTTP 502 Bad Gateway'와 같이 인터넷 사용 중 흔히 볼 수 있는 에러 페이지를 표시한다. 사용자는 일시적인 네트워크 문제 등으로 착각하기 때문에 별다른 의심 없이 재 접속을 시도 하거나 나중에 접속하기 위해 접속을 포기하게 된다. 사용자가 재 접속을 시도하면 피싱 웹사이트는 자연스럽게 진짜 웹사이트로 접속을 전환 시키기 때문에 사용자는 피싱 웹사이트에 접속했다는 사실조차 인식하지 못한 채 지나가고 사용자의 로그인 정보는 공격자에게 전달된다.

둘 째, 다시 로그인할 것을 요구하면서 진짜 웹사이트의 로그인 페이지로 이동시킨다. 사용자의 로그인 정보나 금융 정보 등을 목적으로 하는 경우 많이 발생한다. 일반적으로 비밀번호나 중요한 정보를

변경하는 경우 또는 금융 정보 등을 입력하도록 요구한 뒤에는 사용자의 신분 재확인을 위해 다시 로그인할 것을 요구하는 경우가 많다는 점을 이용한다. 사용자의 입장에서는 정상적인 동작과 구분하기가 쉽지 않기 때문에 공격에 노출된 사실을 인지하지 못하게 된다.

셋 째, 추가 보안을 위한 보안 프로그램 설치 권유 페이지로 전환한다. 보통 계정의 보안 강화를 위한 안내문의 형식으로 위조한 스미싱 공격에서 주로 나타난다. 요구하는 내용에 따라 계정 관련 정보를 입력한 뒤 보안 프로그램 설치를 통해 추가로 보안을 강화할 수 있다는 안내와 함께 설치 페이지로 이동한다. 이때 설치되는 보안 프로그램은 악성코드의 한 유형으로 결국은 악성코드를 설치하기 위한 목적으로 위장된 피싱 웹사이트에 해당한다. 최근에 급증하고 있는 스미싱 및 피싱 공격으로 인해 금융 기관이나 공공 기관 등에서 보안 강화를 위한 절차를 안내하거나 보안 프로그램을 설치하는 경우가 늘어나고 있기 때문에 이와 동일한 형식을 빌린 피싱 공격은 그만큼 사용자의 의심을 덜 받을 수 있다는 이점이 있다.

마지막으로 접속과 동시에 파일 다운로드를 시작하는 유형이 있다. 보통은 사용자가 알지 못하는 사이에 악성코드를 설치하기 위한 목적이지만, 최근에는 보안 프로그램을 설치해야 접속을 정상적으로 할 수 있다는 이유로 위장해 악성코드의 설치를 유도하는 경우도 많이 발생하고 있다. 위 세 번째 경우와 마찬가지로 보안에 대한 사용자의 높은 관심과 막연한 두려움을 역으로 이용하는 방법으로 이렇게 설치된 악성코드는 스마트폰에 저장된 개인정보를 모두 유출 시키고, 스마트폰을 동작 불능 상태로 만들거나 사용자가 알지 못하는 사이에 전달되는 메시지들을 공격자에게 재전송 시키는 방법으로 공격자가 사용자의 신분을 위장할 수 있게 해준다.

중요 정보 입력을 요구하는 피싱 웹사이트들은 원하는 정보를 입력받은 후 위와 같은 공통적인 동작 패턴을 보이기 때문에 이것을 반대로 이용한다면 의심스러운 웹사이트가 피싱 웹사이트인지 아닌지 판별해내는 근거가 될 수 있다. 만일, 진짜 웹사이트에 허위 사용자 정보를 전송한다면 접속한 웹사이트는 전달된 정보의 유효성을 검사한 뒤 잘못된 정보임을 확인하고 올바른 정보를 다시 입력할 것을 반복 요청한다. 하지만, 피싱 웹사이트는 전달된 정보의 유효성을 검사하지 못하고 목적으로 한 정보가 모두 입력 되었는지 확인 후 정해진 동작을 수행할 수 밖에 없기 때문에 잘못된 정보에 대해서도 재입력 요청을 하지 않는다면 피싱 웹사이트인 것으로 간주할 수 있게 된다.

위와 같은 피싱 웹사이트의 공통적인 동작 패턴을 분석하기 위해 알려진 피싱 웹사이트의 URL 목록을 수집하고 직접 접속하여 요구하는 정보를 허위로 입력한 뒤 나타나는 동작 결과를 관찰하고 분석하는 작업을 진행하였다. 자세한 분석 과정에 대해서는 4장에서 자세히 설명한다. 다음 장에서는 본 장에서 설명한 허위 사용자 정보를 이용한 피싱 웹사이트 판별 기법과 함께 다른 제안 기법까지 포함해 'Phishing URL Detector'의 전체적인 동작 내용을 설명한다.

3.2.2 Phishing URL Detector

본 논문에서 제안하는 'Phishing URL Detector'는 위에서 설명한 핵심적인 기법 외에도 whitelist와 blacklist를 사용하는 기법과 URL에서 피싱 URL 패턴을 분석하는 기법을 함께 포함하고 있다. 이를 통해 개별 기법을 상호 보완하며 'Phishing URL Detector'가 전체적으로 하나의 완성된 솔루션으로써 동작하는 것을 목적으로 한다.

첫 번째 단계는 'Phishing URL Detector'에 전달된 URL에서 알려

진 피싱 URL 패턴이 있는지 분석하는 부분이다. 그리고 두 번째 단계는 스마트폰 모바일 웹 브라우저의 북마크와 접속 이력을 이용해 구성한 whitelist에 전달 받은 URL이 포함되어 있는지 검색하는 부분이 해당한다. 세 번째는 blacklist에 전달 받은 URL이 포함되어 있는지 검색하는 부분이며, 네 번째 단계가 의심스러운 웹사이트에 대해 위에서 설명한대로 허위 사용자 정보를 보내 웹사이트의 동작을 분석하고 피싱 웹사이트인지 판별하는 부분이 해당한다. 그리고 별도로 사용자의 로그인 정보나 폼(form) 형식의 결제 정보, 금융 정보 등을 'security token'이라 칭하는 형식으로 저장하고 사용자의 선택에 따라 접속한 웹사이트에 전송할 수 있는 기능을 담당하는 부분이 'Phishing URL Detector'의 사용자 인터페이스를 담당한다.

그림 3.2는 'Phishing URL Detector'의 전체적인 동작 흐름을 나타내고 있다. 'Phishing URL Detector'는 평소 사용자가 자주 입력하는 로그인 정보나 금융 및 결제 관련 정보를 'security token'의 형태로 별도 저장해 관리한다. 그리고 사용자는 메뉴를 통해 필요한 'security token'을 선택하여 접속한 웹사이트에 전송할 수 있다. 이것은 모바일 웹 브라우저가 자체적으로 제공하는 로그인 정보 저장 기능이나 폼(form) 정보 저장 기능에 기반한 것으로 사용자가 필요한 정보를 매번 일일이 입력하는 번거로움을 덜고 중요 정보를 모두 기억하고 있어야 하는 불편함을 덜어준다. 또한, 본 논문의 제안 기법에서 허위 사용자 정보를 전송하기 위한 방법을 제시하기도 한다. 이와 같이 자동화된 사용자 정보 입력 기능이 없다면 의심스러운 웹사이트에 접속해 허위 사용자 정보를 사용자가 직접 입력해야 하기 때문에 솔루션 방지 기법으로써의 의미가 부족하기 때문이다.

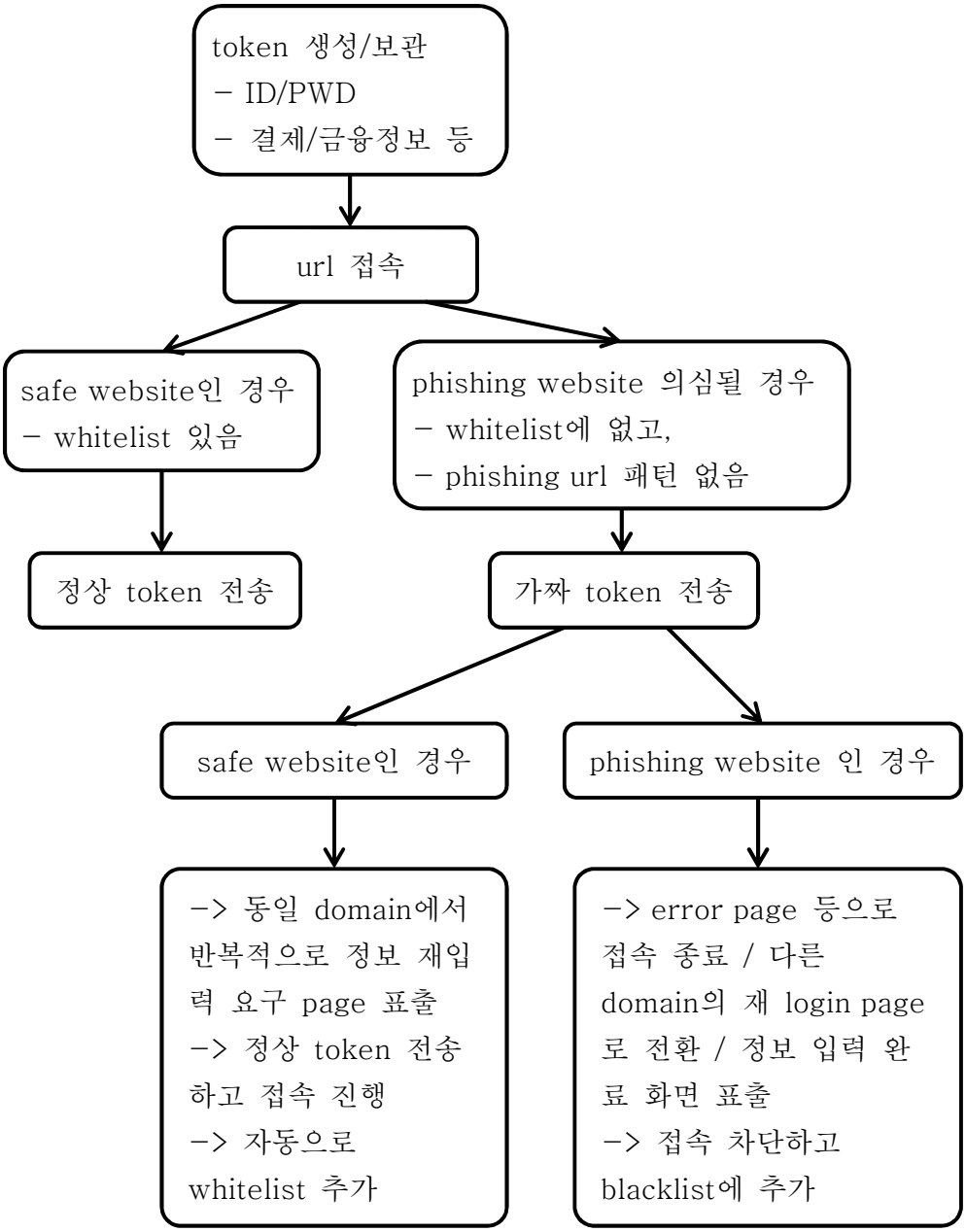

그림 3.2 Phishing URL Detector 동작 흐름도

사용자가 메시지를 통해 수신한 URL에 접속을 시도하면

‘Phishing URL Detector’는 우선 전달 받은 URL에서 아래와 같은 기준에 따라 알려진 피싱 URL의 패턴이 있는지 분석한다.

- URL의 호스트 명(hostname. 이하 ‘hostname’)을 IP 주소로 변경한 경우.
  접속 대상을 감추기 위해 hostname에 해당하는 부분을 IP 주소로 변경한다. 보통 위조의 대상이 되는 웹사이트의 진짜 hostname은 이어지는 경로(path. 이하 ‘path’)에 들어 있다.
  예) http://210.80.154.30/~test3/.signin.ebay.com/ebayisapidllsignin.html
- 진짜 hostname을 다른 domain과 함께 붙여 넣는 경우.
  피싱 URL의 hostname은 진짜와 구분하기 어렵게 꾸미고 위조의 대상이 되는 진짜 hostname을 path에 위치시킨 경우.
  예) http://21photo.cn/https://cgi3.ca.ebay.com/eBayISAPI.dllSignIn.php
- hostname을 매우 길게 변경하는 경우
  위조의 대상이 되는 진짜 hostname이 URL에 포함되어 있지만 길이가 긴 문자열을 domain의 형식으로 덧붙여 구분을 곤란하게 만든 경우.
  예) http://www.volksbank.de.custsupportref1007.dllconf.info/r1/vm/
- hostname 불명 또는 유사해 보이는 틀린 글자를 넣는 경우.
  사용자가 알기 어려운 전혀 새로운 hostname을 적거나 쉽게 구분이 되지 않는 틀린 글자를 포함 시켜 진짜 hostname과 유사하게 보이도록 만드는 경우.
  예) http://accounts.goog1e.com/ServiceLogin?hl=en
  (‘google’의 영문자 ‘l’ 대신 숫자 ‘1’이 쓰임)

만일 전달된 URL에서 위의 기준에 해당하는 패턴이 하나라도 발

견되면 피싱 URL로 판별하고 blacklist에 저장한 뒤 사용자 경고와 함께 접속을 차단한다.

하지만, URL에서 피싱 URL의 패턴이 발견되지 않으면 다음으로 whitelist에 전달 받은 URL이 포함되어 있는지 확인한다. whitelist는 모바일 웹 브라우저의 북마크와 접속 이력으로 구성된다. 북마크에 저장되어 있는 URL 목록은 기본적으로 사용자의 활동을 통해 생성된 것이므로 안전한 접속을 보장하는 웹사이트들일 확률이 높고, 접속 이력에 저장된 URL 역시 사용자가 지금까지 직접 저장하고 관리하는 기록이므로 비교적 안전한 URL 목록의 가치가 있다고 판단되기 때문에 이들을 기반으로 한 whitelist에 저장된 URL이라면 접속해도 안전한 것으로 간주할 수 있다. 이에 따라, whitelist에서 전달 받은 URL이 검색되면 접속을 허용하며, 사용자는 해당 URL에 접속한 뒤 필요한 경우 원하는 'security token'을 선택해 전송할 수 있다.

반면, 전달 받은 URL이 whitelist에서 검색되지 않으면 다음 순서로 'Phishing URL Detector'는 blacklist에 포함되어 있는지 확인한다. blacklist에는 지금까지 접속이 차단된 URL의 목록이 기록되어 있으므로 blacklist에 포함되어 있다면 위험한 URL로 간주하고 사용자에게 경고한 뒤 접속을 차단한다.

위의 단계를 모두 통과한 뒤에도 안전한 URL인지 판단할 수 없을 경우 'Phishing URL Detector'는 일단 모바일 웹 브라우저에서 전달 받은 URL에 대한 접속을 허용한다. 만일 접속과 동시에 파일 다운로드가 발생하는 웹사이트라면 자동으로 파일 다운로드를 차단한다. 그리고 필요에 따라 사용자가 'security token'을 선택해 전송하면 선택된 'security token'을 그대로 전송하지 않고 임의로 생성된 'fake security token'을 접속한 웹사이트에 전송한다. 그리고, 해당 정보가 전달된 후 나타나는 웹사이트의 동작을 분석하여 3.2.1 절에서 분석

했던 피싱 웹사이트의 공통 동작 패턴에 해당하면 피싱 웹사이트로 판별하고 사용자에게 경고한 뒤 접속을 차단하고 해당 URL을 blacklist에 추가한다.

위와 같이 'Phishing URL Detector'는 여러 단계에 걸쳐 복합적으로 스미싱 URL을 분석하고 공격을 방지하기 위한 기능을 제공한다. 이 중 가장 중요한 기능은 의심스러운 웹사이트에 'fake security token'을 전송한 결과를 토대로 피싱 웹사이트를 판별하는 부분이라 할 수 있다. 이와 같은 동작 방식은 기존의 피싱 방지 솔루션 제품들이 제공하는 방지 기법과는 큰 차이를 보인다. 기존 제품들은 주로 서버 의존형 blacklist 기반의 방지 기법을 채용하고 있다. 대표적인 예는 안랩에서 출시한 'AhnLab 안전한 문자'로, 독자적으로 운영하는 서버에서 URL을 분석한 결과와 자체적으로 유지하고 있는 blacklist를 기반으로 하여 URL의 피싱 위험 여부를 판단한다 [19]. 그러나 이와 같은 blacklist 기반의 서버 의존형 제품은 이미 알려진 유형이 아닌 새로운 유형의 피싱 URL은 올바르게 방지해낼 수 없다는 단점이 있다. 그리고 그러한 사례는 그리 어렵지 않게 찾아볼 수 있다[5]. 실제 스미싱 SMS도 안전한 것으로 판정할 수 있기 때문에 판정 결과를 믿은 사용자들이 큰 피해를 당할 수 있다. 하지만, 'Phishing URL Detector'는 직접 의심스러운 웹사이트에 접속하고 피싱 웹사이트의 공통적인 동작 패턴을 판정 기준으로 하고 있기 때문에 blacklist와 달리 새로운 유형의 피싱 URL이 수신 되더라도 이를 안전한 것으로 잘못 분석하는 경우는 발생하지 않는다.

[5] 머니투데이. "보안앱도 인식 못하는 스미싱 문자 등장". http://news.mt.co.kr/mtview.php?no=2013111808444279648&type=1&MLA. Nov. 2013.

본 논문에서는 또한 ‘Phishing URL Detector’ 외에 ‘Challenge-Response Authentication’ 기법을 MC에 적용할 것을 함께 제안하고 있다. 본 제안은 통신 사업자가 관리하는 MC에 URL이 포함된 메시지가 발신 요청 되었을 경우 발신자의 신원을 확인하기 위한 challenge 메시지를 발신자에게 전송한 뒤 발신자가 정상적으로 response 메시지로 회신한 경우에만 요청된 메시지를 지정된 수신자에게 전달하는 것을 내용으로 한다. 이를 통해, 스미싱 메시지의 전송을 미연에 차단하는 효과를 얻는 것을 목적으로 한다.

앞서 설명한 바와 같이 본 제안은 대부분 스미싱 메시지가 URL을 포함하고 있다는 점과 자동화된 컴퓨터를 이용해 대량으로 전송된다는 점을 이용한다. 따라서, ‘Challenge-Response Authentication’ 기법이 적용되면 컴퓨터는 올바른 응답을 할 수 없게 되므로 스미싱 메시지가 쉽게 차단될 수 있다. 앞서 3.1.1 절에서 분석한 바와 같이 본 제안은 스미싱 공격의 가장 처음에 해당하는 메시지의 발신 과정을 차단할 수 있으므로 큰 방지 효과를 기대할 수 있다.

‘Challenge-Response Authentication’을 사용한 사례는 [11]에서도 확인할 수 있지만, 본 제안은 다음과 같은 차이점을 가진다.

[11]의 기법은 스팸 메시지로 의심받을 수 있는 모든 경우에 적용되는 것을 전제로 하고 있다. 하지만, 스팸 여부를 판단하기 위한 단어나 표현은 상황에 따라 의미가 달라질 수 있으며, 모든 경우를 고려할 수 있는 스팸 단어와 표현을 선정해 content-based filtering 기법을 적용하는 것도 큰 부담이 된다. 따라서, 현실적인 방지 효과를 얻기에는 많은 제약이 따른다는 단점이 있다. 또한, SMS의 경우 약자나 축약된 표현, 신조어 등이 많이 사용되는 경향이 있기 때문에 효율적으로 스팸 단어나 표현을 탐지해낼 수 없다는 제약도 있다. 하지

만 본 제안은 공격 방지의 대상을 스미싱으로 한정 짓고 메시지에 URL이 포함된 경우만을 탐지하므로 오탐률을 줄이고 상대적으로 간단하게 동작이 가능하다는 장점이 있다. 물론, 스미싱 메시지에만 집중하므로 다른 종류의 스팸 메시지는 방치될 수 있다는 지적이 가능하다. 하지만, 실제로 스마트폰 환경에서 발생하는 피싱 공격의 대다수가 스미싱 공격의 형태를 취하고 있음을 감안한다면 스미싱 메시지 차단만으로도 의미 있는 방지 효과를 얻을 수 있을 것으로 여겨진다.

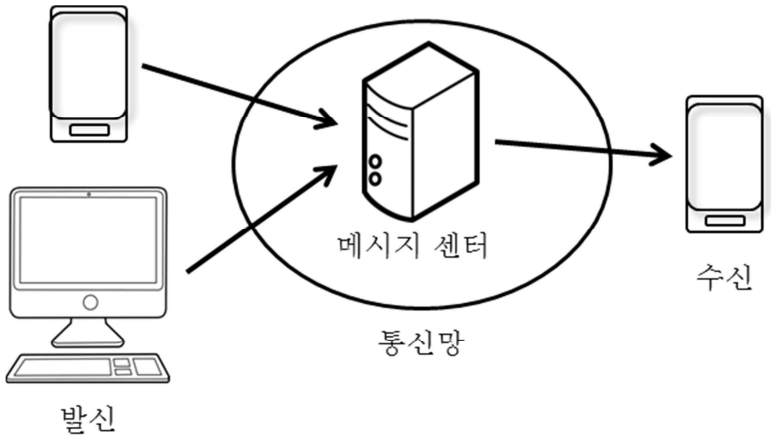

그림 3.3 메시지 전송 구조

물론, 스마트폰의 특성상 URL을 공유하는 경우가 많기 때문에 본 제안이 SMS/MMS의 이용을 불편하게 만들 수 있다는 지적도 가능하다. 그러나 인증을 위한 메시지에 응답하는 것은 매우 간단한 절차에 해당하며, 스미싱 공격의 피해 규모가 2013년 10월 기준 54억원 상당[20]에 달하는 점을 볼 때 얼마간의 불편을 감수하더라도 유효한 방지 기법의 적용은 반드시 필요하다.

제 4 장 실험 및 구현

본 장에서는 피싱 웹사이트들의 공통적인 동작 패턴을 분석하고 확인하기 위해 진행된 실험 과정과 결과에 대해 설명한다. 또한, ‘Phishing URL Detector’의 구현작업을 프로토타입의 형태로 제안하고 구현 시 고려해야 할 사항들에 대해 살펴본다.

4.1 피싱 웹사이트 공통 동작 패턴 확인 실험

‘Phishing URL Detector’의 주요 기법으로 본 논문에서 제안하고 있는 피싱 웹사이트의 공통 동작 패턴에 기반한 허위 사용자 정보를 이용한 피싱 웹사이트 판별 기법의 실효성을 확인하기 위해 실제로 피싱 웹사이트의 공통적인 동작 패턴을 확인하는 실험을 진행 하였다.

실험은 ‘PhishTank’ [22]와 같이 알려진 피싱 URL의 목록을 제공하는 곳에서 최근에 등록된 피싱 URL들을 임의로 선정하여 직접 스마트폰에서 접속해 보고 허위 정보 입력 후 동작을 관찰하는 방법으로 진행 하였다. 선정된 URL 목록은 모두 ‘VALID PHISHI’ 상태 즉, 확실하게 피싱 URL로 판정된 것들로 한정 지었으며, 처음에는 200개의 URL 목록을 선택하였으나 스마트폰에서 실제로 접속이 가능한 URL보다 접속이 불가능하거나 더 이상 유효하지 않은 URL의 수가 더 많아 추가적으로 더 많은 URL 목록을 선정하여 실험을 진행하였다. 단, 목록 중 동일한 domain에 대해 path를 조금씩 달리한 피싱 URL들의 경우는 하나의 대표 URL만 선택하였으며, 가능한 한 많은 URL에 접속을 시도하여 충분한 자료를 수집하기 위해 노력하였다.

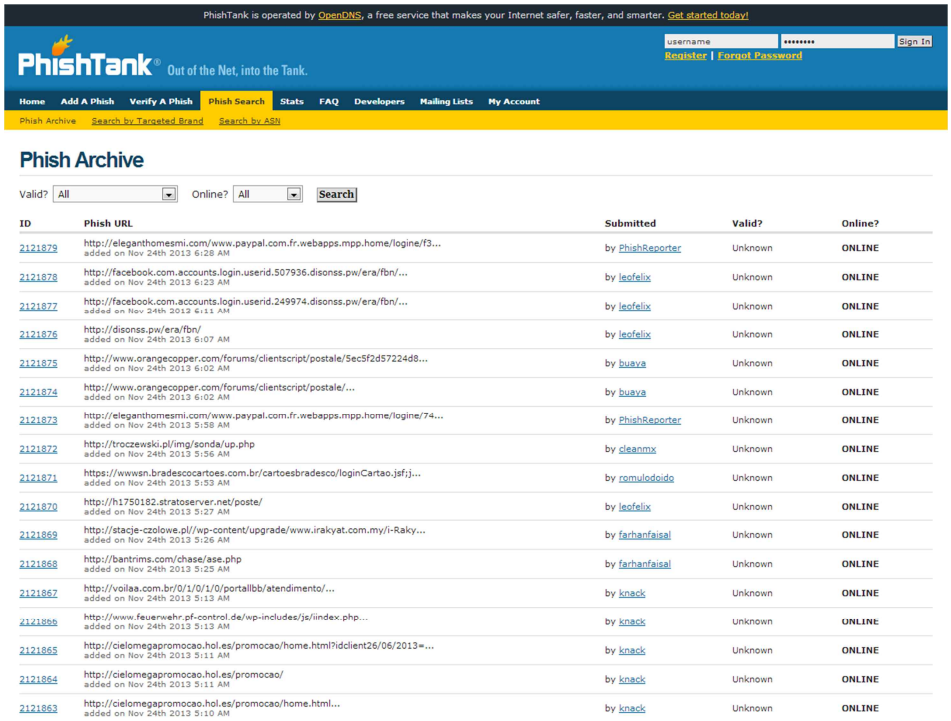

그림 4.1 PhishiTank Phishi Archive

실험 과정은 아래와 같은 절차로 이루어졌다.

1. 스마트폰에서 선택된 피싱 URL에 접속한다.
2. 접속 후 파일 다운로드가 시작되는 형태인지 정보 입력을 요구하는 형태인지 확인한다.
3. 접속 후 곧바로 파일 다운로드가 시작되는 경우 악성코드 설치를 목적으로 하는 피싱 웹사이트로 간주하고 분류한다.
4. 정보 입력을 요구하는 형태인 경우 접속한 웹사이트에서 요구하고 있는 정보의 범주를 분석한 후 요구하는 정보를 허위로 입력한다.
5. 정보 입력을 완료한 후 접속한 웹사이트가 보이는 동작을 분석

하고 분류된 패턴에 해당하는지 확인한다.

실험을 통해 스마트폰에서 접속에 성공한 피싱 URL은 전체 1,000여 개의 URL 중 모두 300개로 나머지는 스마트폰에서 접속할 수 없거나 URL이 더 이상 유효하지 않았다. 접속한 피싱 웹사이트를 3.2.1절의 동작 패턴에 맞춰 구분한 결과는 아래와 같다.

표 4.1 피싱 웹사이트 공통 동작 패턴 분석 결과

동작 패턴		웹사이트 수	비율(%)
정보 입력 요구	고의적인 오류화면 후 접속 차단	57	19
	재 로그인 요구 페이지로 전환	123	41
	추가 프로그램 설치 페이지 전환	27	9
접속 후 프로그램 다운로드		64	21.3
기타		29	9.7
계		300	100

스마트폰에서 접속에 성공한 300개의 피싱 웹사이트 중 정보 입력을 요구하는 형태는 모두 69%인 207개이고, 21.3%인 64개의 웹사이트가 접속과 동시에 파일 다운로드를 시작하였다. 그리고 9.7%에 해당하는 29개 피싱 웹사이트는 유형을 구별하기 어렵거나 의도된 동작인지 오류인지 구분이 안되고 패턴 분류가 어려운 동작을 보였다.

정보 입력을 요구하는 형태의 피싱 웹사이트 중에는 19%인 57개가 정보 입력 후 고의적인 것으로 보이는 오류화면을 표시하면서 접속을 차단하였으며, 41%인 123개는 정상 웹사이트의 로그인 요청 페이지나 정보 입력 페이지로 전환되었다. 그리고 9%인 27개는 허위 정보 입력 후 정보 입력에 감사하거나 완료되었다는 안내와 함께 추

가 보안 강화를 위한 프로그램 설치 화면으로 유인하였다. 결과적으로 69%의 피싱 웹사이트가 허위로 입력된 정보에 대해 공통적인 동작 패턴에 해당하는 동작을 보여주었으며, 이를 이용해 피싱 웹사이트임을 판별해낼 수 있음을 보여주었다.

많은 피싱 URL 목록 중에서 실제로 접속이 가능했던 피싱 웹사이트의 수가 매우 적었던 것은 피싱 웹사이트의 특성 상 짧은 시간 동안만 존재하다 사라지는 경우가 많기 때문으로 보인다. 오랜 시간 인터넷 상에서 노출될 경우 피싱 웹사이트라는 사실이 노출되어 공격이 무의미해질 가능성이 크므로, 자주 URL을 바꾸고 반복적으로 피싱 공격을 시도해야 성공 확률을 높일 수 있기 때문이다. 비교적 최근에 등록되는 피싱 URL의 경우는 접속에 성공할 수 있는 경우가 많았지만, 어느 정도 시간이 지나면 대부분 다시 URL에 접속할 수 없었다. 공격자 스스로가 URL을 삭제 하였거나 인터넷 상의 피싱 방지 솔루션 등에 의해 접속이 차단되었기 때문으로 판단된다.

4.2 Phishing URL Detector 구현

‘Phishing URL Detector’는 기능에 따라 여러 구성 요소로 나뉘어 구현될 수 있다.

첫 번째는 ‘security token’을 구성하고 전송하는 부분이 해당한다. ‘security token’은 사용자의 ID 및 암호와 같은 계정 정보, 신용카드와 같은 결제 정보와 기타 다양한 종류의 폼(form) 정보를 저장할 수 있는 개념적인 매개체로 정의된다. 웹 브라우저에서 제공하는 비밀번호 및 폼(form) 저장 기능을 기본으로 하고 있으며, ‘Phishing URL Detector’에서 사용자 정보를 저장하고 사용자 선택 시 자동으

로 접속한 웹사이트에 전송하는 기능과 함께 허위 사용자 정보를 생성해 의심스러운 웹사이트에 자동으로 전송한다. 사용자는 그림 4.2와 같이 ‘security token’의 종류를 선택하고 개별적으로 생성하고 저장하여 관리할 수 있으며, 그림 4.3과 같이 모바일 웹 브라우저에서 메뉴를 통해 원하는 ‘security token’을 선택하여 전송할 수 있다.

그림 4.2 Security Token 생성 개념도

‘security token’은 암호화되어 저장할 수 있도록 하여 만일의 유출 사태에 대비하며, 의심스러운 웹사이트에 대해 ‘fake security token’을 전송할 때는 임의로 생성한 문자열로 각 내용을 대체시켜 전송하도록 한다.

두 번째 구성 요소는 전달 받은 URL에 알려진 피싱 URL 패턴이 포함되어 있는지 분석하는 부분이 해당된다. 3.2.2 절에서 설명한 바와 같이 알려진 피싱 URL 패턴 중 하나 또는 그 이상이 발견되는지

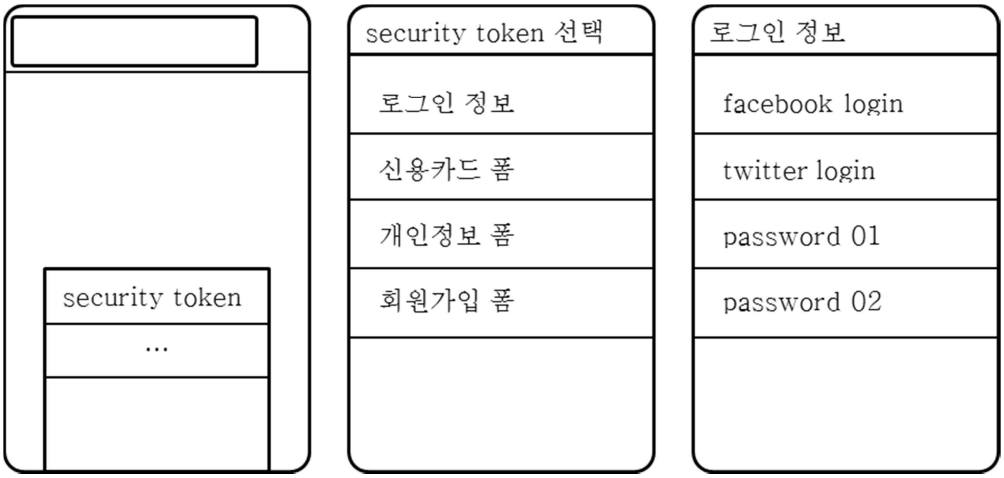

그림 4.3 Security Token 사용 개념도

분석한다. 첫 번째, hostname이 IP 주소 형식인 경우는 URL에서 hostname 부분만 추출해 IP 주소 형식을 나타내는 정규 표현식(regular expression)을 이용해 판단한다. 두 번째 패턴은 URL에서 hostname을 제외한 나머지 path 부분에서 다시 한 번 hostname의 형식과 일치하는 부분이 있는지 분석해 판단한다. 정상적인 URL은 path에 hostname의 형식이 다시 포함되는 경우가 없다. 세 번째 패턴은 URL의 hostname에서 '.'으로 구분되는 한 단어의 길이가 25자를 넘는지 확인하여 판단한다. 이는 정상 URL인 경우에도 피치 못하게 단어를 길게 쓸 수도 있지만 널리 사용되는 URL 목록을 확인해본 결과 한 단어가 25자를 넘는 경우가 매우 적었기 때문에 정해진 숫자이다. 따라서, 필요에 따라 단어 길이의 제한은 변경할 수 있다. 마지막 네 번째 패턴은 사용자의 시각 정보에 의존하는 경향이 크고 소스 코드 상으로 판단할 수 있는 방법이 없으므로 구현에서 생략한다.

다음 구성 요소는 whitelist를 구성하고 관리하는 부분이 해당된다.

whitelist는 앞서 설명한 바와 같이 모바일 웹 브라우저의 북마크와 접속 이력을 이용해 구성된다. 현재 가장 널리 사용되고 있는 안드로이드 플랫폼[21]을 예로 들면, 모바일 웹 브라우저의 북마크와 접속 이력을 하나의 데이터 베이스(database)에 합쳐서 저장하고 있으며, 다른 app에서 간단한 방법으로 읽고 검색할 수 있다. 따라서, 'Phishing URL Detector'도 별도 whitelist를 생성하고 관리하지 않고 모바일 웹 브라우저의 데이터 베이스를 실시간으로 whitelist로 활용한다. 또한, 모바일 웹 브라우저에서 접속하는 웹사이트의 URL은 자동으로 접속 이력에 기록되므로 접속이 허용된 URL은 항상 자동으로 whitelist에 추가되는 것과 동일한 효과를 얻을 수 있다.

네 번째 구성 요소는 blacklist를 구성하고 관리하는 부분이 해당한다. whitelist와는 달리 blacklist는 'Phishing URL Detector'가 개별적으로 생성하고 관리한다. 접속이 차단된 URL은 모두 blacklist에 저장되며, 일단 blacklist에 저장된 URL은 이후에도 항상 접속이 차단된다.

마지막 구성 요소는 'fake security token'을 전달 받은 웹사이트의 동작을 분석하고 결과에 따라 피싱 웹사이트를 판별해 내는 부분이 해당한다. 앞서 3.2.1 절에서 분류한 바와 같이 피싱 웹사이트들은 입력된 정보의 유효성을 검사할 수 없으며, 정보의 유효성과 상관없이 정해진 동작을 수행한다. 따라서, 의심되는 웹사이트에 'fake security token'을 전송한 뒤 동작을 관찰하여 피싱 웹사이트의 공통 동작 패턴에 해당하면 피싱 웹사이트로 판별해낼 수 있다. 다만, 이 부분은 현재 기술적으로 소프트웨어 수준에서 완벽하게 구현하는데 한계가 있을 것으로 예상되므로 추가적인 기술 연구 및 보완이 필요

할 것으로 보인다. ‘security token’을 전달 받은 웹사이트가 보일 수 있는 다양한 동작이 각 웹사이트 별로 사용하는 기술이나 프로그래밍 언어 및 제작자의 의도에 따라 차이가 있기 때문에 소프트웨어적으로 모든 동작의 범주를 나누고 정해진 규칙에 따라 판별할 수 없기 때문이다. 예를 들어, 전달된 ‘security token’에 따른 결과로 로그인 오류 페이지가 보이는 경우만 해도, 이것이 정상적인 웹사이트가 유효성 검사 후 표시하는 진짜 페이지인지 공격자가 임의로 구성한 가짜 페이지인지 소프트웨어 수준에서 구별하기 위해서는 웹 페이지의 내용을 모두 분석하는 것 뿐만 아니라 접속한 URL의 domain이 변경되었는지, 별도의 오류 코드가 포함되어 있는지 등 다양한 부분을 검토해야 한다. 따라서, 이 부분은 다양한 경우에 대해 포괄적으로 대응할 수 있는 소프트웨어를 구성할 수 있도록 기술적인 지원이 필요하다.

위와 같이 ‘Phishing URL Detector’는 여러 구성 요소를 하나로 합쳐 완전한 하나의 스미싱 공격 방지 솔루션으로써 동작하도록 제안되고 있다. ‘Phishing URL Detector’의 프로토타입은 안드로이드 플랫폼을 기준으로 설계 되었으며, 실제로 구현 및 적용이 가능한 기술들을 위주로 사용하였다. 다만, ‘fake security token’을 전송한 뒤 웹사이트의 동작을 분석하는 부분에 있어서는 전술한 바와 같이 보다 포괄적이고 대규모의 기술적인 지원이 필요한 내용이므로 실제 구현을 위한 추가적인 연구가 필요하다.

제 5 장 결론

스마트폰의 사용자가 지속적으로 증가하고 있는 만큼, 앞으로도 스미싱 공격은 계속해서 발생할 것이며 끊임없이 새로운 형태가 등장할 것이다. 스미싱 공격은 사용자를 현혹시켜 피싱 웹사이트에 접속해 개인정보를 스스로 유출 시키도록 유도하거나 악성코드를 설치해 개인정보를 탈취한 뒤 금전적인 피해를 입힌다. 스미싱 공격이 사용자를 속이는 방법은 SMS 뿐만 아니라 다양한 매개체를 활용해 점점 더 교묘해지고 있으며, 스미싱 공격에 사용되는 피싱 URL 은 실제로 접속해 보기 전에는 명확히 판별하기 어렵다는 문제점이 있다.

이와 같은 문제점을 해결하기 위해 본 논문에서는 'Phishing URL Detector'를 통해 피싱 웹사이트들이 공통적으로 보이는 동작 패턴을 기반으로 의심스러운 웹사이트에 허위 사용자 정보를 전송하여 나타나는 동작을 분석하고 피싱 웹사이트를 판별하는 기법을 제안하고 있다. 아울러, 'Phishing URL Detector'는 접속 대상 URL 에 알려진 피싱 URL 패턴이 포함되어 있는지 분석하는 기능과 whitelist, blacklist 를 이용해 접속한 URL 의 목록을 관리하는 기능을 함께 포함하여 하나의 완성된 스미싱 공격 방지 솔루션으로써 동작하도록 제안되었다.

또한, 허위 사용자 정보를 이용한 피싱 웹사이트 판별 기법의 효용성을 확인하기 위해 직접 알려진 피싱 웹사이트에 접속해 허위 정보를 입력하고 웹사이트의 동작 결과를 관찰함으로써 본 논문의 기법이 제안하고 있는 내용이 실제로도 적용 가능한 기법임을 확인하였다.

마지막으로, 'Phishing URL Detector'를 실제로 구현하기 위해 기능별로 구성 요소를 나눠 프로토타입의 형식으로 구현 방안을 제안하였다.

‘Phishing URL Detector’의 효과적인 방지 성능에도 불구하고 스미싱 공격을 원천적으로 방지하기 위해서는 여전히 사용자의 각별한 주의와 노력이 필요하다. 기본적으로 사용자를 현혹시켜 피싱 웹사이트로 접속을 유도하는 만큼, 전달 받은 URL 에 의심 없이 접속하거나 방지 기법의 경고를 무시하는 등의 부주의한 행동은 큰 피해로 이어질 수 있기 때문이다. 또한, 아무리 허위 사용자 정보를 이용해 피싱 웹사이트를 역으로 속이고 판별해낼 수 있다고 하더라도 분석된 범주에 속하지 않는 새로운 동작 패턴을 보이는 피싱 웹사이트가 언제든 등장할 수 있기 때문에 URL 접속 시에는 항상 주의를 기울여야 한다. 이는 스마트폰 뿐만 아니라 PC 에서도 동일하게 해당한다.

비록 현재는 스미싱 공격으로 인한 피해가 급격히 증가하고 있는 추세지만, 스미싱 공격 방지에 대한 사용자의 인식 변화와 함께 ‘Phishing URL Detector’와 같은 효율적인 방지 기법을 적극적으로 활용하면 충분히 피해를 예방하고 스미싱 공격을 방지할 수 있을 것으로 기대된다.

참고문헌

[1] Orbit Media Studios. Mobile Explosion: 3 Tipping Points. http://www.orbitmedia.com/blog/mobileexplosion/. Jul. 2010.

[2] AhnLab. 안랩, “하반기 스미싱 악성코드 급증”. http://ahnlabgirl.cafe24.com/ahnlab/1844?TSSESSIONblogahnlabcom=22ed7cd546d41dfa2a8852a61e73da21. Sep. 2013.

[3] Wikipedia. Phishing. http://en.wikipedia.org/wiki/Phishing.

[4] Microsoft (2011). Email and Web Scams: How to Help Protect Yourself. http://www.microsoft.com/security/online-privacy/phishing-scams.aspx

[5] PCWorld (2003). Spam Slayer: Do You Speak Spam?. http://www.pcworld.com/article/113431/article.html. Nov. 2003.

[6] A.P. Felt and D. Wagner. “Phishing on Mobile Devices,” 2011.

[7] AhnLab. ASEC 리포트 2013.

[8] M. Boodaei, “Mobile Users Three Times More Vulnerable to Phishing Attacks,” in *Trusteer* vol. 2012, ed, 2011.

[9] Soni, Pravin, Shamal Firake, and B. B. Meshram. "A phishing analysis of web based systems." Proceedings of the 2011 International Conference on Communication, Computing & Security. ACM, 2011.

[10] K. Dunham, "Chapter 6 - Phishing, SMishing, and Vishing," in Mobile Malware Attacks and Defense, D.Ken, Ed., ed Boston: Syngress, 2009, pp. 125-196.

[11] Yoon, Ji Won, Hyoungshick Kim, and Jun Ho Huh. "Hybrid spam filtering for mobile communication." computers & security 29.4 (2010): 446-459.

[12] Huh, Jun Ho, and Hyoungshick Kim. "Phishing detection with popular search engines: simple and effective." Foundations and Practice of Security. Springer Berlin Heidelberg, 2012. 194-

207.
[13] Zhang, Yue, Jason I. Hong, and Lorrie F. Cranor. "Cantina: a content-based approach to detecting phishing web sites." Proceedings of the 16th international conference on World Wide Web. ACM, 2007.
[14] Xiang, Guang, et al. "Cantina+: A feature-rich machine learning framework for detecting phishing web sites." ACM Transactions on Information and System Security (TISSEC) 14.2 (2011): 21.
[15] Chhabra, Shalendra. Fighting spam, phishing and email fraud. Diss. UNIVERSITY OF CALIFORNIA, 2005.
[16] C.F.M. Foozy, R. Ahmad and M.F. Abdollah. “Phishing Detection Taxonomy for Mobile Device,” 2013.
[17] Yue, Chuan. "Preventing the revealing of online passwords to inappropriate websites with logininspector." Proceedings of the USENIX Large Installation System Administration Conference (LISA). 2012.
[18] Wikipedia. Social Engineering (security). http://en.wikipedia.org/wiki/Social_engineering_(security)
[19] AhnLab. AhnLab 안전한 문자. http://www.ahnlab.co.kr/kr/site/product/productView.do?prodSeq=89&svccode=aa1001&contentscode=483
[20] 사이버 경찰청. “(보도자료) 스미싱 기획 홍보”. Nov. 2013.
[21] Strategy Analytics. Android Captures Record 81 Percent Share of Global Smartphone Shipments in Q3 2013. http://blogs.strategyanalytics.com/WSS/post/2013/10/31/Android-Captures-Record-81-Percent-Share-of-Global-Smartphone-Shipments-in-Q3-2013.aspx. Oct. 2013.
[22] PhishiTank. Phishi Archive. www.phishitank.com/phishi_archive.php

Abstract

Preventing SMishing Attack Using Fake User Information Based on Common Behavior of Phishing Websites

Seunghwan Han
School of Computer Science Engineering
College of Engineering
The Graduate School
Seoul National University

SMishing attack is a sort of the Mobile Phishing attacks and it is the act of attempting to acquire personal information such as passwords and credit card details to cause monetary losses of users. Nowadays mobile devices such as smartphones are widely used and SMishing attack is becoming a significant problem. SMishing attack uses text messages to deliver the bait URL to induce people to divulge their sensitive personal information in attacker's malicious fake web sites.

In this thesis, a 'Phishing URL Detector', the name of SMishing defense mechanism for Android based smartphones and its analysis are proposed. 'Phishing URL Detector' combines several defense techniques together to serve as a complete SMishing defense solution. It depends on the common behavior of phishing websites that they do not verify if the input information was correct. They just check if all of requested information was input. 'Phishing URL Detector' cheats the suspicious

phishing websites by sending fake user information instead of real one to determine if they are real phishing websites. If they perform one of common behavior of phishing websites although the fake user information was input, we can judge them as phishing websites. In order to collect the common behaviors of phishing websites after receiving the desired information and verify if the proposed technique can really defense the SMishing attack, we tried to connect more than 1,000 known phishing URLs in a real smartphone and analyzed their behaviors.

In addition, 'Phishing URL Detector' provides an analysis of the URL itself to figure out if it has the common patterns of phishing URL in it and uses a blacklist to store those phishing URLs to block the connection of them. 'Phishing URL Detector' also uses a whitelist to allow the connection of URLs in the list and it uses the database of bookmarks and history of mobile web browser in an android smartphone as a whitelist.

'Phishing URL Detector' is showing a positive effect as a SMishing defense mechanism and it is very important to protect users from phishing attacks. It solves the known problem that the phishing URL cannot be completely determined as real dangerous one before users connect to it in a web browser. In the situation that not any defense mechanisms can cover all of mobile phishing strategies, 'Phishing URL Detector' could be the first defense line of smartphone to protect users from SMishing attacks.

keywords : Mobile Phishing, SMishing, Fake User Information, Common Behavior of Phishing Websites

student number : 2012-20883