Whois 와 DNS 정보를 활용한 RealURL 안티피싱 기법

하정애*, 이희조**
*고려대학교 컴퓨터정보통신대학원 소프트웨어공학과
**고려대학교 컴퓨터. 통신공학부
e-mail : {janetha, heejo}@korea.ac.kr

RealURL Anti-Phishing using Whois and DNS Record

JeongAe Ha*, HeeJo Lee**
*Graduate School of Computer and Information Technology, Korea University
**Dept. of Computer Science & Engineering, Korea University

요 약

해들 거듭하면서 피싱 사이트의 수는 지속적으로 증가하고 이로 인한 피해가 끊임없이 보고 되고 있는 가운데, 보안업체들은 블랙리스트 데이터베이스를 이용한 피싱 방지 브라우저 플러그인을 제안, 공급하고 있다. 한편, 2007 년 APWG 에 의한 보고에 따르면 피싱 사이트의 평균 수명은 짧게는 몇 시간에서 길게는 30 일 이내로 평균 3.8 일 밖에 되지 않는 것으로 보고 되었다. 이는 블랙리스트 데이터베이스를 이용하는 기존 안티피싱 플러그인이 신규 피싱 사이트에 대해서는 대처 할 수 없는 한계를 가지고 있음을 의미한다. 피싱 사이트의 라이프사이클을 가만하여 실시간 사이트의 진위 여부를 판단하고, 사용자 정보 유출을 방지하는 것이 시급함에도 불구하고 지금까지의 안티피싱 플러그인은 실시간 사이트 진위 여부를 판단할 수 없어 신규 피싱 사이트에 대처하지 못하고 있다. 이에 본 논문은 Whois 와 DNS 정보를 활용하여 실시간 사이트의 진위여부를 판단하는 개선된 안티피싱 기법(RealURL)을 제안한다. 또한 제안하는 기법은 사용자의 적극적인 개입을 유도하는 브라우저 플러그인으로 구현 되었다. RealURL 은 기존 블랙리스트를 데이터베이스를 이용한 방법을 탈피하여 사이트의 진위여부를 실시간 판단하는 새로운 방법으로 사용될 수 있다.

1. 서론

피싱은 사회공학적 기법과 기술 은익을 통해 개인 신상 정보나 금융 정보를 훔치는 공격이다. 파밍은 피싱과 같은 목적으로 HOSTS 나 DNS 정보를 속여 사용자를 피싱 사이트로 연결시키는 신종 기법이다[1]. 언론 매체를 통한 피싱 피해 사례 보고와 이에 대한 주의 홍보에도 불구하고 피싱으로 인한 피해는 계속 늘어나고 있다. 이러한 가운데 보안 업체들은 저마다 블랙리스트 데이터베이스를 이용한 안티피싱 브라우저 플러그인을 제시 하였다[2][3][4]. 한편, 2007 년 APWG 에 의한 보고에 따르면 피싱 사이트의 평균 수명은 짧게는 몇 시간에서 길게는 30 일 이내로 평균 3.8 일 밖에 되지 않는 것으로 보고 되었다[5]. 이는 블랙리스트 데이터베이스를 이용하는 안티피싱 플러그인이 신규 피싱 사이트에 대해서는 대처 할 수 없는 한계를 가지고 있음을 의미한다. 이러한 문제를 해결하고자 한편에서는 블랙리스트와 화이트리스트 데이터베이스를 동시에 구축하는 방안이 모색되고 있다[6]. 유명사이트의 화이트리스트 데이터베이스를 구축하고 여기에서 제공하는 정보를 이용하여 사용자가 접속한 사이트가 신뢰 가능한 사이트인지 사용자의 확인과 개입을 요구하는 방법이 특허로 제시되기도 했다[7]. 연구결과에 따르면 경고를 표시하는 소극적인 툴바 보다는 팝업과 같은 적극적인 중단을 통해 사용자의 개입을 유도하는 것이 더 효과적인 것으로 나타났다[8]. 그러나 화이트 리스트 데이터베이스는 그 규모가 너무 방대하여 데이터베이스를 설계, 운용, 유지하는 것이 현실적이지 못하다는 문제점을 가지고 있다.

다양한 피싱 방법이 보고되고 있지만, 피싱은 사용자의 눈을 속이는 것이다. 접속한 사이트의 진위여부를 실시간 판단하고 개인 금융정보 유출을 차단할 수 있다면 피싱으로 인한 피해를 막을 수 있다. 이러한 요구에도 불구하고 지금까지의 안티피싱 플러그인은 실시간 사이트 진위 여부를 판단할 수 없어 신규 피싱 사이트에 대처하지 못하고 있다.

이에 본 논문에서는 현재 브라우저의 주소창에 보여지는 URL 관련 정보를 Whois 와 DNS 검색을 통해 얻고, 해당 브라우저가 맺은 세션과 비교함으로써 합법적인 사이트에 접근했는지를 판단할 수 있는 RealURL 안티피싱 기법을 제시한다. RealURL 은 접속했던 사이트에 대해 로컬 데이터베이스에 그 정보를 등록 하기 때문에 시간이 지남에 따라 실시간 검색에 대한 부담이 줄어 든다. 뿐만 아니라, 사용자의 접속 URL 을 기반으로 데이터베이스가 구축되기 때문에 데이터베이스 크기가 작고 사용자 환경에 최적화된 데이터베이스 구성을 기대할 수 있다. 다만, 제시되는 방법은 DNS 정보를 이용하기 때문에 DNS 서버 자체

를 해킹한 파밍에 대해서는 정상적인 결과를 기대할 수 없다. 파밍은 DNS 자체 보안과 관련된 부분이므로 본 논문의 범위에서는 제외하며, 제시하는 브라우저 플러그인은 DNS 가 안전하다는 가정하에 동작한다.
2 장에서는 논문의 배경을 설명하고 3 장에서는 Whois 와 DNS 를 이용한 RealURL 안티피싱 기법을 제안하며, 4 장에서는 타 기법과 비교 평가하고, 5 장에서는 결론을 제시 하였다.

2. 배경

2.1 피싱 기법의 변화

eBay 고객을 대상으로 이루어진 피싱 공격이 '04 년 3 월 처음 보고되었다[9]. 이 공격은 수신자의 계정 정보가 유효하지 않으니 이메일에 제공된 링크에 접속하여 자신의 정보를 업데이트 하라는 내용을 담고 있었다. 메일 발신자는 S-Harbor@eBay.com로 나타났으며, cgil.ebay.com 으로 보여지는 접속 링크를 가지고 있었다. 그러나 제공된 링크는 eBay 와 전혀 상관없는 한국의 210.93.131.250 서버로 연결하는 링크였다. 제공된 링크는 eBay 의 로그를 이용했을 뿐만 아니라 실제 서버와 비슷한 페이지 디자인을 가지고 있었고, 사용자들의 신용카드 정보와, 사회보장 번호, 및 eBay 의 계정과 암호를 묻고 있었다. 사용자들은 해당 사이트를 의심할 이유가 없었고, 입력한 정보를 제출하는 순간 정보는 피셔의 서버로 전송되어 악용되었다. 이후 정상 도메인 이름을 변경한 유사 도메인 명의 이용이나, 스크립트를 이용한 브라우저의 주소창 위조 기법이 나타났다. 최근에는 취약점을 가진 포털 사이트에 악성 코드를 삽입하여 해당 사이트에 접속한 사용자들을 피싱 서버로 재 연결하는 형태의 공격들이 나타나고 있다.

2.1 Anti-Phishing 에 대한 연구와 평가

최근 안티피싱에 관한 연구가 활발히 이루어지고 있으며, 각각에 대한 연구는 크게 다음과 같은 세가지 방법으로 구분 된다.

2.2.1 패스워드 강화기법

대부분의 피싱은 개인 정보를 웹 폼에 입력하도록 하는 것이고, 합법적인 사이트에서도 회원 가입시 이런 개인 정보를 입력 받는 것을 기본으로 하고 있어 피싱 방지를 더욱 어렵게 한다[10]. 사용자들의 접속 사이트 수는 많아졌고 이에 따른 회원 가입도 늘어났지만 인간의 기억력 한계로 사용자들은 거의 대부분의 사이트에서 동일한 계정과 암호를 사용하게 된다. 이러한 점을 악용한 공격에 대응하기 위해, 사용자가 하나의 패스워드를 사용하더라도 접속되는 대상 서버에 따라 다른 암호를 생성하도록 하는 패스워드강화 기법이 연구되었다[11]. 그러나 패스워드강화기법은 패스워드 자체에 대한 보안은 가능하지만 피싱으로부터 개인 금융정보를 지켜주지는 못한다.

2.2.2 브라우저 플러그인을 이용한 기법

다양한 형태의 플러그인이 소개되었고, 보안업체들을 통해 공급되고 있다[2][3][4]. 각 플러그인은 저마다 특징이 있겠지만 일반적인 동작을 정리하면 다음과 같다. 1) 서버에 존재하는 블랙리스트 데이터베이스를 통해 피싱 사이트인지 아닌지를 검사한다. 2) 페이지 소스를 분석하여 패턴인식을 통한 피싱 가능 여부를 사용자에게 알린다. 3) 사용자에게 보안경고 및 접속 URL 에 대한 Whois 정보를 제공한다. 4) 피싱 신고가 가능한 채널을 사용자에게 제공한다. 한편, AntiPhish 플러그인은 브라우저의 폼에 입력된 개인 정보가 사용자의 제출 없이 서버로 전송되는 피해를 막기 위해, 브라우저에 입력 폼이 사용된 경우 해당 브라우저에서의 스크립트 실행을 중지하였다. AntiPhish 는 폼에 입력된 내용을 암호화하여 임시 저장했다가 대상 서버가 블랙리스트에 없는지 확인한 다음 폼 내의 정보를 서버로 전송하는 방법을 제안했다[12].

2.2.3 블랙리스트와 화이트 리스트 데이터베이스

블랙리스트 데이터베이스는 피싱 사이트로 알려진 URL 이나, 피싱 서버의 IP 주소를 가진 데이터베이스이다. 이 데이터베이스는 사용자들의 "피싱 신고" 와 관리자의 검토를 거쳐 갱신 된다. 이러한 방법 때문에 블랙리스트 데이터베이스를 이용한 피싱 확인은 신규 피싱 사이트에 대해 실시간 방어가 불가능 하다. 또한 데이터베이스를 항상 최신의 상태로 유지 해야 하는데, 이에 따른 관리적인 부담도 크다.
화이트리스트 데이터베이스는 합법적으로 등록된 사이트에 대한 URL 이나 서버의 IP 주소를 가진 데이터베이스 이다. 화이트리스트 데이터베이스를 이용하면 블랙리스트 데이터베이스가 가지는 신규 피싱 사이트에 대한 업데이트 시간지연 문제를 해결 할 수 있다. 그러나 피싱 사이트를 제외한 나머지 모든 사이트가 합법적일 수 있기 때문에 화이트리스트 데이터베이스는 방대해야 하고 이를 설계하고 유지 관리한다는 것은 현실적이지 못하다.

3. Whois 와 DNS 를 이용한 RealURL

RealURL 은 현재 브라우저에 보여지는 URL 의 정보와 화면에 보여지는 사이트 정보가 합법적인 것인지 Whois 와 DNS 를 이용하여 실시간 판단하는 기법이다. 이 기법은 브라우저 플러그인(RealURL AntiPhishing)으로 개발 되어 사용자의 개인 정보를 보호한다.

3.1 RealURL Flow

ReaRUL Anti-Phishing 은 크게 7 단계로 동작한다. <그림 1>은 RealURL 이 사이트의 진위여부를 판단하고 로컬 데이터베이스에 등록하기까지 과정이다.
1 단계: RealURL 은 해당 페이지에 Form 이 있는지 확인하고, 있으면 브라우저의 스크립트를 비활성화 한다.
2 단계: 브라우저에 보여지는 URL 상의 도메인이 로컬 DB 에 등록되었는지 확인한다.
3 단계: DB 에 등록이 되었으면 DB 의 정보와 현재 브

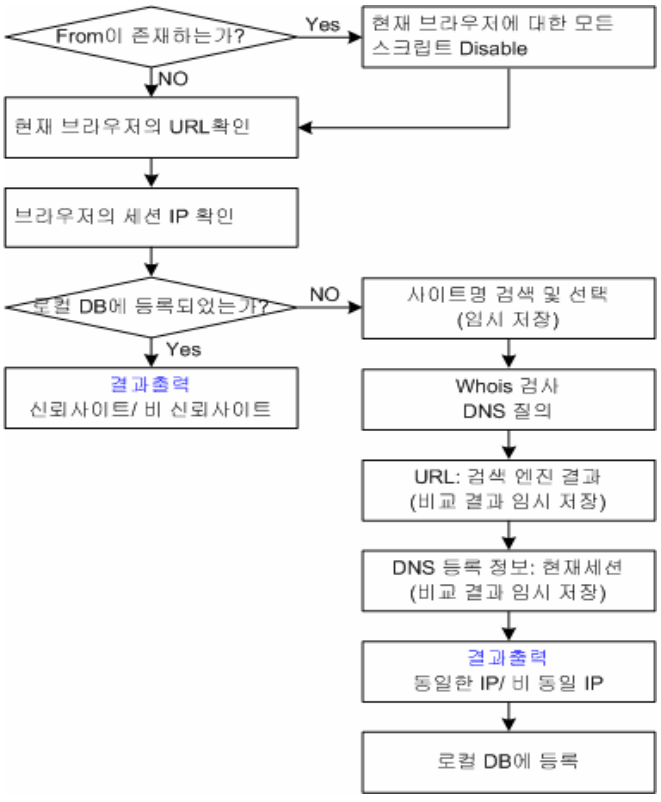
라우저의 세션을 비교하여 그 신뢰결과가 “신뢰”이면 현 브라우저의 스크립트를 활성하고, 그렇지 않으면 브라우저를 중지 시킨다. DB 에 등록되지 않은 사이트에 접속했다면 검색엔진을 통해 접속된 사이트 이름을 검색하게 한다. 검색된 리스트 중 상위 10 개를 사용자에게 표시하여 사용자로 이들 중 한 개를 선택하게 한다. 사용자가 선택한 사이트에 대한 URL 정보와 IP 정보를 임시 저장한다.

4 단계: Whois 와 DNS 를 통해 브라우저상의 URL 에 대한 도메인 및 호스트 정보를 확인한다.

5 단계: 3 단계에서 임시저장 검색 결과와, 4 단계에서 확인된 URL 정보를 비교하여 동일하면, DNS 에 등록된 IP 주소와 현재 세션 IP 가 동일한지 비교하여 그 정보를 사용자에게 출력한다.

6 단계: 3 단계에서 검색된 URL 이 현재 브라우저의 주소와 다르거나, DNS 에 등록된 IP 주소가 현재 브라우저의 세션 IP 주소와 다르면 “비 신뢰 사이트”로 표시하고, 브라우저를 중지 시킨다. 모든 정보가 일치하면 “신뢰 가능”으로 표시하고 해당 브라우저의 스크립트를 활성화 시킨다.

7 단계: 접속 URL 에 대한 결과 정보를 데이터베이스에 등록한다.



(그림 1) RealURL Flow

3.2 사이트명 검색

로컬 데이터베이스에 등록되지 않은 처음 방문 사이트는 사용자가 접속하기 원하는 합법적인 사이트인지 확인하는 과정을 거쳐야 한다. 그러나 브라우저 자체에는 진위여부를 판단할 아무런 기준정보가 없다. RealURL 에서는 검색엔진을 통한 사용자 확인을 이용한다. 사용자의 확인이 끝나면, RealURL 은 그 정보를 로컬에 임시 저장한 다음 Whois 와 DNS 를 통해 얻은 정보와 현재 브라우저의 세션정보를 비교한다.

3.3 데이터베이스 설계

RealURL 은 한번 방문했던 사이트에 대한 정보를 로컬 데이터베이스로 유지한다. <표 1>은 RealURL 의 데이터베이스가 포함하는 컬럼이다.

<표 1> RealURL Database

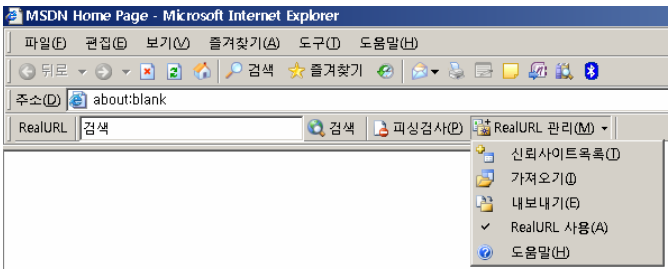
NO	URL	IP lists	사이트 이름	도메인등록자	신뢰성
1	www.kbstar.com	211.181.199.211	국민은행	㈜ 국민은행	신뢰
2	www.wooribank.com	210.182.9.227	우리은행	Woori Bank	신뢰
3	www.kbstar.com	211.182.9.227	국민은행	㈜ 국민은행	비신뢰
4	www.microsoft.com	207.46.19.254 207.46.192.254 207.46.193.254 207.46.19.190	한국MS	Microsoft Corporation	신뢰
5	www.lgcard.com	210.112.177.1	LG 카드	LG Card Co.,	신뢰

사용자로 부터 입력받은 정보 / Whois 에서 얻은 정보

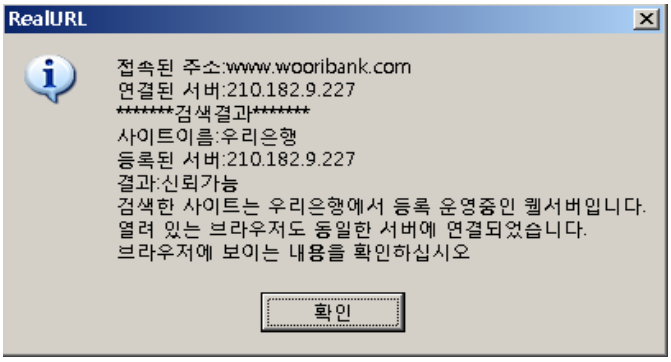
URL 컬럼에는 브라우저에 표시된 URL 주소가 입력되고 IP Lists 컬럼에는 해당 브라우저가 세션을 맺었던 IP 주소가 기록된다. 해당 URL 에 대한 피싱 사이트가 존재 하느냐 그렇지 않으냐에 따라 동일 URL 에 대한 레코드는 여러 번 나타날 수 있다. 도메인 등록자에는 URL 에 대한 Whois 검색을 통해 얻은 도메인 등록자 이름이 기록 된다. 사이트 이름은 사용자가 브라우저에 보여지는 사이트의 이름을 입력함으로써 얻은 정보이다. 사이트의 신뢰성 여부는 검색엔진 및 DNS 에 등록된 URL 의 IP 정보와 현재 브라우저의 세션 IP 주소를 비교하여 얻은 결과에 의해 결정된다. 기본적으로 비교 결과가 같아야만 신뢰 가능한 사이트 이다.

3.4 구현

RealURL 기법은 RealURL Anti-Phising 플러그 인으로 개발 되었다. RealURL 이 설치되면 기본적으로 [사용] 상태가 되어 피싱을 방지 한다. RealURL DB 에 등록된 정보는 사용자가 검색해 볼 수 있으며, 현재 사이트에 대해 매뉴얼 하게 피싱을 검사하는 메뉴를 가지고 있다. 구성된 DB 를 내보내거나 가져 올 수 있게 하여 시스템 변화에도 적응 가능하도록 했다.



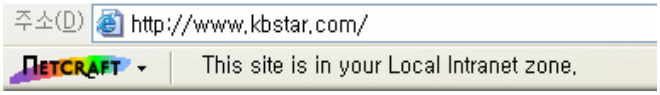
(그림 2) RealURL Anti-Phising 플러그인



(그림 3) 신뢰 사이트 접속 결과

4. 비교 평가

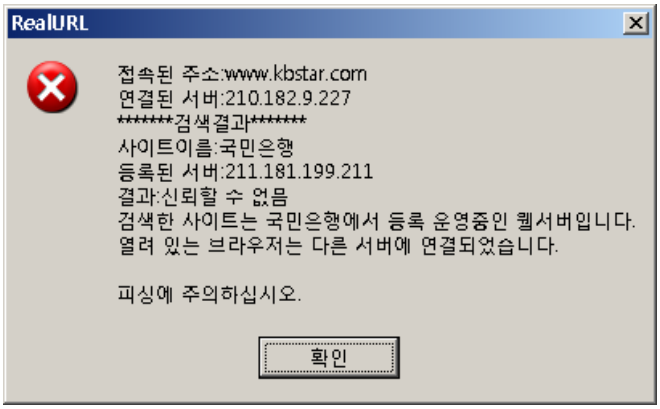
잘 알려진 플러그인을 이용하여 국내 금융권사이트와 쇼핑사이트 및 일반사이트에 접속했을 때 각각은 다르지 않은 결과를 표시했다. NetCraft 의 경우 회사 방화벽 내에서 사용하면 대상 사이트와 상관없이 로컬 인트라넷에 있는 것으로 표시했고<그림 4>, EarthLink Toolbar 의 경우에는 한 두 개의 사이트를 제외한 나머지 사이트에 대해서는 보여지는 웹 페이지가 안전한지 여부를 보증할 수 없다는 내용을 화면에 보여주었다<그림 5>.



(그림 4) Netcraft 를 이용한 피싱 검사

(그림 5) EarthLink 를 이용한 피싱 검사

제안한 RealUR 을 이용한 했을 때에는 사이트에 대한 정보와 더불어 사이트의 신뢰성을 명확히 확인 할 수 있었다.



(그림 6) RealURL 을 이용한 피싱 검사

5. 결론

실시간 사이트의 진위여부 판단이 요구되는 피싱 사이트의 라이프사이클을 가만한 개선된 안티피싱 기법을 제안했다. RealURL 은 이미 구축된 정보를 이용하는 화이트.블랙리스트 기법을 벗어나 신규 피싱 사이트에 대한 실시간 진위여부 판단 기법을 제시했음에 의의가 있다.

본 논문이 제시한 RealURL 을 이용하면 다음의 효과를 기대할 수 있다. 첫째, 블랙리스트에 등록되기까지 걸리는 지연시간으로 인한 피해를 최소화 하고 실시간 사이트의 진위여부를 판단할 수 있다. 둘째, 사용자의 적극적 개입을 통해 보안 인식을 고취하고 피싱에 대한 교육 효과를 기대할 수 있다.

참고문헌

[1] Anti-Phishing Working Group, “What is Phishing and Pharming?”, http://www.anti-phishing.org, 2007

[2] Microsoft, “Anti-Phishing Technologies”, http://www.microsoft.com/mscorp/safety/technologies/antiphishing/overview.mspx, June 2007

[3] Netcraft, “Netcraft Toolbar”, http://www.toolbar.netcraft.com, 2004.07

[4] EarthLink, “Your Web, Your way. Secure & always at your fingertips. EarthLink Toolbar”, http://www.earthlink.net/software/free/toolbar/, 2007

[5] Anti-Phishing Working Group, “Phishing Activity Trends Report”, http://www.anti-phishing.org/reports/apwg_report_may_2007.pdf, May 2007

[6] 한국정보보호진흥원, “ 피싱 사이트 공동 DB 만든다”, http://www.krcert.or.kr/index.jsp, June 2007

[7] Hwang Jey-yeob, “Method of anti-Phisihing” http://www.wipo.int, January 2007

[8] Rachna Dhamija, J. D. Tygar,Marti Hearst, “Why Phishing Works”, CHI Proceedings of Security, 2006

[9] Anti-Phishing Working Group, “eBay – NOTICE eBay Obligatory Verifying - Invalid User Information”, http://www.antiphishing.org/phishing_archive/eBay_03-09-04.htm, March 2004,

[10] Min Wu, Robert C. Miller, Greg Little, “Web Wallet: Preventing Phishing Attacks by Revealing User Intentions”, Symposium On Usable Privacy and Security, 2006

[11] J.A.Halderman, B.Waters, and E.Felten, “A Convenient method for securely managing passwords”, Proceedings International World Wide Web Conference , 2005

[12] Engin Kirda and Christopher Kruegel, “Protecting Users Against Phishing Attacks with AntiPhish”, Proceedings Annual International Computer Software and Applications Conference, 2005