DNS 스푸핑을 이용한 파밍 공격 방어에 관한 연구

박정혁*, 안성환**, 박민우**, 정태명***
*성균관대학교 컴퓨터공학과
**성균관대학교 전자전기컴퓨터공학과
***성균관대학교 정보통신대학
e-mail : ganggiyam@gmail.com*, {shahn, mwpark}@imtl.skku.ac.kr**, tmchung@ece.skku.ac.kr***

A Study on the Pharming Attack Protection using DNS Spoofing

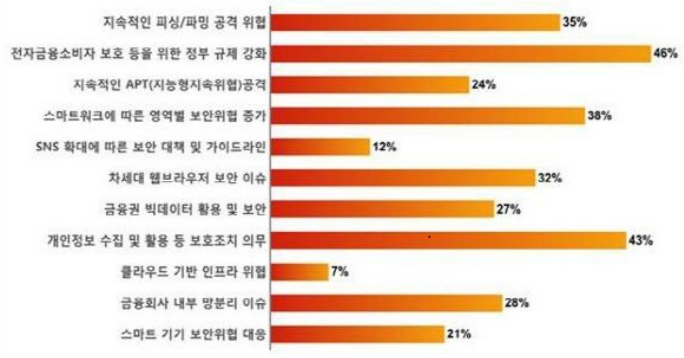
JeongHyuk Park*, Sung-Hwan Ahn**, Min-Woo Park**, Tai-Myoung Chung***
*Dept. Computer Engineering, Sungkyunkwan University
**Dept. Electrical and Computer Engineering, Sungkyunkwan University
***College of Information and Communication Engineering, Sungkyunkwan University

요 약

최근 피싱의 한 유형으로 등장한 파밍은 웹 사이트를 위조하여 개인정보를 탈취하는 공격이다. 신뢰받는 기관(금융, 정부 등)의 사이트로 위장하여 개인정보를 탈취하는 방식은 같으나 차이점은 피싱의 경우 유사 도메인을 이용하는 경우가 많아 사용자가 주의를 기울이면 공격을 피할 수 있다. 하지만, 파밍의 경우 DNS 스푸핑을 이용하여 사용자가 정확한 도메인주소(URL)를 입력 하더라도 공격자가 미리 만들어둔 위장 웹 서버로 접속이 되기 때문에 사용자가 주의 깊게 살펴보아도 공격을 인지하기 어렵다. 본 논문에서는 파밍 공격에 사용되는 DNS 스푸핑에 대해 논의하고 파밍 탐지 기법에 대해 소개한다. 궁극적으로는 파밍 탐지기법들을 비교 및 분석한 후 실제 구현을 위해서 극복해야 할 한계점을 알아본다.

1. 서론

최근 인터넷의 급격한 발달로 인해 인터넷 상에서 금융, 결제 등의 서비스를 제공하고 사용량이 많아짐에 따라 이를 악의적으로 이용하는 각종 보안 위협이 발생하고 있다. 그 중에서도 피싱의 한 유형으로 등장한 파밍의 위협이 증가하고 있다. 파밍은 사용자가 정상적인 웹 사이트로 접속을 시도하여도 공격자가 미리 위조해 놓은 사이트로 유도되게 하는 공격 방식으로 개인정보를 탈취하는 공격이다. 그림 1 은 최근 보안 위협의 전망을 나타내고 있고 파밍 공격이 큰 비중을 차지하고 있음을 보여준다[1].



(그림 1) 다양한 보안 위협

피싱은 사용자의 부주의로 실수를 유발해 스스로가 정보를 유출시키게 하는 사회공학적인 방법을 이용하므로 사용자가 주의를 기울인다면 피해를 예방할 수 있지만 피싱과는 다르게 파밍은 네트워크의 취약점을 이용하여 실제 웹사이트와 동일한 URL 과 형태로 공격이 이루어 지기 때문에 사용자가 공격 사실을 쉽게 인지하기 어렵다. 또한 공격이 이루어지고 난 후에는 곧 바로 경제적인 피해로 연결될 수 있기 때문에 사용자가 사전에 공격을 탐지하지 못한다면 큰 피해가 발생할 수 있다.

파밍 공격은 다양한 형태로 이루어질 수 있지만 주로 DNS 스푸핑을 통해 공격이 이루어진다. DNS 스푸핑은 DNS 서버의 정보를 공격자가 임의로 변경함으로써 사용자가 DNS 서버를 통해 웹 사이트에 접속할 때 공격자가 조작해놓은 정보를 통해 위조된 웹 사이트로 접속하게 만드는 공격 방법이다.

DNS 스푸핑을 이용하는 파밍 공격을 방어하는 방법 중에는 DNS 서버가 주고받는 메시지를 암호화하는 DNSSEC 이나 Trusted Third Party(TTP)를 통하여 웹을 인증하는 등의 연구가 다양하게 이루어지고 있다.

본 논문에서는 이러한 DNS 스푸핑을 이용한 파밍 공격을 방어하는 방법들을 소개하고 비교 분석을 하고자 한다. 2 장은 DNS 와 DNS 스푸핑의 동작원리에 대해 설명한다. 3 장은 알려진 방어방법을 살펴보고 각각의 방어 기법들을 비교 및 분석한다. 4 장은 결론을 말한다.

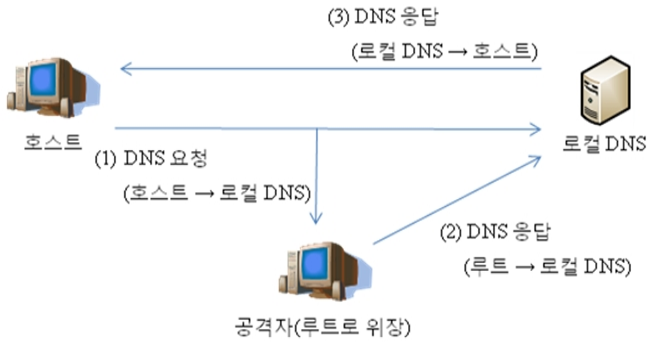
2. 관련연구

2.1 Domain Name System(DNS) 동작과정

인터넷 사용자가 인터넷 호스트 서버에 접속하기 위해서는 해당 호스트 서버의 IP 주소를 통해서 접속을 해야 한다. 하지만 숫자로만 이루어진 IP 주소를 기억하기 어렵기 때문에 문자로 된 도메인 주소를 사용할 수 있다. 이 때 문자로 된 도메인 주소를 해당 IP 주소로 대응 시켜주는 시스템을 Domain Name System (DNS)이라 한다.

DNS 는 성능 향상을 위하여 로컬 DNS 서버를 두고 있다. 로컬 DNS 서버는 캐시를 가지고 있어서 도메인 주소에 대응된 IP 주소 정보들을 Resource Record(RR) 형태로 저장한다[2]. 사용자가 매칭되는 IP 주소를 얻기 위해 DNS 요청 메시지를 보내면 우선적으로 로컬 DNS 서버의 캐시에서 검색해 해당 IP 주소를 찾고 없을 경우에만 로컬 DNS 서버가 루트 서버에게 해당 IP 주소의 검색을 재 요청 한다. 로컬 DNS 서버가 루트 서버로부터 IP 주소와 함께 DNS 응답 메시지를 받으면 해당 정보를 RR 의 형태로 일정 시간 동안 캐시에 저장한다.

2.2 DNS 스푸핑



(그림 2) DNS 스푸핑

DNS 는 대표적으로 다음과 같은 취약점을 지니고 있다. 첫째, 로컬 DNS 서버가 루트서버에게 DNS 요청 메시지를 전송하지 않았더라도 DNS 응답 메시지를 받으면 그 메시지를 유효한 메시지로 취급해 해당 정보를 캐시에 저장한다. 둘째, 로컬 DNS 서버가 루트로부터 DNS 응답 메시지를 받을 때 이 메시지가 실제 루트 서버로부터 온 것인지 검증하지 않는다. 셋째, DNS 메시지가 암호화되지 않고 전송된다.

DNS 스푸핑(DNS Cache Poisoning)은 이와 같은 취약점을 이용한 공격이다. 이 공격은 공격자가 루트 서버로 위장해 로컬 DNS 서버에게 IP 주소가 변조된 DNS 응답메시지를 보냄으로써 로컬 DNS 서버 캐시에 저장된 RR 을 변조하는 공격이다. 공격자가 로컬 DNS 서버에게 DNS 응답 메시지를 보내기 위해서는 DNS 요청과 응답메시지를 구분할 수 있는 Transaction ID (TxID)를 알아야 한다. 이 TxID 는 호스트가 로컬 DNS 서버에게 보내는 DNS 요청 메시지를 중간에서 가로챔으로써 알 수 있다. 따라서 공격자는 Man-In-The-Middle(MITM) 공격을 통해 DNS 요청 메시지를 가로채고 DNS 메시지는 암호화 되어있지 않기 때문에 TxID 를 쉽게 알아낼 수 있다. 로컬 DNS 서버는 루트서버에게 DNS 요청 메시지를 보내지 않은 상태여도 DNS 응답메시지를 허용하고 이 DNS 응답 메시지가 실제 루트서버에서 전송 받은 것인지 확인하지 않으므로 공격자가 보낸 DNS 응답 메시지를 받아 정보를 캐시에 저장한다. 결과적으로 로컬 DNS 서버는 잘못된 RR 을 가지게 되고 호스트에게 DNS 응답 메시지를 통해 변조된 IP 주소를 전송한다.

3. 파밍 공격에 대한 방어 기법

알려진 파밍 방어 기법은 크게 두 종류로 분류할 수 있는데 통신을 암호화 하는 방법과 제 3 의 서버를 통해 IP 주소를 검증하는 방법이 있다. 통신을 암호화 하는 방법에는 표준으로 채택된 DNSSEC 과, TTP 를 이용한 웹 인증방식이 있고 제 3 의 서버를 이용하는 방법은 사전 검출 기반 예방 시스템과 A Dual Approach 가 있다.

3.1 DNSSEC

DNSSEC 은 Internet Engineering Task Force (IETF)의 DNSEXT 워킹그룹에서 DNS 의 취약성을 극복하기 위하여 DNS 데이터에 대한 인증과 무결성 서비스를 제공하여 DNS 에 보안요소를 추가 확장하는 것으로 이를 위해서 DNSSEC 프로토콜은 새로운 RR 유형의 정의와 각 구성요소들의 안전한 상태(Secure Status)에 대한 요구사항들을 정의한다. DNS 보안 확장기술은 RFC2535 에서 기본적인 내용이 기술되어 있으며 표준화 대상이 계속 추가되면서 수정·보완이 진행되고 있다[3].

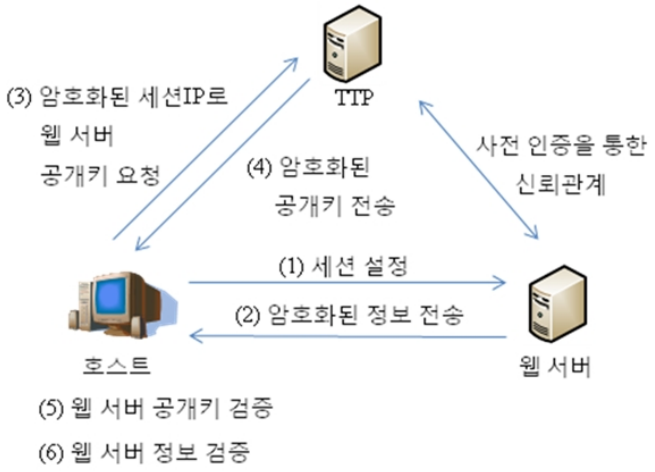
DNSSEC 은 Authoritative DNS 에 설정된 권한 있는 데이터에 대하여 공개키 암호 방식의 전자서명 체계를 적용함으로써 DNS 데이터가 전달되는 과정에 있어서 DNS 데이터의 위·변조 여부를 서명검증을 통해서 검증할 수 있는 보안 체계를 구현하는데 있다. DNSSEC 표준은 RFC4033, RFC4034, RFC4035 의 3 개의 문서로 채택되어 자세히 기술되어 있다[4].

DNSSEC 에서는 로컬 DNS 서버가 응답메시지를 받을 때 RRSIG 라고 불리는 서명도 함께 받는데 이 서명을 검증하기 위해서는 로컬 DNS 서버가 DNSKEY 를 통해 복호화를 해야 한다. 또한 이 DNSKEY 의 유효성을 검사하기 위해 해시과정을 거친 후에 상위 DNS 서버로부터 받은 DS 레코드와 대조하여 확인한다. 공격자는 이 서명검증을 할 수 없으므로 MITM 공격을 방어할 수 있다.

하지만, DNSSEC 기법은 위와 같은 공개키 암호화 방식을 이용함으로 인해 각 DNS 서버에서 처리해야 할 데이터의 양도 커지고 암호화·복호화의 과정에 드는 연산도 필요하기 때문에 기존의 DNS 시스템에 비하여 성능이 크게 저하되어 실제로 적용하기 위해서는 연구가 더 진행되어야 한다.

3.2 TTP 인증

파밍 공격을 해결하기 위한 방법 중 하나는 웹 사이트가 위조되지 않았음을 검증하는 것이다. 그러기 위해서 웹 사이트는 상호간에 신뢰할 수 있는 제 3 의 기관(TTP)으로부터 인증을 받아 사용자에게 자신이 위조되지 않았음을 증명해야 한다. 사용자가 사이트가 위조되지 않았음을 인지하고 이러한 인증과정을 통해 사용자와 사이트간의 신뢰관계를 형성하여 파밍 공격을 방지할 수 있다.



(그림 3) TTP 인증 동작과정

그림 3 는 TTP 인증방식의 동작과정을 보여준다. 사용자는 웹 서버에 접속을 하면서, 세션을 설정 하고 웹 서버의 정보를 요청한다. 웹 서버는 사용자 에게 임의의 문자를 웹 서버의 개인키 암호화 시킨 정보와 함께 보내어 사용자가 증명할 수 있도록 한다. 사용자는 신뢰할 수 있는 TTP 에게 현재 세션의 IP 를 TTP 의 공개키로 암호화하여 전송하고, 웹 서버의 공개키를 요청한다. TTP 는 웹 서버의 공개키를 TTP 의 개인키로 암호화한 정보와 함께 보내어 사용자가 증명할 수 있도록 한다. 사용자는 TTP 의 공개키로 TTP 에게 전송 받은 정보를 복호화하여 검증하고, 이를 이용해 웹 서버가 보내온 정보를 복호화한다. 복호화된 정보 와 수신한 정보를 비교하여 웹 서버가 신뢰할 수 있는 사이트인지 증명한다[5].

3.3 사전 검출 기반 예방 시스템

사전 검출 기반 예방 시스템은 로컬 DNS 서버가 포함되어 있는 인트라넷 상에 검출서버를 추가로 두어 검출서버를 통해 로컬 DNS 서버의 캐시가 변경되었을 때 변경사항을 검출하는 방법이다. 검출서버는 로컬 DNS 서버와 동일한 데이터베이스 정보를 가지고 동일한 인트라넷 안에 구성되어 외부에서는 그 존재를 알 수 없어야 한다.

사전 검출 기반 예방 시스템의 동작과정은 다음과 같다. 호스트가 로컬 DNS 서버에게 DNS 요청 메시지를 전송하면 로컬 DNS 서버는 데이터베이스에서 해당 IP 주소를 찾고 찾은 IP 주소와 사용자가 요청한 도메인주소를 검출서버에 전송한다. 검출서버는 전달받은 값을 이용하여 검출서버의 데이터베이스에서 도메인주소에 해당하는 IP 주소를 찾는다. 그 후 검출서버에서 찾은 IP 주소와 로컬 DNS 서버로부터 받은 IP 주소를 비교하여 결과를 로컬 DNS 서버에게 전송한다. 이 때 만약 비교 값이 다르다면 검출서버에서 찾은 IP 주소도 함께 전송한다.

검출서버의 데이터베이스는 DNS 스푸핑 공격받더라도 변조되지 않기 때문에 검출 서버를 통하여 데이터베이스의 조작 여부를 판별할 수 있다[6].

3.4 A Dual Approach

A Dual Approach 는 Third-Party DNS 서버(e.g. OpenDNS, Google DNS, etc.)의 정보와 로컬 DNS 서버의 정보를 대조하여 IP 주소와 웹 페이지의 내용을 검증함으로써 클라이언트 측에서 공격을 탐지하는 기법이다. 이 검증 과정은 호스트가 사용하는 웹 브라우저에 통합시켜 공격 위협이 감지되면 클라이언트에게 경고함으로써 피해를 예방한다.

A Dual Approach 의 동작과정은 다음과 같이 이루어진다. 호스트가 로컬 DNS 서버에게 DNS 요청 메시지를 전송하면 동시에 DNS 요청 메시지가 Third-Party DNS 서버에도 전송된다. 로컬 DNS 서버로부터 받은 IP 주소와 Third-Party DNS 서버로부터 받은 IP 주소를 대조하여 IP 주소가 같다면 공격위협이 없는 것으로 판단한다. 만약 IP 주소가 다르면 다음 과정으로 웹 페이지 내용을 검증하기 위해 양측에서 받은 IP 주소에 HTML 요청을 전송해 웹사이트의 소스 코드를 전송 받고 비교 검증한다[7].

이 방법은 DNS 스푸핑 공격을 효과적으로 예방할 수 있지만 Third-Party DNS 서버를 항상 신뢰할 수 있는 것이 아니고 개인정보가 Third-Party DNS 서버에 유출되므로 privacy 보호 문제를 가진다. 또한 호스트가 URL 에 접속할 때마다 매번 Third-Party DNS 서버에 인증하는 과정을 거치는데 호스트와 Third-Party DNS 서버의 물리적인 위치가 멀리 떨어져 있다면 처리속도가 늦어지는 단점이 있다.

3.5 방어 기법의 비교 및 분석

먼저, DNSSEC 은 DNS 메시지를 공개키 암호화 방식을 통해 암호화 하기 때문에 DNS 의 근본적인 보안 취약점을 극복함으로써 파밍 공격을 방어할 수 있다. 하지만 암호화하는 과정으로 인하여 메시지를 처리하는 속도가 느리고, 서명용 키를 생성하고 관리해야 하며 서명된 데이터도 주기적으로 관리해야 한다. 이러한 문제점은 현실적으로 DNSSEC 을 적용하는 데에 어려움을 가져다 준다.

TTP 인증 방법은 웹 서버가 신뢰할만한 제 3 의 기관과 암호화된 인증 방식을 통해 웹 서버 자체를 검증 받는 방식이다. 이 방법은 웹 사이트가 자발적으로 인증과정을 거쳐야 하기 때문에 모든 웹사이트가 검증을 받아야 하지만 현실적으로 한계가 있고 인증받는 과정으로 인해 처리 성능 또한 저하된다.

사전 검출 기반 예방 시스템은 기존의 로컬 DNS 서버와 같은 데이터베이스를 가지는 검출서버를 따로 두어 이 둘을 대조하는 방식으로 IP 주소를 인증하였다. 이로 인해 모든 로컬 DNS 서버는 검출서버를 구축하기 위한 추가비용이 발생한다. 또한 로컬 DNS 서버와 검출서버간의 추가적인 검증과정으로 인해 네트워크의 성능이 저하된다.

A Dual Approach 는 Third-Party Public DNS 서버의 정보와 로컬 DNS 서버의 정보를 대조하여 IP 주소와 웹 페이지 내용을 인증한다. Third-Party DNS 서버를 사용하는 특성상 공식적으로 DNS 서버를 신뢰할 수 없고 DNS 메시지를 통하여 개인정보(사용자의 IP 주소, 방문한 웹 사이트 등)가 누출되는 문제가 발생한다. 또한 Third-Party DNS 서버가 물리적으로 사용자와 멀리 떨어져 있다면 매번 Third-Party DNS 서버와 대조하여 인증을 하기 때문에 그에 따른 성능저하도 발생한다.

표 1 은 파밍 공격에 대한 탐지 및 방어 방법들을 비교하기 위해 몇 가지 특성들을 정리한 것이다.

<표 1> 파밍 공격 방어기법 비교

특징	서버	암호화	성능	한계점
DNSSEC	X	O (DNS 메시지 암호화)	DNS 메시지 암호화로 처리성능 저하	서명용 키・데이터 관리 곤란, 암호화로 인한 성능 저하
TTP 인증	X	O (TTP 인증과정 중 암호화)	인증과정과 암호화로 인한 성능 저하	모든 웹 서버가 TTP 인증을 받을 수 없음
사전 검출 기반 예방 시스템	O (검출서버 추가 구축)	X	검출서버와 로컬 DNS 서버 간의 추가적인 통신으로 인한 성능 저하	검출서버를 위한 추가비용이 큼
A Dual Approach	O (Third-Party DNS 서버 이용)	X	Third-Party DNS 서버의 물리적 위치에 따라 다름	Third-Party DNS 서버의 신뢰도 문제, 개인정보유출 문제, 속도가 느릴 수 있음

4. 결론

피싱 공격과는 다르게 파밍 공격은 원래 도메인 주소와 동일한 도메인 주소로 공격이 이루어지고 웹 사이트의 형태도 원래의 것과 동일한 형태로 위조되어 공격이 이루어 지기 때문에 피해자는 주의를 기울여도 공격을 인지할 수 없는 것이 가장 큰 문제점이다. 본 논문에서는 이러한 파밍 공격에 기초가 되는 DNS 스푸핑 공격을 호스트 측에서 탐지할 수 있는 방법을 소개하였다. 기존의 DNS 는 별도의 인증과정이 없이 로컬 DNS 서버를 신뢰하였기 때문에 DNS 스푸핑 공격에 노출되었다. 이 취약점을 극복하기 위해 본 논문에 소개된 방어법은 암호화를 통해 인증하거나 제 3 의 서버로부터 인증을 받는 방법으로 공격을 예방하였다. 가장 이상적인 방법은 전 세계의 모든 웹사이트가 TTP 인증을 통해 검증을 받는 것이지만 이는 현실적으로 불가능하다. 검출서버를 두는 방식은 추가적인 비용을 감수해야 하지만 속도적인 측면에서는 복잡한 암호화 과정도 없고 검출서버가 물리적으로 가깝게 위치하기 때문에 가장 우수하다고 예상된다. A Dual Approach 는 현실적으로 적용하기 가장 효과적이지만 Third-Party DNS 서버를 신뢰해야 한다는 문제점이 있다. 마지막으로 DNSSEC 은 아직 현실에 적용하기에는 비효율적인 측면이 더 크기 때문에 더 연구가 진행되어야 한다.

DNSSEC 은 암호화로 인한 성능저하를 극복하고 서명용 키・데이터에 대한 관리가 잘 이루어 진다면 DNS 의 근본적 문제인 인증과정의 결여를 해결함으로써 파밍을 완벽히 방어할 수 있다. TTP 인증을 통한 방어법 또한 TTP 인증을 한 웹 사이트라면 사용자 측에서 파밍 공격을 사전에 탐지할 수 있다. 사전 검출 기반 예방 시스템을 통한 방어법은 검출서버의 안전성이 보장되고 데이터베이스의 관리가 잘 이루어 진다면 DNS 스푸핑을 방어할 수 있다. A Dual Approach 는 사용자의 개인정보노출에 대한 동의와 Third-Party 의 신뢰도가 보장된다면 사용자 스스로가 파밍 공격에 적극적으로 대응할 수 있다.

참고문헌

[1] 금융보안연구원, “2013 년 금융 IT 보안 이슈 전망 설문조사 결과”

[2] Ramzi Bassil. “Security Analysis and Solution for Thwarting Cache Poisoning Attacks in the Domain Name System” Telecommunications (ICT), 2012 19th International Conference on

[3] D. Eastlake, “Domain Name System Security Extensions,” RFC 2535. http://www.ietf.org/rfc2535.txt, 1999.

[4] Yong Wan Ju, “Cache Reliability Enhancing Method for Recursive DNS”, Journal of Korea Information Processing Society C, 2008.

[5] Dong-og Min, “A Study on the Phishing Attack Protection using URL Spoofing”, Journal of Korea Institute of Information Security & Cryptology Vol.15, No.5, 2005

[6] Woong Go, “Phishing and Pharming Prevention System used Pre-Extraction”, Journal of Korean Society For Internet Information, 9(2), 2008.11, 521-526 (6 pages)

[7] Sophie Gastellier-Prevost, “A dual approach to detect pharming attacks at the client-side”, New Technologies, Mobility and Security (NTMS), 2011 4th IFIP International Conference on