DNS 상에서 Pseudonoise Sequence 를 사용한 안전한 질의/응답 시스템에 관한 연구

석우진, 이만희, 최홍진, 변옥환
한국전자통신연구원 슈퍼컴퓨터센터 고성능망기반연구팀

A Study on Secure Query/Response System using Pseudonoise Sequence in DNS

Woojin Seok, Manhee Lee, Hyungwoo Park, Okhwan Byun
High Performance Networking Research Team, Supercomputer Center, ETRI

요약

DNS 는 인터넷상에서 도메인 네임과 IP 주소간의 상호 전환의 동작을 수행하는 시스템이다 DNS 상에서 도메인 네임이나 IP 주소를 요청하는 질의나 이에 대한 응답은 네트워크상에서 UDP 를 사용한 메시지 형식으로 전송된다. 이때 제 3 자의 개입에 의한 조작의 가능성이 있다. 이러한 질의와 응답 메시지의 조작을 방지하고자 RFC2065 에서는 RSA 공개키 방식을 사용하였다. RSA 공개키 방식은 현재 국내에서 직접 사용하기에는 많은 애로사항이 있으며 속도 측면에서 좋지 않은 면을 보여주고 있다.

본 논문에서는 Pseudonoise Sequence 와 MD5 를 사용하여 DNS 상에서의 안전한 질의 응답을 가능하게 하고자 한다. Pseudonoise Sequence 와 MD5 를 사용함으로써 메시지를 암호화하지 않아도 되며 또한 많은 계산을 요구하지도 않는다. 메시지에 Pseudonoise Sequence 를 기입하고, 그 메시지의 MD5 를 송수신측에서 검사함으로써 제 3 자 개입에 의한 조작 방지와 메시지 데이터의 무결성을 보장할 수 있다.

1. 서론

DNS는 TCP/IP 기반에서 도메인 네임(domain name)을 IP 주소로 변환시켜주는 역할을 한다. DNS는 host.txt를 기반으로 이루어졌던 과거의 네임 변환이 엄청난 수의 호스트의 증가로 새로운 개념을 요구함으로써 나타나게 되었다. DNS를 사용하기 전에는 각 호스트에 host.txt 파일을 이용하여 네임 변환을 하였다. 하지만 인터넷의 사용증가로 인하여 host.txt파일 사용에 그 한계가 생기게 되었다. DNS는 이러한 정적인 네임 변환체계를 동적으로, 또한 분산적으로 구현함으로써 호스트 수의 증가에 따른 해결 방법이 된 것이다 DNS는 다음의 3가지 요소로 구성되어 있다 도메인 네임 공간, 리졸버(Resolver), 네임 서버 (Name Server) 등이 그것이다[1][2]. 도메인 네임 공간에 존재하는 정보를 바탕으로 네임서버는 사용자의 질의 요청에 응답을 하게 된다. 리졸버는 사용자와 네임서버 사이에서 질의와 응답의 메시지를 전송해 주는 역할을 해준다. 메시지 전송과정에서 제3자의 침입으로 존 정보의 조작을 가져올 수 있다. 조작된 존 정보로 인하여 질의 요청자는 제3자의 의도에 의해 많은 손실을 볼 수도 있다. 이러한 제3자의 조작 혹은 전송 상에 발생한 네트워크의 오류로 말미암은 잘못된 정보의 전송을 막기위한 시스템이 요구된다[3].

본 논문은 DNS 상에서의 안전한 질의 응답을 구현할 수 있는 시스템을 구현하여 제3자 개입에 의한 조작으로 사용자에게 손실을 가져올 수 있는 환경을 방지하고자 한다. 리졸버와 네임서버 간의 메시지 전송에 있어 Pseudonoise Sequence 와 MD5를 이용한 시스너처의 사용으로 메시지의 안전한 전송과 존 정보의 무결성을 보장하고자 한다. 이는 캐쉬 정보의 안정성도 보장하여 캐쉬에 의한 지속적인 오류 발생도 방지할 수 있게 된다.

2. RFC2065 에서의 안전한 DNS 질의와 응답

도메인 네임 시스템에서의 질의는, 응답을 요구하며 네임 서버에게 보내어 지는 메시지이다. 인터넷 상에서, 질의는 UDP 데이터그램으로 전송되어진다. 네임서버에 의한 응답 메시지는 질의 메시지에 대한 응답으로 보내지거나, 혹은 다른 네임서버를 지칭하는 내용으로 보내어진다 또한 에러가 발생하였을 경우 에러에 대한 내용으로 보내어 진다[1][2].

도메인 네임 서버의 질의와 응답들은 일반적으로 표준 메시지 형식으로 전송되어진다. 이러한 메시지 형식은 그림1과 같이 몇 개의 고정된 필드를 포함하고 있는 헤더와 질의 내용이나 응답에 대한 RR을 담고 있는 네 개의 섹션으로 구성되어 있다[2].

이러한 구조를 가지는 메시지가 전송 경로를 통해 전송되는 도중 제3자의 가로채기 등의 수법으로 네임 서버에 대한 질의 메시지를 조작할 수 있다.

RFC 2065에서는 RSA 공개키 방식에 의한 인증과 데이

터 무결성을 근간으로 한다. 즉 RSA 공개키로부터 생

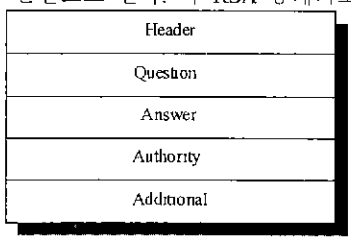


그림 1. 메시지 형식

성된 시그너쳐를 메시지와 함께 네임 서버에 전송되어진다[3]. 물론 RSA 공개키 값을 사용하기 위해서는 키의 분배가 먼저 선행되어야 한다. 하지만 RSA 공개키 방식으로 구현되는 DNS 시스템은 아래와 같은 여러 가지 문제점을 발생시킬 수 있다[4].

- RSA 알고리즘의 저작권 문제
- RSA 알고리즘의 많은 계산량으로 인한 오버헤드
- RSA 공개키 관리를 위한 하부구조 설정

위의 단점을 극복하기 위해서 본 논문에서는 Pseudonoise Sequence와 MD5의 사용을 제안한다.

3. Pseudonoise Sequence 를 이용한 안전한 질의와 응답

3.1 Pseudonoise Sequence 와 MD5

Pseudonoise 또는 Pseudoransom 은 엄격한 의미에서의 Random 은 아니다. 결정적이며 주기적인 코드를 생성한다 즉 무작위 같은 코드가 주기적으로 반복된다 이는 그림 2 에서 보는 바와 같이 LFSR(Linear Feedback Shift Register)를 사용하여 코드를 생성한다. 아래 그림 2 와 같은 경우는 15 clock cycle 만에 같은 문자열이 반복된다. 하지만 비트가 100 개면 2^{100} - 1 clock cycle 이 되어야 문자열이 반복된다. 주기가 길 경우에는 마치 Random 코드처럼 생성된다[6]

위와 같은 Pseudonoise Sequence 가 질의와 응답 시에 질의를 요청하는 곳과 응답을 하는 곳 각각에서 생성된다. 양측에서 동시에 생성되기 시작한다면 Pseudonoise Sequence 는 항상 같은 값을 발생시킨다. 하지만 제 3 자의 측면에서는 다음에 발생될 값을 전혀 예상할 수 없다. 그래서 Pseudonoise Sequence 에 의한 MD5 시스너쳐 값을 송수신측에서 검사함으로써 제 3 자의 조작이나 데이터의 오류를 파악할 수 있다[5][6].

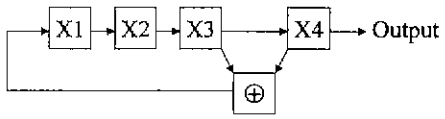


그림 2. LSFR 을 사용한 Pseudonoise Sequence

3.2 제안된 방법을 이용한 안전한 DNS 의 질의와 응답

질의와 응답에 사용되는 메시지는 질의 요청자에 의해 만들어 진다. 질의 메시지에 대하여 각 네임 서버는 도메인 네임 공간 상에서 적절한 답을 골라 응답 메시지로 만들어 질의 요청자에게 전달한다. 이 과정에서 Pseudonoise Sequence 와 MD5 에 의한 시그너쳐는 아래 그림 3 과 같이 적용된다.

1) 전제 조건

Pseudonoise Sequence 를 질의 요청자와 네임 서버에서 사용하기 위해서 먼저 Pseudonoise Sequence 를 발생시키는 초기값이 설정되어야 한다. 이 초기값은 Random Number 생성에 의해 생성된다. 질의 요청자는 시스템의 부트 시에 이미 설정되어 있는 네임 서버로부터 초기값을 전달받는다. 네임 서버는 질의 요청자의 IP 주소와 초기값으로써 상호 매핑 테이블을 구성한다. 구성된 테이블을 이용하여 각각의 질의 요청자의 질의 응답 시에 Pseudonoise Sequence 를 생성하여 전송하게 된다.

2) 1'st stage

첫번째 단계는 질의를 요청하는 단계로써, PS (Pseudonoise Sequence)를 생성한다. 생성된 PS 와 전송하고자 하는 메시지에 대한 SIG(시그너쳐)를 생성한다. 생성된 시그너쳐는 메시지의 Additional 섹션에 실려 네임 서버로 전송된다.

3) 2'nd stage

두번째 단계는 응답을 하는 네임 서버에서 수행되는 동작이다. 네임 서버에서는 전송되어 온 메시지에 대해서 SIG 를 생성한다. 질의 요청에 대한 SIG 와 네임서버에서 생성된 SIG 값이 같을 경우는 전송상의 오류가 발생하지 않았음을 의미한다. 만일 두개의 SIG 값이 상호 다를 경우는 전송상의 오류가 발생했음을 의미하므로 폐기된다.

4) 3'rd stage

세번째 단계는 네임서버에서 질의에 대한 응답 메시지를 만들어 질의 요청자로 응답하는 과정을 보인 것이다. 먼저 두 번의 과정을 거쳐 새로운 PS 를 생성한다. 이는 질의 요청에 사용되어진 PS 의 다음 값을 이용하기 위함이다 그리고 생성된 PS 와 응답 메시지에 대한 SIG 를 생성하여 질의 요청자로 전송된다.

5) 4'th stage

네번째 단계는 응답에 대한 질의 요청자에서 수행되는 단계로써, 먼저 질의 요청자에서의 새로운 PS 값을 생성한다. 그리고 생성된 PS 와 전송되어진 메시지의 SIG 를 구한다. 구해진 SIG 와 전송되어온 SIG 를 비교하여, 서로 같을 경우는 전송상에서 제 3 자의 개입에 의한 조작이나 전송상의 데이터 오류가 없음을 의미한다. 서로 같지 않을 경우는 전송상에서 제 3 자의 개입에 의한 조작이나 전송상의 데이터 오류가 발생했음을 의미한다.

3.3 기존의 방법과의 비교

제안된 방법에서의 안전한 DNS 의 질의와 응답은 RSA 공개키에서 요구되는 많은 계산량을 요구하지 않는다. 또한 공개키를 사용함으로써 발생되는 공개키 분배 문제와는 달리 네임 서버에 접속되는 질의 요청자에 대한 테이블만을 요구한다. 이 테이블에는 Pseudonoise Sequence 코드와 각 질의 요청자의 IP 주소의 매핑에 대한 정보가 담겨져 있다. 공개키를 사용하는 방법과 본 논문에서 제안된 방법을 다음 표 1 에서 비교하였다.

4. 결론

DNS 는 도메인 네임 공간 상에서 도메인 네임이나 IP 주소에 대한 질의에 대한 응답을 하는 시스템이다. 특히 인터넷의 사용의 증가로 계층적인 도메인 네임 공간을 구현하게 되었다. 이러한 DNS 상에서 질의와 응답은 제 3 장의 개입에 의한 조작이 가능하다. 공개키를 사용하는 방법이 RFC 2065 를 통해서 제시되었다. 하지만 국내에서의 저작권 문제나 알고리즘의 복잡성으로 인하여 많은 계산량을 요구한다. 본 논문에서는 이러한 단점을 극복할 수 있는 방법을 제시하였다. Pseudonoise Sequence 와 MD5 를 사용하여 제 3 자 개입에 의한 조작을 방지할 수 있으며 데이터의 무결성도 보장할 수 있는 방법이다. 제안된 방법은 많은 계산량을 요구하지도 않으며 공개키를 사용하지 않기 때문에 키 분배를 위한 하부구조를 구축할 필요도 없다. 제안된 방법을 구현한 DNS 로써 DNS 상에서의 안전한 질의와 응답을 보장할 수 있다.

참고문헌

[1] RFC1034, "Domain Names - Concepts and Facilities" IETF, November, 1987

[2] RFC1035, "Domain Names - Implementation and Specification", IETF, November, 1987

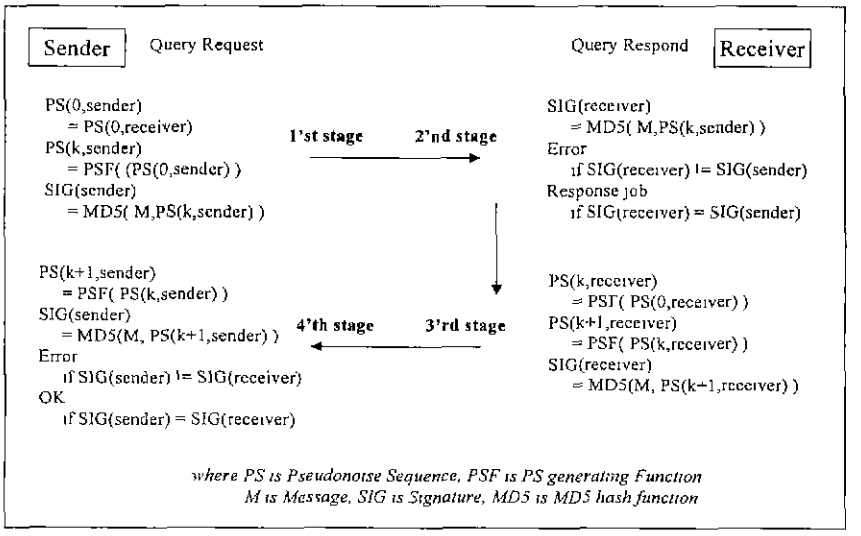
[3] RFC 2065, "Domain Name System Security Extensions" IETF, January, 1997

[4] Internet-Draft, "Secret Key Transaction Signatures for DNS", IETF, June, 1998

[5] 김칠, 암호학의 이해, 영풍문고(주), pp.166-181, 1996

[6] Bernard Sklar, Digital Communications Fundamental and Applications, Prentice Hall International editions, pp.546-549, 1988

그림 3. Pseudonoise Sequence 를 이용한 안전한 질의와 응답 시스템



	RSA, MD5 in RFC2065	제안된 방법
메시지 생성 속도	RSA 가 요구하는 많은 계산량으로 인하여 다소 느린 편임	Pseudonoise Sequence 의 생성에 있어서 상대적으로 계산량이 적음
사용되는 키	RSA 공개키를 사용	Pseudonoise Sequence
키 분배 및 관리	공개키 분배를 위한 하부구조가 필요함	네임 서버 내에서 질의 요청자의 ID 와 Pseudonoise Sequence 의 매핑 테이블이 필요
저작권 문제	국내 사용에 이로점이 있음	해당 사항 없음

표 1. 공개키 방법과 Pseudonoise Sequence 를 사용한 제안된 방법 비교