암호화 알고리즘이 웹 서버에 미치는 영향에 대한 연구

정기훈° 노삼혁
홍익대학교 컴퓨터공학과, 정보컴퓨터공학부

khchong@cs.hongik.ac.kr, samhnoh@hongik.ac.kr

A Study of Performance Effects of Encryption Algorithms on Web Servers

Kihun Chong° Sam H. Noh
Dept. of Computer Engineering, Information and Computer Engineering, Hongik Univ.

요 약

웹 환경에서 금융거래관련 사이트의 증가로 인하여 암호화 모듈을 장착하는 웹 서버 시스템 역시 증가하는 추세이다. 이런 경향에 맞추어 본 논문에서는 웹 환경에서 사용하는 다양한 암호화 알고리즘에 대하여 조사하고 각 알고리즘이 웹 서버에 얼마나 많은 성능상의 영향을 미치는지에 대하여 연구하였다. 실제 웹 서버에 암호화 프로세스를 구현하여 실험한 결과, 암호화 모듈을 장착한 웹 서버는 그렇지 않은 웹 서버에 비해 약 4.5배의 성능저하를 보였으며, 암호화 알고리즘 중에는 AES 알고리즘이 가장 좋은 성능을 나타냈다.

1. 서론

늦은 출발에도 불구하고 전세계에서 가장 높은 인기를 얻고 있는 월드와이드웹(World Wide Web; WWW)은 이제 인터넷에 있어서 없어서는 안될 중요한 요소가 되었다. 뿐만 아니라 웹의 발달에 따라 부수적으로 여러 가지 웹 기반 기술이 발달하였는데, 그 중에서도 금융관련 분야가 가장 두드러지게 발전하고 있다. 우리 나라는 2004년 1월 현재 인터넷 이용인구가 3000만을 육박하고 있으며, 이 중에서 전자상거래, 인터넷 뱅킹 등 보안이 필수적인 서비스를 이용하는 인구비율은 약 23%로 이것은 약 690만의 사용자가 보안을 필요로 하는 서비스를 사용하고 있다는 것을 나타낸다[1].

이처럼 전자상거래 시스템, 인터넷 뱅킹 등의 서비스에서 꼭 지원해야 하는 것이 바로 개인 정보 보호를 위한 보안인데, 특히 웹 환경에서는 주로 웹 서버와 브라우저 사이에서 데이터의 교환이 이루어지기 때문에 여러 금융거래 관련 시스템에서는 웹 환경의 보안을 위하여 웹 서버와 브라우저사이에서 교환하는 데이터를 암호화하여 개인 정보를 보호하고 있다.

이러한 경향에 맞추어 본 논문에서는 웹 환경에서 사용하거나 사용 가능한 여러 가지 암호화 알고리즘에 대하여 조사하고 각 알고리즘이 웹 서버 시스템에 얼마나 많은 영향을 미치는가에 대하여 연구하였다. 실제로 암호화를 사용하는 웹 환경을 구축하여 실험을 해본 결과, 암호화 알고리즘으로 인하여 웹 서버 시스템의 성능이 현저히 떨어지는 것을 확인할 수 있었다.

논문의 구성은 다음과 같다. 먼저 2절에서는 관련 연구에 대하여 논한다. 3절에서는 여러 가지 암호화 알고리즘에 대하여 알아보고 4절에서는 암호화 알고리즘을 웹 환경에서 구현하여 실험 및 성능 평가를 하고 그 결과에 대하여 논한다. 마지막으로 5절에서 결론 및 향후 과제에 대하여 언급한다.

2. 관련 연구

보안을 필요로 하는 웹 환경으로 가장 대표적인 분야는 전자상거래와 인터넷 뱅킹 사이트이다[1][2]. 이들 사이트에서는 실제 현금이 온라인을 통해서 직접 거래되기 때문에 금융과 관련된 모든 정보를 암호화하여 송수신한다. 전자상거래에서 사용하는 인터넷 결제시스템이나 인터넷 뱅킹 시스템은 서버와 클라이언트 시스템 모두에서 암호화/복호화가 이루어지며, 암호화/복호화 이전 단계에서 인증 절차를 거쳐야 한다. 이러한 보안을 위하여 서버나 클라이언트 시스템에는 독립적인 보안 모듈을 첨가한다[3].

웹 환경에서 암호화를 구현하기 위해서는 사실상 웹 서버 시스템에 암호화 프로세스가 동작해야 하며 아파치 웹 서버의 경우 SSL 등의 알고리즘이 구현되어 있다[4]. 그렇기 때문에 더욱 높은 보안 레벨을 유지하기 위해서는 웹 서버 시스템에 부가적으로 암호화 프로세스를 동작시켜야 하며 이것은 웹 서버에 많은 영향을 미친다. 따라서 본 논문에서는 부가적인 암호화 프로세스를 제작하여 웹 서버에 얼마나 큰 영향을 미치는 가에 대하여 연구한다.

3. 암호화 알고리즘

3절에서는 암호학에서 많이 다루는 암호화 알고리즘에 대하여 언급한다. 본 논문에서는 메시지 요약에 대해서는 언급하지 않으므로, 메시지 요약을 제외한 대칭키 암호화 알고리즘과 비대칭키 암호화 알고리즘에 대해서만 논하기로 한다.

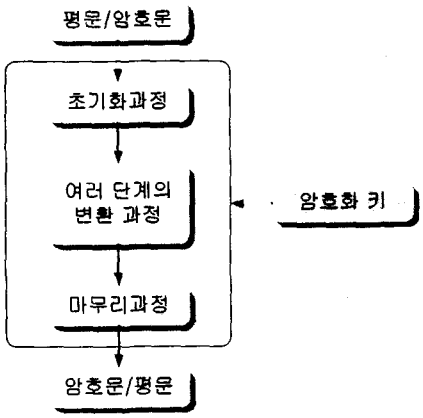

그림 1. 암호화 알고리즘 구조

3.1 대칭키 암호화 알고리즘

대칭키 암호화 알고리즘은 암호화/복호화 과정에서 동일한 비밀키(Secrete Key)를 사용하는 알고리즘으로. 암호화 모델 중 기밀성, 무결성, 인증 모델을 지원한다. 이러한 대칭키 암호화 알고리즘의 키의 길이는 보통 56~128비트이며 대부분의 연산이 MOD, XOR, SHIFT 등의 비트연산위주로 구성되어 있기 때문에 암호화/복호화 속도가 빠르다는 장점을 가지고 있다. 그러나 키 교환이 어려우며 비밀키의 노출에 매우 취약하다는 단점을 가지고 있다. 하지만 데이터의 크기와는 상관없이 암호화/복호화를 할 수 있기 때문에 인터넷 환경에서 가장 많이 사용하고 있다. 이러한 알고리즘으로는 DES(Data Encryption Standard), 3DES(Triple-DES), AES(Advanced Encryption Standard), IDEA(International Data Encryption Algorithm) 등이 있으며 각각의 알고리즘의 특징을 표 1에서 정리하고 있다.

알고리즘	키 길이	암호화 블록 길이
DES	56비트	64비트
3DES	168비트	64비트
AES	128, 192, 256비트	128, 192, 256비트
IDEA	128비트	64비트
Blowfish	32~488(보통 128)비트	64비트
Cast5	40~128(보통 128)비트	64비트
RC2	가변길이	64비트

표 1. 대칭키 암호화 알고리즘

그림 1은 암호화 알고리즘의 동작 원리를 보여주고 있다. 대칭키 암호화 알고리즘은 동일한 비밀키를 사용하기때문에 비밀키 알고리즘이라고도 하며 키의 길이가 길수록 암호화 정도는 더욱 견고해진다. 현재는 DES와 같은 알고리즘은 키의 길이가 길지 않기 때문에 비밀키를 찾아내는데 많은 시간을 필요로 하지 않으며, 따라서 현재는 적어도 키의 길이가 128비트 이상이 되어야 하는 암호화 알고리즘을 사용한다. 마이크로소프트의 IIS를 비롯한 여러 소프트웨어는 128비트 이상의 비밀키를 지원하고 있다[3]. 키의 길이와 키를 찾아내는데 걸리는 시간을 표 2에서 정리하고 있다.

키 길이	키 개수	소요시간(10^{12}개/초)
32비트	$2^{32} = 4.3 \times 10^{9}$	2.15밀리초
56비트	$2^{56} = 7.2 \times 10^{16}$	10.01시간
128비트	$2^{128} = 3.4 \times 10^{38}$	5.4×10^{18}년

표 2. 키 길이에 대한 키 탐색 소요시간

3.2 비대칭키 암호화 알고리즘

비대칭키 암호화 알고리즘은 암호화/복호화 과정에서 사용하는 키가 다른 알고리즘으로 기밀성, 무결성, 인증, 부인방지 등의 암호화 모델을 모두 지원한다. 비대칭키 암호화 알고리즘의 가장 큰 특징이 바로 서로 다른 두 개의 키로 인한 암호화의 확장이다. 대칭키 알고리즘으로는 구현할 수 없었던 비밀키 교환이나 부인방지 등을 구현할 수 있기 때문에 대칭키 암호화의 단점을 극복할 수 있는 알고리즘으로 많이 사용된다. 그러나 키의 길이가 적어도 1024비트 이상은 되어야 하며, 대부분의 연산이 정수론에 바탕을 둔 소수 구하기, 2의 거듭제곱 연산이기 때문에 암호화/복호화 속도가 매우 느리다는 단점을 가지고 있다.

비대칭키 암호화 알고리즘은 그림 1의 암호화 알고리즘과 같은 형태를 띠고 있으며 암호화, 복호화 과정시 사용되는 키만 다르다. 이러한 서로 다른 키를 각각 개인키(Private Key), 공개키(Public Key)라고 부르며, 개인키를 이용하여 암호화를 한 암호문은 공개키를 이용해서만 복호화할 수 있으며, 공개키를 이용하여 암호화를 한 암호문은 개인키를 이용해서만 복호화할 수 있기 때문에 문서보호가 대칭키 알고리즘 보다 훨씬 용이하다. 이러한 알고리즘으로는 대표적으로 RSA가 있다.

4. 실험 및 성능 평가

이번 절에서는 웹 기반 환경에서의 암호화 알고리즘에 대한 실험 환경 및 성능 평가에 대한 결과를 차례로 논한다.

4.1 실험 환경

실험 환경은 웹 서버 시스템으로 가장 많이 사용하는 리눅스 운영체제상의 아파치 웹 서버 환경으로 구축하였다[5]. 서

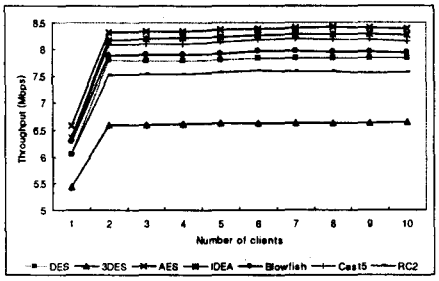

그림 2. 대칭키 암호화 알고리즘을 이용한 서버의 처리율
(암호화 알고리즘을 사용하지 않은 서버의 처리율: 38Mbps)

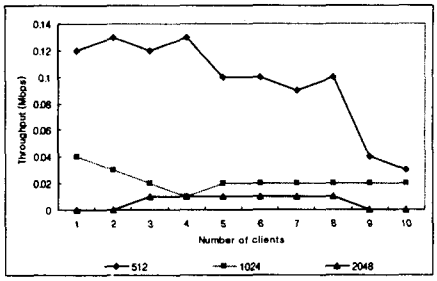

그림 3. 비대칭키 암호화 알고리즘을 이용한 서버의 처리율

버 시스템은 750MHz P-III/256MB/Linux 2.4.20을 사용하였으며, 클라이언트 시스템은 1.7GHz P-IV/512MB/Linux 2.4.20을 사용하였다.

웹 서버는 아파치 웹 서버 1.3.29 버전을 사용하였으며, 웹 서버의 벤치마크는 WebStone 2.5를 사용하였다[4][6]. 워크로드(Workload)는 모든 문서에 대해서 암호화를 해야 하기 때문에 WebStone의 CGI 프로그램에 각각의 암호화 알고리즘을 담은 암호화 엔진을 추가하여 요청하는 모든 파일에 대하여 해당 알고리즘으로 암호화 할 수 있도록 하였다. 암호화 알고리즘으로는 대칭키 암호화 알고리즘으로 DES, 3DES, AES, IDEA, Blowfish, Cast5, RC2를, 비대칭키 암호화 알고리즘으로 RSA를 사용하였다. 결과는 각 집단마다 클라이언트의 수를 1에서 10까지 증가 시키면서 세 번씩 실험하여 그 평균을 구하였다.

4.2 실험 결과

암호화 알고리즘마다 클라이언트 수에 따른 초당 접속률(connection rate), 응답시간(response time), 처리율(throughput)을 측정하였으며, 본 논문에서는 공간의 제약상 처리율만을 나타내었으며 대칭키와 비대칭키 암호화 알고리즘간의 성능이 엄청난 차이를 보였기 때문에 각각 다른 그래프로 나타내었다. 그림 2에서 볼 수 있는 것과 같이 대칭키 암호화 알고리즘을 이용한 경우에는 AES가 가장 우수한 성능을 보여준다. AES는 처리율 뿐만 아니라 응답시간과 접속률에 있어서도 가장 좋은 성능을 나타내었다. AES는 가장 최근에 만들어진 알고리즘이라는 사실을 고려해 볼 때, 최초로 암호화 기법을 적용하는 곳이나 오래된 암호화 알고리즘을 교환하고자 할 때 상당한 이득을 얻을 수 있다는 것을 알 수 있다. 또한 눈여겨볼 부분이 많은 소프트웨어에서 사용하는 암호화 알고리즘인 3DES인데, 안전성의 향상을 위하여 성능상의 많은 손해를 감수하는 것을 알 수 있다. 키의 길이를 조금 줄인 AES, IDEA가 3DES보다 최대 26.7% 효율적이다.

비대칭키 암호화 알고리즘의 성능은 매우 좋지 않은 것으로 나타났다. 키의 길이만큼이나 연산 시간도 길기 때문에 하나의 요청을 처리하는 데에도 수 초에서 수 십 초나 걸렸으며, 이러한 지연은 웹 서버 시스템의 성능 저하를 초래했다. 2048 비트의 키를 사용한 경우는 아예 실험하는 동안 처음 몇 개의 요청을 제외하고는 전혀 처리하지 못하는 현상까지 보여주기도 했다. 따라서 비대칭키 암호화 알고리즘을 단독으로 사용하는 것은 시스템 성능 저하의 결정적인 요인이 된다.

5. 결론 및 향후 연구 과제

본 논문에서는 다양한 암호화 알고리즘이 웹 서버에 얼마나 영향을 미치는가에 대하여 조사하였다. 이를 위하여 웹 서버 시스템에 여러 가지 암호화 알고리즘을 구현하여 웹 서버에 미치는 영향을 측정하였으며, 그 결과 비대칭키 암호화 알고리즘 보다는 대칭키 알고리즘이 훨씬 좋은 성능을 보이며, 대칭키 알고리즘 중에서는 차세대 암호화 알고리즘인 AES가 가장 좋은 성능을 보여주는 것을 확인할 수 있었다.

하지만 암호화 프로세스 자체가 많은 시스템의 자원을 사용하기때문에 암호화를 하지 않는 일반 웹 서버 시스템에 비하여 4.5배 정도의 성능저하를 보여주었다. 따라서 앞으로 이와 관련하여 암호화 프로세스와 웹 서버/클라이언트 간의 효율적인 정보 교환을 위한 연구가 진행되어 암호화로 인한 웹 서버 시스템의 성능 저하를 최소화하는 노력이 필요하다.

참고 문헌

[1] 한국인터넷정보센터, "인터넷통계 월보", 정보통신부, 2004

[2] William Stallings, "Cryptography and Network Security, Third Ed," Pearson Education, 2003

[3] Microsoft Corporation, "Microsoft Internet Information Server Security Overview," 1999

[4] The Apache Group, Apache http Server Project, http://www.apache.org.

[5] Netcraft Web Server Survey, "http://www.netcraft.com/survey"

[6] Mindcraft, Inc., "WebStone—the Benchmark for Web Servers," http://www.mindcraft.com/webstone.