전달 계층의 보안 암호화 알고리즘 개선

Improvement of Security Cryptography Algorithm in Transport Layer

최승권, 김송영, 신동화*, 이병록, 조용환
충북대학교, (주)아이온커뮤니케이션즈*

Choi Seung-Kwon, Kim Song-Young, Shin Dong-Hwa*,
Lee Byong-Rok, Cho Yong-Hwan
Chungbuk National Univ.,
I-On Communications Corp.*

요약

본 논문에서는 MSSL에서 사용되는 전달 계층에서의 암호화 알고리즘을 개선하였는데 보다 높은 효율성을 보장하기위해 기존의 SEED 알고리즘에서 G-함수를 개선한 ISEED (Improved SEED) 알고리즘을 제안하였다. 이를 위해 라운드키 생성과정에서 가장 많은 시간이 소요되는 라운드키 값을 계산할 때 라운드 함수의 구현에서 사용된 모듈만으로 서브키를 생성할 수 있도록 알고리즘을 구현하였다. 또한 키생성 알고리즘에서 암·복호화 과정에서 필요로 하는 암호키를 서브키의 형태로 변환하는 과정에서 ISEED 알고리즘에서는 이 변환 알고리즘을 분석하고 서브키 간의 규칙성을 이용, 차분분석에 필요한 평문의 개수를 최소화함으로써 암·복호화에 소요되는 시간을 줄였다. ISEED를 기존의 알고리즘과 라운드키 생성 시간, 라운드 증가에 따른 키 생성시간과 암호화 및 복호화의 평균 수행속도를 측정하여 비교 분석하여 개선되었음을 증명하였다.

Abstract

As Internet grows rapidly and next electronic commerce applications increase, the security is getting more important. Information security to provide secure and reliable information transfer is based on cryptography technique. The proposed ISEED(Improved SEED) algorithm based on block cryptography algorithm which belongs to secret-key algorithm. In terms of efficienty, the round key generation algorithm has been proposed to reduces the time required in encryption and decryption. The algorithm has been implemented as follow. 128-bit key is divided into two 64-bit group to rotate each of them 8-bit on the left side and right side, and then basic arithmetic operation and G function have been applied to 4-word outputs. In the process of converting encryption key which is required in decryption and encryption of key generation algorithm into sub key type, the conversion algorithm is analyzed. As a result, the time consumed to encryption and decryption is reduced by minimizing the number of plain text required differential analysis.

I. 서 론

정보보호란 안전하고 신뢰성 있게 정보를 전달할 수 있도록 하는 것으로 암호 기술에 기반을 둔다. 이러한 정보보호 서비스를 제공하기 위하여 암호 시스템을 이용한다. 암호 시스템의 안전성은 많은 환경-

암호 알고리즘/프로토콜, 난수 생성기, 구현방법, 암호 시스템의 물리적인 보호, 네트워크 사이의 보호, 시스템관리, 사용자 관리 등등-에 의존하며, 어느 한 부분이 더 중요하고 덜 중요하다고 말하기 어렵다. 즉, 안전한 암호 시스템을 구축하기 위해서는 모든 환경들의 서로 유기적인 조화가 필요하다. 특히, 인터넷의 발달로 네트워크에서의 보안에 대한 인식이 높아지고 있다.

SSL(Secure Socket Layer)은 클라이언트/서버 네트워크 환경에서 종단 간 트랜잭션의 보호를 위하여 정보보호 서비스를 제공하는 프로토콜이다. 이 프로토콜은 클라이언트와 서버 사이에 교환되는 데이터에 기밀성을 제공하기 위하여 암호 알고리즘을 이용한다. 이러한 SSL 프로토콜의 사용은 키 길이의 제한으로 안전성을 보장하기에는 미흡한 실정이다[1]. 이를 해결하기위해 전 세계는 자체적인 암호 알고리즘 개발에 힘쓰고 있고 국내에서도 SEED 암호 알고리즘 연구가 진행되었다.

본 논문에서는 MSSL에서 사용되는 전달 계층에서의 암호화 알고리즘을 제안하고자 한다. 효율성을 보장하기위해 기존의 SEED 알고리즘에서 G-함수를 개선한 ISEED(Improved SEED) 알고리즘을 제안한다.

효율성의 개선을 위해 라운드키 생성과정에서 가장 많은 시간이 소요되는 라운드키 값을 계산할 때 B||A, D||C의 회전이동과 덧셈과 뺄셈을 각 1회만 수행하고 나면, 라운드 함수의 구현에서 사용된 모듈만으로 서브키를 생성할 수 있도록 알고리즘을 구현하고자 한다. 또한 키 생성 알고리즘에서 암·복호화 과정에서 필요로 하는 암호키를 서브키의 형태로 변환하는 과정에서 ISEED 알고리즘에서는 이 변환 알고리즘을 분석하고 서브키 간의 규칙성을 이용, 차분분석에 필요한 평문의 개수를 최소화함으로써 암·복호화에 소요되는 시간을 줄이고자 한다.

Ⅱ. 전달계층의 암호화 알고리즘

인터넷상에서 보안 서비스를 제공하는 프로토콜은 기존의 HTTP 프로토콜에 보안 서비스를 제공하는 SHTTP(Secure Hypertext Transfer Protocol), 응용 계층과 TCP 계층 사이에 SSL, 그리고 IP 프로토콜 수준에서 보안 서비스를 제공하는 새로운 프로토콜 IPsec(IP Security) 등이 있다. 그러나, SHTTP 프로토콜은 여러 응용 계층의 서비스 중에 HTTP 프로토콜에만 보안 서비스를 제공한다는 단점이 있으며, IPsec은 구현의 복잡성과 비용의 문제로 현재까지 발전 단계에 있다. 이러한 점에서 볼 때, SSL 프로토콜은 현재 인터넷을 이용하는 전자거래 응용에 가장 많이 쓰이고 있는 보안 프로토콜이다. SSL프로토콜은 TCP와 HTTP, NNTP, FTP 등과 같은 응용계층 사이에 위치하는 프로토콜이며 기존의 프로토콜에 대한 영향을 최소화할 수 있어 다양한 응용계층의 프로그램들이 SSL을 이용하여 보안기능을 수행할 수 있게 된다. 하지만, SSL은 웹 보안에 기초한 프로토콜이므로 TCP 상에서만 동작하는 프로토콜이다[2][3][4].

SSL은 모든 메시지를 캡슐화하기 위해, 레코드 계층 프로토콜을 사용한다. 레코드 계층은 Alert, ChangeCipherSpec, Handshake, ApplicationD-

ata 프로토콜 메시지를 프레임으로 만들기 위한 일반적인 형식을 제공한다.

레코드 계층의 헤더는 5바이트로 구성되며, 상위 프로토콜 메시지들과 메시지 무 결성 서비스를 제공하기 위해 메시지 인증 코드(MAC: Massage Authentication Code)가 첨부된다. 또한 암호 서비스가 진행 중 이라면 레코드 계층은 암호화의 의무도 가지고 있다[5][6][7].

SSL 명세서는 레코드 계층이 캡슐화 할 수 있는, 서로 다른 4개의 상위 계층 프로토콜을 정의하고 있다. 특정 메시지에 대해, 프로토콜 필드는 지정된 상위 계층 프로토콜의 유형을 기술한다.

각각의 프로토콜에 의한 통신 방법은 먼저 클라이

언트가 Handshake 프로토콜을 이용하여 안전한 통신을 서버에게 요청을 하면서 필요한 파라미터들을 서버에게 제안한다. 서버는 클라이언트의 요청에 응답하여 통신에 필요한 파라미터들을 설정한다. Handshake 프로토콜에 의해 설정된 파라미터들은 ChangeCipherSpec 프로토콜에 의해 사용할 수 있도록 활성화되며, ApplicationData 프로토콜에 의해 데이터가 전송된다. 또한, 통신과정에서 발생한 오류는 Alert 프로토콜을 이용하여 처리된다. 각 프로토콜의 모든 메시지는 레코드 계층을 통하여 캡슐화함으로써 통신이 완료된다.

Ⅲ. 라운드키 생성시간의 단축을 통한 효율성 개선

SEED의 효율성을 개선하는 방법으로는 라운드 함수의 횟수를 줄이는 것이 가장 효과적일 것이다. 하지만 이는 암·복호화 하는 시간이 덜 걸리겠지만 안전성은 떨어뜨리게 된다. 본 논문에서는 라운드키 생성시간을 단축할 수 있도록 개선된 키 생성 알고리즘을 구현하고자 한다. 개선된 SEED의 키 생성 알고리즘은 128비트의 암호키를 64비트씩 좌우로 나누어 이들을 교대로 8비트씩 좌/우로 회전이동한 후, 결과의 4워드들에 대한 간단한 산술연산과 G 함수를 적용하여 암호화나 복호화시 암호키로부터 필요한 라운드 키를 간단히 계산할 수 있도록 구현하였다.

각 라운드에 사용되는 라운드 키는 다음과 같은 생성된다.

단계 1 : 128비트 입력키를 32비트씩 4개의 조각으로 쪼갠 후(A, B, C, D),

단계 2 : = G(A+C-KC0) ; = G(B+KC0-D) (단, KC0 : 라운드상수)로 1라운드 키를 생성하고,

단계 3 : B|| A=(B|| A)>>8 8비트 오른쪽으로 순환 이동 연산

단계 4 : = G(A+C-KC1) ; = G(B+KC1-D) (단, KC1 : 라운드상수)로 2라운드 키를 생성하고,

단계 5 : D|| C=(D|| C)<<8 8비트 왼쪽으로 순환 이동 연산

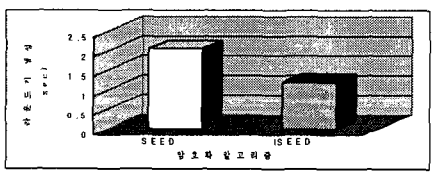
단계 6 : = G(A+C-KC2) ; = G(B+KC2-D) (단, KC2 : 라운드상수)로 3라운드 키를 생성하고,

단계 7 : 계속해서 16라운드 키를 생성할 때까지 반복한다.

IV. 실험 및 성능분석

분석하고자 라운드키 생성 시간, 라운드 증가에 따른 키 생성시간과 암호화 및 복호화의 평균 수행속도를 측정하여 비교 분석하였다.

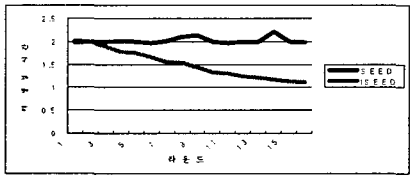
각 알고리즘에 대하여 100,000개의 라운드키를 임의로 생성하여 평균값을 측정하였으며 암호화와 복호화는 128비트 블럭 100,000개를 생성하여 평균값을 구하였다.



▶▶ 그림 1. 알고리즘의 라운드키 생성시간

그림 1은 블록 암호 알고리즘의 라운드키 생성시간을 기존의 SEED 알고리즘과 비교한 것이다. 본 결과를 통하여 ISEED 알고리즘의 속도가 기존 알고리즘보다 약 0.86 μsec의 라운드키 생성시간을 단축된 것을 알 수 있다. 이는 라운드키 생성과정에서 가장 많은 시간이 소요되는 라운드키 값을 계산할 때 B||A, D||C의 회전이동과 덧셈과 뺄셈을 각 1회만 수행하고 나면, 라운드 함수의 구현에서 사용된 모듈만으로

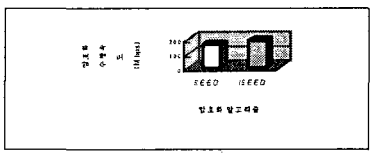
서브키를 생성할 수 있도록 설계하여 라운드 키 상수의 생성이나 라운드별 서브키 생성방법이 매 라운드마다 동일하므로 라운드가 증가할 때마다 키 생성 시간을 단축시켰기 때문이다. 그림 2는 라운드 증가에 따른 키 생성 시간을 보여주고 있다.



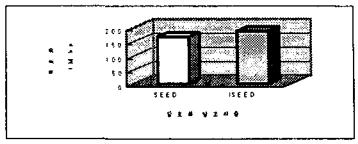
▶▶ 그림 2. 라운드 증가에 따른 키 생성시간

그림 3과 그림 4는 암호화와 복호화 성능을 비교한 것이다. 암호화와 복호화에 걸리는 시간은 별 차이가 없으며 라운드 키 생성 시간의 단축으로 ISEED 알고리즘이 기존의 SEED 알고리즘 보다 암호화와 복호화 수행속도가 약 28Mbps 정도 향상되었음을 알 수 있었다. 이것은 키생성 알고리즘에서 암·복호화 과정에서 필요로 하는 암호키를 서브키의 형태로 변환하는 과정에서 ISEED 알고리즘에서는 이 변환 알고리즘을 분석하고 서브키 간의 규칙성을 이용, 차분분석에 필요한 평문의 개수를 최소화함으로써 암·복호화에 소요되는 시간을 줄였기 때문이다.

하지만 앞서 라운드 키 생성 시간을 기존의 SEED 알고리즘 보다 많이 개선되었음에도 불구하고 암·복호화의 성능이 그에 비해 저조한 결과로 나타난 것은 안전성의 개선을 위해 적용된 논리합과 비트-치환 연산이 알고리즘의 복잡도를 증가시켜 효율성의 저하를 발생시켰던 것으로 분석되어 진다.



▶▶ 그림 3. 암호화 성능 비교



▶▶ 그림 4. 복호화 성능 비교

V. 결 론

본 논문에서는 차분 공격과 선형 공격에 대한 안전성을 증명하였다. 하지만 블럭암호의 안전성의 문제는 차분 공격과 선형 공격에 대한 증명만으로는 충분하지 않다. 왜냐하면 블럭암호의 구조는 차분 및 선형 공격이 아닌 다른 공격에 더 취약할 수 있기 때문이다. 따라서 ISEED 알고리즘에 대한 엄밀한 안전성의 평가를 위해서는 다양한 공격에 대한 분석이 필요하며 또한 안전성의 개선을 위해 적용된 논리합과 비트-치환 연산이 알고리즘의 복잡도를 증가시켜 효율성의 저하를 발생시켰던 것으로 분석되어 추후 안정성을 강화하면서 효율성의 저하를 최대한 줄일 수 있는 최적의 암호 구조를 찾아내는데 더 많은 연구가 이루어져야 한다.

본 논문에서 제안한 ISEED 알고리즘을 통하여 향후 현대 정보사회 진입의 커다란 이슈로 부각되고 있는 정보보호 서비스를 제공함에 있어 안전성과 효율성에 기여할 것으로 기대된다.

▌참 고 문 헌▐

[1] W. Stallings, "Network and Internetwork Security, Principles and Practice", IEEE Press, 2001.

[2] J. Bruke, J. McDonald, T. Austin, "Architectural Support for Fast Symmetric-key Cryptography", pp.335-339. ASPLOS, 2000.

[3] A. Freier, P .Karlton, and P. Kocher, "The SSL Protocol Version 3.0", Netscape Corporation, March 4 1996, http://www.netscape.com/eng/ssl

[4] S. Thomas, "SSL and TLS Essentials : Securing the Web", John Wiley & Sons, 2000.

[5] SEED Algorithm and Specifications, Available at the KISA's web page, http://www.kisa.or.kr/seed/index.html

[6] E. Biham, A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems,"

[7] B. V. Rampay, L. R. Knudsen, V. Rijmen, "Differential Cryptanalysis of the ICE Encryption Algorithm, " in Fast Software Encryption - 5th International Workshop, FSE'98, Vol.1372 of Lecture Notes in Computer Science, pp.270-283, Springer-Verlag, 1998.