MD5와 Crypt를 이용한 안전한 웹 인증 시스템의 설계 및 구현

윤 현 경, 김 완 경, 소 우 영
한남 대학교 컴퓨터공학과

Design and Implementation of Reliable Web Authentication System Using MD5 and Crypt

Hyun-Kyoung Yoon, Wan-Kyung Kim, Woo-Young Soh
Dept. of Computer Engineering, HanNam University

요 약

현재 구축되고 있는 대부분의 업무용 시스템은 C/S 환경에서 벗어나 인터넷이라는 매체를 통해 하나의 웹 정보시스템으로 구축되어지고 있고 이를 업무시스템으로 활용하고 있다. 하지만 웹을 통한 정보 제공은 다수의 사용자에게 노출되어 있는 상태이며 여러 가지 보안 위험에 노출되어있는 것이 사실이다. 특히 Web시스템 초기 인증부분은 사용자의 ID 와 Password가 평문 이나 다름없는 단순인코딩 상태로 노출되는 문제점이 있다. 본 논문에서는 이러한 업무시스템의 불안전한 인증 시스템을 보완하고자 MD5 와 Crypt 함수에 기반 한 인증시스템의 구축을 위하여 웹 인증 메커니즘을 제안하고, 실제 인증 시스템에 적용하여 구현하였다.

1. 서론

인터넷이 사회 전반에 걸쳐 보편화 되어 감에 따라 학술, 연구용의 범위를 벗어나 이제는 기업에서부터 일반 사용자들이 인터넷을 활용하여 업무 및 학습, 상거래 등 전분야에 걸쳐 사용되어 지고 있다. 특히 기업에서는 기존의 C/S 시스템 구조에서 탈피하여 하나의 Web 정보시스템을 구축하여 업무시스템으로 사용하고 있으며, 신규로 구축 또는 개선되는 모든 업무용 시스템들이 Web 정보시스템으로의 변화를 꾀 하고 있다. 하지만 웹을 통한 정보 제공은 외부의 다수의 사용자에게 노출되어 있는 상태이며 서버에 접근하려는 클라이언트는 익명으로 접근하며 서버 측에서는 접근한 사용자를 확인할 길이 없다. 웹과 관련된 모든 기술적인 사항이 공개되어 있다. 그러므로 정보 제공용 웹 서버는 여러 가지 보안 위험에 노출되어 있다[1].

기존의 구축되어진 Web정보시스템 및 현재 구축이 진행 중이거나 계획하고 있는 모든 시스템들 역시 방화벽 등으로 외부와 단절되어 있다는 안일한 생각에 내부 보안문제에 대해서는 소홀하게 대비를 하고 있으며 시스템 관리자들 역시 방화벽 안쪽 그

본 연구는 과학기술부 지역협력연구사업
(R12-2003-004-01002-0) 지원으로 수행되었음

룹에 대해서는 통상적인 백업 외에는 아무런 대비도 하지 않고 있다.

또한 이 모든 시스템들이 정작 사용자가 최초 로그인 하는 시점에 대해서는 모두 별다른 대비책을 갖추고 있지 않고 있다. 말 그대로 사용자의 아이디와 암호가 그대로 네트웍 및 제 3자에게 노출이 되고 있다는 것이다. 몇몇 사이트 들은 사용자의 암호를 암호화 하여 데이터 베이스에 저장해 놓는 사이트 들도 있다. 하지만 이미 아이디 와 암호가 Text로 Open 된 상태에서는 아무런 효과를 거두지 못할 것이다.

본 논문에서는 기존의 인증 시스템에 약간의 암호알고리즘을 적용함으로써 가볍고 차별화 된 Web인증시스템의 구축을 목적으로 사용자 인증 시 안전하게 보호 되고 Web정보시스템으로의 효율적인 암호 전송 방법을 제안한다. 본 연구에서 구축하게 될 인증 시스템은 기존의 Web정보 시스템과의 호환성을 유지하면서 현재의 인증방법에서 문제점으로 노출되고 있는 암호 Text 전송방법 및 저장/유지 방법을 구현한다. 따라서 본 논문에서는 Web정보시스템에서 전송되는 Text 암호를 MD5로 암호화 하고 이를 서버에 전달하며 서버에서는 전달 받은 암호문에 대해 Crypt를 이용하여 변환 데이터베이스 저장 및 인증할 수 있도록 시스템을 설계 구현한다.

2. 관련연구

2.1 해쉬 알고리즘[2]

해쉬 함수(H 혹은 Hash로 표기)는 임의의 길이의 입력 메세지를 고정된 길이의 출력 값으로 압축시키는 함수이다. 데이타의 무결성 검증, 메세지 인증에 사용한다. 해쉬 함수는 다음의 성질을 만족해야 한다.

일방향성 : 주어진 해쉬값 h에 대해서 **H(x) = h**를 만족하는 x를 찾는 것 이 계산적으로 불가능

강한 충돌 회피성 : 주어진 x에 대해 **H(x) = H(y)**를 만족하는 임의의 입력 메시지 y(≠x)를 찾는 것이 계산적으로 불가능

(표 1) 해쉬 알고리즘

알고리즘	출력길이	블럭의 크기	라운드 수	Endianness
MD5	128	512	64	Little
SHA1	160	512	80	Big
SHA256	256	512	64	Big
SHA384	384	1024	80	Big
SHA512	512	1024	80	Big
RMD128	128	512	128	Little
RMD160	160	512	160	Little
RMD256	256	512	128	Little
RMD320	320	512	160	Little
HAS160	160	512	80	Little
TIGER	192	512	56	Little

일반적으로 널리 쓰이는 해쉬 함수로는 MD5, SHA1, RMD160, TIGER 등이 있다. 이중 MD5 는 메시지 다이제스트 계열에서 가장 잘 알려진 128비트의 해쉬 결과를 나타내며, 해쉬 알고리즘 중 연산속도가 가장 빠르기 때문에 가장 널리 사용된다. 그러나 컴퓨터가 발전하면서 과거의 알고리즘들이 점차 풀리고 있다. MD4의 경우는 이젠 아주 간단하게 원본 메시지 값을 알아낼 수 있게 되었고, MD5도 펜티엄 급 컴퓨터에서 연립방정식을 이용하여 충분한 시간만 주어진다면 인위적으로 풀어 낼 수 있다는 것을 알고 있다. 또한, 인위적이 아니더라도 비밀번호와 같은 8자리 정도의 숫자를 해쉬 한 값들은 이미 단순한 반복대입에 의해 어느 정도 우력화되어 있다. 하지만 아직까지도 이러한 암호문을 해독하는 데는 엄청난 비용과 시간이 소요된다. 대소문자 52자, 특수문자 30자 정도가 대부분의 시스템이 사용하고 있는 비밀번호 집합이며, 2,044,140,858,654,976 가 총 조합 가능한 양이다. 이 숫자의 절반이 기대 값이므로, 만약 초당 1백만번 MD5 연산이 가능하다면 단순히

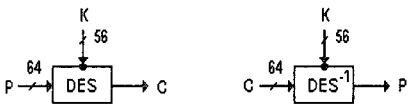
대입해서라도 8개월 내에 웬만한 비밀번호는 나오는 셈이다. 테라플롭스급의 수퍼컴퓨터를 사용하면 1-2년 내에 메시지 다이제스트 계열은 무력화된다고 볼 수 있으며, 더구나, 가능성이 높은 비밀번호 위주로 추측한다면 이보다 훨씬 짧은 시간 내에 알고리즘을 깰 수 있는 방법은 엄청나게 많다. 물론 이러한 여러 결함에 훨씬 더 견고하게 설계된 SHA 알고리즘이 있으나 본 연구에서는 MD5를 사용하여 Client Side 암호함수를 구현하고 적용해 보도록 하겠다.

2.2 DES 알고리즘[2]

DES는 IBM의 Water Tuchman과 Carl Meyer가 만든 암호학 알고리즘으로 NBS(National Bureau of Standard, NIST-National Institute of Standards and Technology의 전신)에서 미 연방표준 암호학 알고리즘으로 공모된 것이다. 안전성에 대한 평가를 거친 후에 1977년 1월 FIPS(Federal Information Procession Standard) Publication No.46으로 표준화되어 현재까지도 널리 사용되고 있다.

DES는 블록 단위로 계산되는 암호화 알고리즘이다. 따라서, 이런 종류의 알고리즘을 불록 암호화 라고도 한다. 입력 값은 64비트씩 잘려진 블록이며 암호화된 결과 역시 64비트 블록으로 나타난다. 사용되는 키는 56비트와 8비트 패리티로 구성된 64비트블록으로 구성되며, 56비트의 확률(약 7.2E16)의 키를 구성하고 있기 때문에 키를 유추하는 것이 쉽지 않다.

P:평문, K:키, C:암호문



[그림 1] DES 알고리즘

본 논문에서는 DES를 기본 알고리즘으로 채택하여 구현되어 있는 crypt() 라는 libcrypt 함수를 JAVA Bean으로 구현하고 최종적인 해쉬암호Text를 암호화하여 데이터 베이스에 저장하는데 사용한다.

3. MD5&Crypt를 이용한 안전한 웹 인증 시스템

3.1 설계

3.2 MD5를 이용한 Web 로그인 암호화

본 연구에서 구축하고자 하는 Web인증 시스템은 기존의 Web정보시스템과 호환성을 가지도록 설계되었으며, 기존 Web인증시스템과 차별화 된 기능을 지원하기 위해 MD5 알고리즘을 자바 스크립트로 작성하여 Client Side Function 인 자바스크립트의 효율성을 활용 함으로써 서버에 부하를 주지 않고 안전하게 사용자가 입력한 로그인 정보를 서버까지 전달할 수 있도록 하였다. 또한 중간에 전송문자열에 대한 Sniffing으로 사용자 인증정보를 도용하는 것을 막기 위해 서버에서는 입력 받은 해쉬 암호를 Crypt 함수를 이용해 다시 한번 암호화 하여 데이터 베이스에 저장하게 된다. 이때 Crypt 함수에 적용되는 Key 값은 Web정보시스템을 사용하는 사용자의 IP 또는 구별되는 특정 값을 가져와 적용함으로써 원격지 또는 다른 컴퓨터의 인증도용을 막을 수도 있다.

Client 로그인 정보 암호화 자바스크립트 소스:

document.frm.pswd.value

calcMD5(document.frm.pswd.value);

document.frm.submit();

암호문 변화 :

평문 : **eas718**

MD5(eas718) : **56ff23eb22a26483b70a53dd1a8e33f1 (해쉬암호문)**

Server 로그인 정보 암호화 Java 소스:

EncPwd = crypt.crypt(Salt,pwd);

암호문 변화 :

Crypt(56,56ff23eb22a26483b70a53dd1a8e33f1)

56Jh9K3fKHorc (Crypt 한 최종 암호문)

4. 구현 및 고찰

본 시스템은 Windows 환경에서 MD5 해쉬 알고리즘을 자바스크립트로 구현 하여 Client Side 암호화 모듈을 생성하였으며 DES 의 대표적인 Crypt 함수를 Java Class 함수로 구현하여 Client 에는 MD5 자바스크립트로 서버에는 Class Bean 을 사용하여 구현하였다. 물론 웹 인증에 대해 SSL 이나 커버로스, 타임스탬프 등 많은 방법이 있다. 하지만 이들은 별도의 서버구성 과 네트워크 성능을 급격히 떨어뜨리는 단점, 운영상의 비용 및 유지보수의 어려움 그리고 타 시스템과의 연동문제 등으로 일반적인 Web정보시스템에서는 많이 외면당하는 것이 사실이다. 하지만 본 논문에서 제시한 시스템은 특별한 비용 없이 누구나 쉽게 구축할 수 있으며 값의 변화 및 시스템별로 지원하는 암호 알고리즘의 응용으로 얼마든지 빠르고 안전한 시스템을 구축할 수 있다. 또한 약간의 응용으로 픽스시트온 등 여러 가지 기술에 응용될 수 있으며 향후 시스템의 발전에 따라 쉽게 유지보수/운영될 수 있다.

5. 결론

본 논문에서는 회사 내부 또는 연구실 내부에서 사용하는 행정 또는 업무용 시스템들의 안전한 로그인 및 사용자의 ID/PWD 유출을 막고 시스템의 불법 사용을 차단하며 약간의 유일한 키의 첨가로 픽스시트온 등의 기능을 추가할 수 있도록 설계하였다.
또한 검증하고자 구현한 시스템 역시 이러한 기능을 위하여 해쉬와 DES 알고리즘을 사용한 MD5 와 Crypt 함수를 이용하여 안전한 Web로그인 메커니즘을 설계 및 구현 하였으며 Client Side 언어인 자바스크립트와 서버 사이드 언어인 Java Class를 명확히 구분하여 각각의 동작을 분리하여 구현하였으며 해쉬 와 DES를 이용하여 2단계의 암호화를 적용하였다.

향후 연구계획으로는 RSA 와 해쉬 또는 DES 의 응용으로 사용자가 직접 로그인 하지 않아도 해당 사용자의 전자서명의 전달만으로 시스템을 사용하는 방법을 연구해볼 필요가 있다. 특히 이러한 연구는 앞으로 다가올 개인 인증서 또는 전자서명 시대에 더욱더 필요하게 될 것이며 각 사이트 별로 개인의 정보를 일일이 입력해야 되는 불편함 그리고 개별 인증서의 사용으로 개인정보의 유출을 막아줄 수 있을 것으로 기대된다.

[참고문헌]

[1] "웹 환경 구축 및 운영을 위한 보안 기술 연구", 한국전산원 최종 보고서, 1997. 12.

[2] 소우영 외 3명, "컴퓨터 통신보안", 그린출판.

[3] "IETF RFC 1321", http://www.ietf.org/rfc/rfc1321.txt.