RF 카드 기반 웹보안 시스템 설계 및 구현

이 권 일, *이 종 후
대덕대학, *㈜시큐컴
전화 042-866-0398 / 핸드폰 019-460-6603

Design and Implementation of Web Security System Using RF Card

Kwonil Lee, Jong Whoo Lee
E-mail : kilee@mail.ddc.ac.kr

Abstract

This paper has been designed and implemented of web security system using RF card. A security mechanism that was proposed in this paper provides web services on card reader reads RF card of user only.

In this paper, user authentication and server authentication was provided by challenge/response mechanism. Also, this system was provides confidentiality of communication messages.

I. 서 론

전자 거래 시스템, 기업의 그룹웨어 시스템 등이 웹을 이용하여 구축되고 활용되면서 웹보안 문제가 수면위로 떠오르게 되었다. 웹보안이 제공되지 않은 상태에서의 웹을 이용한 전자 거래나 기업의 결재 시스템 등은 경제적, 정치적 문제를 일으킬 수 있다.

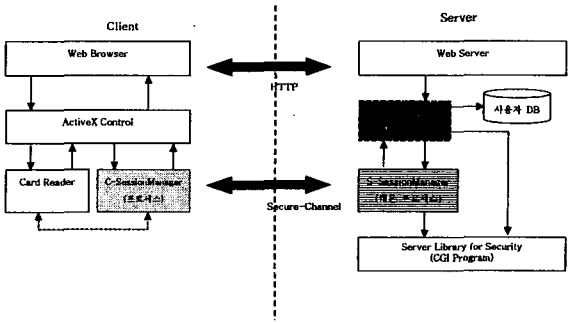
웹보안 역시 다른 네트워크 보안에서와 마찬가지로 인증, 기밀성, 무결성, 부인봉쇄 등의 보안 서비스를 요구한다. 특히 사용자 인증은 웹보안 서비스 중 가장 기본적으로 요구되는 서비스이다. 웹을 통해 전자 거래 또는 기업의 문서 결재 등을 처리할 때 사용자 계정과 패스워드를 입력하는 사용자 인증 방식이 일반적으로 사용된다. 그러나 점차로 개인용 RF 카드나 스마트 카드를 이용한 사용자 인증 방법이 확산되고 있다. 카드를 이용하는 사용자 인증 방법은 사용자 정보의 누출로 인한 사용자 위장에 안전하고, 카드에 저장되어 있는 시드값(seed)을 이용한 일회용 패스워드 방식을 사용하므로 패스워드 누출로 인해 발생하는 위험으로부터 안전하다.

본 논문에서는 RF 카드를 이용하여 웹보안 시스템을 설계하고 구현하였다. 본 논문에서 구현한 보안 기법은 사용자가 카드 리더기에 카드가 접속되어 있는 경우에 한해 웹 서비스를 제공하도록 하였다. 즉 카드 리더기에서 카드를 제거하면 웹 서비스가 중단되도록 설계, 구현하였다. 이는 카드를 인증에만 이용하는 다른 웹보안 시스템과는 차별화 되는 점으로 사용자가 자리를 이탈할 때 별도의 로그아웃 절차 없이 자신의 카드를 가지고 자리를 이탈하면 악의의 사용자가 서비스를 유용하는 것을 방지할 수 있다. 또한 사용자의 총 접속 시간 등을 기록하여 추후 감사에 활용할 수 있다.

II. 시스템 설계 및 구현

본 논문에서 설계 구현한 시스템 구조 및 시스템 동작에 대해 설명한다.

2.1. 시스템 개요



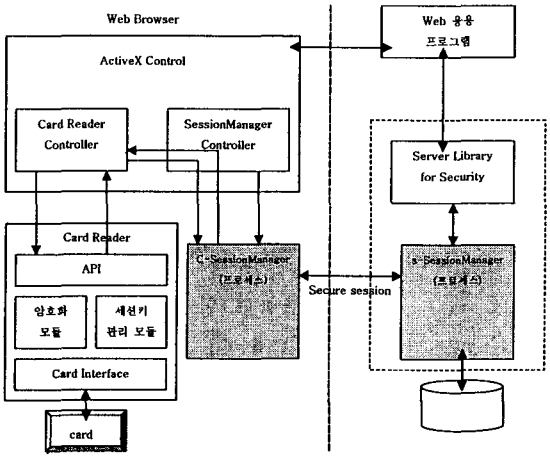
(그림 1) 전체 구성 요소

본 논문에서 설계 구현한 시스템은 사용자 정보가 기록되어 있는 RF 카드를 이용하여 웹 보안을 제공하는 것을 목적으로 하며, RF 카드를 이용하여 사용자 인증을 제공하며, 클라이언트와 웹 서버 사이의 접속 유지를 제공하는 것을 특징으로 하고 있다. 또한 클라이언트와 웹 서버 사이에 전송되는 데이터 암호화 기능도 제공한다. 개발 환경으로 클라이언트쪽은 Windows 운영체제, 서버는 Linux 운영체제를 사용하였다.

본 시스템의 주요 목적은 사용자가 RF 카드를 카드 입력기에 접속한 상태에 한해 클라이언트가 웹 서버의 서비스를 받을 수 있게 하는데 있다. 즉 카드 입력기에서 카드를 제거하면 클라이언트는 더 이상 웹 서버의 서비스를 제공 받을 수 없게 되는 것이다. 웹 서버는 자신에게 접속한 사용자의 접속 시간을 기록하여 추후 사용자가 서버를 사용한 총 시간을 계산할 수 있다.

본 논문에서 설계 구현한 시스템의 전체 구조를 (그림 1)에 나타내었다.

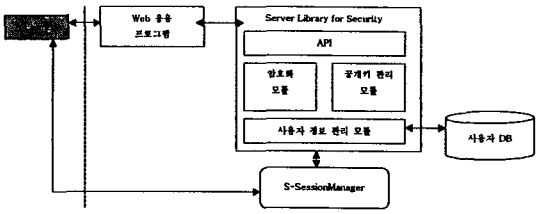
2.2. 클라이언트 구성 요소



(그림 2) 클라이언트 구성 요소

(그림 2)의 구조를 가지는 웹 보안 시스템의 클라이언트 쪽에는 카드의 내용을 읽어 오는 카드 리더 모듈, 서버와의 통신에 필요한 정보를 유지 관리하는 클라이언트쪽 세션 관리자(Session Manager), 클라이언트와 서버 사이의 세션을 초기화/종료하는데 관여하는 ActiveX 컨트롤러로 구성된다.

2.3. 서버 구성 요소



(그림 3) 서버 구성 요소

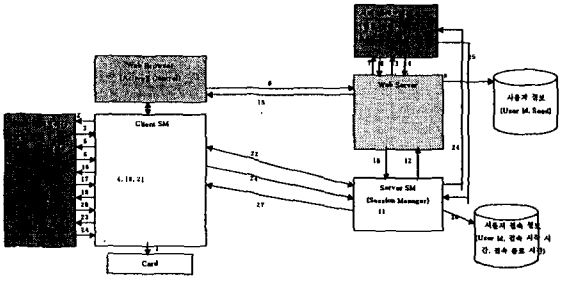
서버쪽에는 사용자 식별자와 시드값(seed)을 저장하고 있는 사용자 데이터베이스, 클라이언트와의 연결(connection)을 유지하고, 클라이언트와의 통신에 필요한 정보를 유지 관리하는 서버쪽 세션 관리자(Session Manager), 웹 서비스를 제공하는 웹 응용 등으로 구성된다. 서버쪽 구성 요소는 (그림 3)에 표현 하였다.

2.4. 시스템 동작

시스템 동작 과정은 크게 시스템의 사용자 인증, 클라이언트의 서버 인증 과정을 거쳐 클라이언트와 서버 사이의 보안 통신을 위한 보안 세션을 설정하는 과정, 설정된 보안 세션을 통해 데이터를 전송하는 과정, 설정된 보안 세션을 종료하는 과정으로 이루어진다.

이 논문의 초점이 RF 카드를 이용한 사용자 인증 및 서버 인증에 관한 것이므로, 본 절에서는 보안 통신을 위해 보안 세션을 설정하는 과정과 세션을 종료하는 과정 위주로 기술하였다.

(1) 세션 설정



(그림 4) 세션 설정 과정

웹 서버와 클라이언트 사이에서 보안이 제공된 상태로 통신을 제공하기 위해서는 우선 웹 서버와 클라이언트인 웹 브라우저 사이에 보안 세션이 설정되어야 한다. (그림 4)는 이 과정을 보여 주고 있다.

세션 설정 과정을 살펴보면 다음과 같다.

우선 1) 사용자 RF 카드에서 사용자 식별자와 시드값(seed)을 가져와 2) 3) 사용자 인증에 필요한 Challenge 값을 계산하여 4) 보관하고 5) 6) 사용자 식별자와 Challenge 정보를 서버의 공개키로 암호화하여 서버에게 전달한다. 7) 8) 9) 서버는 클라이언트가 넘겨준 인증 정보를 확인하고 10) 11) 12) 13) 클라이언트와의 세션 유지에 필요한 세션 식별자를 생성 관리한다. 그리고 클라이언트에게 전달할 14) Response 값을 생성하여 이를 15)클라이언트에게 전달한다. 16) 클라이언트는 서버가 넘겨준 Response 값을 해석하여 정당한 서버인지 서버 인증을 한다. 20) 21) 22) 클라이언트는 서버와의 통신을 위한 세션 키를 생성하고 이를 이용한 세션 컨텍스트를 초기화하여 보관하고 23) 24) 이 정보를 서버쪽에 전달한다. 25) 서버는 클라이언트가 전달한 정보를 가지고 서버쪽 세션 컨텍스트를 초기화하여 저장하고, 26) 현재 로그인한 사용자 정보를 기록한 후 27) 접속을 완료한다.

Challenge/Response 값은 아래와 같다.

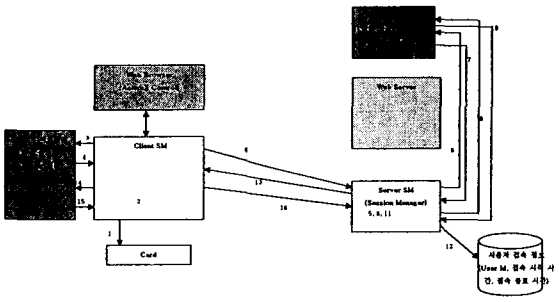
- Challenge: EKseed[Rand(seed)]
  - Kseed : RF 카드에 보관된 사용자 시드값을 해쉬함수로 실행 시킨 결과. 암호키로 사용.
  - Rand(seed) : 사용자 시드값를 시드로하여 난수 생성기를 실행한 결과.
  - EKseed[Rand(seed)] : Kseed를 키로하여 Rand(seed)를 암호화
- *Response* : *EKseed[Session Id, Challenge]*
  - Kseed : 서버에 저장되어 있는 사용자 시드값
  - Challenge : 클라이언트가 보낸

Challenge 값

- Session ID : 서버가 서비스 요청을 초기화한 클라이언트와의 세션 유지에 필요한 세션 구별자.
- EKseed[Session ID, Challenge] : Kseed를 키로하여 세션 식별자와 Challenge를 암호화

(2) 세션 종료

사용자가 카드 리더기에서 자신의 카드를 제거하면 웹 서버와 클라이언트 사이에 설정된 보안 세션을 종료하여 사용자가 더 이상 웹 서비스를 받을 수 없게 하여야 한다. 세션 종료 과정은 (그림 5)와 같다.



(그림 5) 세션 종료 과정

1) 클라이언트쪽 세션 관리자는 카드 리더기에 카드가 존재하는지를 주기적으로 점검한다. 2) 카드 리더기에서 카드가 제거되었음을 탐지한 세션 관리자는 세션 종료 메시지를 생성하고, 3) 4) 이를 암호화하여 서버에게 전달한다. 클라이언트로부터 메시지를 접수한 서버는 5) 6) 7) 클라이언트의 요청을 복호화하여 세션 종료 메시지를 가져온다. 8) 세션 종료 메시지를 확인한 서버는 세션 종료 허용 메시지를 생성하고, 9) 10) 이를 암호화한다. 그리고 11) 클라이언트와의 세션 연결 정보를 삭제하며, 12) 사용자의 사용 시간 등의 사용자 로그를 기록한 후, 13) 암호화된 세션 종료 허용 메시지를 클라이언트에게 보낸다. 14) 15)클라이언트는 서버가 전달한 메시지를 복호화하여 세션 종료 허용 메시지를 접수한 후 서버와 관련된 세션 정보를 삭제한다. 16) 마지막으로 서버는 클라이언트와의 접속을 종료한다.

III. 결 론

웹이 전자 거래, 기업 내 인트라넷 구축 등에 활용되면서 웹보안이 중요한 이슈로 떠오르게 되었다.

본 논문은 사용자 정보가 기록된 RF 카드를 이용하여 웹 보안을 제공하는 시스템에 관한 것이다. 본 논문에서 설계 구현한 시스템은 RF 카드를 이용한 사용자 인증을 제공하며, 클라이언트와 웹 서버 사이의 접속 유지를 제공하는 것을 특징으로 하고 있다. 또한 클라이언트와 웹 서버 사이에 전송되는 데이터 암호화 기능도 제공한다.

본 논문에서 제안 시스템의 특징을 정리하면 아래와 같다.

- 사용자 RF 카드를 이용한 사용자 인증
- Challenge/Response 방식을 이용한 서버 인증
- 연결 기반 (connection oriented) 웹 브라우저/웹 서버 통신 제공
- 사용자 접속 정보 기록

참고 문헌

[1] Rile Kaufman, Radia Perlman, Mike Speciner, Network Security, Prentice Hall, Englewood Cliffs, New Jersey, 1995.

[2] T. Dierks, C. Allen., IETF RFC 2246, The TLS Protocol Version 1.0. January 1999

[3] William Stallings, Network and Internetworking Security, Prentice Hall International, 1995.