5. 그룹웨어에서의 보안을 위한 일회용 패스워드 알고리즘의 설계 및 구현

전자통신공학과 김 영 수
지도교수 임 재 홍

정보화 사회에서 컴퓨터의 역할은 사무자동화의 기능은 물론이고 조직 구성원과 구성원 사이에서 눈에 보이지 않는 대화창구로서의 기능을 수행할 수 있어야 한다.

이러한 기능을 수행하기 위해 연구하고 있는 분야로써 컴퓨터 지원 협동작업(CSCW)이 있으며, CSCW란 사람들의 협동작업을 지원하기 위한 분야로써 이를 실현시키기 위한 소프트웨어를 그룹웨어(group ware)라고 한다.

기업 내에 인트라넷이 도입된 후, 인터넷과 연동되는 인트라넷 그룹웨어를 선호하게 되었으며, 인터넷에서는 보안이 취약하므로 그룹웨어 보안에 대한 대비책이 필요하다.

본 논문에서는 web 기반의 그룹웨어에서 발생할 수 있는 보안의 문제와 보안체계에 대해서 고찰했으며, 그에 대한 개선점으로 일회용 패스워드 알고리즘의 개선방안을 제시하였다.

제안한 알고리즘은 기존의 방식보다는 네트워크 사용을 적게 한다는 장점이 있어서 사용자들의 로그인 시간을 단축시켜 준다. 또한 서버에 접속할 때마다 패스워드가 변경되는 일회용 패스워드를 사용하며, 일회용 패스워드의 갱신은 사용자가 직접 생성하는 것이 아니라 소프트웨어에서 난수를 이용하므로 양질의 패스워드를 생성할 수 있다.

본 알고리즘은 서버에 접속할 때마다 패스워드가 변경되므로 그 자체로서 보안성을 내포하고 있으나, 배타적 논리연산(XOR)을 사용하여 패킷을 암호화하여 전송하는 방식을 취하여 비도(秘度)를 더욱 높였다. 그리고 패스워드를 사용자가 직접 관리하게 되므로, 서버 주도로 이루어져 왔던 기존의 방식에 비해서 서버의 부담을 경감시키는 효과가 있다.

향후 연구·보완되어야 할 사항으로는 첫째 클라이언트의 패스워드 파일을 저장하는 매체에 대한 연구와, 둘째 전송되는 패킷의 포맷이 계정, old-password, new-password의 순서로 전송되고 있으나 이 순서가 무작위로 위치하여 보안성을 더욱 높일 수 있는 방안과 셋째 배타적 논리연산 수행시 제어문자의 발생을 방지할 수 있는 알고리즘의 개선방안이 연구되어야 할 것으로 사료된다.