전자상거래 보안을 위한 SSL 기반의 고객비밀정보보호 프로토콜 설계

권도윤 · 김정호
한발대학교 컴퓨터공학과 통신서비스연구실
wolf21@hananet.net jhkim@hanbat.ac.kr

요 약

전자상거래의 보안을 위해서는 다양한 형태의 정보보호 프로토콜들이 이용될 수 있으나, 현재 가장 널리 사용되고 있는 것은 SSL(Secure Socket Layer)이다. SSL은 Application Layer와 Transport Layer 사이에 위치하는 보안 프로토콜로서 기밀성, 인증, 무결성 등의 보안기능을 제공한다. SSL은 안전한 채널설정을 위해서 Handshake Protocol을 통해 전자상거래 당사자간의 인증작업과 암호알고리즘, 암호키 등의 보안속성을 협상하게 되며, Handshake Protocol에서 설정된 보안속성을 이용하여 Record Protocol이 이후 전송되는 메시지에 대해 기밀성과 무결성을 제공한다. 그러나, 전자상거래 과정에서 요구되는 신용카드정보 및 카드유효기간 등의 고객비밀정보가 특별한 보안절차를 거치지 않고 그대로 전자상점에 전송되게 되므로, 전송도중 또는 전자상점에서 고객비밀정보의 유출 가능성이 존재한다. 전자상점에서는 이러한 고객비밀정보를 이용해 주문내용 및 가격 등의 허위조작 및 이를 도용한 허위거래가 가능하다. 또한, 미국의 수출용 암호 알고리즘에 대한 제한으로 인해 국내에서 사용되는 대부분의 SSL 기반의 전자상거래는 40비트 대칭키 암호를 사용하고 있는데, 이는 쉽게 해독 가능하므로 안전성에 심각한 문제가 있다. 따라서, 전자상거래 과정에서 요구되는 신용카드정보 및 카드유효기간 등의 고객비밀정보를 신뢰할 만한 제 3자(신용기관)의 공개키로 암호화하여 전송함으로써, 전송과정에서의 안전성 강화와 더불어 전자상점에서의 고객비밀정보 유출 및 이를 이용한 허위거래를 방지하여 안전한 전자상거래가 가능하다.