퍼지서명볼트스킴을 이용한 인증 프로토콜

문현이○ · 김애영 · 이상호
이화여자대학교 컴퓨터학과
{hyunyi02, kay}@ewhain.net, shlee@ewha.ac.kr

Authentication Protocol using Fuzzy Signature Vault Scheme

Hyun-Yi Moon○, Ae-Young Kim and Sang-Ho Lee
Dept. of Computer Science and Engineering, Ewha Womans University

1. 서 론

본 논문에서는 사용자의 편의 및 전자상거래의 효율성을 위하여 경량화된 서명의 특징추출기법을 이용하여 퍼지볼트스킴에 기반한 인증 프로토콜을 설계한다. 전자상거래에서 보편적으로 사용되는 서명은 다른 생체정보들에 비해 간편하고 저렴한 아이템 중 하나이다. 따라서 본 논문에서는 서명의 특성에 적합한 특징추출기법으로부터 추출된 서명의 특징을 비밀정보를 정확하게 유도해내는 퍼지볼트스킴에 적용한다. 그리고 이 과정에서 적용된 파라미터들을 활용하여 서명 기반의 효율적인 사용자 인증 프로토콜을 설계한다.

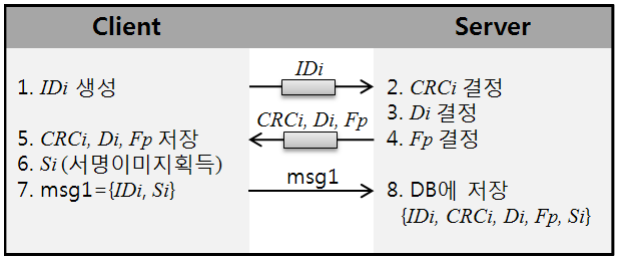
2. 서명기반의 퍼지볼트스킴

서명의 특징점은 획득한 서명 이미지를 이진화·세선화한 후, 서명의 형태에 따른 6가지 분류를 이용하여 특징점을 추출한다. 이 특징점은 서명의 끝점, 꺾어지는 점, 이어지는 선, 갈라지는 부분, 획이 교차한 부분, 단점으로 분류된다[1]. 이 특징점은 Juels와 Sudan에 의해 제안된 방법을 모델로 하는 퍼지볼트스킴에 볼트로 이용하여 비밀키 교환을 위해 암호화·복호화에 사용된다. 퍼지볼트스킴의 안전성은 다항식의 재구성을 위해 필요한 계산량에 기반한다[2].

3. 서명기반 인증프로토콜 설계

퍼지볼트스킴을 이용한 서명기반의 인증프로토콜은 등록단계, 로그인단계, 검증단계로 나눌 수 있다.

등록단계에서는 클라이언트에서 사용자 ID_i를 결정하여 안전한 채널을 통하여 서버로 전송한다. 서버에서는 CRC_i, D_i, F_p 값을 결정하여 안전한 채널을 통하여 클라이언트로 전송한다. 클라이언트에서는 사용자로부터 서명 이미지를 입력 받은 후, 사용자 ID_i와 획득한 서명이미지를 포함하는 msg1을 일반 채널을 통해 서버로 전송한다. msg1을 전송받은 서버는 사용자 ID_i와 위에서 결정한 CRC_i, D_i, F_p 값들과 서명이미지를 데이터베이스에 저장한다. 이 때, 서버의 데이터베이스는 안전한 것으로 가정한다.

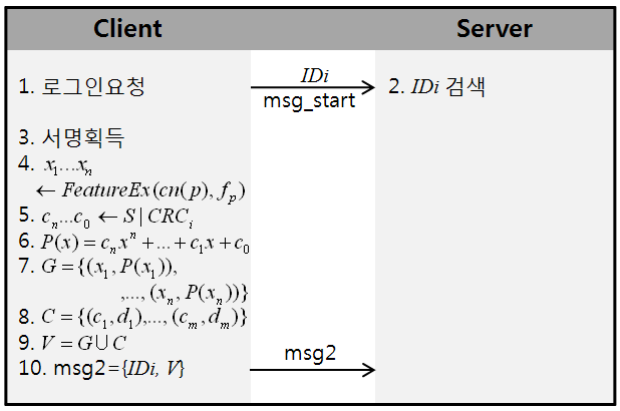


[그림 1] 제안한 인증프로토콜의 등록단계

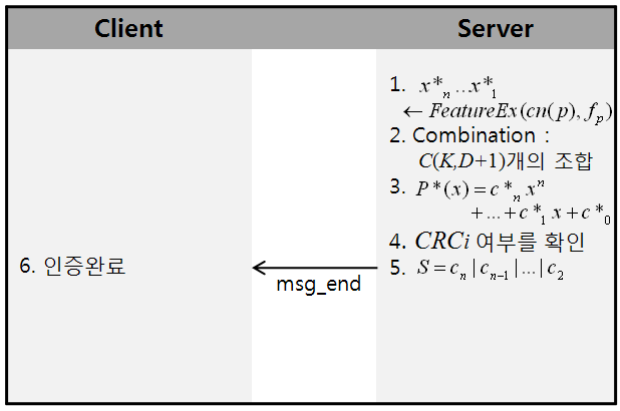
로그인단계에서 클라이언트는 사용자로부터 서명을 획득하고 F_p를 이용하여 획득한 서명이미지로부터 F_p에 해당하는 특징점을 추출한다. 그 다음으로는, 비밀 값 S와 CRC_i를 덧붙인 후 이를 계수로 사용한 다항식 $P(x)$을 만든다. 그리고 추출된 특징점을 x_i로 하여 다항식에 x_i를 대입한 값 $P(x_i)$와의 순서쌍 $(x_i, P(x_i))$의 집합으로 genuine set G를 만든다. Chaff point들의 집합인 chaff set C와 genuine set G의 합집합인 vault set V를 만든 후 사용자의 ID_i와 vault set V를 msg2로 하여 서버로 전송한다.

검증단계에서 서버는 클라이언트로부터 전송받은 ID_i와 vault set V 그리고 서버의 데이터베이스에 저장된 서명이미지 S_i와 특징점 추출을 위한 파라미터 F_p를 이용하여 특징점 $x^*_1 \cdots x^*_n$를 생성하고, 이 특징점과 유사한 D+1개의 점으로 구성된 모든 가능한 조합을 구한다. 이 조합을 이용하여 D차 다항식

$P^*(x)$를 재구성한다. 재구성된 다항식의 계수중에서 1차항과 상수항인 $c^*_1 + c^*_0$ 값을 서버에 저장된 CRC_i와 같은 값인지를 비교·확인한다. 비교 결과가 참인 경우 해당 후보 다항식이 최종 다항식으로 선택되어 각 계수의 합으로부터 비밀 값 S를 찾아내면 인증이 완료된다.



[그림 2] 제안한 인증프로토콜의 로그인단계



[그림 3] 제안한 인증프로토콜의 검증단계

4. 효율성 및 안전성 분석

- 서명 이미지 하나에 대한 특징점추출에 따른 실행빈도수와 수행시간

  이진화의 경우 3r+3과 0.25초, 세선화의 경우 8r+1과 0.56초, 특징점 추출의 경우 r과 0.02초이다. 그리고 퍼지서명볼트스킴의 수행시간은 0.13초이다.

- 비밀 값 S를 알아내기 위한 전수조사를 통한 공격

  CRC_i의 길이를 CRC_LEN, D_i의 차수를 D, F_p의 전체 패턴의 개수를 F_N, 그 중 필요한 특징점의 개수를 n, vault set의 개수를 V라고 할 때, 필요한 전체 계산량은 $2^{CRC_LEN} \times D \times C(F_N, n) \times C(V, D+1)$이다.

- 서명이 노출되었을 때

  서명은 이미 공개된 정보이지만, CRC_i, D_i, F_p 값을 알 수 없으므로 이 세 값을 알지 못하는 경우에는 위와 같은 전수조사를 통한 공격과 동일한 계산량이 필요하다.

- 서명의 특징점이 노출되었을 때

  본 논문에서는 서명의 특징점이 일반 채널 상에서 공개될 수 없도록 서버와 클라이언트 사이에서는 일반 채널을 통해 서명 이미지만을 전송한다. F_p를 사용하여 서버와 클라이언트에서 직접 특징점을 추출하도록 프로토콜이 구성되었기 때문에 특징점이 노출되는 경우는 F_p가 저장된 데이터베이스와 시스템의 보안이 깨졌을 때이다.

5. 결 론

본 논문에서는 간편하고 가벼운 서명의 특징추출기법을 설계하고 이 기법으로 생성된 특징점을 이용한 퍼지볼트스킴을 기반으로 유비쿼터스 상거래에 적합한 사용자 인증 프로토콜을 설계하였다. 이 인증 프로토콜은 기존의 전자상거래 시스템에 간단히 적용하여 더욱 강한 안전성의 확보가 가능함을 실험으로 확인하였다. 또한, 이 프로토콜은 인증과 동시에 별도의 처리 없이 비밀값의 공유가 효율적으로 이루어짐을 확인하였다.

향후 이 인증프로토콜을 유비쿼터스 및 모바일 환경에 적합한 시뮬레이터에 구현하여, 유비쿼터스 상거래 시스템과 같은 서비스에서의 사용자 인증을 실험해 볼 필요가 있다. 또한, 다항식의 차수 D의 결정 및 chaff point들의 집합을 구성시 각 서비스별로 필요한 차수와 chaff point의 개수에 대한 고찰이 필요하다.

참 고 문 헌

[1] 문현이, 김애영, 이상호, "사용자 인증을 위한 서명기반의 경량화된 특징추출기법," 한국정보처리학회 춘계학술발표대회, Vol. 14, pp.1129-1132, 2007.

[2] A. Juels and M. Sudan, "A Fuzzy Vault Scheme," in Proc. IEEE International Symposium on Information Theory, pp.408, 2002.