TTA Standard

정보통신단체표준(국문표준)

TTAK.KO-xx.xxxx 제정일: 2018년 12월 xx일

퍼지 인증 프로토콜 - 제1부: 일반 모델

Fuzzy Authentication Protocol - Part1: General Model

한국정보통신기술협회
Telecommunications Technology Association

표준초안 검토 위원회 **정보보호기반 프로젝트그룹(PG501)**

표준안 심의 위원회 **정보보호 기술위원회(TC5)**

	성명	소 속	직위	위원회 및 직위	표준번호
표준(과제) 제안	황정연	한국전자통신연구원	책임	PG501 위원	
표준 초안 작성자	황정연	한국전자통신연구원	책임	PG501 위원	TTAK.KO-xx.xxxx
	조상래	한국전자통신연구원	PL	PG502 위원	TTAK.KO-xx.xxxx
	김수형	한국전자통신연구원	기술총괄/PL	PG502 의장	TTAK.KO-xx.xxxx
사무국 담당	박수정	TTA	책임	-	

본 표준 발간 이전에 접수된 지식재산권 확약서 정보는 본 표준의 '부록(지식재산권 확약서 정보)'에 명시하고 있으며, 이후 접수된 지식재산권 확약서는 TTA 웹사이트에서 확인할 수 있습니다.
본 표준과 관련하여 접수된 확약서 외의 지식재산권이 존재할 수 있습니다.

발행인 : 한국정보통신기술협회 회장
발행처 : 한국정보통신기술협회
13591, 경기도 성남시 분당구 분당로 47
Tel : 031-724-0114, Fax : 031-724-0109
발행일 : 2018.xx

서 문

1 표준의 목적

본 표준의 목적은 고유 비밀 정보가 유일하게 고정된 형태로 정의되지 않는 퍼지(fuzzy) 정보를 인증키로 이용하여 인증을 수행하는 '퍼지 인증 프로토콜'의 일반 모델을 제시하는 것이다.

2 주요 내용 요약

본 표준은 퍼지 인증 프로토콜의 일반 모델을 제시한다. 퍼지 인증 프로토콜은 사용자가 유일하게 고정된 형태로 정의되지 않는 퍼지 정보(예. 바이오 정보)를 비밀 인증키로 이용하여 인증을 수행할 수 있는 프로토콜이다. 본 표준은 퍼지 인증 프로토콜의 개요, 참여자들, 그리고 일반적인 동작 방식에 대한 설명을 포함한다. 일반적인 동작 방식은 등록과 인증의 두 단계를 구성한다. 등록단계에서 증명자(prover)는 퍼지 정보로부터 생성된 검증키를 검증자(verifier)에 등록한다. 인증단계에서 증명자(prover)는 퍼지 정보로부터 생성된 인증 값을 제공하고 검증자(verifier)는 등록된 검증키를 이용하여 인증 값을 검증하여 증명자(prover)를 인증한다. 검증키로부터는 합리적인 수준의 보안 강도로 본래의 퍼지 정보가 누출되지 않는다고 가정되며, 따라서 검증자(verifier)에게 퍼지 정보가 직접 노출되지 않는다.

3 인용 표준과의 비교

3.1 인용 표준과의 관련성

- 해당사항 없음

3.2 인용 표준과 본 표준의 비교표

- 해당사항 없음

Preface

1 Purpose

The standard specifies a general model of a fuzzy authentication protocol which is capable of using noisy fuzzy data as an authentication factor.

2 Summary

The standard specifies a general model of a fuzzy authentication protocol. In the fuzzy authentication protocol, a client makes use of non-deterministic fuzzy information such as biometrics as an private authentication key. The standard includes overview, participants, and a general procedure. The general procedure consists of two phases, registration and authentication. In the registration phase, a prover registers a verification key, which is generated with fuzzy information, to a verifier. In the authentication phase, the prover provides an authentication value to the verifier and the verifier verifies the authentication value using the registered verification key to authenticate the prover. It is assumed that no useful information for the fuzzy information is revealed (to even the verifier) from the verification key.

3 Relationship to Reference Standards

None

목 차

1 적용 범위 ····· 1

2 인용 표준 ····· 1

3 용어 정의 ····· 1

4 약어 및 기호 ····· 2

5 개요 ····· 3

6 프로토콜 참여자들 ····· 3
6.1 증명자 (Prover) ····· 3
6.2 검증자 (Verifier) ····· 4

7 프로토콜의 보안 고려사항들 ····· 4

8 퍼지 인증 프로토콜 (Fuzzy authentication protocol) ····· 4
8.1 등록 (Registration) ····· 5
8.2 인증 (Authentication) ····· 5

부록 I-1 지식재산권 확약서 정보 ····· 7
I-2 시험인증 관련 사항 ····· 8
I-3 본 표준의 연계(family) 표준 ····· 9
I-4 참고 문헌 ····· 10
I-5 영문표준 해설서 ····· 11
I-6 표준의 이력 ····· 12

퍼지 인증 프로토콜 - 제1부: 일반 모델
(Fuzzy Authentication Protocol - Part1: General Model)

1 적용 범위

본 표준에서 기술하고 있는 퍼지 인증 프로토콜은 증명자(prover)와 검증자(verifier)로 구성된 퍼지 인증 응용 환경을 대상으로 한다. 바이오, 물리적 복제 방지(PUF)와 통신 환경 등의 정보로부터 추출된 노이즈가 있는 비결정형 데이터를 인증키로 이용한다. “비결정형”은 등록 및 인증 과정에서 매 획득 시 마다 개인키가 달라질 수 있음을 의미한다. 본 표준은 퍼지 인증 프로토콜의 일반 모델을 설명한다. 본 표준은 퍼지 인증 프로토콜의 개요, 참여자들, 그리고 일반적인 동작 방식에 대한 설명을 포함한다.

HV-KEM을 이용한 퍼지 인증 프로토콜 [1]과 퍼지 볼트 (Fuzzy Vault) 기반 인증 방법 [2] 등 구체적인 퍼지 인증 프로토콜들에 대한 내용은 제2부를 참조한다.

2 인용 표준

해당 사항 없음.

3 용어 정의

3.1 공개 파라미터 (public parameter)
인증 프로토콜을 수행하는데 이용하며 모든 개체가 접근 가능한 공개 정보

3.2 물리적 복제 방지 (physically unclonable function, PUF) [출처] TTA 정보통신용어사진
직접 회로의 예측 불가능한 지연 성분을 이용한 일종의 난수 발생 장치. 주어진 직접 회로의 지연 성분의 편차는 고르지 않고 이를 측정하는 것도 불가능하기 때문에 보안 측면에서 큰 장점을 가짐

3.3 보안 파라미터 (security parameter)
프로토콜 또는 시스템의 보안 강도를 결정하는 파라미터

3.4 세션 (session)
인증 프로토콜의 결과로 생성되는 클라이언트와 서버 사이의 통신을 위한 논리적 연결

3.5 식별자 (identifier, ID) [출처] TTAR-06.0153 사물인터넷을 위한 객체식별자 적용 지침(기술보고서)

어떤 대상을 유일하게 식별 및 구별할 수 있는 정보. 주소, 전화번호를 포함하여 개체에 결합된 임의의 문자열이 ID로 이용될 수 있음

3.6 엔트로피 (entropy) [출처] TTAK.KO-12.0189 결정론적 난수 발생기 -제1부- 블록 암호 기반 난수 발생기

데이터가 가지는 정보량을 수치적으로 나타낸 것. 무질서도(disorder) 또는 난수성(randomness)을 나타내며 엔트로피가 높을수록 난수에 가까움

3.7 인증 (authentication) [출처] TTAK.KO-12.0002/R3 정보 보호 기술 용어

정보 교환에 의해 실체 식별을 확실하게 하는 방법. 임의정보에 접근할 수 있는 객체의 자격이나 객체의 내용을 검증하는데 사용되는 수단으로 이를 통해 시스템의 부당한 사용이나 정보의 부당한 전송 등을 방어하는데 사용됨

3.8 은닉 벡터 키 캡슐화 기법 (hidden-vector key encapsulation mechanism, HV-KEM)

비밀 벡터 값을 노출시키지 않으면서, 암호학적 목적으로 이용할 비밀키를 암호화(encryption)하고 복호화(decryption)할 수 있는 공개키 기법. 비밀 벡터값이 일치하는 경우에만 암호문으로부터 복호화 가능

3.9 퍼지 데이터 (fuzzy data)

퍼지 인증 프로토콜에서 인증 요소로 이용되는 비결정형(non-deterministic) 데이터

3.10 템플릿 (template) [출처] TTAK.KO-12.0098 One-Time 템플릿 기반의 바이오 인증 프레임워크

사용자의 바이오 인식 데이터로부터 생성된 인증/인식용 정보 및 데이터

3.11 논스 (nonce)

암호 통신 프로토콜에서 재사용 공격 등을 방지하기 위해서 단 한번만 이용되는 임의의 숫자 값. 난수(random number) 또는 의사 난수(pseudo-random number)를 나타냄

3.12 타임스탬프 (time stamp) [출처] TTAK.KO-12.0002/R3 정보 보호 기술 용어

어느 시점에 데이터가 존재했다는 사실을 증명하기 위하여 특정 위치에 표시하는 시각. 공통적으로 참고하는 시각에 대해 시간의 기점을 표시하는 시간 변위 매개 변수

4 약어

FA	Fuzzy Authentication
VK	Verification Key
PKI	Public Key Infrastructure
HV-KEM	Hidden-Vector Key Encapsulation Mechanism

5 개요

본 표준은 퍼지 인증 프로토콜의 일반모델을 제시한다. 인증을 위해서 증명자는 유일하게 고정된 형태로 정의되지 않는 퍼지 정보를 비밀 인증키로 이용한다. 예를 들어, 얼굴, 지문, 홍채와 같은 바이오 정보, PUF(Physical unclonable function)의 출력값, Wi-Fi 신호 세기와 같은 환경 정보, 유사한 특성을 갖는 검색 문장들 등이 퍼지 정보로 이용될 수 있다. 증명자는 이 퍼지 정보로부터 생성된 검증키(Verification Key, VK)를 등록과정에서 검증자에 등록한다. 인증과정에서, 검증자는 이 검증키를 이용하여 증명자가 제공한 인증 값을 검증하여 그 유효성을 확인한다.

본 퍼지 인증 프로토콜은 단일 인증 수단만을 고려한다. 즉, 퍼지 정보 이외에, 퍼지 정보를 은닉하기 위해서 사용자가 별도의 비밀 난수 키를 부가적으로 저장, 관리 및 휴대하도록 요구하지 않는다. 본 표준의 퍼지 인증 프로토콜은 공개키 인증 테크닉과 유사하게, 고유 퍼지 정보로부터 공개 검증키를 생성하고 이를 이용하여 증명자가 제공한 인증 데이터 값을 검증자가 검증한다.

퍼지 인증 프로토콜의 검증키와 프로토콜 수행 시 생성된 값으로부터 일정 보안 강도로 본래의 퍼지 정보가 누출되지 않는다고 가정된다. 따라서 검증자에게 퍼지 정보가 직접 노출되지 않으므로 고유한 퍼지 정보에 대해서 프라이버시가 강화될 수 있다.

퍼지 인증 프로토콜은 다양한 수학적 지식을 이용하여 구성될 수 있다. 구체적인 퍼지 인증 프로토콜은 제2부를 참조한다. 예를 들어, HV-KEM의 구체적인 파라미터들을 이용한 인증 프로토콜[SHKP16] 등이 제시된다.

6 프로토콜 참여자들

본 표준의 프로토콜 참여자들은 크게 증명자(prover)와 검증자(verifier)로 나누어진다. 검증자는 다수의 증명자들의 검증키들을 관리하며 증명자들과 통신할 수 있다. 일방향 인증의 경우, 증명자와 검증자는 클라이언트(client)와 서버(server)에 대응할 수 있다. 이들 참여자는 단편적인 기능에 따라 구분한 것으로, 실제 응용 서비스에서 본 표준이 사용될 경우 이 참여자들이 결합된 형태로 존재할 수 있다. 예를 들어, 실제 응용 서비스에 따라서는 한 명의 참여자가 증명자와 검증자의 역할을 모두 수행할 수 있다. 아래는 각 참여자의 역할에 대한 설명이다.

6.1 증명자 (Prover)

퍼지 인증 포로토콜에 참가하여 자신의 고유 비밀 퍼지정보를 가지고 있음을 증명하는 개체이다. 통상적으로는 인증 프로토콜과 결합된 서비스를 제공받는 주체이다. 인증을 위해 사용될 자신의 ID를 설정한다. 본 표준에서 증명자는 편의상 ID_C로 표시한다. 프로토콜을 이용하기 위해서 프로토콜에 정해진 절차에 따라서 등록과정을 수행하고 자신의 고유 비밀 퍼지정보로부터 생성된 검증키 또는 공개키를 검증자에게 제공한다. 검증자와

퍼지인증 프로토콜을 실행하여 검증자에게 자신에 대한 인증을 수행한다. 필요에 따라서는 미리 정해진 방법에 따라서 검증자를 인증할 수 있다.

6.2 검증자 (Verifier)

퍼지 인증 포로토콜에 참가하여 증명자가 제공하는 퍼지 인증 프로토콜 값을 검증하여 증명자가 고유 비밀 퍼지정보를 가지고 있음을 검증하는 개체이다. 통상적으로는 인증 프로토콜과 결합된 서비스를 제공하는 주체이다. 표준에서 검증자는 편의상 ID_S로 표시한다. 등록과정에서 증명자가 제공한 검증키 또는 공개키를 저장 및 관리한다. 인증과정에서 증명자와 프로토콜을 실행하여 증명자를 인증한다.

양방향 인증을 제공하는 경우, 인증프로토콜에 이용할 개인키를 키 발급 시스템으로부터 발급받는다. PKI 기반 전자 서명 또는 ID기반 서명[Sha84] 알고리듬 등 별도의 인증 메커니즘을 이용하여 자신을 증명자에게 인증할 수 있다.

7 프로토콜의 보안 고려사항

본 표준에서 고려하는 보안 특성들은 다음과 같다.

- 양방향 인증 (mutual authentication)

  퍼지 인증 프로토콜을 수행하는 증명자와 검증자는 서로를 인증한다.

- 단방향 인증 (unilateral authentication)

  증명자는 자신의 고유 퍼지 정보를 이용하여 검증자에게 자신을 인증한다.

- 키 노출에 대한 강인성 (resilience to leakage of a private key)

  고유 퍼지 정보 노출에 강인함을 가져야 한다. 검증자에게 제공된 검증키를 이용하여 증명자를 가장(impersonation)하는 공격을 할 수 없어야 한다.

- 정확성 (correctness)

  퍼지 인증 프로토콜에 참가하는 정당한 참여자들은 올바르게 인증받아야 한다.

8 퍼지인증 프로토콜

본 절에서는 퍼지 인증 프로토콜에 대한 일반적인 동작 방식을 설명한다. HV-KEM을 이용한 퍼지 인증 프로토콜 [SHKP16]과 퍼지 볼트 (Fuzzy Vault) 기반 인증 방법 등 구체적인 파라미터를 이용한 프로토콜들은 제2부를 참조한다.

퍼지 인증 프로토콜은 크게 2가지 단계로 구성된다. 첫 번째는 등록(Registration) 단계이고 두 번째는 인증(Authentication) 단계이다.

증명자는 별도의 하드웨어 또는 알고리즘을 이용하여 노이즈가 있는 비결정형 정보를

획득한 후, 인증 소스로 이용한다. 이 인증 소스를 본 표준에서는 퍼지 데이터라고 부르기로 한다. 퍼지 데이터는 일정한 포맷을 갖는다고 가정한다. 예를 들어, n차원 벡터, 즉, $w=(w_1,...,w_n)$로 표현된다고 가정할 수 있다. 여기서 구성 원소 w_j는 특정한 형태를 갖는다고 가정한다. 예를 들어, 이진수, 십진수, 실수가 될 수 있다. 따라서 퍼지 데이터는 크기 n인 이진열 또는 정수열이 될 수 있다.

퍼지 데이터는 보안 파라미터(security parameter)를 만족하는 충분한 엔트로피를 가지고 있다고 가정한다.

퍼지 데이터를 획득하는 방법은 본 표준의 범위에 속하지 않는다.

8.1 등록 (Registration)

본 절에서는 퍼지 인증 프로토콜의 등록 단계에 대해서 기술한다.

(1) 증명자는 퍼지 데이터를 입력받는다. 그리고 보안 파라미터(security parameter)를 이용하여 공개 파라미터, 공개키 또는 검증 토큰을 생성한다.
(2) 향후 인증 단계에서, 검증에 이용할 수 있도록 증명자는 퍼지 인증에 관련된 공개 파라미터, 검증키(VK) 또는 공개키를 검증자에 등록한다. 이 때 '검증 기준' 또는 '인증 통과 기준'을 위해서 프로토콜에서 허용하는 오차 범위 기준을 등록한다. 전술한 바와 같이, 등록 시에 이용하는 퍼지 데이터는 인증 시에 이용하는 퍼지 데이터와 다를 수 있으므로 검증 기준이 필요하다.
(3) 선택적으로, 검증자는 증명자의 신원 확인을 요구할 수 있다. 또한 필요한 경우, 보안채널을 통하여 증명자와 검증자 사이에 메시지를 송수신할 수 있다.

검증키 또는 공개키는 증명자가 제공하는 퍼지 인증 데이터를 검증하기 위해서 검증자가 사용한다. 바이오 인식에서 템플릿과 유사한 기능을 수행하지만, 증명자의 고유 퍼지 정보가 검증자에게 일정 보안 강도로 노출되지 않음을 암호학적으로 보장할 수 있어, 퍼지 정보의 프라이버시를 제공할 수 있다. 등록된 데이터를 이용하여 인증 단계에서는 증명자와 검증자 사이에 구체적인 퍼지 인증 프로토콜을 통하여 인증을 수행한다.

8.2 인증 (Authentication)

본 절에서는 퍼지 인증 프로토콜의 인증 단계에 대해서 기술한다.

(1) 증명자는 퍼지 데이터를 입력받고 인증을 수행한다. 전술한 바와 같이, 인증 시에 이용하는 퍼지 데이터는 등록 시에 이용하는 퍼지 데이터와 다를 수 있다. 퍼지 데이터를 이용하여 인증 값을 생성하고 검증자와 통신한다.
(2) 검증자는 클라이언트가 등록한 공개 파라미터와 검증키(VK) 또는 공개키를 이용하여 인증을 수행한다. 검증자는 증명자가 제공하는 인증 값을 검증하기 위해서 검증키(VK) 또는 공개키를 이용한다. 검증 기준 또는 인증 통과 기준은 등록 시 정의한 (프로토콜에서 규정하는 허용하는) 오차 범위 내의 기준을 따른다.

(3) 검증자는 필요 시, 자신을 인증하기 위해서 선택적으로 PKI 기반 전자서명과 같은 별도의 인증수단을 이용할 수 있다.
(4) 위의 과정에서 재사용 공격 등을 방지하기 위해서 난수(nonce) 또는 타임스탬프(time stamp) 등을 이용할 수 있다.

상기의 과정은 단일 인증 세션을 설명하고 있으며, 복수의 과정을 수행하여 다중의 인증 세션을 구성할 수 있다.

부 록 I-1

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

지식재산권 확약서 정보

II-1.1 지식재산권 확약서(1)

해당 사항 없음

II-1.2 지식재산권 확약서(2)

해당 사항 없음

※ 상기 기재된 지식재산권 확약서 이외에도 본 표준이 발간된 후 접수된 확약서가 있을 수 있으니, TTA 웹사이트에서 확인하시기 바랍니다.

부 록 I-2

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

시험인증 관련 사항

I-2.1 시험인증 대상 여부

해당 사항 없음

I-2.2 시험표준 제정 현황

해당 사항 없음

부 록 I-3

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

본 표준의 연계(family) 표준

해당 사항 없음

부 록 I-4

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

참고 문헌

[1] 서민혜, 황정연, 김수형, 박종환, “HV-KEM을 이용한 생체 정보 기반 인증 프로토콜”, 한국정보보호학회 논문지, 26권 1호, 2016

[2] A. Juels, M. Sudan, “A Fuzzy Vault Scheme”, Designs, Codes and Cryptography, Vol. 38, Issue 2, pp 237-257, 2006

[3] A. Shamir, “Identity based cryptosystems and signature schemes,” CRYPTO'84, Vol. 196, pp. 47-53, Springer-Verlag, 1984

※ 상기 기재된 참고 문헌의 발간일이 기재된 경우, 해당 표준(문서)의 해당 버전에 대해서만 유효하며, 연도를 표시하지 않은 경우에는 해당 표준(권고)의 최신 버전을 따름

부 록 I-5

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

영문표준 해설서

해당 사항 없음

부 록 I-6

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

표준의 이력

판수	채택일	표준번호	내용	담당 위원회
제1판	2018.12.xx	제정 TTAK.KO-xx.xxxx	-	정보보호기반 (PG501)