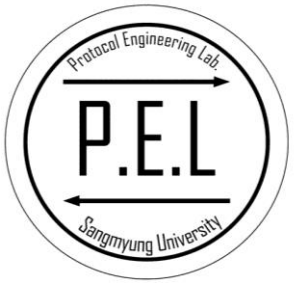


NETWORK SECURITY ESSENTIALS

보충 : 해시 체인(Hash Chain)

Boo-Hyung Lee
(boohyung@pel.smuc.ac.kr)
Protocol **E**ngineering **L**ab., **Sangmyung** University

2015. 01. 20

Content

- 해시 체인(Hash Chain)
- 해시 체인의 응용 : 일회용 패스워드(OTP)

해시 체인(Hash Chain)

- **정의**

  - 수학자 Leslie Lamport가 처음 개발한 기법
  - 랜덤한 seed를 이용하여 연속적으로 해쉬 값을 계산하는 방식을 사용

해시 체인(Hash Chain)

- **계산 과정**

seed는 x이고, 길이가 n(n은 해시 연산 횟수)인 해시 체인을 생성하기 위해서는 다음을 차례로 계산

$$\boldsymbol{C_n = h(x), C_{n-1} = h\big(h(x)\big), \ldots\ldots, C_1 = h^n(x), C_0 = h^{n+1}(x)}$$

- $h^n(x)$는 x를 n번 해시한 값

해시 체인(Hash Chain)

- **특징**

- 실제 사용할 때는 $C_1 = h^n(x)$을 먼저 사용; C_2, C_3 … 순으로 사용

  ex. OTP

- 역연산 불가 : $h^n(x)$를 알고 있어도 $h^{n-1}(x)$는 계산할 수 없음

$$\boldsymbol{h^n(x) = h\left(h^{n-1}(x)\right)}$$

c.f) 해쉬함수의 일방향성 : y = f(x)에서, y를 알 때 x를 계산할 수 없음

응용 : 일회용 비밀번호(OTP)

- **정의**

- 매번 새로운 패스워드를 사용하여 인증을 하는 방식
- 기존의 사용자 아이디/암호를 사용하는 방식보다 안전
- 클라이언트와 서버 간에 대칭키를 공유 : 일회용 패스워드를 생성하기 위함

- **요구사항**

- R1. 이전에 사용된 패스워드로부터 현재 사용할 패스워드를 제3자가 계산하는 것이 계산적으로 어려워야 한다.
- R2. 제시된 OTP 값은 사용자가 쉽게 읽을 수 있어야 하며, 사용자가 화면에 쉽게 입력할 수 있어야 한다.
- R3. 하드웨어적으로 구현이 경제적이어야 한다.

응용 : 일회용 비밀번호(OTP)

- **과정(S/KEY방식; RFC 2289에 정의)**

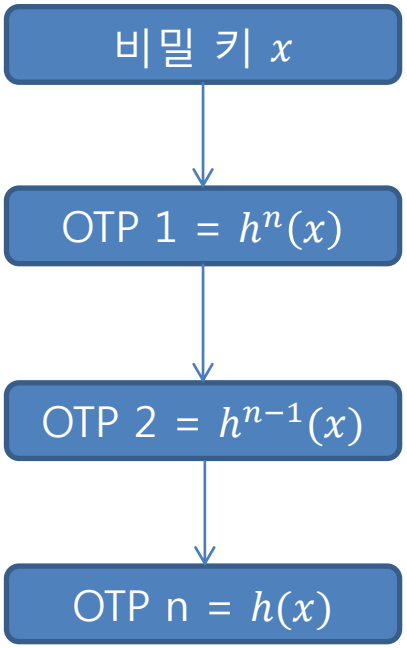
- OTP 생성(x와 n은 클라이언트와 서버가 미리 합의)

1) 클라이언트에서 정한 임의의 비밀 키(x)를 서버로 전송; 전송 후 삭제

2) 서버는 클라이언트로 받은 비밀키를 첫 값으로 사용, 해시 체인 방식으로 이전 결과 값에 대한 해시 값을 구하는 연산을 n번 수행

3) 생성된 n개의 OTP를 서버에 저장

n개의 OTP(비밀키는 x) = $h(x),\ h(h(x)),\ h(h^2(x)),\ \ldots\ldots,h(h^{n-1}(x))$



응용 : 일회용 비밀번호(OTP)

- **과정(S/KEY방식)**

- 인증(i번째로 서버에 인증을 요구할 때)

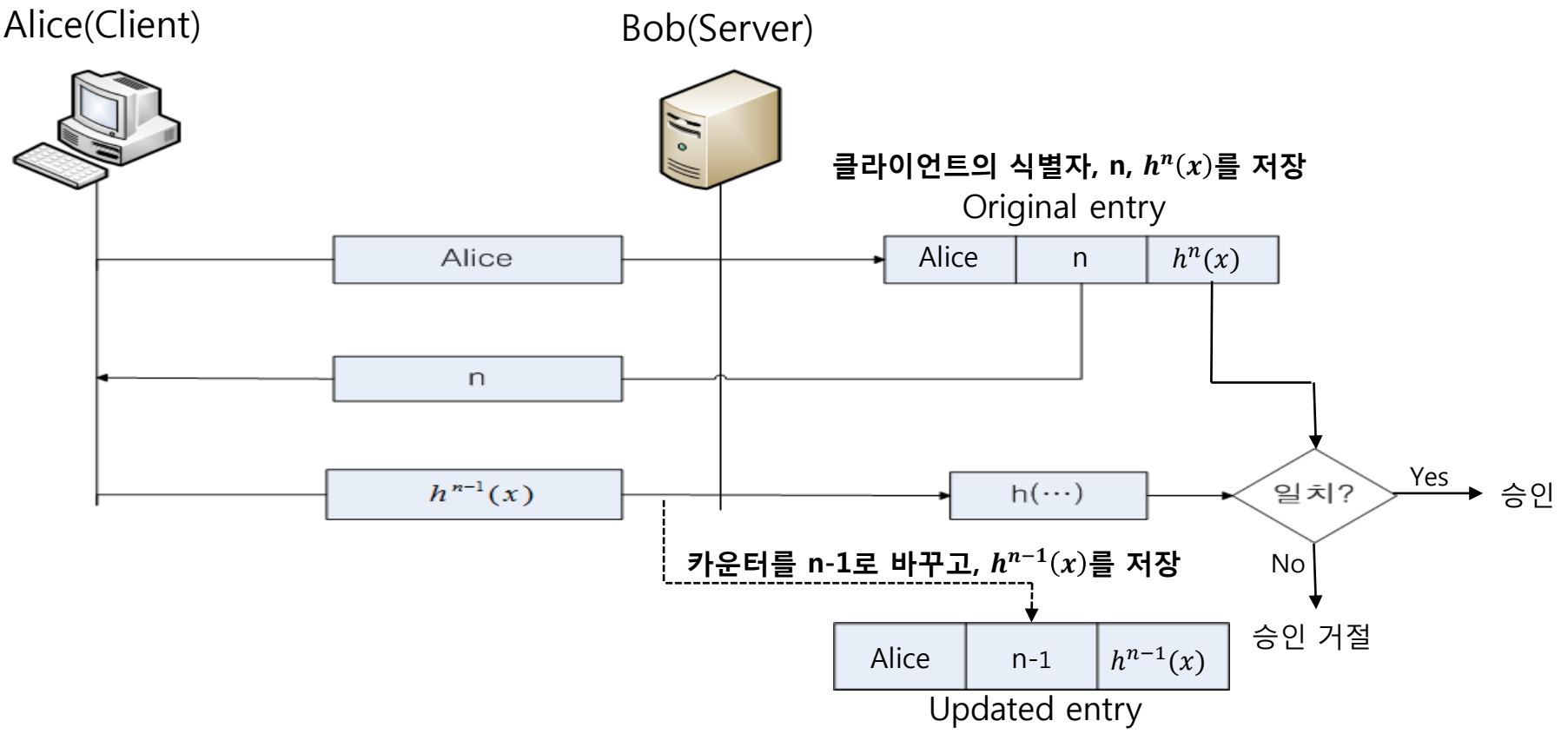
1) 클라이언트에서 정한 비밀 키에 해시 함수를 n-i번 중첩 적용하여 서버로 전송

2) 서버에서는 클라이언트로부터 받은 값에 해시 함수를 적용하여, 그 결과가 서버에 저장된 n-i+1번째 OTP와 일치하는지 검사

3) 일치하면 인증 성공; n값은 매번 접속이 있을 때마다 1씩 감소

응용 : 일회용 비밀번호(OTP)

- **과정(S/KEY방식) : 그림**



응용 : 일회용 비밀번호(OTP)

- **특징**

- 해시 체인의 길이 n이 유한적이므로 인증 횟수도 유한적 → 재설정(초기화)의 필요성
- 서버에 저장되어있는 OTP 목록이 유출될 경우 보안에 취약
- 함수는 MD4 또는 MD5 함수를 사용(input : 8byte, output : 8byte)
- 해시 체인의 특성으로 공격자가 만약 i번째 패스워드를 알고 있다고 해도, i+1번째 패스워드를 알 수 없음

ex. n = 4, s = 사용자가 정한 비밀 키, p(i)를 i번째 패스워드라고 가정하면,

p(1) = $h(h^3(x))$, p(2) = $h(h^2(x))$