One Time Password 프로토콜의 해시 충돌 가능성에 관한 연구

나태경, 장찬국*, 위한샘*, 이옥연**

국민대학교(대학원생), *국민대학교(전임연구교수), **국민대학교(교수)

skxorud@kookmin.ac.kr, *jangchankuk@kookmin.ac.kr, *whssktk@kookmin.ac.kr,
**oyyi@kookmin.ac.kr

A Study on the possibility of hash collision in One Time Password protocol

Tae-Gyeong Na, Changuk Jang*, Hansaem Wi*, Okyeon Yi**

Kookmin Univ(Graduate student), Kookmin Univ(Assistant Professor)*,
Kookmin Univ(Professor)**

요 약

본 논문은 10년 이상 같은 표준을 사용하고 있는 OTP(One-Time Password)[1]의 안전성이 보장되어 있는지 분석하였다. 한국에서 사용 중인 OTP는 TTA 표준을 사용하고 있으며, 해시 알고리즘을 사용해 OTP 숫자를 생성한다. 이 논문에서는 해시 알고리즘을 사용하여 임의의 OTP 값을 생성하고, 같은 OTP 값을 만드는 숫자들의 규칙성 유무를 통해 안전성 여부를 분석하였다.

Ⅰ. 서 론

본 논문에서는 한국에서 사용하는 OTP 표준인 TTA 표준이 HMAC-SHA1, HMAC-SHA256 함수 알고리즘을 사용하는 것에 주목하여 OTP의 안전성을 해시값을 통해 분석한다. TTA 표준 TTAK.KO-12.0193 '일회용 패스워드 알고리즘 프로파일[2]' 에 해당 내용이 작성되어 있으며, 표 1.은 표준에 나와 있는 칩 기반의 모든 일회용 패스워드 알고리즘을 소개한다.

Ⅱ. 본론

2-1. HOTP와 TOTP

해시 알고리즘을 사용하는 OTP는 크게 HOTP와 TOTP로 구분할 수 있다. HOTP(HMAC-based One-Time Password)는 HMAC을 기반으로 한 OTP이다. 2005년 12월에 관련 표준 RFC-4226에서 소개된 표준이며 표준에는 HOTP의 값이 6자리 이상 숫자로 이루어져야 하는 것 등 현재 사용되는 OTP에도 적용되는 사항이 소개되어 있다[3]. TOTP(Time-based One-Time Password)는 HOTP 알고리즘에서 시간을 고유 자원으로 사용하는 알고리즘이다. 2011년 5월 관련 표준 RFC-6238에서 소개된 이 알고리즘은 OTP가 출력되는 간격을 30초로 설정하는 것을 권장하거나, OTP를 다시 사용하기 위해서 10분 이내에 다시 로그인하는 것을 권장하는 설명이 소개되어 있다[4].

2-2. 해시 충돌

해시 알고리즘(Hash algorithm)은 해시 함수(Hash Function)으로도 불리며 임의의 데이터를 고정된 길이 데이터로 변환하는 함수이다. 암호학적 특징을 가지는 해시 알고리즘을 사용해 생성한 해시값은 다음과 같은 특성을 보여준다[5].

표 1. TTAK.KO-1293에 소개된 OTP 알고리즘 분류

사용 용도	권고 알고리즘	암호 키 길이(비트)	보안 강도(비트)	비고
중요 정보 저장	SEED	128	128	
	HIGHT	128	128	
정보 전송	SEED	128	128	
	HIGHT	128	128	
생성 알고리즘	HMAC-SHA1	162	162	
	HMAC-SHA256	256	1256	
	3DES	168	112	3key
	AES	128/256	128/256	
	SEED	128	128	
	HIGHT	128	128	

-역상 저항성: 주어진 출력에 대한 입력값을 구하는 것이 계산적으로 불가능하다. 함수 y=h(x)가 있을 때 x를 구하는 것이 계산적으로 불가능하다.

-제 2 역상 저항성: 주어진 입력에 대한 출력값과 동일한 출력값을 가지는 서로 다른 입력값을 구하는 것이 계산적으로 불가능하다. 변수 x가 있을 때 h(x) = h(x*)를 만족하는 x*가 있을 때 x와 다른 x*를 구하는 것이 계산적으로 불가능하다.

- 충돌 회피성: 서로 다른 입력값이 같은 출력값을 가진다면 입력값을 찾는 것이 계산적으로 불가능하다. 서로 다른 x와 x*가 있을 때 h(x) = h(x*)인 경우 x와 x*를 충돌쌍이라고 지칭하며 이 둘을 찾는 것이 계산적으로 불가능하다.

2-3. 해시 충돌 실험

이번 실험은 서로 다른 입력값이 같은 OTP를 생성할 때 입력값들의 규칙성이나 공통점을 찾기 위해 임의의 해시값을 만드는 python 알고리즘 pyotp를 사용하여 해시값을 생성하였다. 표준에서 사용하는 알고리즘이 OTP를 생성하기 위해서는 임의로 생성한 6자리의 16진수 값을 10진수로 변환한 후 일의 자리부터 6자리 값을 얻어야 하므로 다음과 같은 가정 이후 실험을 진행하였다.

-최소 1,000,000개의 숫자를 입력하여 OTP 값을 만든다면 000000부터 999999까지 최대 1,000,000개의 서로 다른 OTP 값을 만들 수 있다.
-16진수 값은 0부터 A, E까지 총 16가지 숫자로 구성되어 있으며 OTP 값이 16번보다 많이 반복된다면 16진수를 만드는 키 값이 일치할 수 있다.
-숫자가 일정 개수만큼 입력된다면 같은 OTP 값이 17번 이상 생성될 수 있으며, 입력된 값 중 16진수로 변환한 6자리가 일치하는 값이 생성될 수 있다.

```
pip install pyotp
```

```
Collecting pyotp
  Downloading pyotp-2.9.0-py3-none-any.whl (13 kB)
Installing collected packages: pyotp
Successfully installed pyotp-2.9.0
```

```
import pyotp
secret = 'DRQEGAZNX5HZEIXGFDZUTQRDOC4FKIC3'
hotp = pyotp.HOTP(secret)

print(hotp.at(458722))
print(hotp.at(851519))
print(hotp.at(1139292))
print(hotp.at(1183056))
print(hotp.at(1234807))
print(hotp.at(1498478))
print(hotp.at(1510664))
print(hotp.at(1650502))
print(hotp.at(1780782))
print(hotp.at(1799514))
print(hotp.at(1885508))
print(hotp.at(2608690))
print(hotp.at(2842612))
print(hotp.at(3254193))
print(hotp.at(3626805))
print(hotp.at(3747145))
print(hotp.at(3797769))
```

```
118970
118970
118970
118970
118970
118970
118970
118970
118970
118970
118970
118970
118970
118970
118970
118970
118970
```

그림 1. 서로 다른 17개의 숫자로 생성한 같은 OTP값

pyotp 알고리즘은 키 값으로 base32를 요구하여 임의로 생성한 Base32 키값인 DRQEGAZNX5HZEIXGFDZUTQRDOC4FKIC3를 사용하여 OTP 값을 생성하였다. 생성한 키를 사용하고, 서로 다른 17개의 다른 입력값이 같은 OTP 값을 생성할 수 있는 범위를 계산하였다. 입력값의 범위가 0부터 3,800,000 사이일 때, 범위 내에서 서로 다른 17개의 숫자가 같은 OTP 값인 118,970을 생성하였다(그림 1 참고). 하지만 입력값을 16진수로 변환하였을 때 같은 OTP를 생성하는 숫자들은 규칙성을 가지고 있지 않았다. 입력값으로 사용된 숫자는 일의 자리부터 6개의 숫자가 일치하지 않았으며 16진수로 변환한 값은 2개의 연속된 숫자가 같은 자릿수에서 일치하지 않았다(그림 2 참고).

458722	851519	1139292	1183056	1234807	1498489	1510664	1650502	1780782
6FFE2	CFE3F	11625C	120D50	12D777	16DD79	170D08	192F46	1B2C2E
1799514	1885508	2608690	2842612	3254193	3626805	3747145	3797769	
1B755A	1CC544	27CE32	2B5FF4	31A7B1	375735	392D49	39F309	

그림 2. 같은 OTP 값을 생성하는 입력값의 16진수 변환

Ⅲ. 결론

본 논문에서는 해시 함수 HMAC-SHA1 또는 HMAC-SHA256을 사용하는 OTP 표준이 규칙을 가진 숫자가 입력값으로 사용되면 같은 OTP 값을 생성하는지 분석하였다. 같은 OTP 값을 만드는 숫자들 사이에서 규칙성을 찾을 수는 없었지만, 같은 해시값을 만들 수 있을 만큼 입력값이 입력되어 같은 OTP 값을 얻을 수 있게 될 수 있다. 하지만 충돌 데이터 쌍을 찾을 수 있는 확률은 매우 낮다[6]. 컴퓨터의 계산 속도가 비약적으로 빨라지지 않는다면 안전성이 보장된 해시 알고리즘을 사용하여도 되지만, 기술의 발전을 대비하여 다른 방법으로 OTP를 생성할 수 있는 기술이 개발되기를 바란다.

ACKNOWLEDGMENT

이 논문은 2024년도 정부(국방부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임(RS-2022-11220701, 국방정보통신망-상용망(5G) 연동을 위한 보안 기술개발)

참 고 문 헌

[1] N.Haller, C.Metz, P.Nesser, M.Straw, “A One-Time Password System”, RFC2289, pp1-25, Febuary 1998.

[2] 한국정보통신기술협회, “일회용 패스워드(OTP) 알고리즘 프로파일”, TTAK.KO-12.0193, December 2012.

[3] D.M'Ralhi, M.Bellare, F.Hoornaert, D.Naccache, O.Ranen, “Hotp: An HMAC-Based One-Time Password Algorithm”, RFC4226, pp1-37, December 2005.

[4] D.M'Ralhi, S.Machani, M.Pei, J.Rydell, “Totp: Time-Based One-Time Password Algorithm”, RFC6238, pp1-16, May 2011.

[5] 백승준, 조세희, 김종성, “양자 컴퓨팅 환경에서의 해시함수 충돌쌍 공격 동향”, 한국정보보호학회 정보보호학회지, Febuary 2022

[6] 이종관, “전술 무선 네트워크에서 무인체계를 위한 해시 충돌 기반의 양방향 인증 프로토콜”, 한국정보보호학회 정보보호학회지, August 2019