OTP Generation using SHA

Mohammed Hamid Khan
Shah and Anchor Kutchhi Engineering College, Mumbai, India.
Email: mailathamid@gmail.com

Abstract: OTP (One Time Password) is not an old term for security field in computer science. There are various algorithms available to generate OTP for example HOTP (HMAC based OTP), TOTP (Time based OTP), S/Key. In this paper an OTP generation method is advised using SHA-1 algorithm, also how it is calculated and how it delivered to end device. This paper is related to my previous paper on "Securing ATM with OTP and Biometrics".

*****

Introduction:

One time password (OTP) is password that validates an authentic user for only one login to the respective system. If user is unauthorized, system will not allow further access. OTP can be generated by using different cryptographic hash functions that provides a fixed string which can be used as second level security at ATM. In paper [1] it is discussed, why SHA [2] family preferred over MD5 and other cryptographic hash algorithms. RFC

In generation of OTP there are many factors that can make OTP unique every time it is generated. In proposed system [2] OTP generation using SHA-1 is done by merging more than one unique factor that makes OTP unique in every generation. All data about user who is accessing ATM machine will be fetched by bank server, i.e. Mobile number of the user, current time of ATM access (dd/mm/yyyy-ss:mm:hh), account number of user etc.

When all required information is fetched, system will convert data into a string form using system code. Now that string will be considered as message in SHA-1 algorithm. SHA-1 algorithm will calculate hash string of 160 bits long. After calculation of SHA-1 hash value proposed method will be applied. And it will send 5 digit long numerical OTP to the registered mobile number of the user.

Method SHA-OTP calculation:

A. SHA-1 hash value calculation

1. Fetch current time of the ATM transaction (After card and user validation) is done by the bank system.
2. Fetch user information stored in the bank database (User Account number, IMEI Number, Mobile Number etc.)
3. Merge all the information fetched with date and time in a string form.
4. Now pass this string (say raw-string to the SHA-1 method.
5. SHA-1 method will operate on raw-string and it will generate 160 bit long hash value string (say H-string).

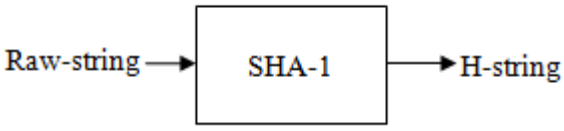

Figure1. Raw-string to H-string

B. Hash String (H-string) to OTP

1. Now, H-string will be having numeric digits present in it, system will select numeric digits from H-string (say N-string).
2. Size of N-string may vary from 14-19 digits.
3. A random selector method will be applied on N-string to select a random number from N-string (say R-number).
4. Here R-number is selected at random. So, it is possible that the number got selected is of two digit (Since reaching position 53 is not possible because of size of N-string , If R-number is of two digits for example 53, than Unit value will be selected i.e. 5.) than R-number will hold value of unit position of selected digit.
5. Now, pointer will point to the position of R-number on N-string.
6. OTP selector will select 5-digit OTP from that position and that OTP will be sent on user mobile number for further access.

Example of OTP calculation:

Table 1: User information

User Name	SAKEC
Account Number	0123456789
Mobile number	9870908062
Address	chembur
IMEI	12345678932
Current Time	10.30.12:12-12-2014

Table 2: SHA-1 calculation of string

String	Hash Value
SAKEC	534480d2acc986f8ebb895655dc8b6280a98f57
SAKEC0123456789	e2ea34548628caf9278a225c456c60597f26cb8
SAKEC012345678998709 08062chembur12345678932	fcdf34826cfd5c6c7813b667f466fab49d609aa8
SAKEC012345678998709 08062chembur12345678932 10.30.12:12-12-2014 (raw-string)	29699c7fc6a0dc40cba6671486393d8f59e87ec (H-string)

Change in hash values after one second

Raw-string = SAKEC012345678998709 08062chembur12345678932 10.30.13:12-12-2014:

H-string= 9cc1f30d516e4ec1202d174b352262bcdcca7149

1. When Hash Value (H-string) is calculated, following step will take numeric values from hash string (N-string).
   Since H-string = 9cc1f30d516e4ec1202d174b352262bcdcc
   So, N-string = 913051641202174352262 7149
2. Random selector in the program will select one number randomly from that string for example say 64 (R-number) is selected from string. This proposed system will select first number from randomly selected number i.e. 6 (R-number).
3. Now OTP will be selected from 6^{th} position till 5 counts. i.e. 64120 will be considered as an OTP.
4. These 5 digits will be considered as OTP and send to registered mobile number of the user [4].

Delivery of OTP:

For delivery of OTP to the user at registered mobile number, in proposed system SMS gateway is used. There is one constrain for OTP delivery, that is number of the user should not be registered with DND facility. This constrain can be resolved by bank, by purchasing better SMS gateway service.

Advantage and Future work:

The basic advantage of this system is the generated OTP will less repetitive, Since SHA-1 getting unique string every time, it will produce unique hash value and produces fewer chances of attacks.

In the future, this OTP generation can used with more cryptographic hash functions. As newer algorithms getting advised (like SHA-3), this system can generate more unique OTPs to secure the system.

References:

[1] Mohammed Hamid Khan, Jyoti Joglekar, "A review paper on cryptographic hash functions", *International conference on recent trends in computer & electronics engineering*. Jan 2015.
[2] D. Eastlake, P. Jones. A US Secure Hash Algorithm 1 (SHA1), RFC 3174, September 2001.
[3] Mohammed Hamid Khan, "Securing ATM with OTP and Biometric", *"International Journal on Recent and Innovation Trends in Computing and Communication"*, Volume: 3 Issue: 4, ISSN: 2321 -8169.
[4] "Methods_of_delivering_the_OTP" [Online] http://en.wikipedia.org/wiki/Onetime_password#Methods_of_delivering_the_OTP. [Accessed: 12 Nov 2014].