Multiple-Factor Authentication

Cryptography – Project 2

THITEUX Lucas

BODSON Fabrice

Master en Architecture des systèmes informatiques
2022 - 2023

Summary

- What is Multiple-Factor Authentication ?
- Which problems MFA can solve in practice ?
- One Time Password generators
- HOTP
- TOTP
- HOTP vs TOTP

What is Multiple-Factor Authentication ?

- Combination of different types of authentication :
  - What the entity knows (password, pin code, ...)
  - What the entity owns (chip card, OTP generators, ...)
  - What the entity is (facial recognition, fingerprint, ...)
  - What the entity can do or does (voice recognition, handwritten signature, ...)
  - Where the entity is situated (localization)

Which problems MFA can solve in practice ?

- Disclosure of login and password
  - Databases publication
- Weakness of login and password
  - Social engineering, cracking

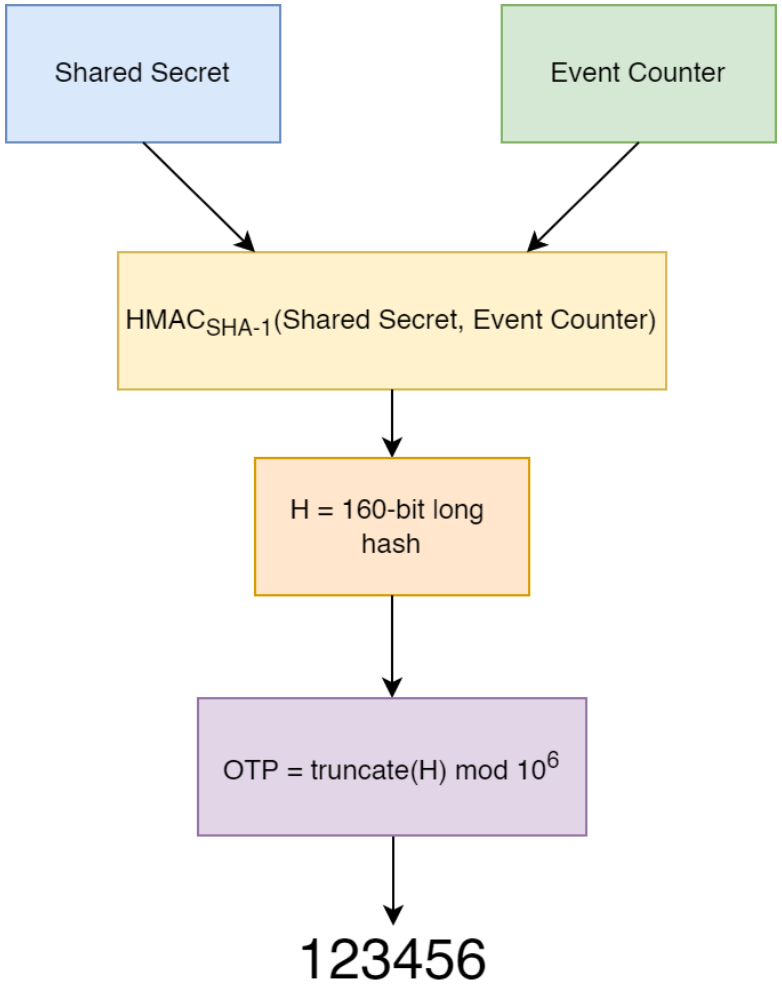
One Time Password Generator

- Easy to implement because it is open source
- They generate single-use codes which allows them to avoid "replay" attacks
- They do not necessarily require the use of the Internet

HMAC-based OTP

Event based OTP

- Shared secret key + event counter = 160 bits long hash
- Truncation to 31 bits
- Convertion to human readable integer

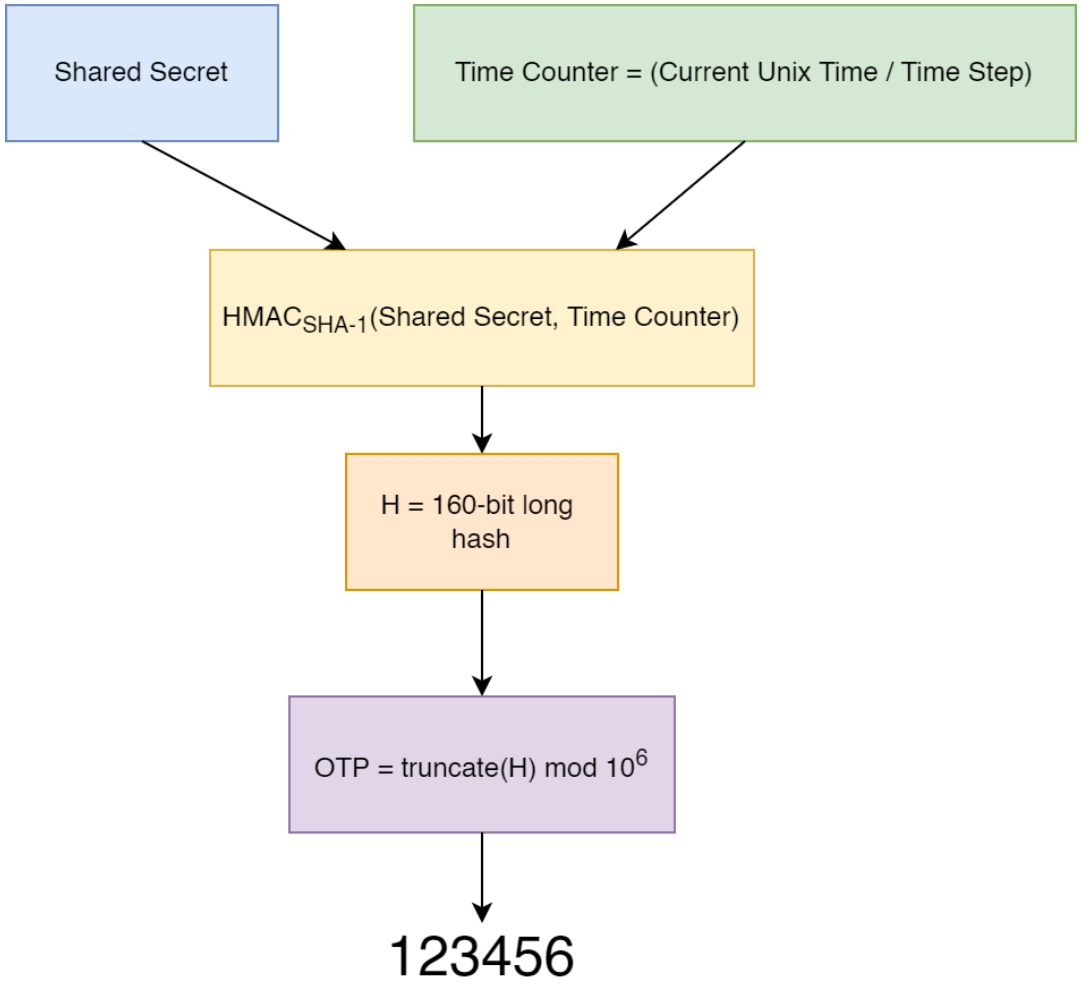


Time-based OTP

Time based OTP

Time step is chosen

- Shared secret key + time counter = 160 bits long hash
- Truncation to 31 bits
- Convertion to human readable integer



HOTP vs TOTP

HMAC-Based One-Time Password (HOTP)	Time-Based One-Time Password (TOTP)
Event Counter	Time Counter
The counter is incremented after successful authentication or on button press	The counter is incremented every 30 seconds
OTP is valid for an unlimited time (until a new OTP is generated)	OTP is valid for 30 seconds only
Requires a validation window	Requires no validation window

Thank you for listening us

Do you have any questions?