ndgtriluugnghggtkhvrbbrrgtdfeivgklbkviteggcu: The Yubikey One Time Password Scheme

Brouzioutis Charisis

0x375 0x05

July 4, 2011

What is this Yubikey anyway?

A security token device

- Connected token
  USB HID (Keyboard) a.k.a. “No drivers needed”
- Multi use
  - Yubikey OTP
  - OATH/HOTP
  - Static passcode
  - Challenge-Response
- Open source software
- Looks cool on the keychain

USB Keyboard emulation challenges

The problem: Keyboards generate scancodes

- Scancodes are mapped to different keys depending on keyboard layout
- Keyboard modifiers affect end ASCII codes

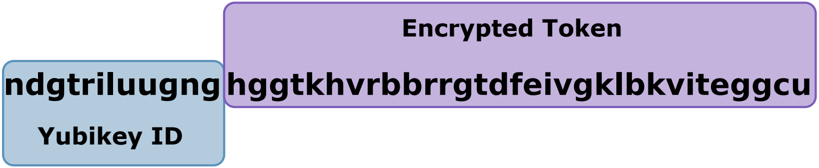
Best effort solution: ModHex coding

- base16 encoding
- use the least affected subset of Latin alphabet

hex	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
modhex	c*	b	d	e	f	g	h	i	j	k	l	n	r	t	u	v

eg. 0x5b9b ⇒ gnkn

Who's ndgtriluugnghggtkhvrbbrrgtdfeivgklbkviteggcu?



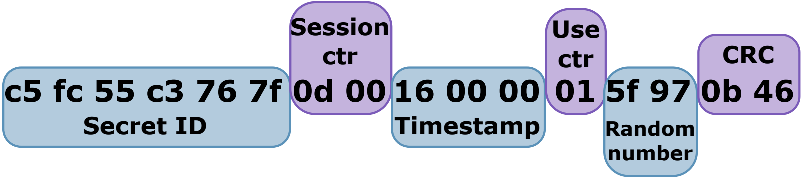
Encrypted Token

ndgtriluugng hggtkhvrbbrrgtdfeivgklbkviteggcu

Yubikey ID

- Yubikey ID: 0 - 6 bytes long
- 16 bytes encrypted token
  - AES-128 in raw (ECB) mode

Token format



```
#define UID_SIZE 6
typedef struct {
  uint8_t secretId[UID_SIZE];     /* Secret ID */
  uint16_t sessionCtr;            /* Session counter *
  uint24_t timestamp;             /* Timestamp */
  uint8_t sessionUse;             /* Session use counter */
  uint16_t rnd;                   /* Pseudo-random value */
  uint16_t crc;                   /* Checksum */
} TOKEN;
```

Challenge - Response

HID Feature reports are used for two-way communication

1. Yubikey challenged with 48 bit challenge
2. User responds by pressing the button (optional)
3. Secret ID gets XORed to challenge
4. Business as usual...

Replay attacks

The problem

Generated OTPs are valid until a newer OTP is used.

Mitigation

- Ask for multiple OTPs per session
- Use OTP's timestamp to validate its freshness:
  Last validation time + timestamp diff = time now
  (timestamp: 8Hz clock, 2% drift)

Integrating with your applications

Common pitfalls

- OTPs are case insensitive
- Session counter, usage counter and checksum are little-endian
- A delay of 30-500ms is introduced in challenge/response mode

(Brainfart) Authentication server checklist

- Triple check your OTP validation code
- Take care of your key storage
- Set up revocation procedures
- Consult a cryptologist

FIN

Thank You!
More Questions?