Yubikey dla użytkowników

FreeBSD

Jarosław Żurek

Czym jest YubiKey?

- USB all-in-one - sprzętowe uwierzytelnienie;
- Możliwość integracji offline z PAM, SSH (2FA);
- Integracja z serwisami np.:

  Facebook, Gmail, GitHub, LastPass, KeePass, GitHub, GitLab, Bitbucket.

Zalety:

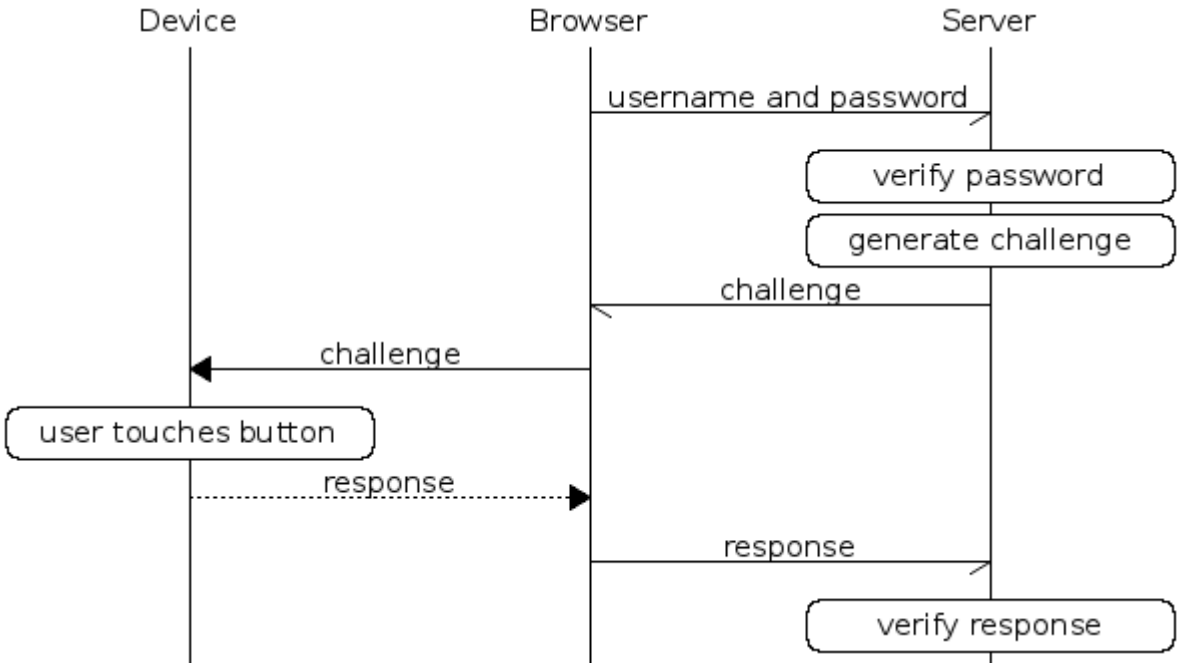
- łatwość użycia;
- wsparcie dla wielu standardów komunikacji i uwierzytelnienia;
- wysokie bezpieczeństwo dzięki użyciu sprawdzonej kryptografii;
- oprogramowanie OpenSource.

Modele YubiKey

	FIDO U2F	Yubikey 4	Yubikey 4 NEO
OTP		✓	✓
OATH		✓	✓
OpenPGP		✓	✓
FIDO U2F	✓	✓	✓
FIDO2	✓		
PIV		✓	✓
NFC			✓

Tabela 1. Porównanie modeli Yubikey pod względem wspieranych technologii.

Jak działa Yubikey U2F?



Źródło: https://developers.yubico.com/U2F/

Konfiguracja Yubikey

Port: security/ykpers

- ykpersonalize(1) - konfiguracja urządzenia
- ykinfo(1) - informacje o urządzeniu
- ykchalresp(1) - realizacja operacji challenge-response

Port: security/pam_yubico

- ykpamcfg(1) - zarządzanie ustawieniami PAM Yubico.

Port: security/pam_per_user

Port: security/oath-toolkit

Przydatne manuale: pam_per_user(5), pam_yubico(8).

Konfiguracja 2FA

Konsola – konfiguracja Yubikey:

```
# ykpersonalize -2 –o chal-resp –o chal-btn-trig –o chal-hmac –o hmac-lt64 –o serial-api-visible

# ykpamcfg -2 –v
```

/etc/pam.d/system:

```
auth       required       /usr/local/lib/security/pam_per_user.so.1
```

/etc/pam.d/system-yubico:

```
auth       required       /usr/local/lib/security/pam_yubico.so          mode=challenge-response
```

/etc/pam_per_user.map

```
root: system-yubico

*: @SUCCEED
```

Konfiguracja SSH

Konsola – konfiguracja Yubikey:

```
# ykpersonalize -1 –o oath-hotp –o oath-hotp8 –o append-cr
```

/usr/local/etc/users.oath:

```
# echo ”HOTP user – key” >> /usr/local/etc/users.oath
```

/etc/pam.d/sshd:

```
auth    required    /usr/local/lib/security/pam_oath.so  usersfile=/usr/local/etc/users.oath  window=16
digits=8
```

/etc/ssh/sshd_config:

```
ChallengeResponseAuthentication yes
PasswordAuthentication no
UsePAM yes
```

Przydatne źródła

Przewodniki do konfiguracji Yubikey z popularnymi serwisami:

https://support.yubico.com/support/solutions/folders/15000002765

Wsparcie Yubikey dla FIDO2, OTP, OATH, PGP, PIV:

https://developers.yubico.com/

Źródła Yubikey:

https://github.com/Yubico