CERN openlab

Exploring Cybersecurity Frontiers

Challenges regarding 2FA, Incident Response, and Web Scanning

Mihai-George Licu

Supervisor: Dr. Stefan Lüders

16th Aug 2023

Cybersecurity Operations

Direct involvement in the following projects

1. 2FA - Merging YubiKey Registration
2. Incident Response and OSINT
3. Web Scanning – Automated tech detection and penetration testing

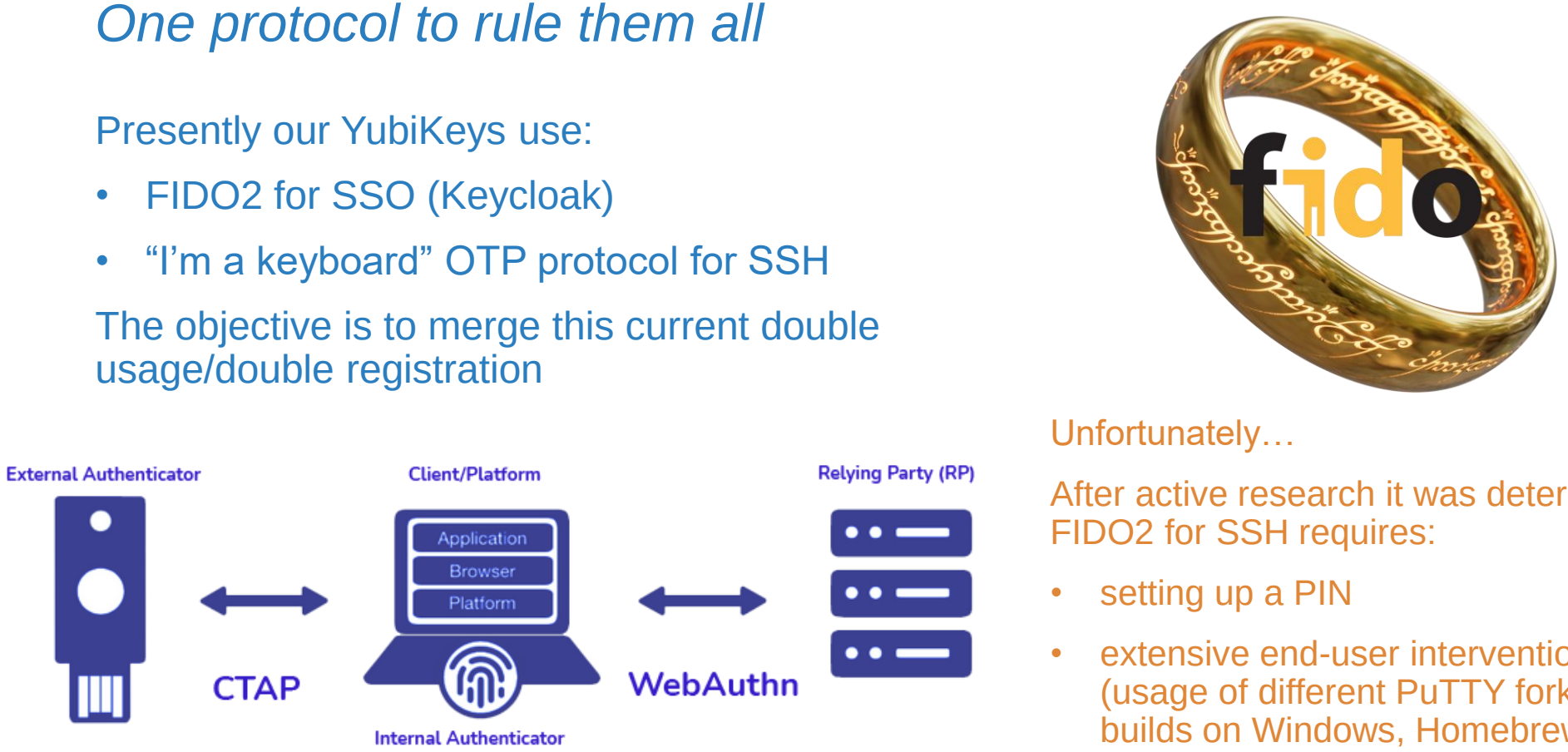
2FA - Merging YubiKey Registration

One protocol to rule them all

Presently our YubiKeys use:

- FIDO2 for SSO (Keycloak)
- “I’m a keyboard” OTP protocol for SSH

The objective is to merge this current double usage/double registration



Unfortunately…

After active research it was determined that using FIDO2 for SSH requires:

- setting up a PIN
- extensive end-user intervention and configuration (usage of different PuTTY fork and beta OpenSSH builds on Windows, Homebrew for compatible OpenSSH version for Mac users)

Project stopped as it would be unfeasible to roll out currently, further work from third parties required

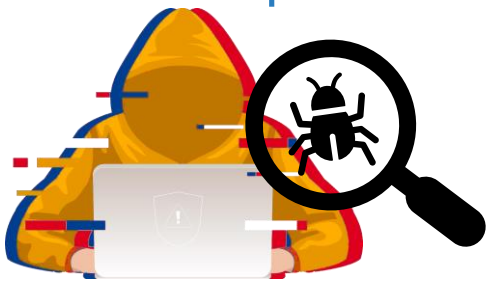
Incident Response and OSINT

MICI-BICA, an Incident Involving IRC-Based Malware Deployment

High-profile incident targeting CERN and affiliated universities

Assisted Pau Cutrina by investigating and translating Romanian hackers' content from different social media and sources to cross corelate actors and similar behaviour

Identified key users within the channels, techniques used and motivation of operations



Attend the upcoming talk by Pau Cutrina Vilalta in September https://indico.cern.ch/event/1314294

Web Scanning – Automated tech detection and penetration testing

Motivation

17000+ websites hosted at CERN

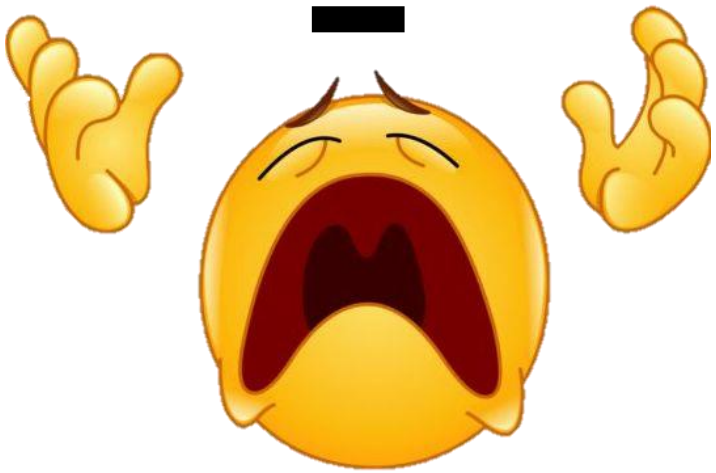
+

a large non-standard tech stack
(besides Drupal, MKdocs, Sharepoint, Twiki)

+

limited security resources

=

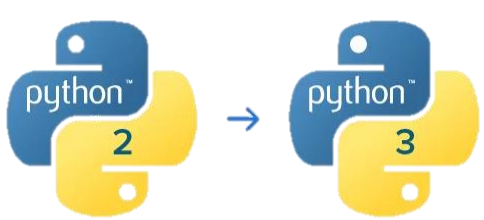


Web Scanning

The present

WAD: tool developed and used at CERN for maintaining an inventory of technologies used on the CERN web landscape, leveraging open-source Wappalyzer's rules, it analyses URLs via GET requests, examining HTTP response and HTML body to detect web tech.

- migrated scripts from Python2 ➜ Python3
- ensured continuous compatibility with Wappalyzer’s detection rules set
- integrated with new SSO
- developed new automation scripts



Web Scanning

The future

- contribute to the detection rules set for technologies used specifically at CERN
- move WAD from regex to BeautifulSoup for HTML parsing purposes
- investigate the possibility of developing a tool in Go using Nuclei, a fast and customizable vulnerability scanner based on simple YAML based DSL with technology detection, fuzzing and a variety of scan capabilities alongside ZAP and WAD

Thank you!
Questions?

✉ *mihai-george.licu@cern.ch*