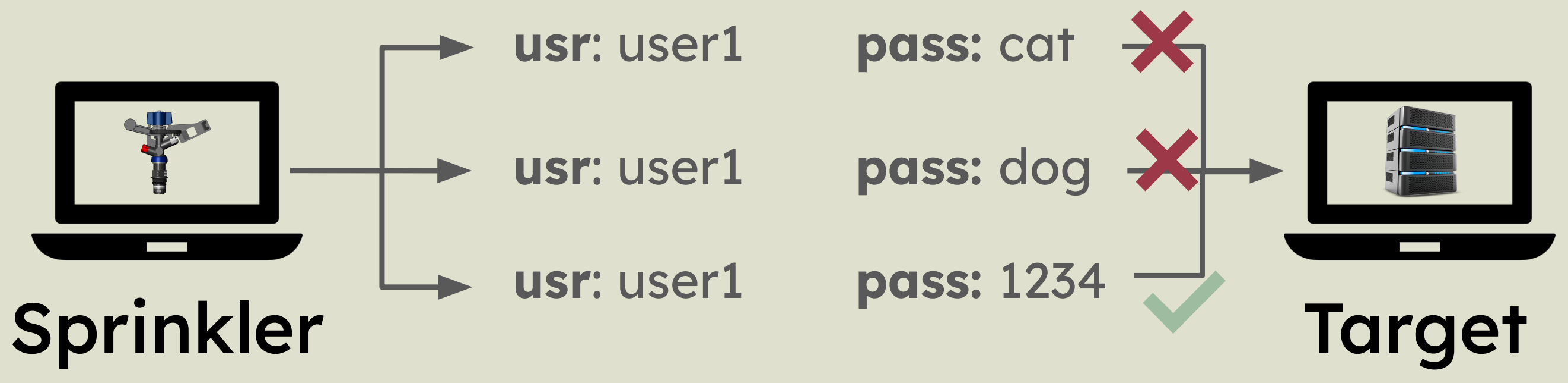
Sprinkler: A Multi-Service Password Sprayer

Sam Ederington, Prompt Eua-anant, advised by Jeff Ondich

References

What's password spraying?

- Guessing server login credentials as fast as possible, without getting detected



usr: user1 **pass**: cat

usr: user1 **pass**: dog

usr: user1 **pass**: 1234

Sprinkler

Target

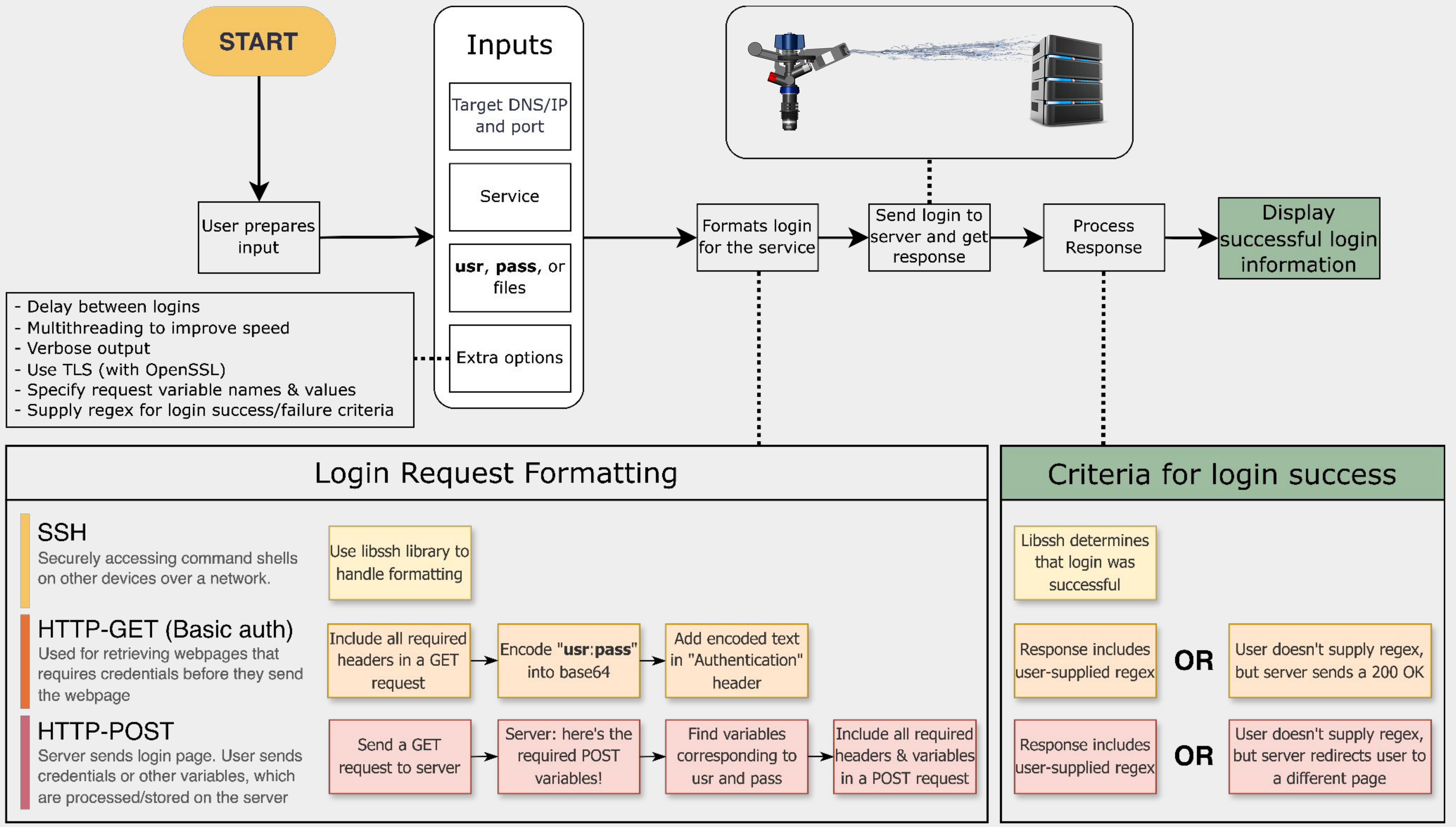
Why it's important?

- It's used for hacking and security purposes, finding accounts with vulnerable login permissions to attack or require changing.

Our goal

- Make a fast password sprayer that works for ssh, http-get (basic auth), http-post. Language = C
- Prepare Apache2 test servers on Ubuntu compatible with the services we need
- Compare Sprinkler's performance with Hydra, a popular password sprayer

How Sprinkler works



START

User prepares input

Inputs

Target DNS/IP and port

Service

usr, **pass**, or files

Extra options

- Delay between logins
- Multithreading to improve speed
- Verbose output
- Use TLS (with OpenSSL)
- Specify request variable names & values
- Supply regex for login success/failure criteria

Formats login for the service

Send login to server and get response

Process Response

Display successful login information

Login Request Formatting

SSH

Securely accessing command shells on other devices over a network.

Use libssh library to handle formatting

HTTP-GET (Basic auth)

Used for retrieving webpages that requires credentials before they send the webpage

Include all required headers in a GET request → Encode "**usr**:**pass**" into base64 → Add encoded text in "Authentication" header

HTTP-POST

Server sends login page. User sends credentials or other variables, which are processed/stored on the server

Send a GET request to server → Server: here's the required POST variables! → Find variables corresponding to usr and pass → Include all required headers & variables in a POST request

Criteria for login success

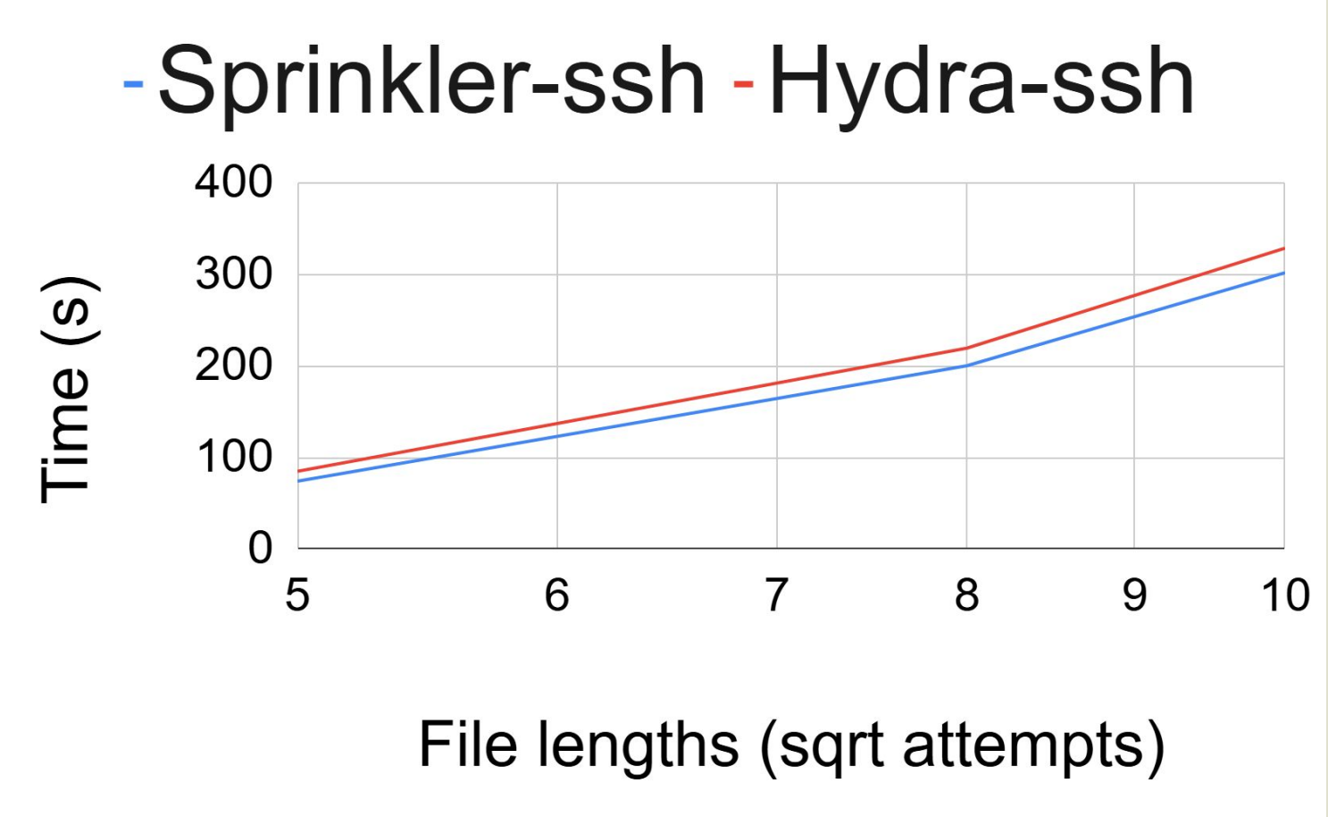
Libssh determines that login was successful

Response includes user-supplied regex OR User doesn't supply regex, but server sends a 200 OK

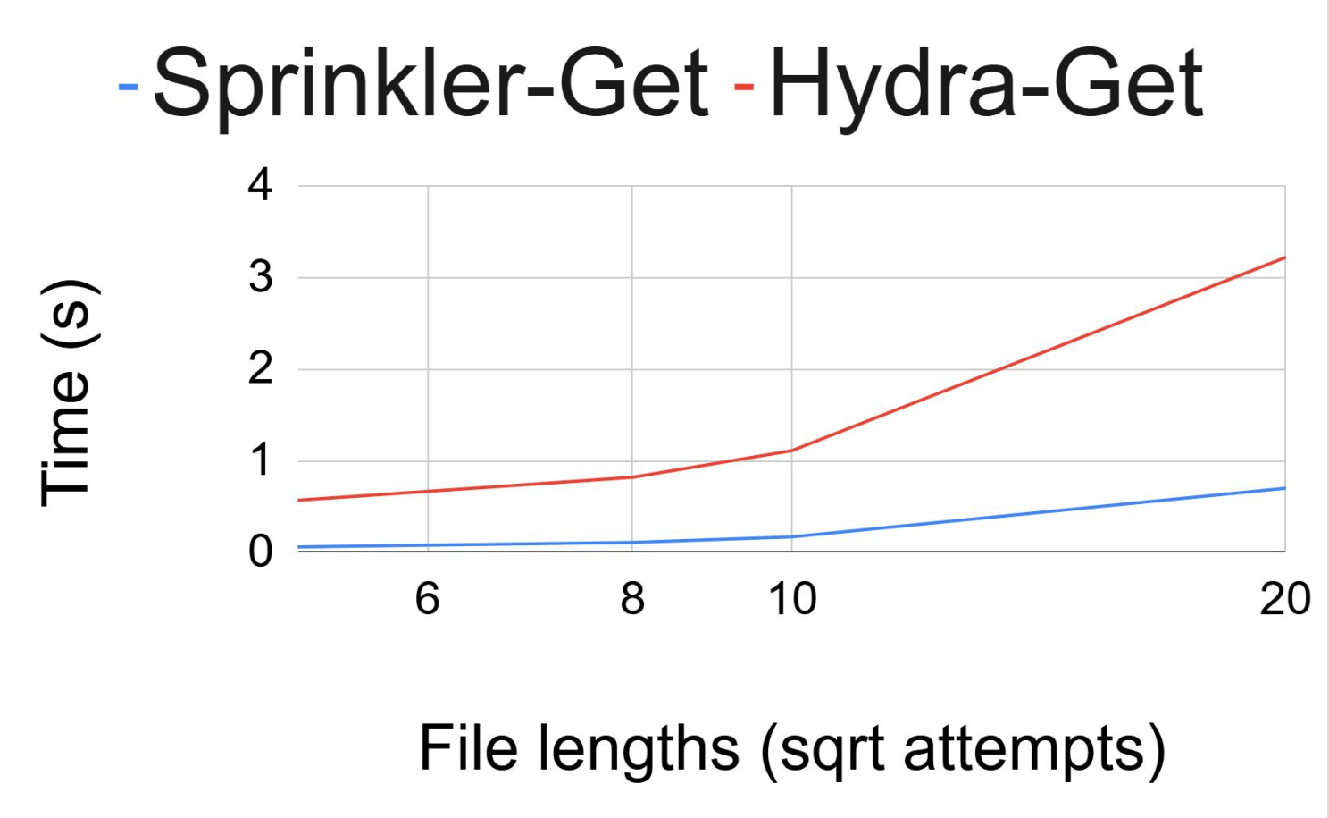
Response includes user-supplied regex OR User doesn't supply regex, but server redirects user to a different page

Performance

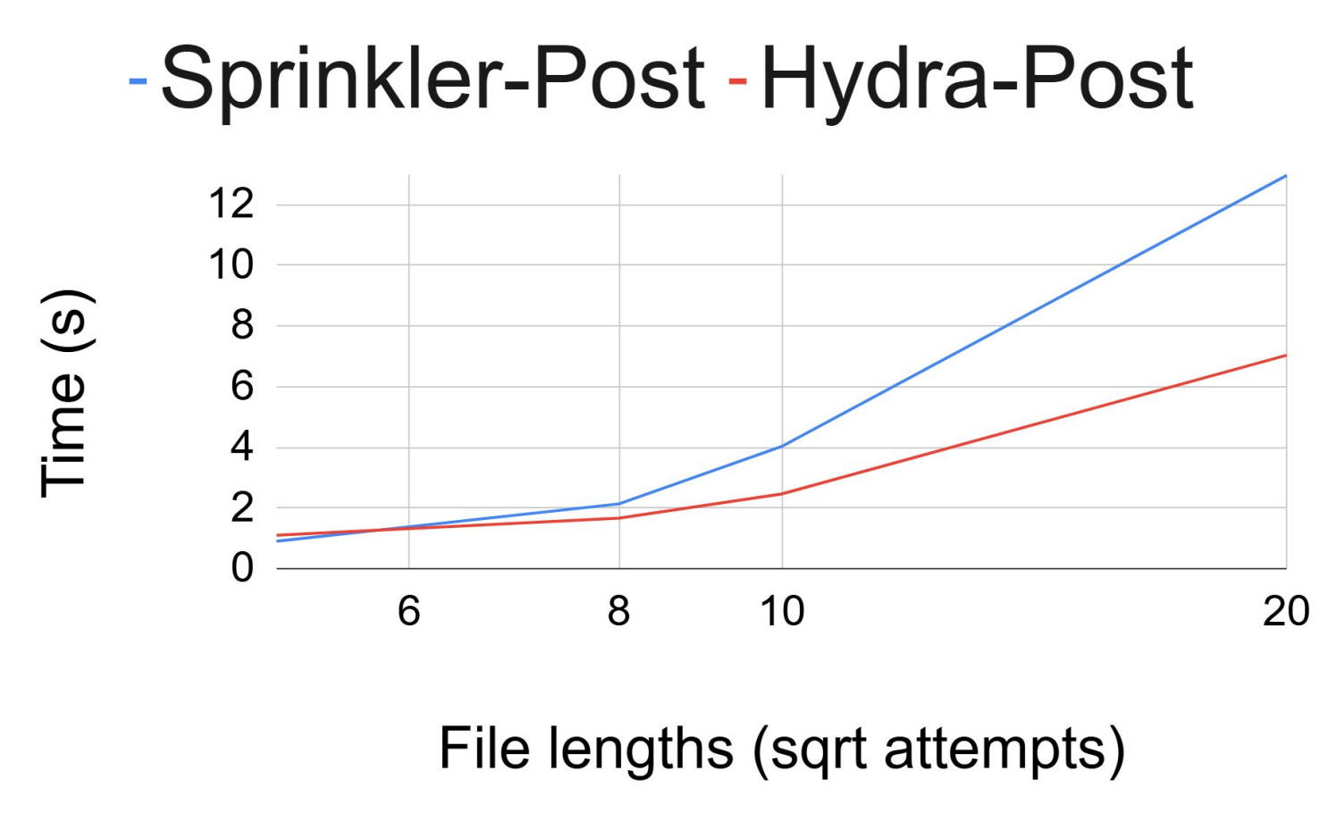
SSH



HTTP-GET



HTTP-POST



Acknowledgements: we would like to thank Jeff Ondich, our friends and classmates for supporting us throughout this project