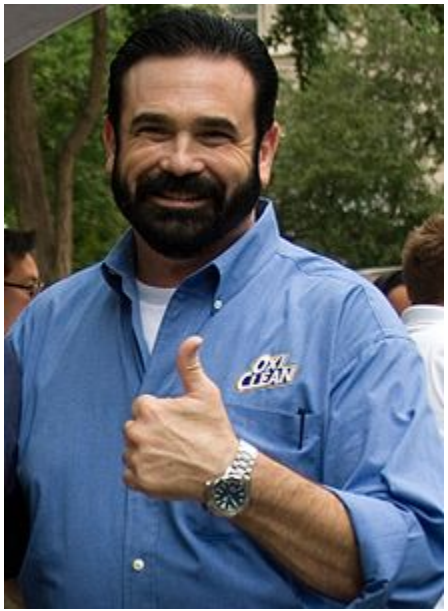
Firefox + TUF

Orange Team

Why Firefox+TUF?

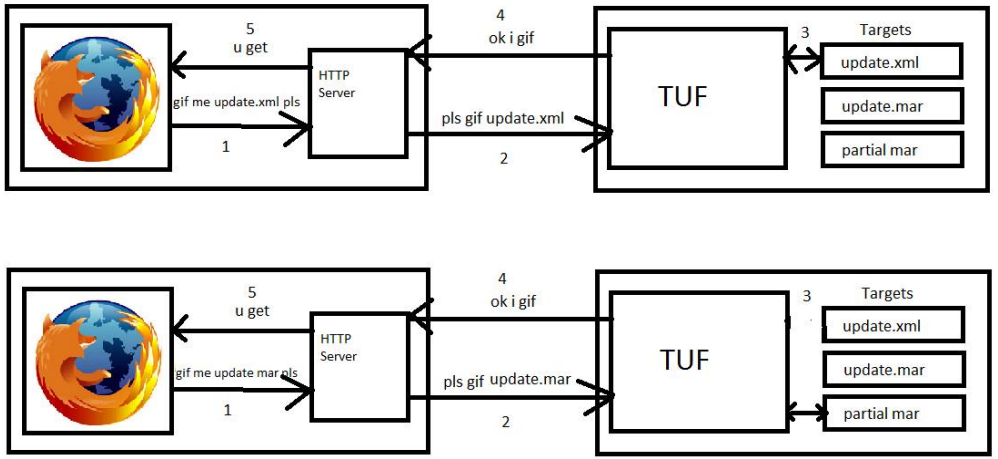
- “Like the S in HTTPS”
- Easy to setup and deploy
- Very little overhead
  - TUF metadata less than 50Kb!
- Firefox vulnerable to certain attacks
  - TUF mitigates them!

- Satisfaction guaranteed!



How does it work?

- Local proxy server running with Firefox
- Firefox set to contact the local server for updates
- Proxy server contacts TUF repository and retrieves updates securely



Security

- Two servers
  - One to act as keystore
  - One as main repo
- Targets delegates to Nightly
  - Nightly restricted to only signing for files in the nightly folder (Nightly/Aurora builds)
  - Trying to sign release using Nightly gives error
    - `tuf.Error: ("Not enough signatures for '/root/scripts/repository/metadata.staged/targets.txt'",`
- Release/Beta builds are signed by offline key

Setup & Updates

- Convenience scripts provided
  - Run setup.py to setup TUF on repository server
  - That’s it!

- Repository update scripts provided
  - updatenightly.py and updaterelease.py
    - Updates Nightly/Aurora and Stable/Beta builds

Vulnerabilities

- Replay Attack
- Arbitrary Package Attack
- Indefinite Freeze Attack
- Slow Retrieval Attack
- Endless Data Attack

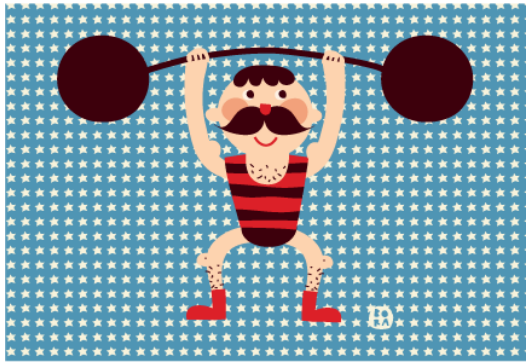
Vulnerabilities

- ~~Replay Attack~~
- ~~Arbitrary Package Attack~~
- Indefinite Freeze Attack
- Slow Retrieval Attack
- Endless Data Attack

Firefox already protects against these

Vulnerabilities

- ~~Replay Attack~~
- ~~Arbitrary Package Attack~~
- Indefinite Freeze Attack ✓
- Slow Retrieval Attack ✓
- Endless Data Attack ✓



Protected by TUF

Indefinite Freeze (w/o TUF)

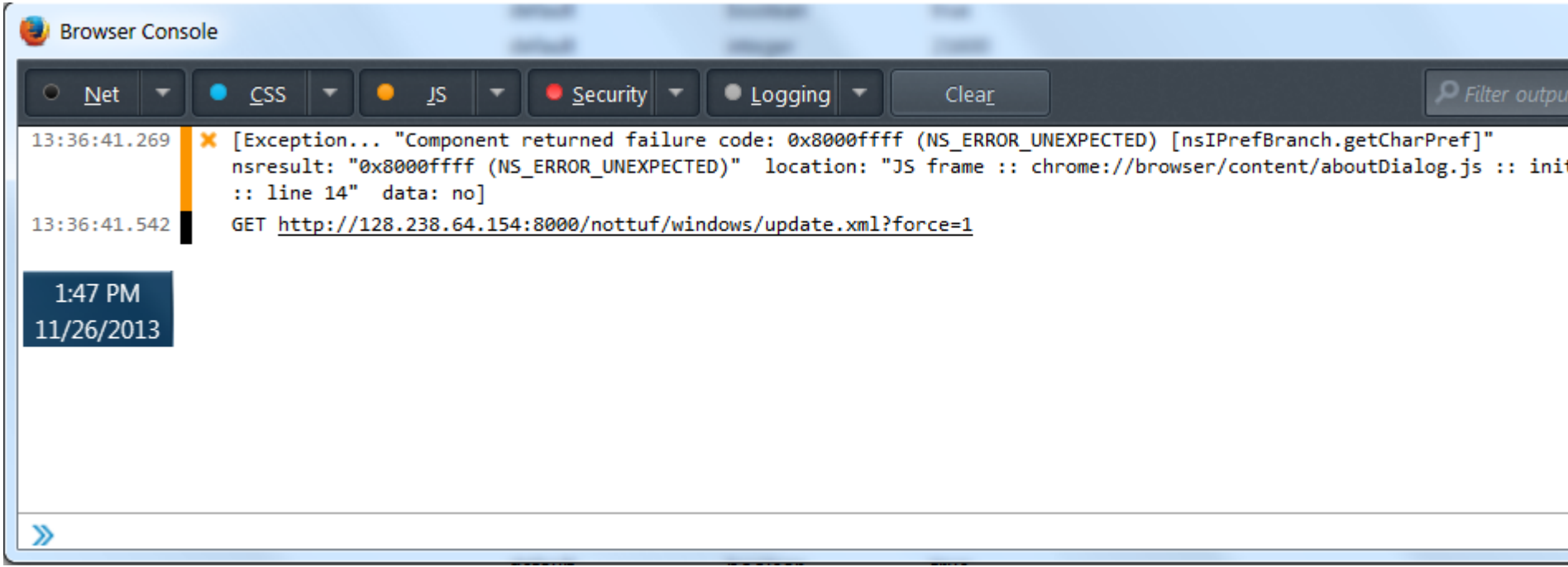
- Firefox knows its own version number
- Send Firefox an older update.xml
  - Firefox reports it is up to date

Indefinite Freeze (w TUF)

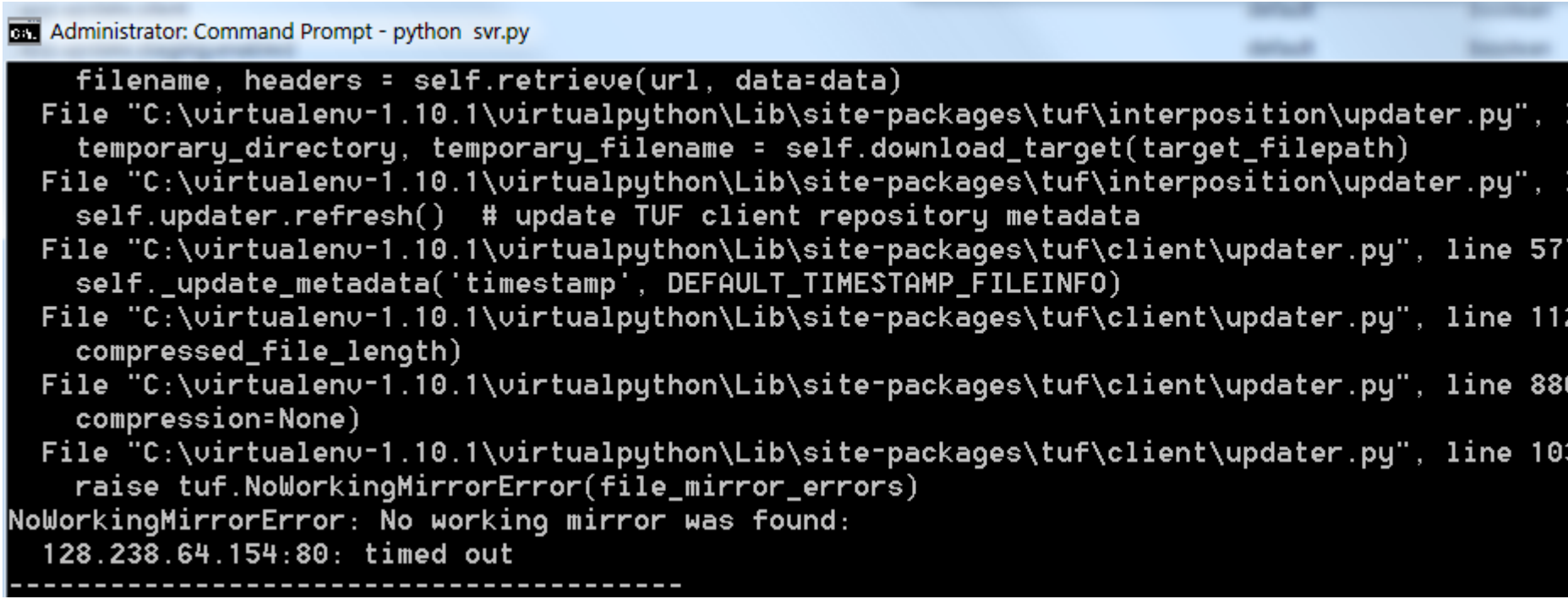
- Send Firefox an older update.xml
  - Firefox reports it is up to date

- Firefox's update URL gets intercepted by the local server to redirect to the correct file on the TUF repository

Slow Retrieval (w/o TUF)



Slow Retrieval (w/ TUF)



Endless Data (w/o TUF)

- Firefox downloads data nonstop
  - Fills up system's memory

conhost.exe	Dennis Mira...	00	1,964 K	Console Windo...
csrss.exe		00	2,084 K	
dwm.exe	Dennis Mira...	01	24,020 K	Desktop Windo...
explorer.exe	Dennis Mira...	00	54,372 K	Windows Expl...
firefox.exe *32	Dennis Mira...	12	1,266,700 K	Firefox
googledrivesync.ex...	Dennis Mira...	00	27,604 K	Google Drive
googledrivesync.ex...	Dennis Mira...	00	200 K	Google Drive
GoogleToolbarNotifi...	Dennis Mira...	00	480 K	GoogleToolbar...
HCMSoundChanger...	Dennis Mira...	00	840 K	SoundChanger...
HDMICtrlMan.exe	Dennis Mira...	00	1,724 K	HDMICtrlMan.e...

Endless Data (w/ TUF)

- TUF cuts off download after limit is passed

```
NoWorkingMirrorError: No working mirror was found:
  <mirror IP>: Unterminated string starting at: line 6 column 11 (char 142)
```

Firefox ♥ TUF

- TUF makes Firefox tough