Firefox

(without TUF)

Update Process

- Downloads metadata file *update.xml* from Mozilla server over HTTPS
- Downloads *.mar* files containing program updates from Mozilla server over HTTP
- *update.xml* contains:
  - filesize and SHA-512 hashes for the .mar files
  - links to mirrors hosting the .mar files

Inherent Weakness

- Model is dependent on the metadata server being secure
- Compromised server/certificate would inherently allow all following exploits
- We focus on model where server is NOT compromised

Indefinite Freeze

- Change configuration string in Firefox configuration
  - Set *app.update.url.override* to URL for version 25
  - https://aus3.mozilla.org/update/3/Firefox/24.0/20130910160258/WINNT_x86-msvc/en-US/release/Windows_NT%206.1.1.0%20%28x64%29/default/default/update.xml?force=1
  - Firefox will report that it is up to date

Endless Data Attack

- If *update.xml* is somehow compromised:
  - Updater xml parser seems to be vulnerable to “billion laughs attack”
    - ```
      <?xml version="1.0"?>
      <!DOCTYPE lolz [
       <!ENTITY lol "lol">
       <!ELEMENT lolz (#PCDATA)>
       <!ENTITY lol1 "&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;">
       <!ENTITY lol2 "&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;">
       <!ENTITY lol3 "&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;">
       <!ENTITY lol4 "&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;">
       <!ENTITY lol5 "&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;">
       <!ENTITY lol6 "&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;">
       <!ENTITY lol7 "&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;">
       <!ENTITY lol8 "&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;">
       <!ENTITY lol9 "&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;">
      ]>
      <lolz>&lol9;</lolz>
      ```
      ```

Rollback Attack

- Firefox does not appear vulnerable to this
- Trying to force it to update to an older version leads to Firefox reporting it is up to date

Mix and Match Attack

- Firefox does not appear vulnerable to this
- Would require SHA-512 collision.

Slow Retrieval Attack

- Set up server with copy of *.mar* files
- Limit upload speed to ridiculously slow
- DNS Cache poisoning would work
  - Firefox downloads *.mar* files over HTTP

Extraneous Dependencies Attack

- Does not seem possible
- Firefox updates using proprietary archive format that contain self-contained patches