The Clock is Still Ticking: Timing Attacks in the Modern Web

Tom Van Goethem, Wouter Joosen, Nick Nikiforakis

Background: Timing attacks

- Introduced by Felten et al. in 2000.
- A side-channel attack analyzing the time that it takes to a cryptographic algorithm/requesting a webpage/etc.

Background: Timing attacks

- Introduced by Felten et al. in 2000.
- A side-channel attack analyzing the time that it takes to a cryptographic algorithm/requesting a webpage/etc.
- If someone has recently visited a particular website, then cache will store it.

Background: Timing attacks

- Introduced by Felten et al. in 2000.
- A side-channel attack analyzing the time that it takes to a cryptographic algorithm/requesting a webpage/etc.
- If someone has recently visited a particular website, then cache will store it.
- Cache will save time the next time the website is requested, where attackers can analyze the time difference and get valuable information.

Timing attacks in modern web

- This paper proposes new timing attacks using modern web features (HTML5, etc).

Timing attacks in modern web

- This paper proposes new timing attacks using modern web features (HTML5, etc).
- Purpose of attacker in this paper is a bit different: estimate the size of a resource.

Timing attacks in modern web

- Basic version: Image object is useful.

```
var img = new Image();
img.onerror = function() {
  var end = window.performance.now();
  alert('Result: ' + (end - start));
};
var start = window.performance.now();
img.src = 'http://example.org/dashboard.php';
```

- The image src is set to be an HTML page, which will eventually result in error when the image object parses it.
- The onError function will always be called

Advanced versions of timing attack in web

- Using audio or video object instead of image.

Advanced versions of timing attack in web

- Use audio or video object instead of image. (HTML5 feature)
- Use ApplicationCache: attacker can force an external resource to be cached
  - Although reading a small file takes less than 1ms, the size of a file still has measurable influence on reading from cache.

Advanced versions of timing attack in web

- Use audio or video object instead of image. (HTML5 feature)
- Use ApplicationCache: attacker can force an external resource to be cached
  - Although reading a small file takes less than 1ms, the size of a file still has measurable influence on reading from cache.
- Use Service Worker: allow time measuring even after user closes browser
  - Service Worker: event-driven scripts whose lifetime is independent of the webpage
  - Use Fetch API to perform network requests, can make authenticated requests without CORS
  - A process running in background

Advanced versions of timing attack in web

- Use audio or video object instead of image. (HTML5 feature)
- Use ApplicationCache (modern browser feature): attacker can force an external resource to be cached
  - Although reading a small file takes less than 1ms, the size of a file still has measurable influence on reading from cache.
- Use Service Worker: allow time measuring even after user closes browser
  - Service Worker: event-driven scripts whose lifetime is independent of the webpage (A process running in background)
  - The time it takes to put a resource in cache and remove it from cache can be used by attacker.
- Use script parsing

Performance of different timing attacks in web

- Performance of these timing attacks:

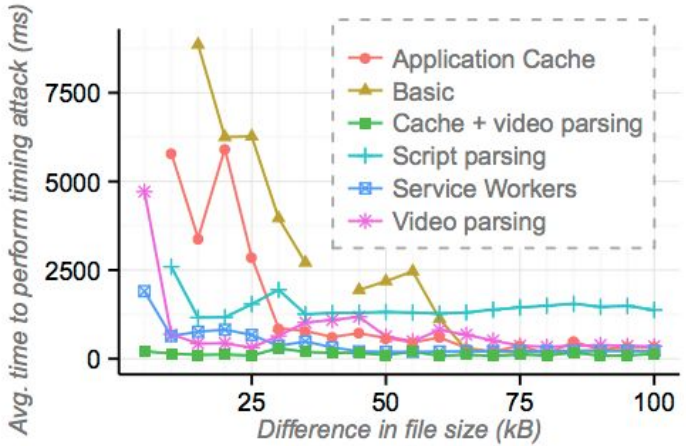
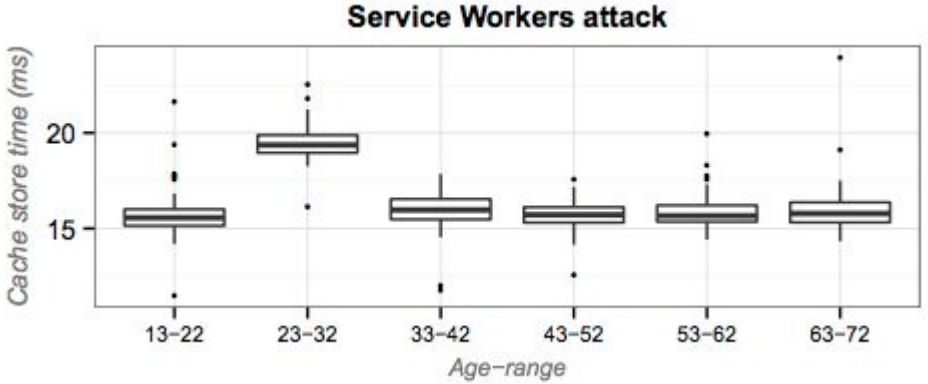


Figure 2: The average time required to perform a cross-site timing attack with 95% accuracy, for each type of web-based timing technique.

Discussion: real-world timing attacks

- Facebook: Age, Gender and Location may be leaked by phishing
  - Facebook page can post to a specific group of users (age 20-30/female only/etc.)
  - Page can post several times with different user group, where the content is a permanent phishing website URL, and different targeted user will see different URL.
  - After the user gets into the website, timing attacks can be performed against private info..



Discussion: real-world timing attacks

- LinkedIn: Contact Search
  - If a user has many connections from Germany, then he or she is likely living in Germany.
  - Query for contacts uses XMLHttpRequest(XHR) and JSON stream, response size depends on the connection numbers.,
  - Timing attack can measure and estimate the number of connections

Discussion: real-world timing attacks

- Twitter: Protected accounts
- Google and Amazon: Search History can be investigated
- Many more...

Discussion: defensive approaches

- Randomized accessing time implemented on browser (client-side)
  - But that may affect performance
- Server side CSRF countermeasures
- What else?

Discussion: Significance

- The above examples show that timing attack can be very harmful toward our private information

Discussion: Significance

- The above examples show that timing attack can be very harmful toward our private information
- However, not a bad way for big data companies/institutions to obtain data.
  - Very crucial in researches.
  - May actually improve people’s life..

Discussion: Significance

- The above examples show that timing attack can be very harmful toward our private information
- However, not a bad way for big data companies/institutions to obtain data.
  - Very crucial in researches.
  - May actually improve people’s life..
- The question is: privacy information or machine learning benefits?

Future Works on Timing attack

- Effective and efficient defensive approaches (Is that possible?)
- The ethical question

Questions?