Distributed computing as a client-side attack

DEFCON Russia, DCG-7812

21/02/2013 Saint-Petersburg, Yandex

Browsers security basics

- Same Origin Policy
- Content Security Policy
- SSL/PKI features

  . . .

- And what about PC resources ?

Resources which available to site through browser

- CPU/GPU utilization
- RAM
- Local storages
- Network connections

Resources which available to site through browser

- CPU/GPU utilization
- RAM
- Local storages
- ~~Network connections~~ <- nothing new

Distributed computing in browsers not so new theme

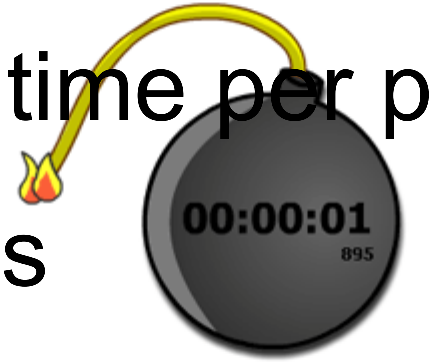
- Browser-based distributed evolutionary computation: performance and scaling behavior [2007]
  - http://dl.acm.org/citation.cfm?id=1274083
- Unwitting distributed genetic programming via asynchronous JavaScript and XML [2007]
  - http://dl.acm.org/citation.cfm?id=1277282

But its may be used as a client-side attack

- XSS
- CSRF
- SWF malware via ad-networks
- Cache-poisoning
- CDN hacks

CPU/GPU usage restrictions

- Max execution time per page
- Freeze timeouts
- Problems for user (cursor freeze, etc)

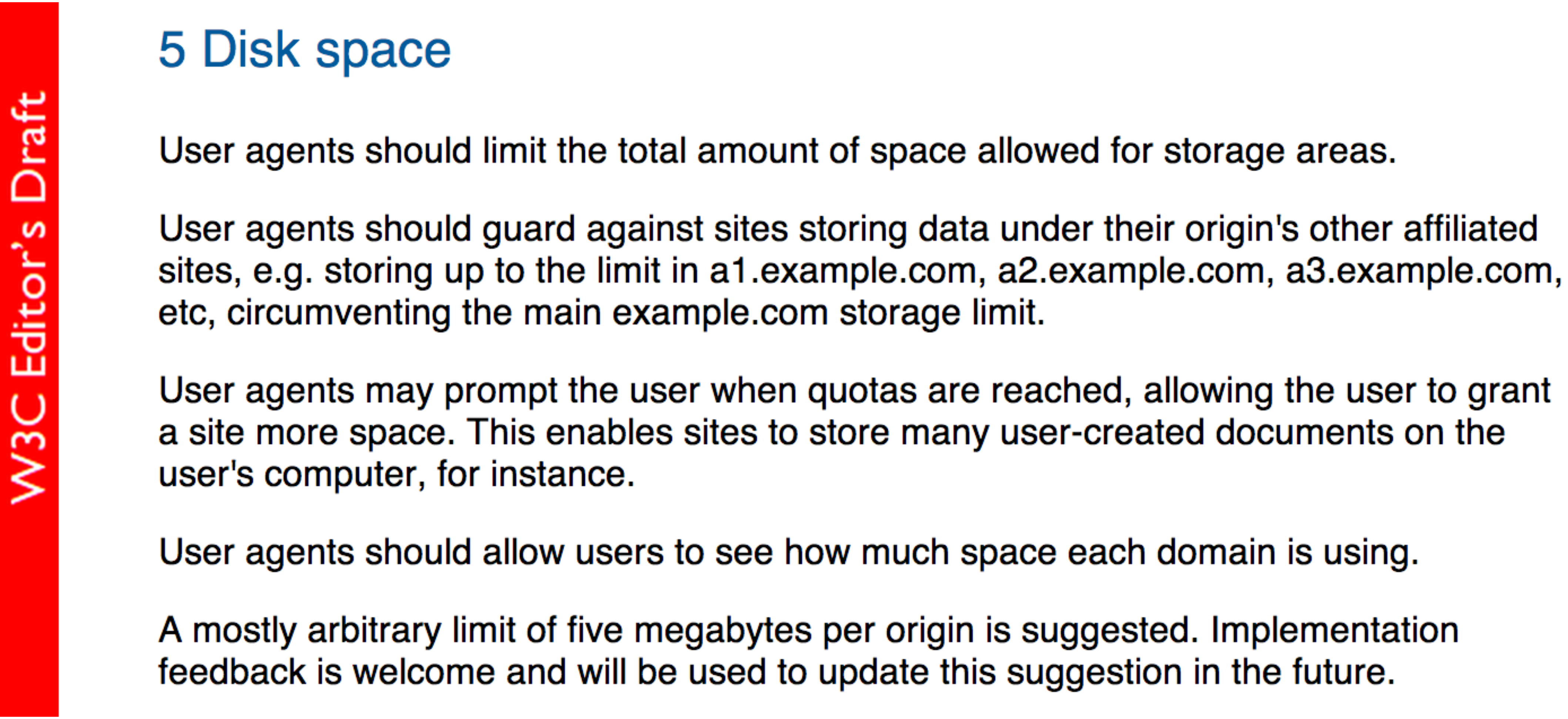


CPU/GPU usage restrictions bypasses

- Web workers
- Low content transferring
- Distracting user's attention (i.e. video)

- Classic COOKIES
- Web Storage (HTML5, localStorage, sessionStorage objects)
- FileAPI (HTML5)
- Flash Local Shared Objects (LSO, flash cookies)

Local storages restrictions



5 Disk space

User agents should limit the total amount of space allowed for storage areas.

User agents should guard against sites storing data under their origin's other affiliated sites, e.g. storing up to the limit in a1.example.com, a2.example.com, a3.example.com, etc, circumventing the main example.com storage limit.

User agents may prompt the user when quotas are reached, allowing the user to grant a site more space. This enables sites to store many user-created documents on the user's computer, for instance.

User agents should allow users to see how much space each domain is using.

A mostly arbitrary limit of five megabytes per origin is suggested. Implementation feedback is welcome and will be used to update this suggestion in the future.

Local storages restrictions

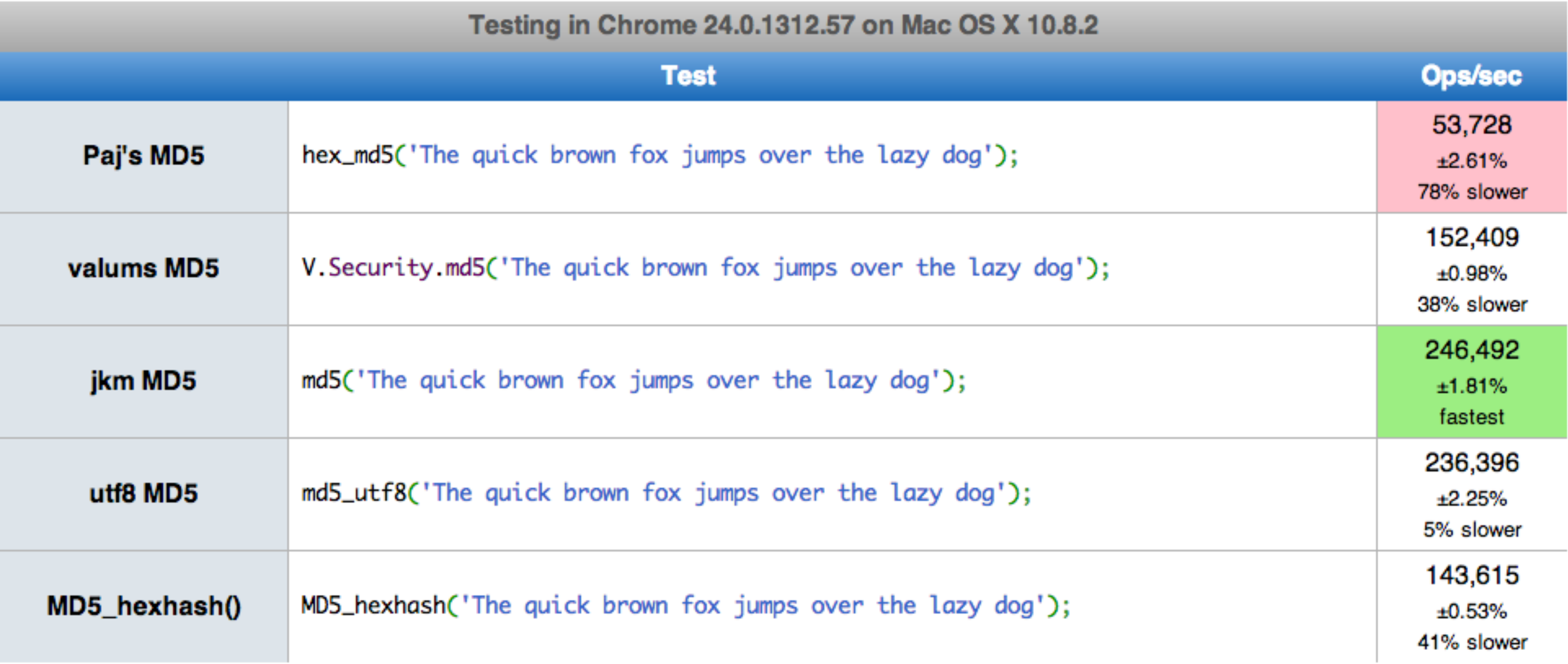
- Flash Local Shared Objects (LSO, flash cookies): 50Kb per domain
- Freeze timeout
- Problems for user (cursor freeze, etc)

Where i can store my rainbows?

- 100'000 subdomains
  - 10'000 * 50Kb = 5Gb per each client's browser (5-10 minutes to fill it)
- 500 unique visitors on your blog
  - 500 * 5Gb = 2.5Tb data for you ;)

How fast JavaScript?

- MD5 (http://jsperf.com/md5-shootout)
- MacBook Air mid 2011 http://support.apple.com/kb/SP631



Testing in Chrome 24.0.1312.57 on Mac OS X 10.8.2

Test		Ops/sec
Paj's MD5	`hex_md5('The quick brown fox jumps over the lazy dog');`	53,728 ±2.61% 78% slower
valums MD5	`V.Security.md5('The quick brown fox jumps over the lazy dog');`	152,409 ±0.98% 38% slower
jkm MD5	`md5('The quick brown fox jumps over the lazy dog');`	246,492 ±1.81% fastest
utf8 MD5	`md5_utf8('The quick brown fox jumps over the lazy dog');`	236,396 ±2.25% 5% slower
MD5_hexhash()	`MD5_hexhash('The quick brown fox jumps over the lazy dog');`	143,615 ±0.53% 41% slower

JavaScript vs HD6990

- AMD Radeon HD6990 + oclHashcat-lite:
  - 11*10^9 ops/sec
- MacBook Air mid 2011 + jkm JS + Chrome 24.0.1312

ess than 5*10^4 times)

=

x 50'000

How fast Flash?

http://www.blooddy.by/ru/crypto/benchmark/

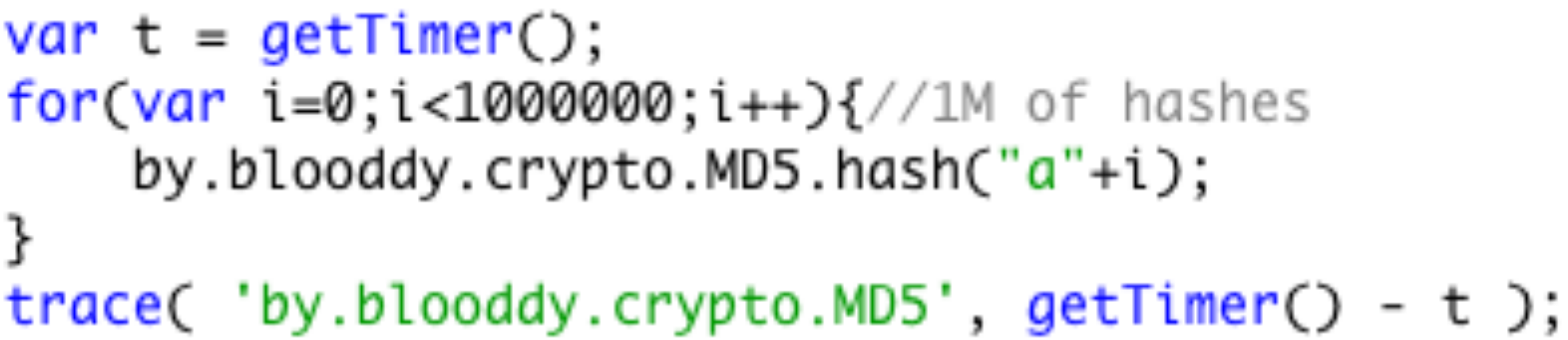
- SHA-256
    - mx.utils.SHA256
    - as3corelib
    - blooddy
- MD5
    - as3corelib
    - blooddy

How fast Flash?

http://www.blooddy.by/ru/crypto/benchmark/

- SHA-256
  - mx.utils.SHA256
  - as3corelib
  - blooddy [x8 faster]
- MD5
  - as3corelib
  - blooddy [x10 faster]

How fast Flash?

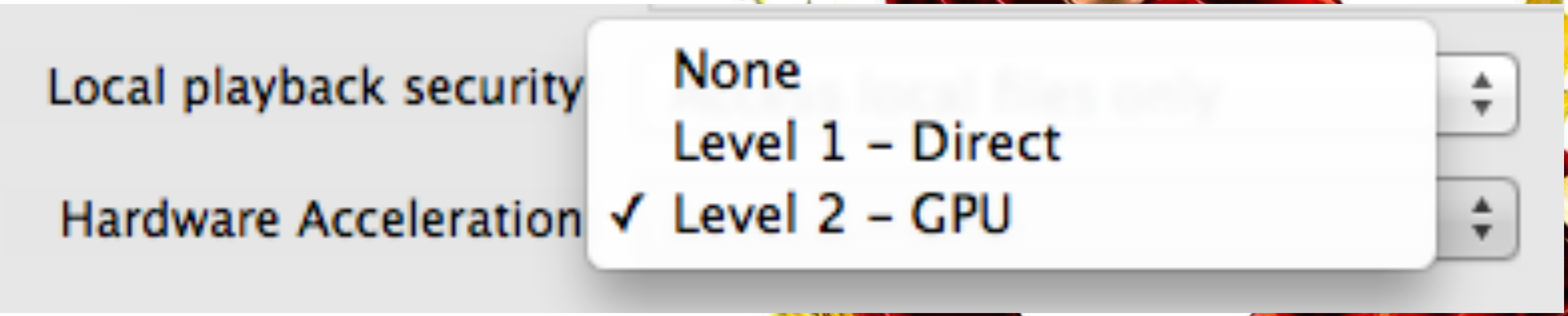


```
var t = getTimer();
for(var i=0;i<1000000;i++){//1M of hashes
    by.blooddy.crypto.MD5.hash("a"+i);
}
trace( 'by.blooddy.crypto.MD5', getTimer() - t );
```

How fast Flash?

Make it faster using optimization! Or not :)))

- None - 1,7*10^5 ops/sec
- Level 1 - 1,7*10^5
- Level 2 - 1,7*10^5



Local playback security

Hardware Acceleration

None
Level 1 – Direct
✓ Level 2 – GPU

???

@ONsec_Lab [http://lab.ONsec.ru]
@d0znpp

d0znpp@onsec.ru

ONSEC.