

Hackers Are Ready. Are You?

H@cker | Halted

TM
USA
2009



So Long, and Thanks For All the Clock Cycles

Greg Ose – gose@neohapsis.com

Cris Neckar – cneckar@neohapsis.com

 NEOHAPSIS

What is XSS? Really...

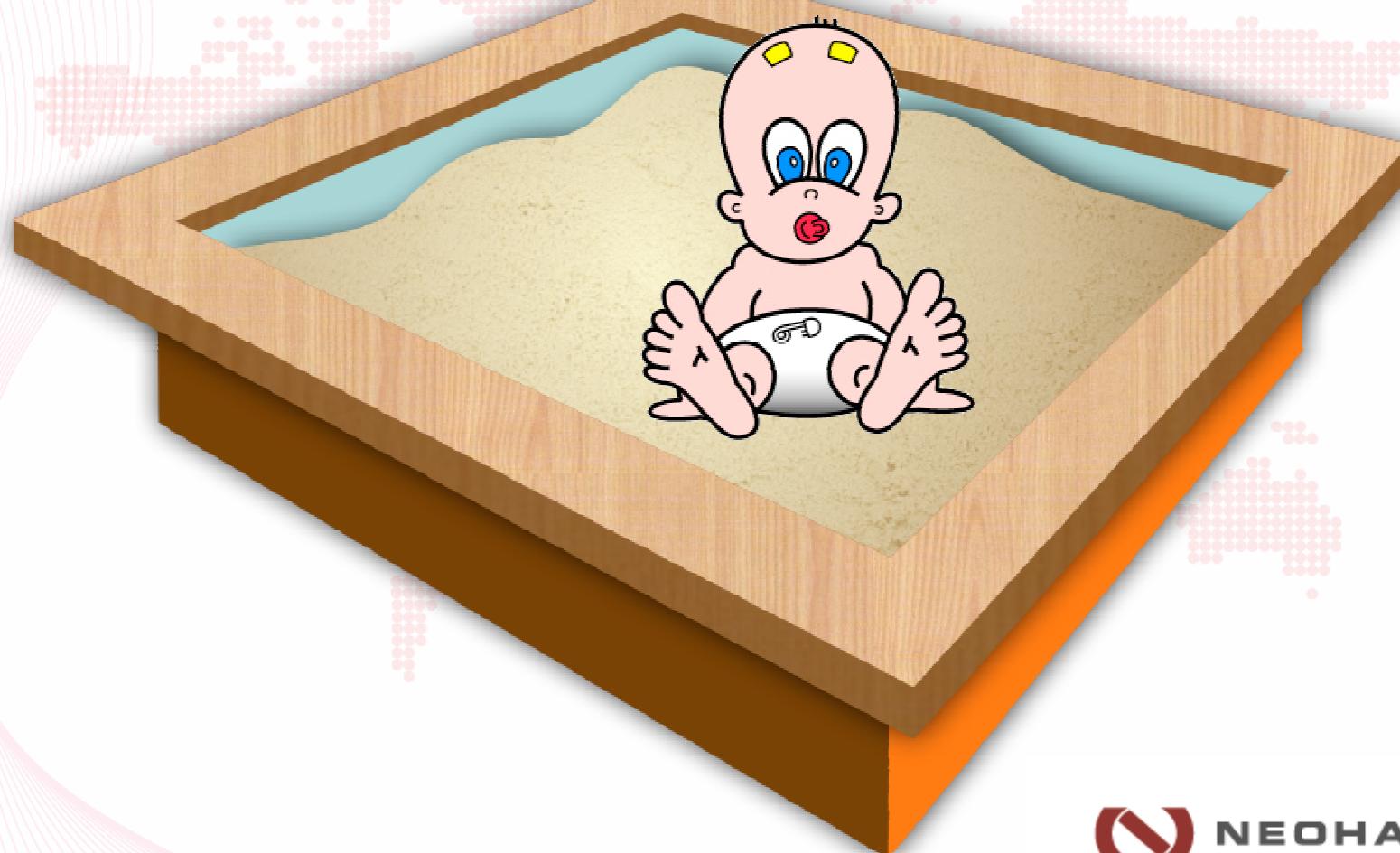
- The browser is the first ubiquitous client application that accepts and carries out tasks assigned by a server.
- The ability of an attacker to control content that will be interpreted in some way in the client application of another user
- This alone does not constitute a vulnerability (you have to be able to do something with it)
- This class of ‘vulnerability’ has been highly publicized but they are still everywhere

Hackers Are Ready. Are You?

H@cker | Halted

TM
U S A
2009

Does XSS Matter?



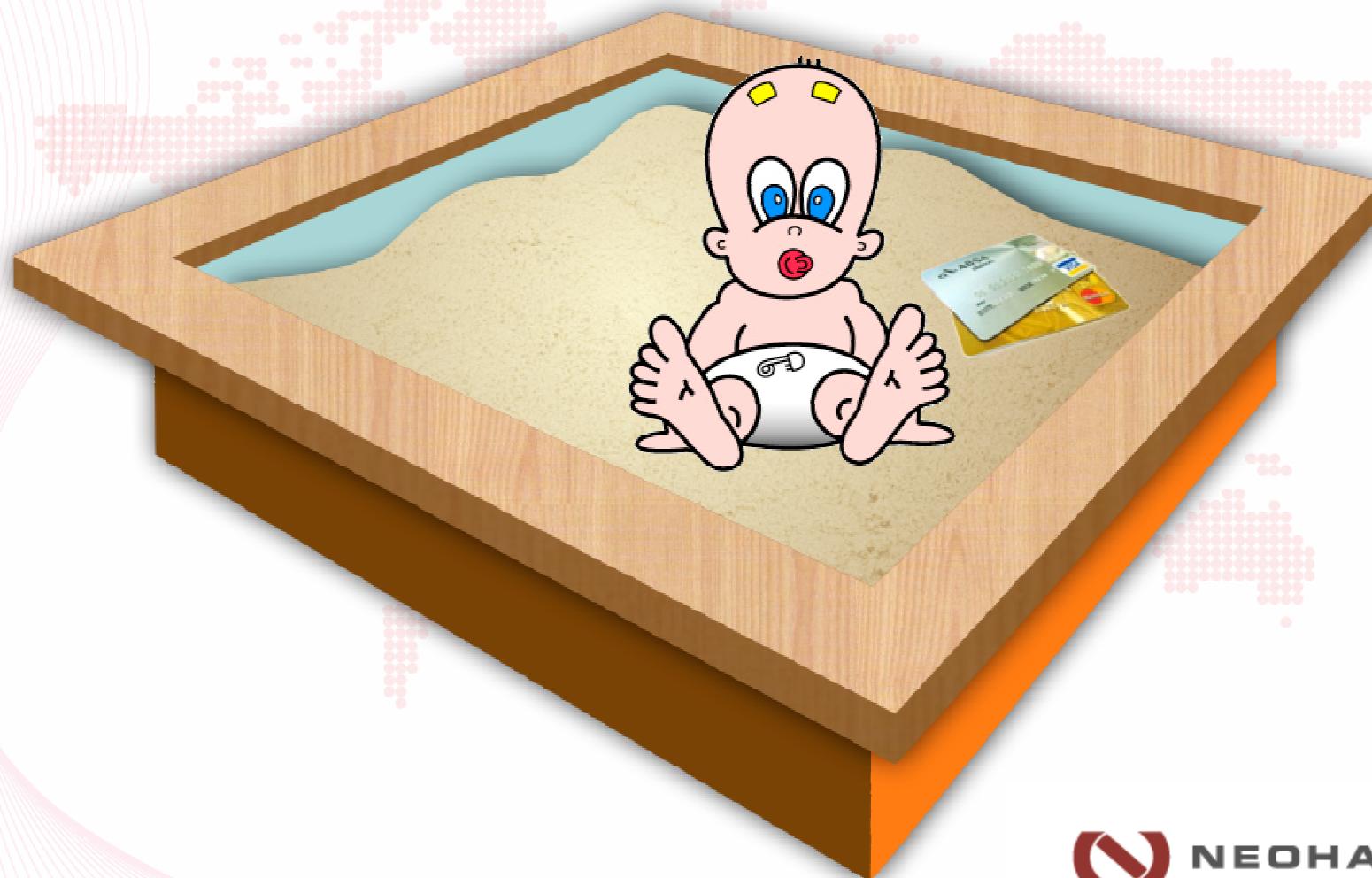
 NEOHAPSIS

Hackers Are Ready. Are You?

H@cker | Halted

TM
U S A
2009

In some cases... Yes...



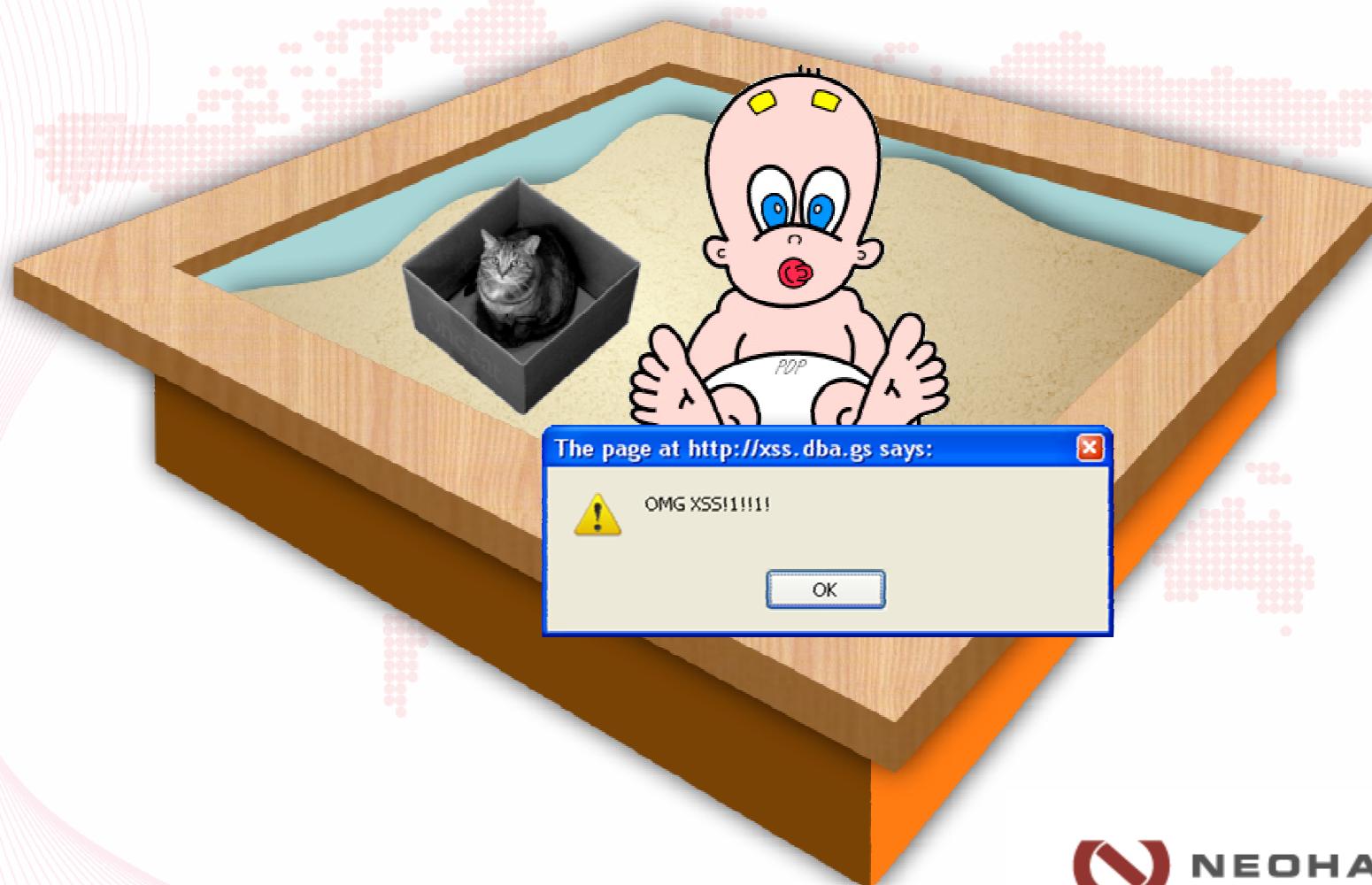
 NEOHAPSIS

Hackers Are Ready. Are You?

H@cker | Halted

TM
U S A
2009

Generally... Not so much...



 NEOHAPSIS

The Protections in Place

- Browser based filtering
 - Checks request against response and does not interpret scripts that are present in both.
 - Only works against reflective
- HTTPOnly cookies
 - Prevents cookies from being accessed from scripting language
 - Prevents session hijacking but not content grabbing
- Re-authentication or CAPTCHAs in front of important functionality or content
 - Effective but annoying
 - Think Microsoft's UAC
- New standards are defining much more configurable policy
 - <http://dev.w3.org/2006/waf/access-control/>

Hackers Are Ready. Are You?

H@cker | Halted

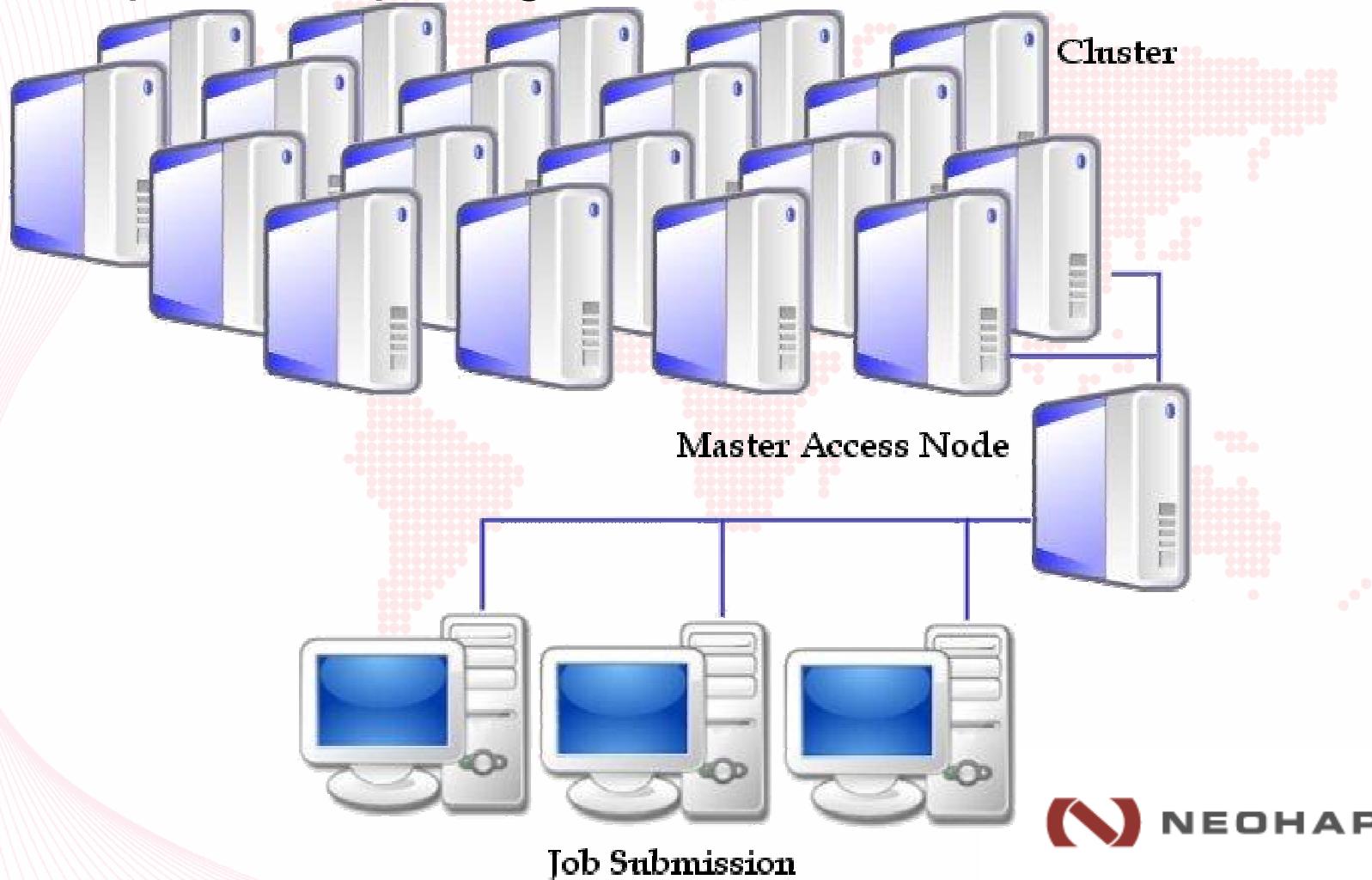
TM
U S A
2009

What is in YOUR sandbox?



 NEOHAPSIS

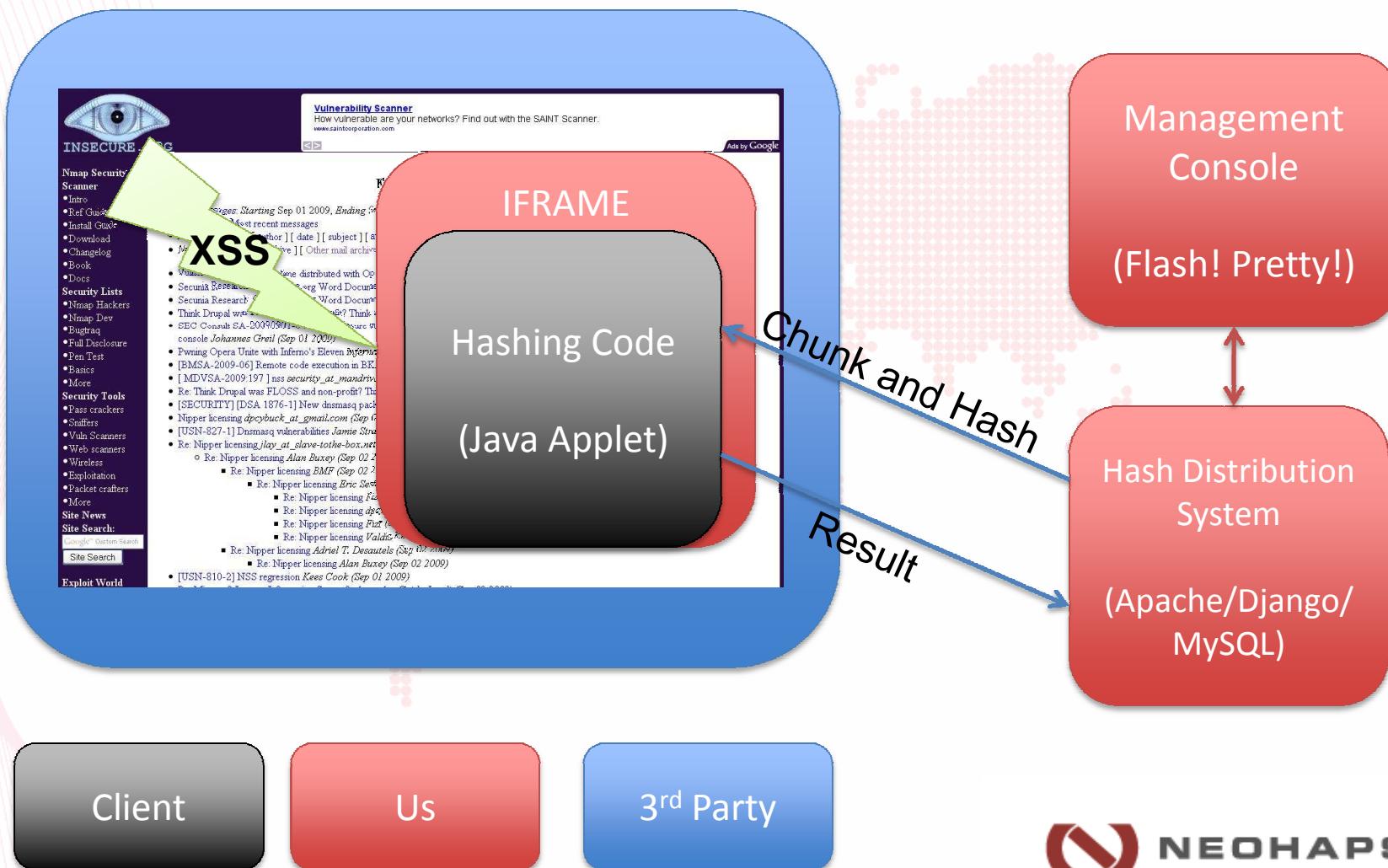
And Now for Something Completely Different: Super Computing Architecture



Implementing a crowd-sourced super(ish) computer

- The task - Password brute forcing
 - Crypt and MD5-crypt
 - Easy to distribute (well kind of)
 - Decent sized computable chunks
- The client-side language
 - JavaScript – Very web 2.0, but way too slow
 - Flash – Still too slow
 - Native Client – Wouldn't that be nice
 - Java – A good balance and some interesting tricks we can use

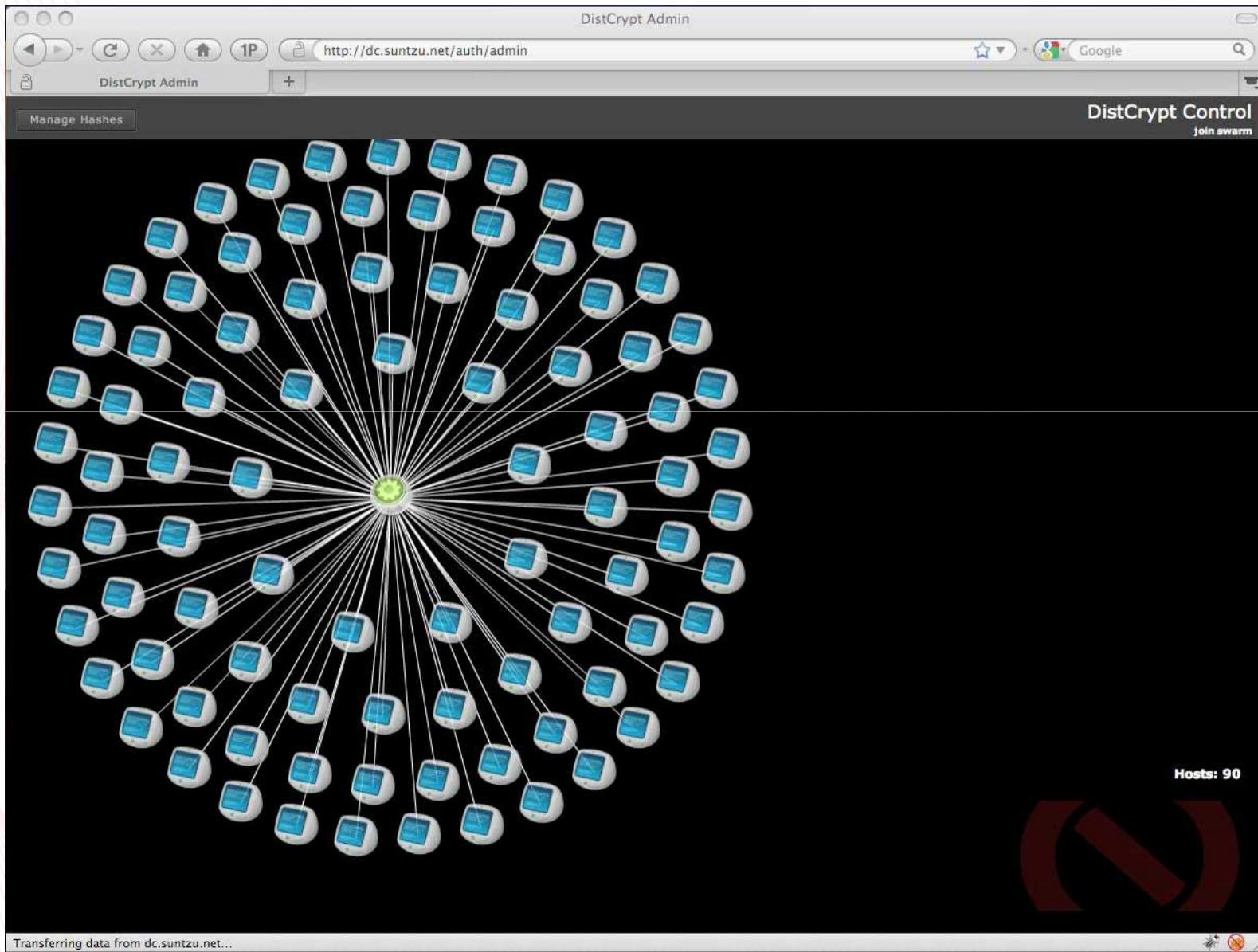
The Architecture



Hackers Are Ready. Are You?

H@cker | Halted

TM
USA
2009



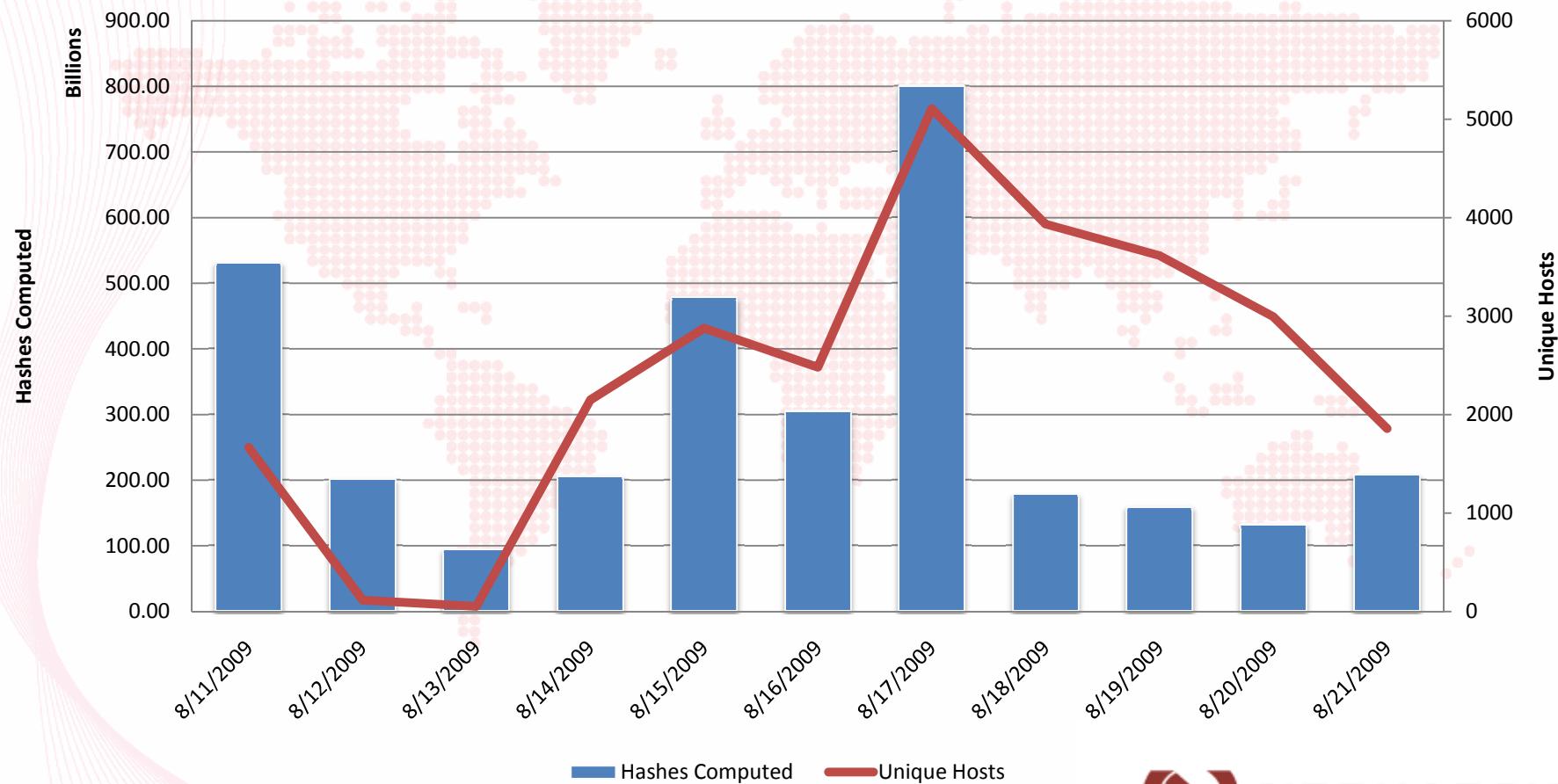
Hackers Are Ready. Are You?

H@cker | Halted

TM
USA
2009

Results

Distributed Computation on archives.neohapsis.com

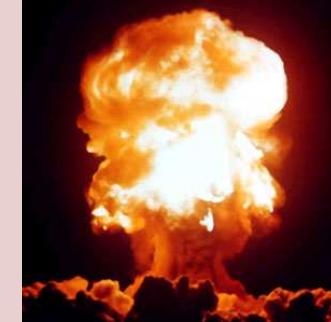


 NEOHAPSIS

Hackers Are Ready. Are You?

H@cker | Halted

TM
U S A
2009

Example	Rate (hashes / sec)	Concurrent Hosts	Total Rate (hashes / sec)
John the Ripper	889,087	1	889,087
archives.neohapsis.com	41,529	100	4,152,900
boards.ign.com	41,529	8,400	348,843,600
4chan	41,529	30,000	1,245,870,000
Facebook	41,529	1,000,000	

Other Interesting Stats

- 26,010 unique hosts with an average of 178 chunks computed
- There were 14,259 hosts with < 5 chunks computed
- Average of 432 chunks computed for hosts with > 5 chunks
- Average user has 2.0281 CPUs
- Some people just don't close their browsers
- **Even people in the security industry don't know what their browser is doing**
- Or how to opt out of things

The Future

- Robust systems for arbitrary computation
 - Folding/SETI@home
 - BOINC - <http://boinc.berkeley.edu/>
- Real-world exploitation
 - Rampant drive-by SQL injections -> Stored XSS
 - Vulnerabilities in popular software spanning numerous sites
 - Using JVM tricks short term visits turn into semi-permanent clients
 - generic forced redirection, submissions to link aggregators