



Clobbering the Cloud!

{ haroon | marco | nick }

@sensepost.com

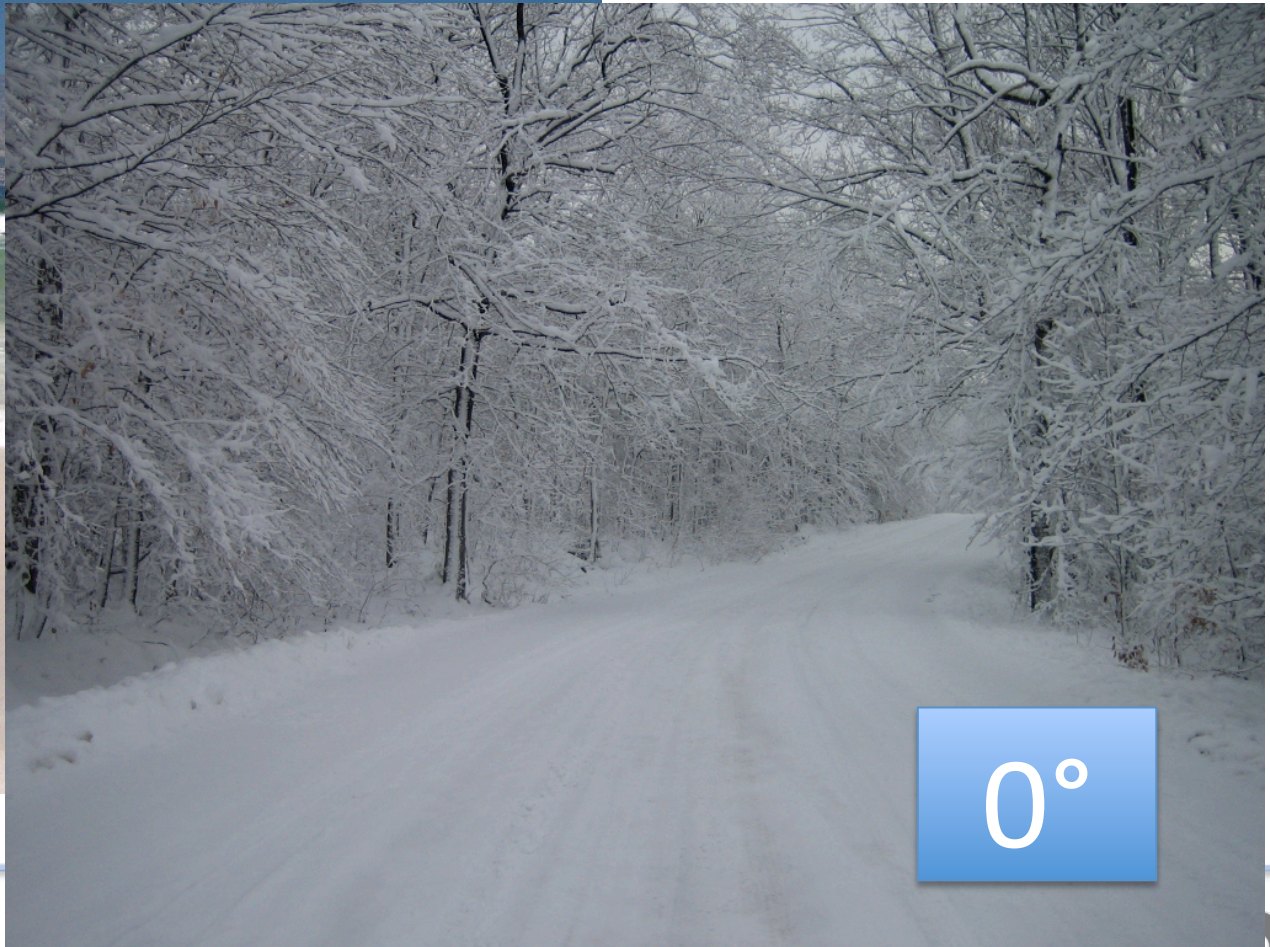
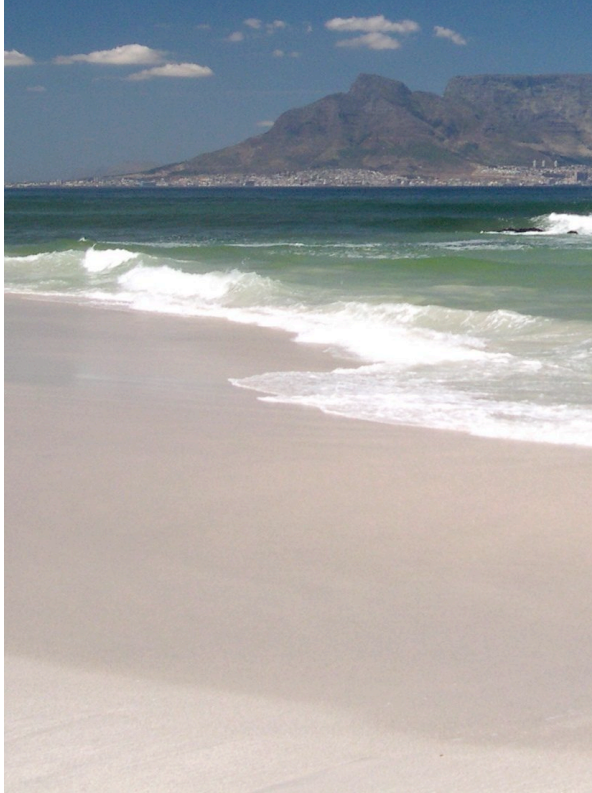
about: us



{ Haroon Meer | Marco Slaviero | Nicholas Arvanitis }



40°



0°

Why this talk ?



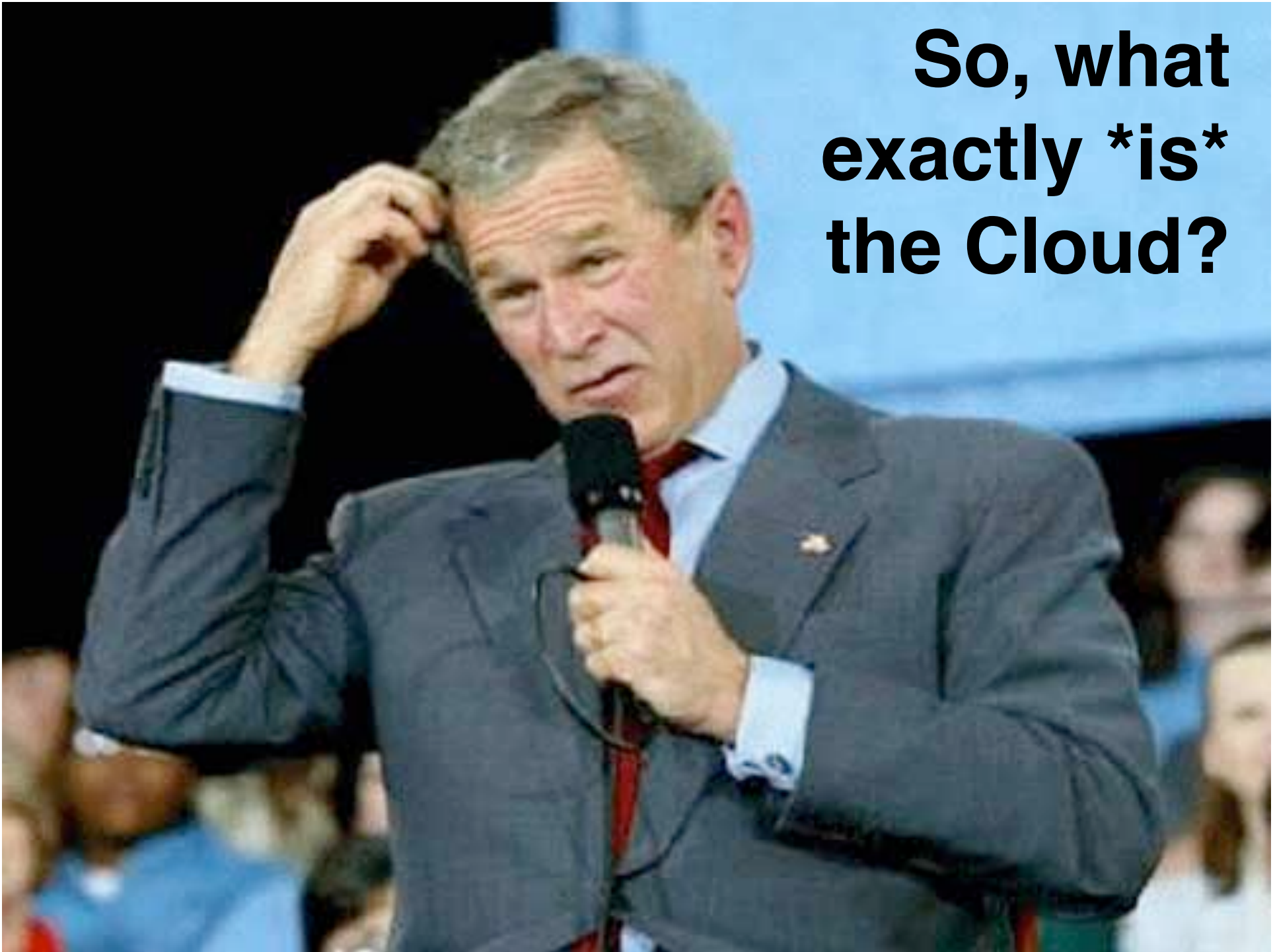
This is not the time to split hairs



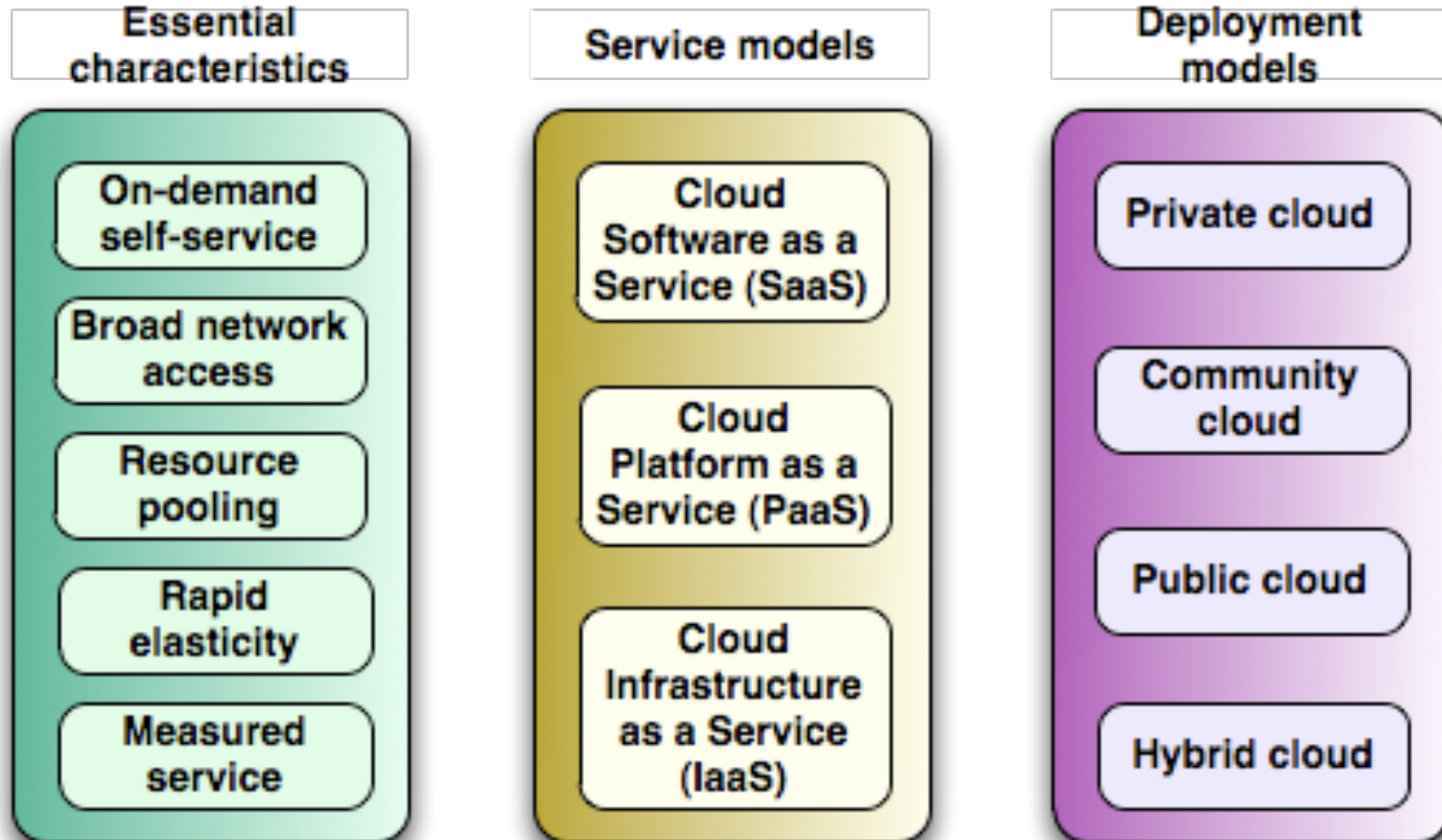
The LOUD in cLOUD security..

- A bunch of people are talking about “the cloud”
- There are large numbers of people who are immediately down on it:
- “There is nothing new here”
- “Same old, Same old”
- If we stand around splitting hairs, we risk missing something important..

**So, what
exactly *is*
the Cloud?**

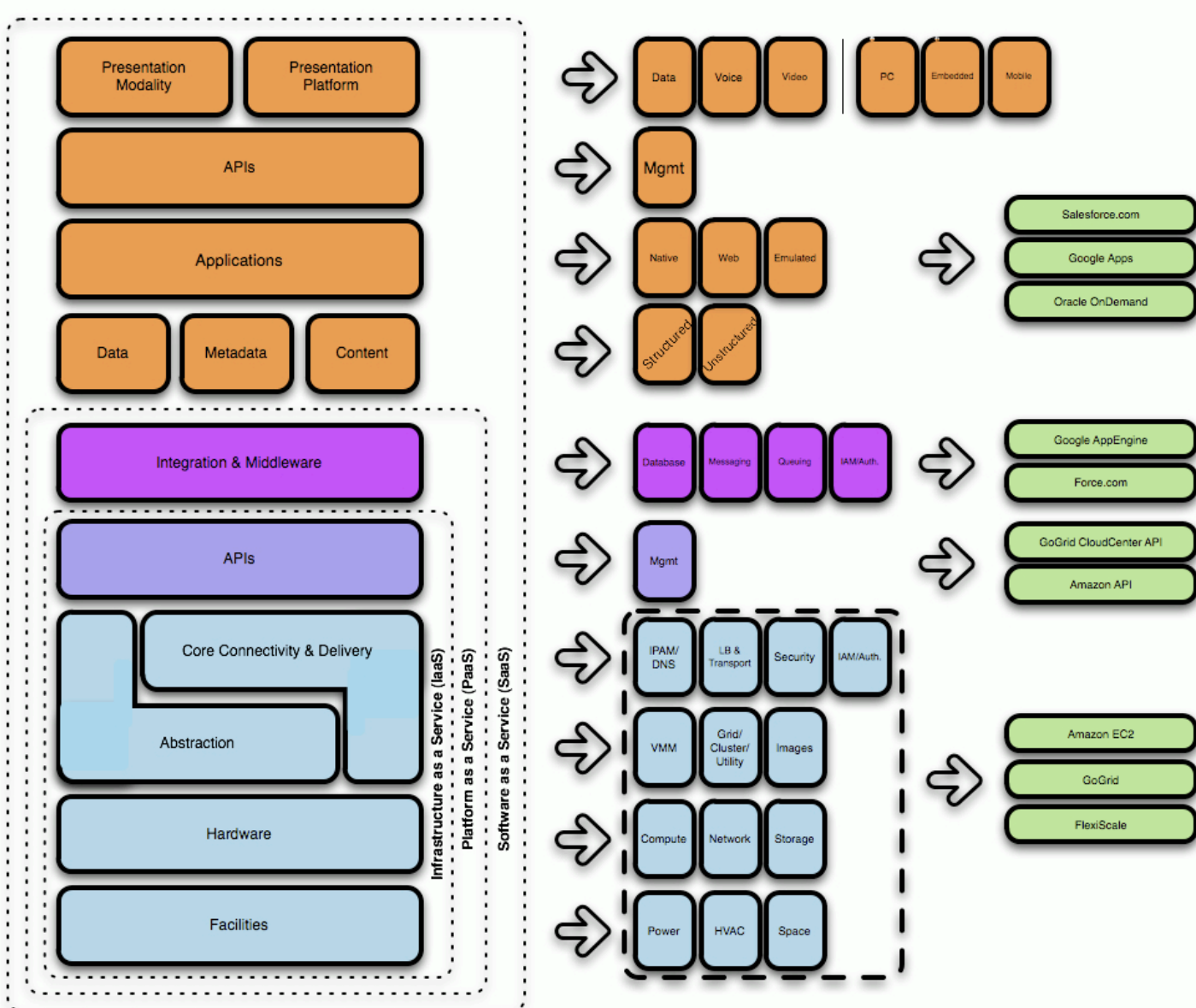


Cloud delivery models



<http://csrc.nist.gov/groups/SNS/cloud-computing/>

Cloud components



Cloud players

Infrastructure Services

Storage

- Amazon S3
- Zetta
- CTERA Portal
- Mosso Cloud Files
- Nirvanix

Compute

- Amazon EC2
- Serve Path GoGrid
- Elastra
- Mosso Cloud Servers
- Joyent Accelerators
- AppNexus
- Flexiscale
- ElasticHosts
- Hosting.com CloudNine
- Terremark
- GridLayer
- ITRICITY
- LayeredTech

Services Management

- Scalr
- CohesiveFT
- Ylastic
- Dynect
- CloudFoundry
- NewRelic
- Cloud42

Cloud Brokers

- RightScale
- enStratus
- Kaavo
- Elastra
- CloudKick
- CloudSwitch

Cloud Software

Data

- 10Gen MongoDB
- Oracle Coherence
- Gemstone Gemfire
- Apache CouchDb
- Apache HBase
- Hypertable
- TerraCotta
- Tokyo Cabinet
- Cassandra
- memcached
- Infinispan

Compute

- Globus Toolkit
- Xeround
- Beowulf
- Sun Grid Engine
- Hadoop
- OpenCloud
- Gigaspace
- DataSynapse
- Xeround

Cloud Management

- 3Tera App Logic
- OpenNebula
- Open.ControlTier
- Enomaly Enomalism
- Altor Networks
- VMware vSphere
- OnPathTech
- CohesiveFT VPN Cubed
- Hyperic
- Eucalyptus
- Reductive Lbs Puppet
- OpenQRM
- Appistry
- VMWare VCloud Express

File Storage

- EMC Atmos
- ParaScale
- Zmamba
- CTERA

Appliances

- PingIdentity
- Simplified
- rPath
- Vordel

CLOUD TAXONOMY

Platform Services

General Purpose

- Force.com
- Etelos
- LongJump
- AppJet
- Rollbase
- Bungee Labs Connect
- Google App Engine
- Engine Yard
- Caspio
- Qrimp
- MS Azure Services Platform
- Mosso Cloud Sites

Business Intelligence

- Aster DB
- Quantivo
- Cloud9 Analytics
- Blink Logic
- K2 Analytics
- LogiXML
- Oco
- Panorama
- PivotLink
- Clario Analytics
- ColdLight Neuron
- Infobright
- Vertica

Integration

- Amazon SQS
- MuleSource Mule OnDemand
- Boomi
- SnapLogic
- OpSource Connect
- Cast Iron
- Microsoft BizTalk Services
- gnip
- SnapLogic SaaS Solution Packs
- Appian Anywhere
- HubSpan
- Informatica On-Demand

Development & Testing

- Keynote Systems
- Mercury
- SOASTA
- SkyTap
- Aptana
- LoadStorm
- Collabnet
- Dynamsoft

Database

- Google BigTable
- Amazon SimpleDB
- FathomDB
- Microsoft SDS

Software Services

Billing

- Aria Systems
- eVapt
- OpSource
- Redi2
- Zuora

Financials

- Concur
- Xero
- Workday
- Beam4d

Legal

- DirectLaw
- Advologix
- Fios
- Sertifi

Sales

- Xactly
- LucidEra
- StreetSmarts
- Success Metrics

Desktop Productivity

- Zoho
- IBM Lotus Live
- Google Apps
- HyperOffice
- Microsoft Live
- ClusterSeven

Human Resources

- Taleo
- Workday
- ICIMS

Content Management

- Clickability
- SpringCM
- CrownPoint

Backup & Recovery

- JungleDisk
- Mozy
- Zmanda Cloud Backup
- OpenRSM
- Syncplicity

CRM

- NetSuite
- Parature
- Responsys
- Rightnow
- Salesforce.com
- LiveOps
- MSDynamics
- Oracle On Demand

Document Management

- NetDocuments
- Questys
- DocLanding
- Aconex
- Xyθος
- Knowledge TreeLive
- SpringCM

Collaboration

- Box.net
- DropBox

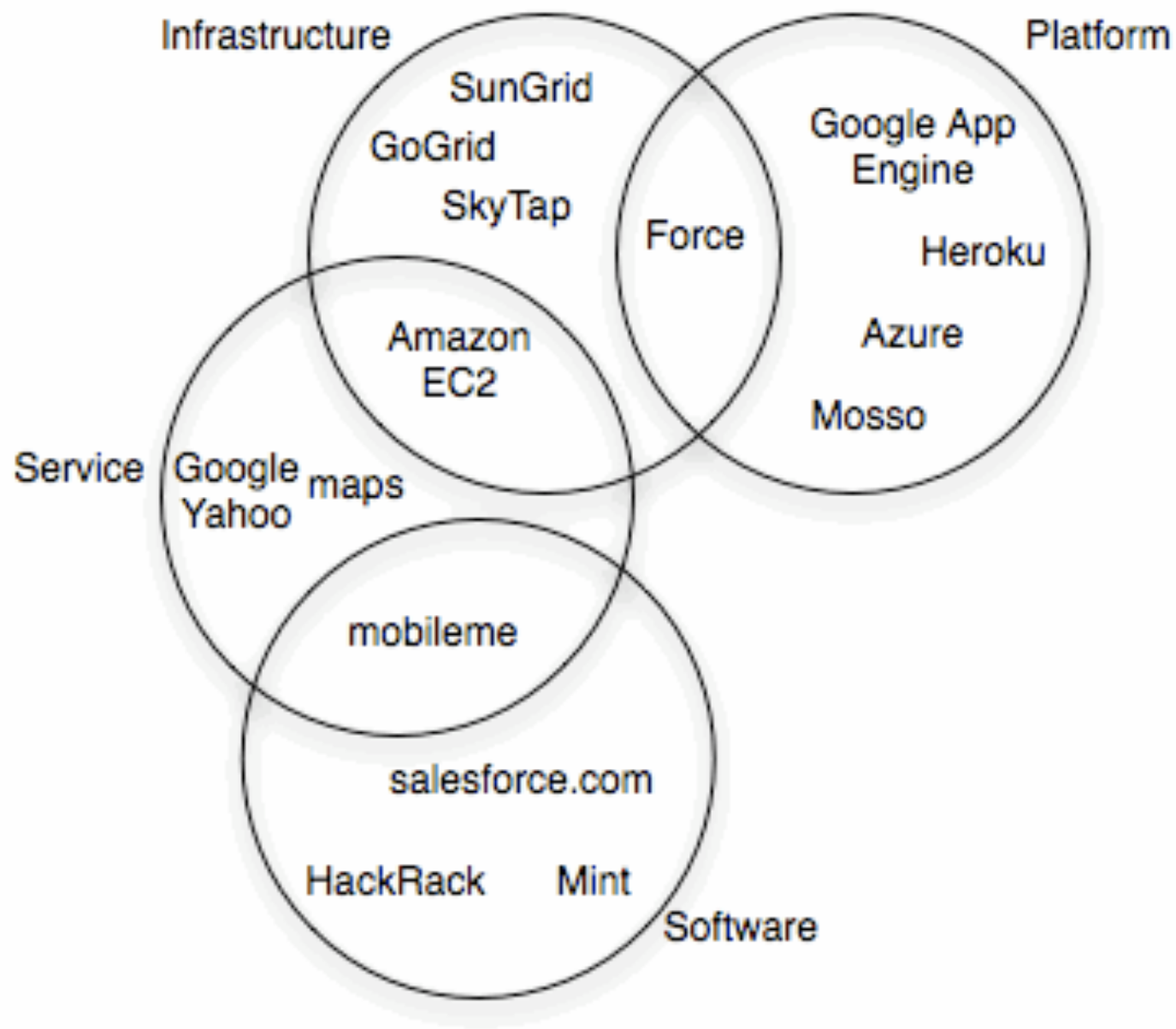
Social Networks

- Ning
- Zembyl
- Amitive



Updated as of September 30, 2009





Why would we want to break it?

- It will be where the action is..
- Insidious the dark side is..
- Amazingly we are making some of the same old mistakes all over again
- We really don't have to be making these mistakes..

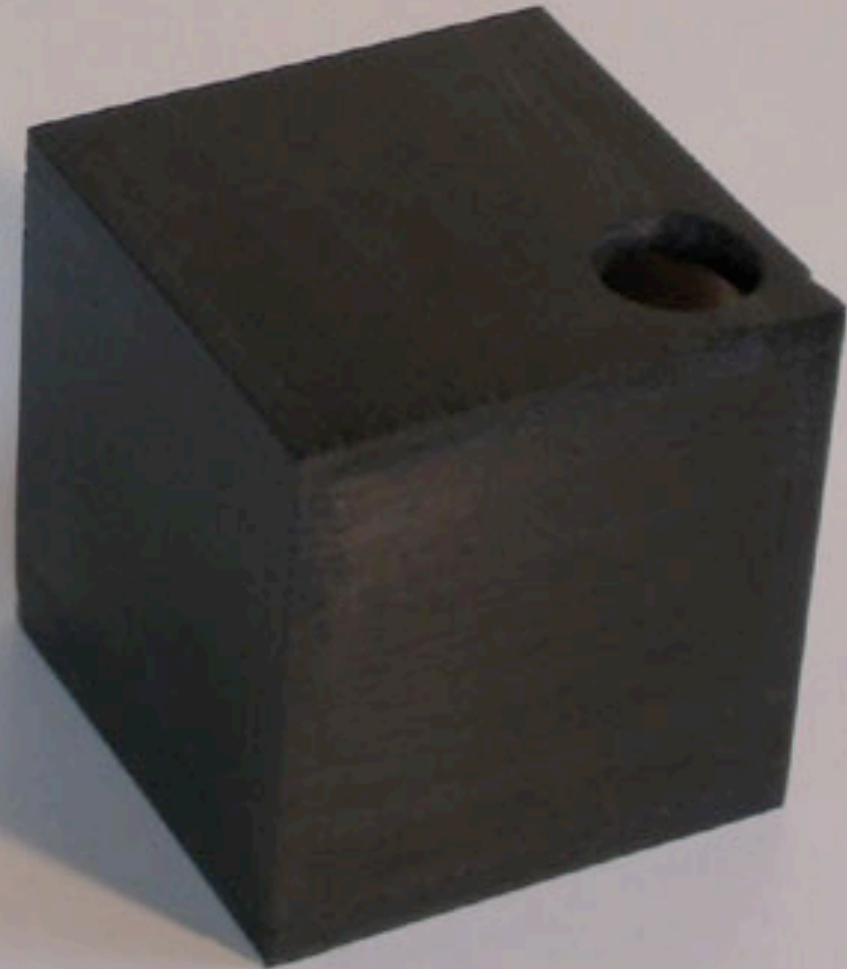
What is driving Cloud adoption?

- Management by in-flight magazine
 - Manager Version
 - Geek Version
- Poor history from IT
 - “Cloud Computing can be seen as the business units' final revenge on IT (and security) for saying ‘no’ one time too many, taking too long, or costing too much.” - Ranum
- Economy is down
 - Cost saving becomes more attractive
 - Cloud computing allows you to move from CAPEX to OPEX
 - (Private Clouds?)

A really attractive option

- EC2 is Cool!
- Like Crack..

Problems testing the Cloud



Transparency

The problem, more than anything else, is a
would have spoken up against it – but Amazon
works or what kinds of control the company

Why has Amazon been less transparent than
Amazon controls the whole system. System
to tell the third-party developers how the system
conflict with third-party applications. Alternatives
than (say) a PC. Less functionality means fear for
themselves.

Going forward, Amazon will face more pressure
with Kindle buyers. It seems that e-books are



known that this sort of thing were possible, they
does offer clear descriptions of how the product

one offer two conjectures. It might be because
to be more open, in the sense that they have
sure to avoid gratuitous changes that might
because the Kindle offers less functionality
need as much information to protect

technology and the company's relationship
free books.

cloudsecurity.org: Trust is often cited as a barrier to enterprise adoption of Cloud Computing. What role do you personally think Google can play in building that trust?

cloudsecurity.org: How do you contain an attacker that exploits bugs in App Engine from exploiting the underlying OS and potentially interfering with other users processes or attacking backend systems?

G
n

GvR: You are correct that there are strong measures in place, but I'm not at liberty to discuss details.

Compliance in the Cloud

“If its non-regulated data, go ahead and explore. If it is regulated, hold on. I have not run across anyone comfortable putting sensitive/regulated data in the cloud”

“doesn’t seem to be there as far as comfort level that security and audit aspects of that will stand up to scrutiny” (sic)

-- *Tim Mather: RSA Security Strategist*

Version 1.3 expected late this year

Privacy and legal issues



Privacy

- Jim Dempsey (Center for Democracy and Technology): “Loss of 4th Amendment protection for US companies”
- A legal order (court) to serve data, can be used to obtain your data without any notification being served to you
- There is no legal obligation to even inform you it has been given

Simple solution..

Crypto Pixie Dust!



Would you trust crypto on an owned box ?

Vendor Lock-in

- Pretty self-explanatory
- If your relationship dies, how do you get access to your data ?
- Is it even your data ?

flickr®



Availability [Big guys fail too?]

The screenshot shows a web browser window with the title "Pardon The Dust - SugarSync". The address bar contains "http://sugarsync.com/". The page header features the SugarSync logo and the tagline "SYNC WITH BENEFITS". The main content area displays a light blue message box with the following text:

We're performing routine maintenance & updating our site and will be back online shortly.
This maintenance window will last from 6PM PDT to 9PM PDT. During this time, all your data is 100% secure.

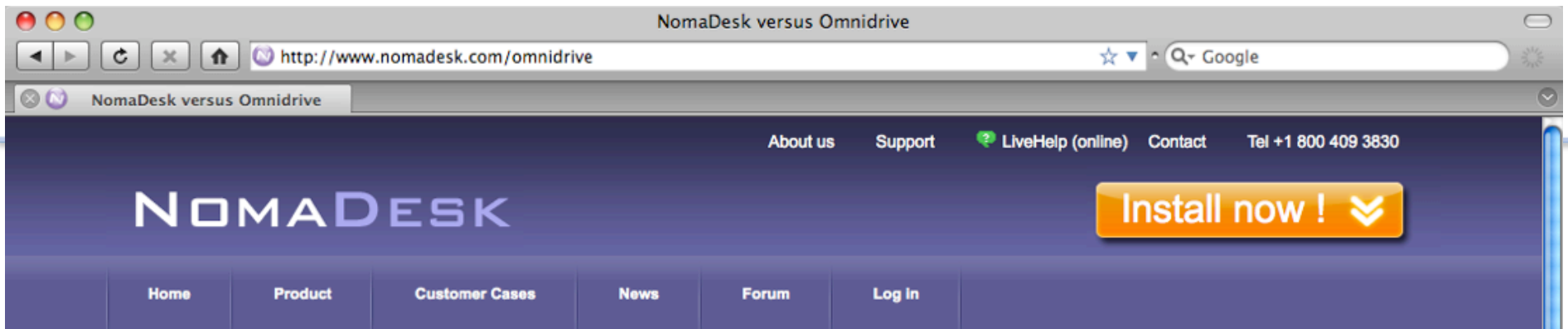
Sorry for any inconvenience.

At the bottom of the page, there is a copyright notice: "© 2009 Sharpcast, Inc. All Rights Reserved."

Read-only mode continues. Elevated latency and error-rates persist for Datastore reads. Memcache writes have been reenabled to better soak read-only load. Our engineering teams are looking into the root cause of the problem. Will post more information as soon as it's available.

[Sense

[Reply](#) [Reply to author](#) [Forward](#)

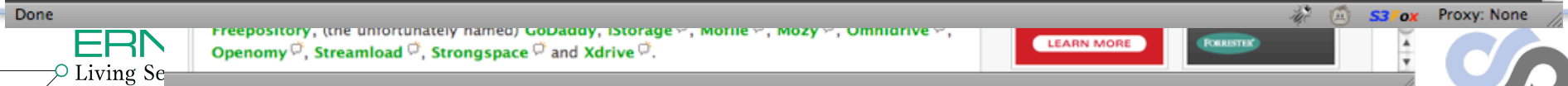
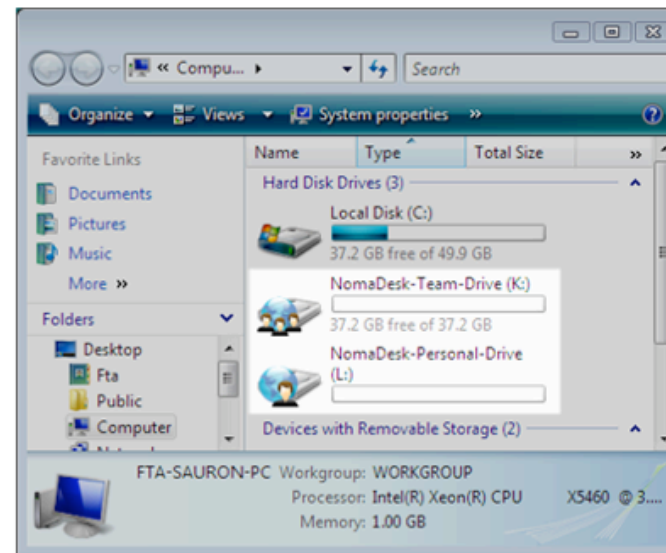


Omnidrive is no longer available, we recommend NomaDesk

Welcome to [NomaDesk](#). We develop a document collaboration software for geographically dispersed professionals who need secure access to shared files daily. NomaDesk was founded in 2004 by Filip Tack, its current CEO, along with CTO Miguel De Buf and COO Peter Geldhof. Based in Gent, Belgium, the company is supported by Gimv, a European independent investment company. NomaDesk has offices and datacenters in the US and Europe.

We are not affiliated with [Omnidrive](#). We feel compelled to maintain the domain name because we are convinced of the business value of a Software-as-a-Service to share, synchronize and backup business critical data. So do thousands of SMB customers that use NomaDesk on a daily basis. NomaDesk has and will be running its service for years to come. You are kindly invited to:

- » [Check out our product offering](#)
- » [Download your 30 day free trial](#)
- » [Contact customer support or a sales representative](#)



Availability [not just uptime!]

- Account Lockout?
- “Malicious activity from your account”

More cloud #fail

- MediaMax Online Storage – inactive account purging script error whacked active customer accounts
- Nokia Ovi (like MobileMe) lost 3 weeks of customer data after crash
- Jan 2009 – SF.com customers couldn't log in – “core network device failed with memory allocation errors”
- Oct 2009 – MS suspended Sidekick sales for 1.5 months due to data loss

Monoculture



Monoculture

- ***MonocultureGate*** is well known in our circles.
- Just viewing that pic resulted in a raised average IQ in this room.
- His (their) thesis:
 - “ *A monoculture of networked computers is a convenient and susceptible reservoir of platforms from which to launch attacks; these attacks can and do cascade.* ”
- Most people agreed with Dr Geer (et al) back then..
- Just because its not Windows, doesn't mean the thesis disappears.

SmugMug Case Study

- Process 50+ terapixels per day
- Posterchild of AWS
- Heavy use of S3 and EC2
- Launched 1920 standard instances in one call
- You don't get monoculture'er than ~2000 machines that are all copies of the same image..



**Extending
your attack
surface**



**While we're
talking
about
phishing...**



But you have to trust someone!

<+ben> kostyas cloudbreak stuff really scares me

<+MH> its impressive for sure, but why would that scare you more than simple Amazon evilness ? (Malfeasance)

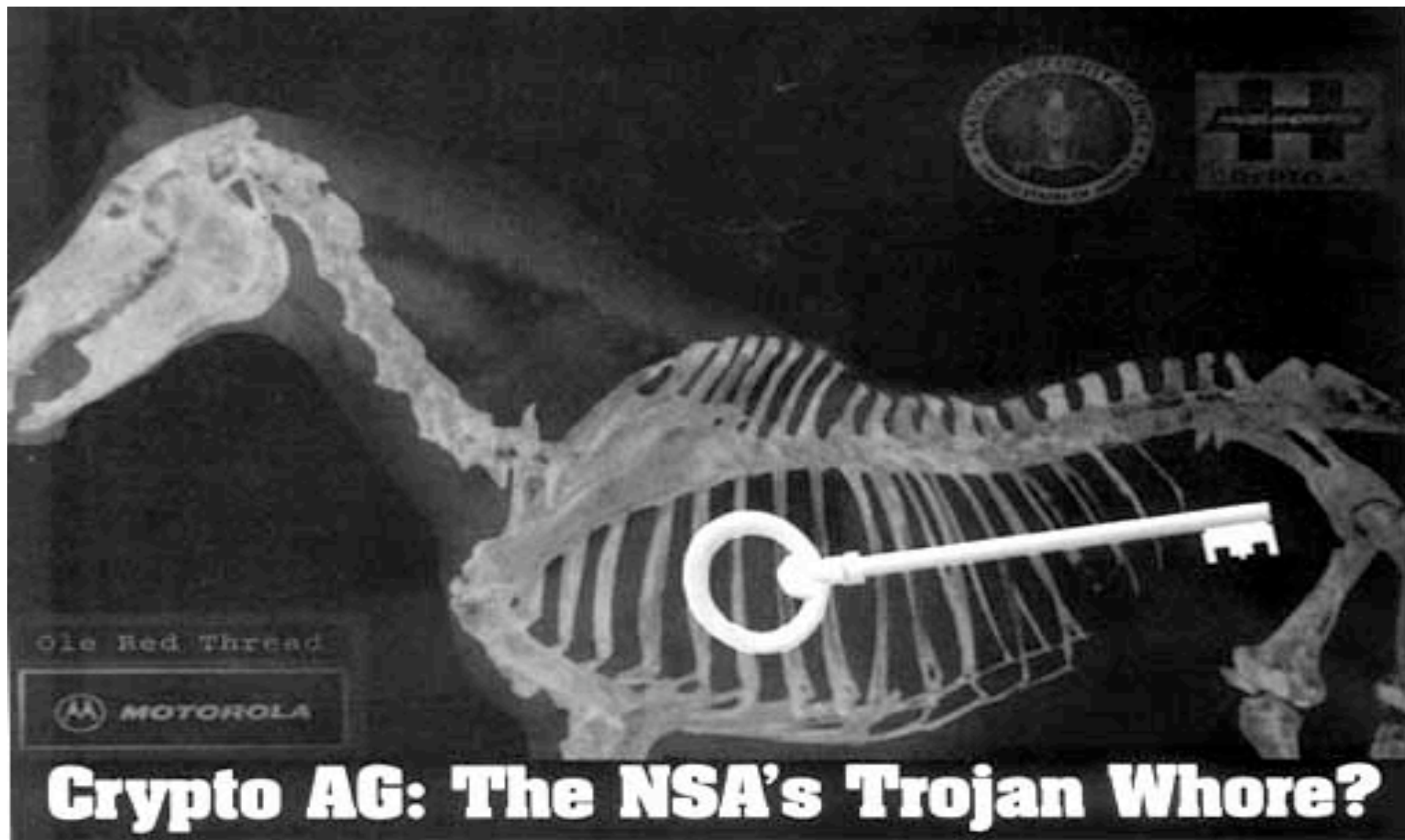
<+ben> You have to trust someone.. Just like how you trust Microsoft not to backdoor your OS, you trust Amazon not to screw you

Red Herring Alert!



Complete the popular phrase.

- You trust Microsoft, why not Amazon?
- Trust, but !
- Reverse Engineers keep Microsoft honest
- (or at least raise the cost of possibly effective malfeasance)
- Even “pre-owned” hardware is relatively easy to spot (for some definition of easy)
- But how do we know that Amazon (or other big names) “Wont be evil”™
- If ok today, what about tomorrow?



by Wayne Madsen

FOR AT LEAST HALF A CENTURY, THE US HAS BEEN
INTERCEPTING AND DECRYPTING THE TOP SECRET
DOCUMENTS OF MOST OF THE WORLD'S GOVERNMENTS

Using the Cloud..

For hax0r fun and profit:

- Dino Dai Zovi vs. Debian
- Ben Nagy vs. MS Office
- Dmolnar & Zynamics



debian

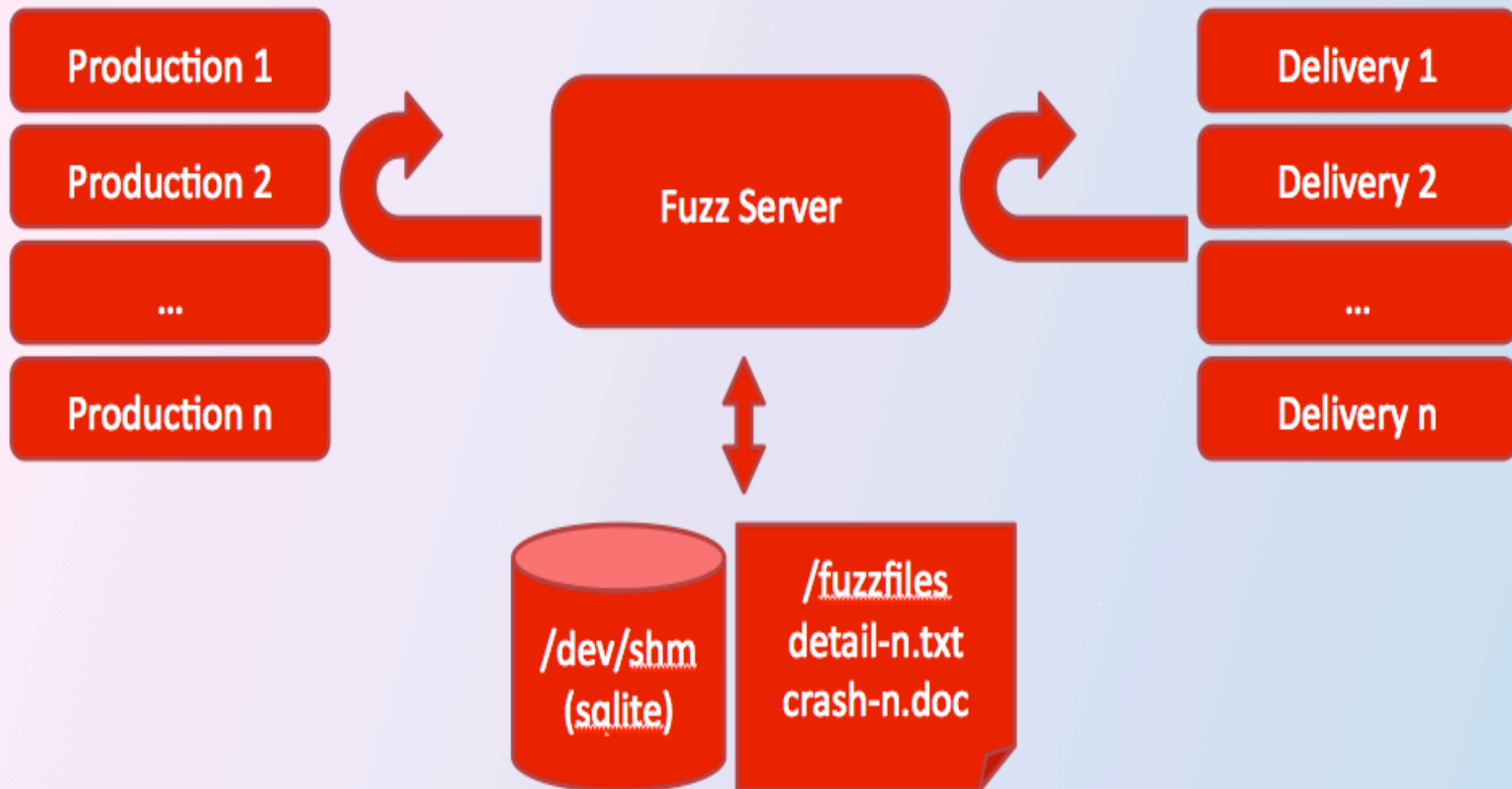


DDZ vs Debian

1. Populate a distributed queue with strings describing which keys to generate
2. Launch 20 VMs (the default limit)
3. Fetch key descriptors from queue, generate batches of keys, and store in S3

524,288 RSA keys – 6 Hours - \$16

Metafuzz "Harness"



Zynamics & DMolnar

- Zynamics use EC2 to demo software and classify malware, upto ~50k samples/day
- David Molnar and friends fuzztest Linux binaries, sift results and notify devs, all on EC2

Some of the players



CITRIX[®]



3tera[™]



salesforce.com
Success. Not Software.[®]



amazon.com[™]



Joyent



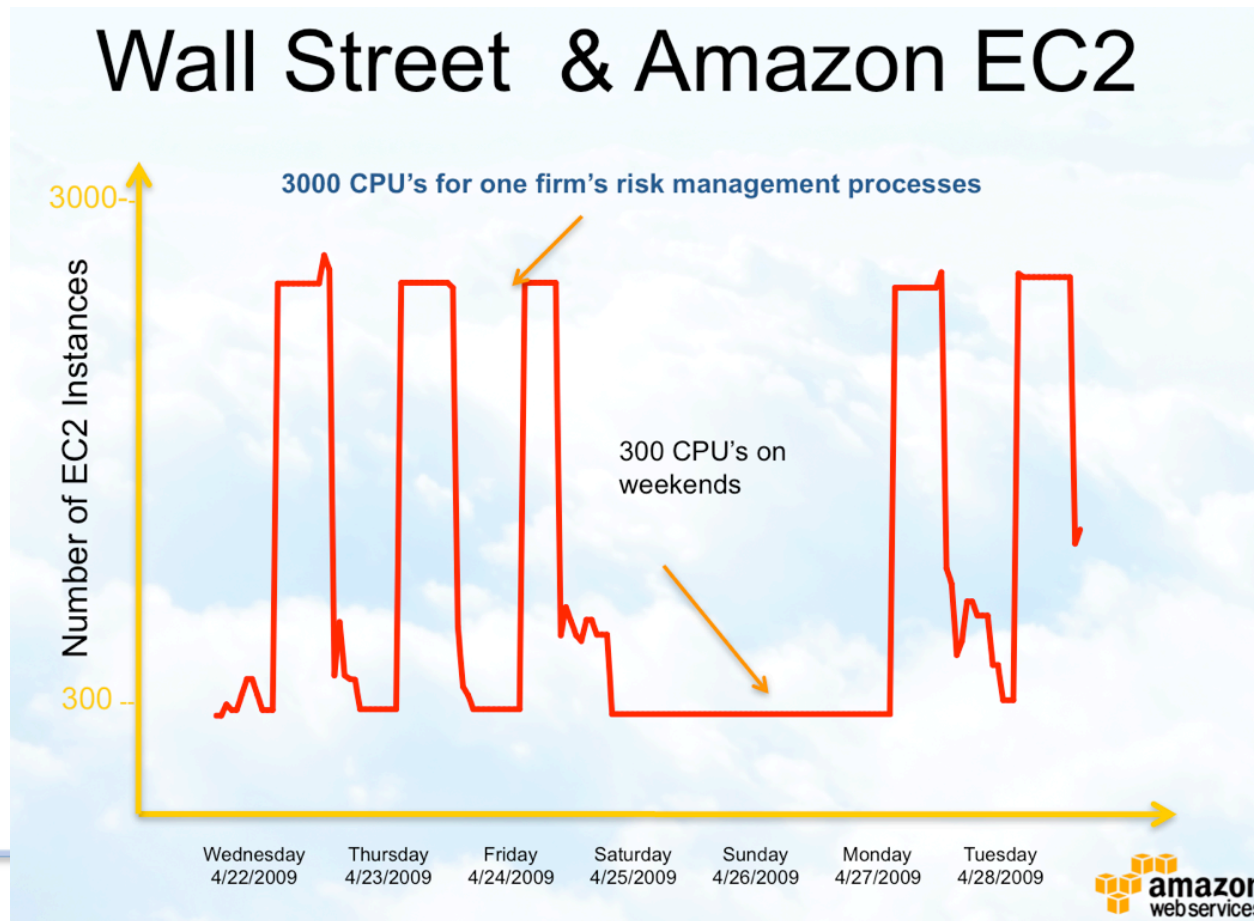
[SensePost – 2009]

The ones we looked at...



Autoscaling / Usage costing

- Autoscaling is a great idea for companies.



Can you spot the danger?



Storage as a Service

- In most cases this is a really simple model
- Faster Internet tubes is making backing up over tubes reasonable
- Disk access anywhere is a nice idea
- All throw crypto-pixieDust-magic words in their marketing documents
- For good measure all throw in Web based GUI access

Web Application Security

YOU'RE DOING IT WRONG



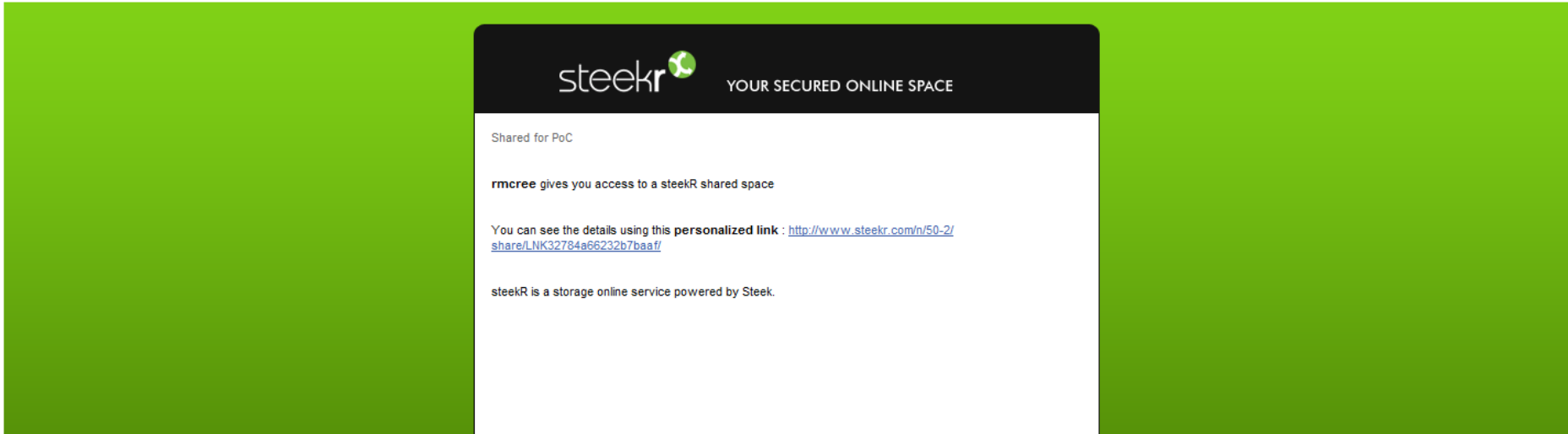
Web Apps + File Systems



Amazon EC2 Secure Wiping



☆ rmcree to me



Welcome 1 GB Free [Sign up in steekR](#)

[My steekR](#) [Slideshow](#)

My shared space

- My Documents
- <iframe src=http://xssed.com>

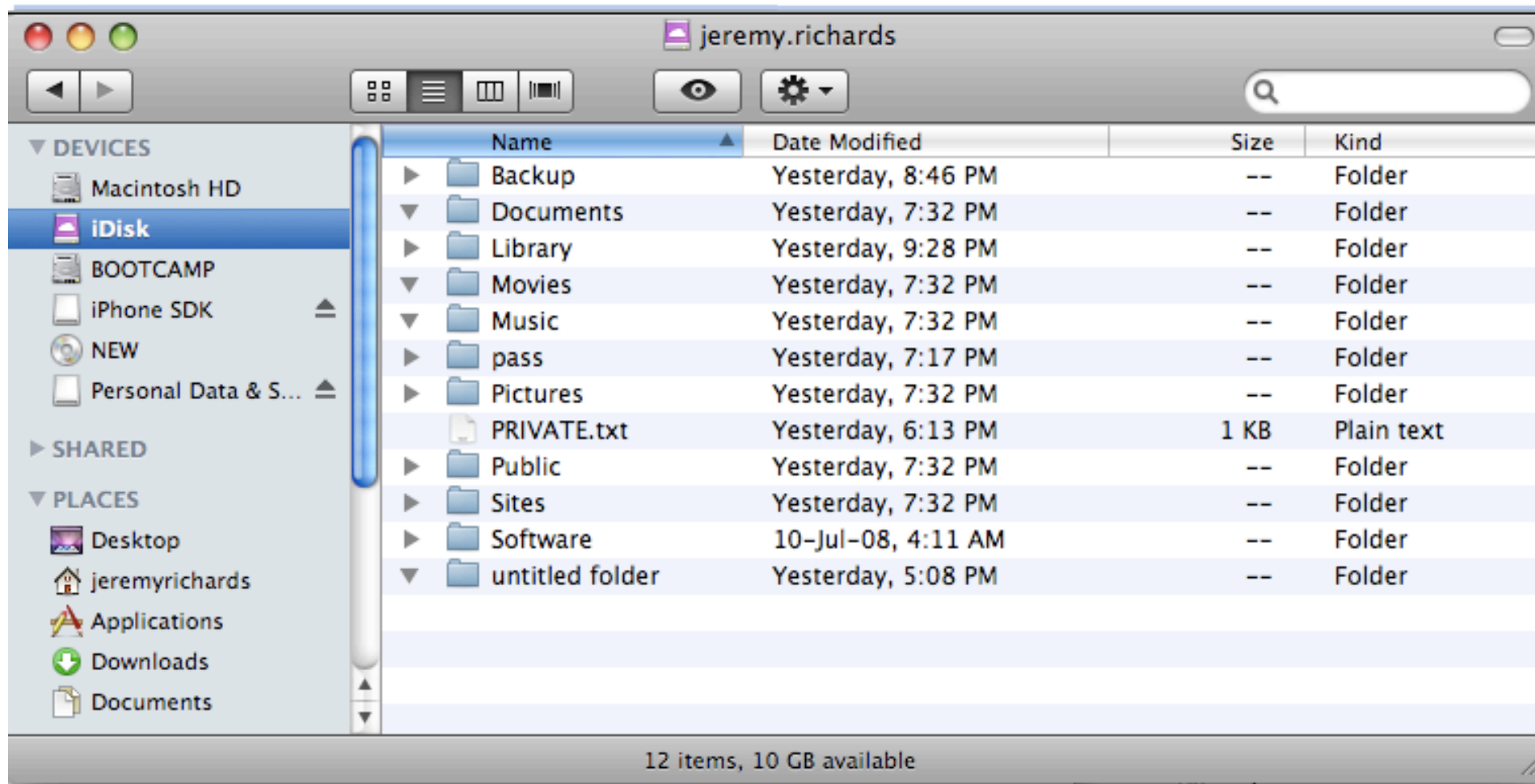
Parent folder Select: **All**, None Sort by: **Name** View:

* <iframe src=http://xssed.com>

A preview of the XSS Archive website. The main heading is '</xssed>' in a large, stylized font, with 'xss attacks information' underneath. Below that, it says 'XSS Archive | XSS Archive ★ | TOP Su'. At the bottom, it shows '0 byte' and '13/07/2009 - 18h20'.



MobileMe: yourDisk is myDisk
by jrichards on Jul.03, 2009, under Uncategorized



PRIVATE.txt

This is a private file that lives outside the "Public folder". It should not be accessible from a Public folder.

request

```
GET /jeremy.ri
Host: idisk.mac
User-Agent: Mo
Accept: text/ht
Accept-Langua
Accept-Encodin
Accept-Charset
Keep-Alive: 300
Proxy-Connect
Referer: http://
```

< >

done

burp suite v1.1 professional – licensed to Michael Hoffman [single user license]

burp intruder repeater window help

proxy spider intruder **repeater** sequencer decoder comparer comms alerts

go cancel host idisk.mac.com

< > port 80 use SSL

request

raw params headers hex viewstate

```
GET /jeremy.richards-Public/%2E%2E%2FPRIVATE.txt?disposition=download+8300 HTTP/1.1
Host: idisk.mac.com
User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.5; en-US; rv:1.9.0.11) Gecko/2009060214 Firefox/3.0.11
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Proxy-Connection: keep-alive
Referer: http://idisk.mac.com/jeremy.richards-Public?view=web
```

< > 0 matches

done length: 457

response

raw headers hex render

```
HTTP/1.1 200 OK
Server: AppleDiskServer-1E2012
x-responding-server: idiskng075
X-dmUser: jeremy.richards
ETag: "u-1g3s18hn-3e0p-1372yjpvf7-2b6d9rze2c0"
Last-Modified: Wed, 01 Jul 2009 15:37:03 GMT
Content-disposition: attachment;
Content-Type: text/plain
Content-Length: 114
Date: Wed, 01 Jul 2009 15:46:34 GMT
Connection: close
```

This is a private file that lives outside the "Public folder". It should not be accessible from a Public folder.

< > href

0 matches

SugarSync



**The Prime Cloud Storage
Solution**

DIVERSION





username=**bob**&password=**cat**



<http://bank.com/login>



```
<html>
<body>
...
Sorry! Please check your
password and try again
..
</body>
</html>
```




username=**bob**&password=**dog**



<http://bank.com/login>

```
<html>
<body>
...
Sorry! Please check your
password and try again
..
</body>
</html>
```



username=**bob**&password=fish



<http://bank.com/login>



```
<html>
<body>
...
Welcome Bob!
..
</body>
</html>
```



username=bob&password=thiscannnevereverberight



<http://bank.com/login>

```
<html>
<body>
...
Sorry! Please check your
password and try again
..
</body>
</html>
```

Page-Sig: 0123984



username=**bob**&password=**fish**



<http://bank.com/login>

```
<html>
<body>
...
Sorry! Please check your
password and try again
..
</body>
</html>
```

Page-Sig: 0123984

Page-diff: 0.23213





username=bob&password=thiscannnevereverberight



username=**bob**&password=**dog**



Failed Login

password and try again

username=**bob**&password=**dog**



Failed Login



<http://bank.com/login>



username=**bob**&password=fish



username=**tom**&password=fish



username=**sam**&password=fish



username=**rick**&password=fish



username=**carp**&password=fish



<http://bank.com/login>

```
<html>
<body>
...
Welcome Carp!
..
</body>
</html>
```



username=**bob**&password=fish

SessionID: **ADSFERDFGDGDSDDFDSFSDFFDSF**



<http://bank.com/login>

```
<html>
<body>
...
Welcome Bob!
..
</body>
</html>
```

GET /balance

Cookie: **ADSFERDFGDGDSDDFDSFSDFFDSF**

Balance = \$123342342423





\$

GET /balance
Cookie: AAAAAAAAAAAAAAAAAAAAAAAAAAA**A**



GET /balance
Cookie: AAAAAAAAAAAAAAAAAAAAAAAAAAA**B**



GET /balance
Cookie: AAAAAAAAAAAAAAAAAAAAAAAAAAA**C**



GET /balance
Cookie: **ZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ**



Balance = \$123342342423



<http://bank.com/login>





GET /balance
Cookie: AAAAAAAAAAAAAAAAAAAAAA

GET /balance
Cookie: ZZZZZZZZZZZZZZZZZZZZZ



ogin

SugarSync



**The Prime Cloud Storage
Solution**

-
- <file:///Users/marco/Desktop/troopers10/1-sugarsync-proj.mp4>
 - Overview of sugarsync + normal password reset
 - Ends with sample link..

Its Short, Brute & Declare Victory

?secret= for472gtb422
= lower case alphanumeric
= 35^{12}
= Still a too big number ☹️

Birthday Attack ?

= $1.2 * \text{sqrt}(35^{12})$
= Still a pretty big number

<https://www.sugarsync.com/reset-password?secret=6076kgbni87b>
<https://www.sugarsync.com/reset-password?secret=bt45nq32gvzc9>
<https://www.sugarsync.com/reset-password?secret=fk0c79goxbzwb>
<https://www.sugarsync.com/reset-password?secret=bzx5gor7yaj45>
<https://www.sugarsync.com/reset-password?secret=b9xhfaitwok6a>
<https://www.sugarsync.com/reset-password?secret=evifc5cud79aw>
<https://www.sugarsync.com/reset-password?secret=d7q7mba80hpqs>
<https://www.sugarsync.com/reset-password?secret=ds3a27qdpoyom>
<https://www.sugarsync.com/reset-password?secret=bms9kxwp2ypeq>
<https://www.sugarsync.com/reset-password?secret=xi3pzry9s7kz>
<https://www.sugarsync.com/reset-password?secret=cs3pd8tyenedp>
<https://www.sugarsync.com/reset-password?secret=dmmzfgvvyqw72>
<https://www.sugarsync.com/reset-password?secret=cw8jqev4yvv0w>
<https://www.sugarsync.com/reset-password?secret=edp9iog7fj60r>
<https://www.sugarsync.com/reset-password?secret=cxom0z2a62iva>
<https://www.sugarsync.com/reset-password?secret=bv45tsonz8tdi>
<https://www.sugarsync.com/reset-password?secret=cv7z95jyctnd5>
<https://www.sugarsync.com/reset-password?secret=cq2j8wdbbo7om>
<https://www.sugarsync.com/reset-password?secret=bmtjn6j3hteky>
<https://www.sugarsync.com/reset-password?secret=fjrofysj887bf>
<https://www.sugarsync.com/reset-password?secret=de4acew6hns4s>
<https://www.sugarsync.com/reset-password?secret=fdie4jk2jy56c>
<https://www.sugarsync.com/reset-password?secret=d20rt64rbywtd>
<https://www.sugarsync.com/reset-password?secret=drdpnygkij2rg>
<https://www.sugarsync.com/reset-password?secret=brnazhekoivr>
<https://www.sugarsync.com/reset-password?secret=ekivezkzgy9oo>
<https://www.sugarsync.com/reset-password?secret=dynnmny3xrcxz>
<https://www.sugarsync.com/reset-password?secret=bwvj29v4ty765>
<https://www.sugarsync.com/reset-password?secret=d2tkoah29zq5p>
<https://www.sugarsync.com/reset-password?secret=fjmhfxr0q8ivk>
<https://www.sugarsync.com/reset-password?secret=kk4e7rs55f60>
<https://www.sugarsync.com/reset-password?secret=bzxejaxd35687>
<https://www.sugarsync.com/reset-password?secret=fc274gqrq03rk>
<https://www.sugarsync.com/reset-password?secret=die4od59cy93d>
<https://www.sugarsync.com/reset-password?secret=epdp3vckqexaj>
<https://www.sugarsync.com/reset-password?secret=zf3fyt7vk9j>
<https://www.sugarsync.com/reset-password?secret=eyir7wd6vfca6>
<https://www.sugarsync.com/reset-password?secret=r7zp8ppjztc>
<https://www.sugarsync.com/reset-password?secret=dadq3z0zgnkqe>
<https://www.sugarsync.com/reset-password?secret=c3hfvavknett0>
<https://www.sugarsync.com/reset-password?secret=3pv2oijt5t40>
<https://www.sugarsync.com/reset-password?secret=d4beabdor72tx>
<https://www.sugarsync.com/reset-password?secret=cq7q5a9imttjp>

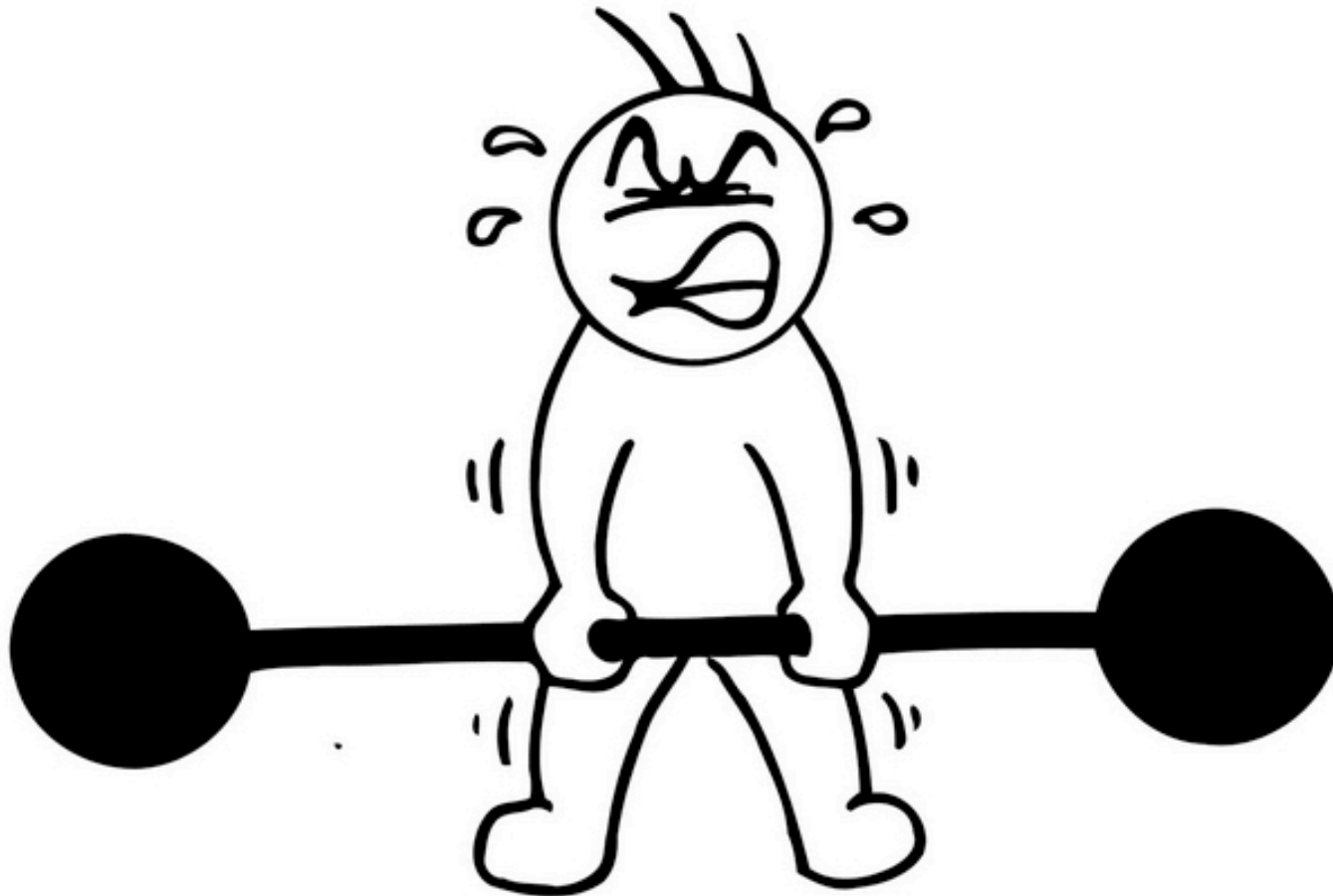
<https://www.sugarsync.com/reset-password?secret=dk0tot820d7vs>
<https://www.sugarsync.com/reset-password?secret=b6bip7pswf9m2>
<https://www.sugarsync.com/reset-password?secret=bx424nj2p2y9e>
<https://www.sugarsync.com/reset-password?secret=bz6to064jf3qp>
<https://www.sugarsync.com/reset-password?secret=ebgbgprc6eq2f>
<https://www.sugarsync.com/reset-password?secret=modziars6o2d>
<https://www.sugarsync.com/reset-password?secret=wi3vkonsia3>
<https://www.sugarsync.com/reset-password?secret=cmbicqc34apjf>
<https://www.sugarsync.com/reset-password?secret=e2fqw2kogy8gc>
<https://www.sugarsync.com/reset-password?secret=fkno8o8ws7th>
<https://www.sugarsync.com/reset-password?secret=8g8jfig0m8hk>
<https://www.sugarsync.com/reset-password?secret=ea760dof3zpv>
<https://www.sugarsync.com/reset-password?secret=dr8rsap8ieinv>
<https://www.sugarsync.com/reset-password?secret=d3hmdc3srnyng>
<https://www.sugarsync.com/reset-password?secret=dcnckpph35vko>
<https://www.sugarsync.com/reset-password?secret=ejr0k3ro4nepm>
<https://www.sugarsync.com/reset-password?secret=etcasjbo2sa9k>
<https://www.sugarsync.com/reset-password?secret=e0ijravm5awrf>
<https://www.sugarsync.com/reset-password?secret=bbjb3rabpnga>
<https://www.sugarsync.com/reset-password?secret=di8qwc355270y>
<https://www.sugarsync.com/reset-password?secret=cm5esewps28y2>
<https://www.sugarsync.com/reset-password?secret=mofph975924>
<https://www.sugarsync.com/reset-password?secret=b5eptnaefja5f>
<https://www.sugarsync.com/reset-password?secret=dqshjvg8pyyn>
<https://www.sugarsync.com/reset-password?secret=byjd3bwq39rgi>
<https://www.sugarsync.com/reset-password?secret=di4wgdecj2ci0>
<https://www.sugarsync.com/reset-password?secret=ebiyxam7cextk>
<https://www.sugarsync.com/reset-password?secret=emxscrt769hi>
<https://www.sugarsync.com/reset-password?secret=ein2b5gwj4vpx>
<https://www.sugarsync.com/reset-password?secret=c485kmqj7jcvo>
<https://www.sugarsync.com/reset-password?secret=x83hrq5zgfkc>
<https://www.sugarsync.com/reset-password?secret=ejrddyrr02pxcz>
<https://www.sugarsync.com/reset-password?secret=dnacznkenc57z>
<https://www.sugarsync.com/reset-password?secret=emmiagm6b55ig>
<https://www.sugarsync.com/reset-password?secret=ca3xztff6pj44i>
<https://www.sugarsync.com/reset-password?secret=dqmejm2dfq8jb>
<https://www.sugarsync.com/reset-password?secret=c9879b9oqzbzj>
<https://www.sugarsync.com/reset-password?secret=d9vc00wo09mci>
<https://www.sugarsync.com/reset-password?secret=e9ghwgd5eze6>
<https://www.sugarsync.com/reset-password?secret=cgk799cwjgmaa>
<https://www.sugarsync.com/reset-password?secret=6pz2nk4sdr20>
<https://www.sugarsync.com/reset-password?secret=fbwgaiqs7o2wp>
<https://www.sugarsync.com/reset-password?secret=eaffpy57jyf78>



We Have 2 Days..

single thread	:	1 hour	:	648
	:	2 days	:	31104
10 threads	:		:	221472
10 machines	:		:	2 214 720

Wont they notice ?





Saved (some pride)

10 seconds of

<file:///Users/marco/Desktop/troopers10/2-sugar-3.mp4>

(multi threaded)

<file:///Users/marco/Desktop/troopers10/3-sugar-2-weeks-project.mp4>

(active 2 weeks later)

PaaS



Actually..

- SF.com is both SaaS and PaaS
- We took a quick look at SaaS
- Good filtering, and held up well to cursory testing
- Why cursory?
- Ultimately, it **is** a web application..

Clickjack

- Nick Clickjack
- <file:///Users/marco/Desktop/troopers10/4-nick-clickjack.mp4>
- 1 min

SalesForce back story



- 10 years old
- Initially web-based CRM software
 - 59 000 customers
 - \$1 billion in revenue
- Distributed infrastructure was created to support CRM (SaaS, weeeee!)
- Platform was exposed to architects and devs, for PaaS and IaaS
 - (Ambitious project with solid aims)



Salesforce business model

- Multi-tenant
 - Customers share infrastructure
 - Spread out across the world
- Subscription model
 - Scales with features and per-license cost
- Free dev accounts
 - More limited than paid-for orgs
- AppExchange
 - Third party apps (ala App Store)

Developing on Salesforce

Apex Class

EmailIterator

Apex

```
2 <apex:page controller="PageIterator" showheader="false">
3 <html>
4   <head>
5     <title>VisualForce Iterator</title>
6   </head>
7   <body>
8     <h1>Page Content Follows (we don't expect to get here, btw)</h1>
9     {!pageData}
10  </body>
11 </html>
12 </apex:page>
```

```
9
10 public void nextLoop(Integer counter) {
11   EmailIteratorObj__c o = [select id,counter__c from EmailIteratorObj__c where name='looper'][0];
12   o.counter__c=counter;
13   update o;
14 }
15
16 //called to initiate loop termination
17 public void endLoop(){
18   insert new Message__c(MsgType__c=Messages.ENDLOOP);
19 }
20
21 //called right at the end of a set of loop iterations
22 public void cleanUp(){
23   //clean out the email iterators objects
24   for (List<EmailIteratorObj__c> o: [select id from EmailIteratorObj__c]){
25     delete o;
26   }
27
28   //clean out messages
29   for (List<Message__c> o: [select id from Message__c]){
30     delete o;
31   }
```

Position: Ln 173, Ch 2

Total: Ln 173, Ch 6239

Other language features

- Make HTTP requests
- Bind classes to WS endpoints
- Can send mails
- Bind classes to mail endpoints
- Configure triggers on datastore activities

Multi-tenancy...

...an obvious problem for resource sharing



The Governor

- Each script execution is subject to strict limits
- Uncatchable exception issued when limits exceeded
- Limits based on entry point of code
- Limits applied to namespaces
 - Org gets limits
 - Certified apps get limits

Published Limits



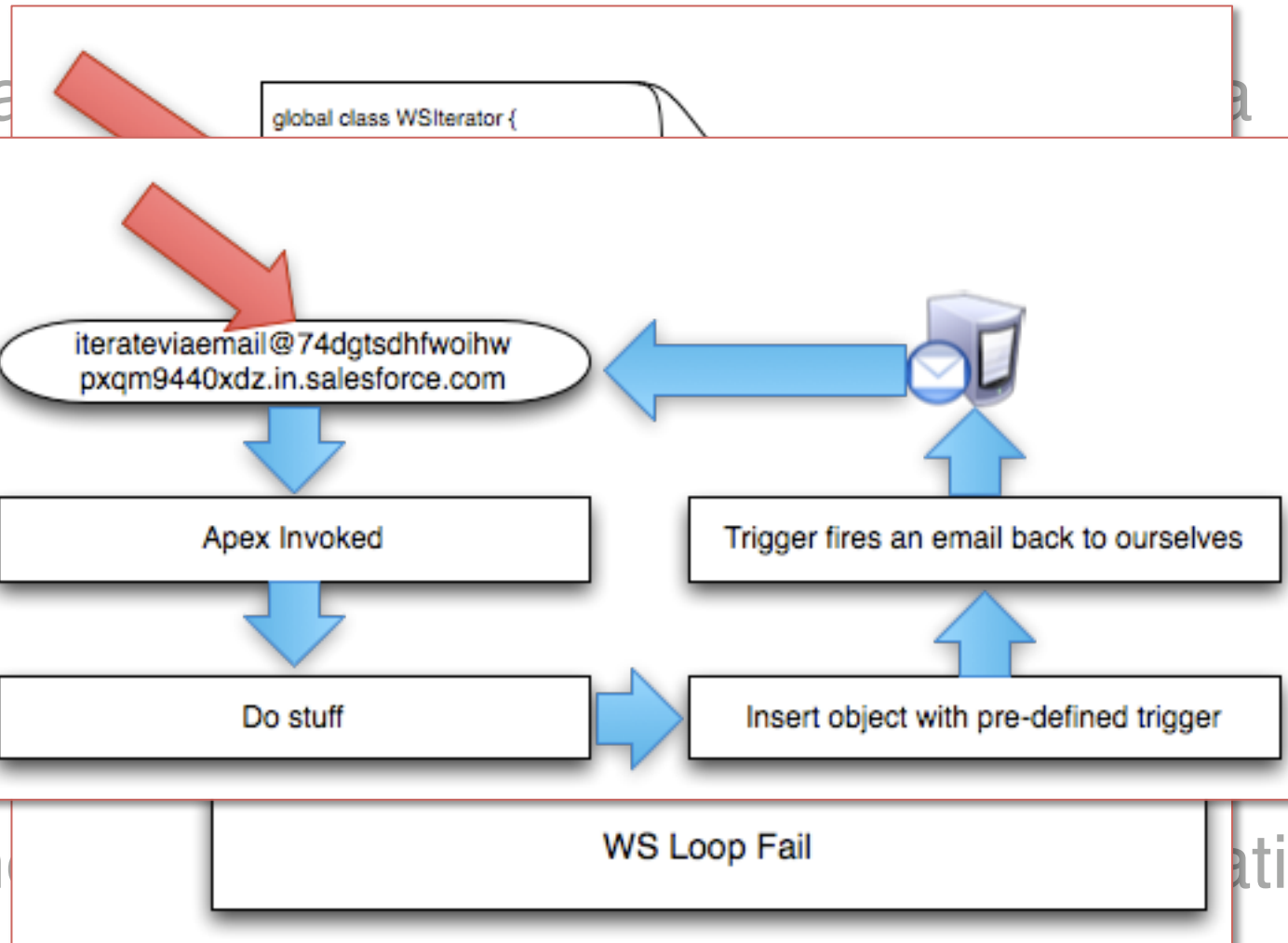
1. Number of received mails
2. Running time
3. ???

Apex limitations

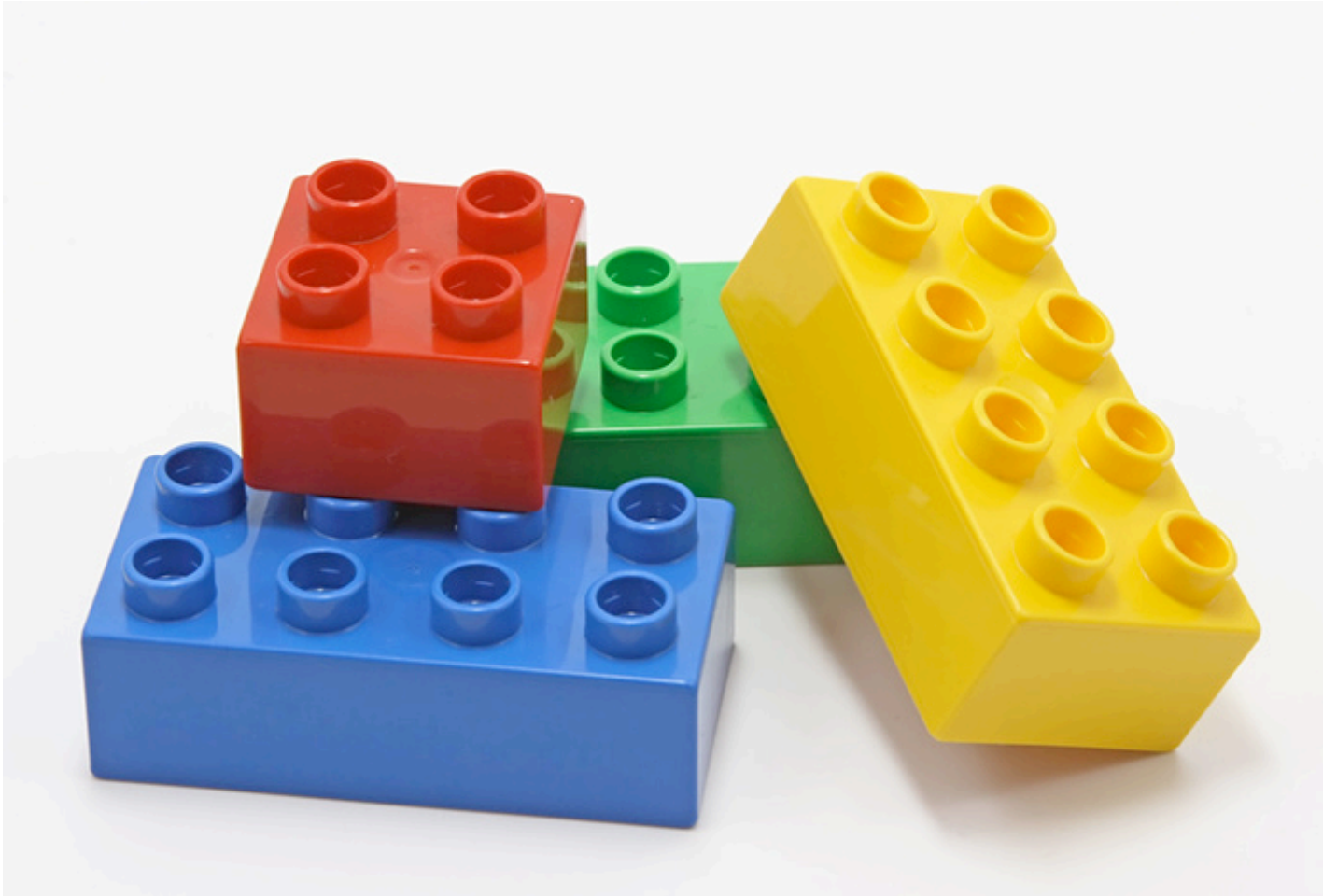
- Language focused on short bursts of execution
- Can't easily alter SF configuration
 - Requires web interface interactions
- APIs short on parallel programming primitives
 - no explicit locks and very broad synchronisation
 - no real threads
 - no ability to pause execution
 - no explicit shared mem
- API call order important

Bypassing the governor

- Wa
- si
- F
- G
- Th



And so?



Sifto!

- Ported Nikto into the cloud as a simple e.g.
- Process
 - Class adds allowed endpoint through HTTP calls to SF web interface
 - Event loop kicked off against target
 - Each iteration performs ten tests
 - State simply inserted into datastore at end of ten tests
 - Trigger object inserted to fire off email for next iteration
 - Results returned via email as they are found
- Why?
 - Free!
 - Fast (for .za)
 - Anonymity

[sifto vid]

- <file:///Users/marco/Desktop/troopers10/5-bh2009-1280.mp4>

Pros / cons

- Pros
 - Fast(er) with more bandwidth
 - Free!
 - Capacity for DoS outweighs home user
 - How about SF DoS?
- Cons
 - Prone to monitoring
 - Custom language / platform
 - Technique governed by email limits

Future Directions

- Sifto is a *really* basic POC hinting at possibilities
 - Turing complete, open field. Limited API though
- Platform is developing rapidly, future changes in this area will introduce new possibilities
 - Callouts in triggers for event loops
 - Reduction in limitations
 - Improvements in language and APIs
- Abstracted functionality on *aaS makes usage easier, but impact remains
- Security is transferred into hands of non-security aware C-levels, ouch.
- Rootkits
- Security community interaction



amazon
web services™



Yes...it's that
cool...

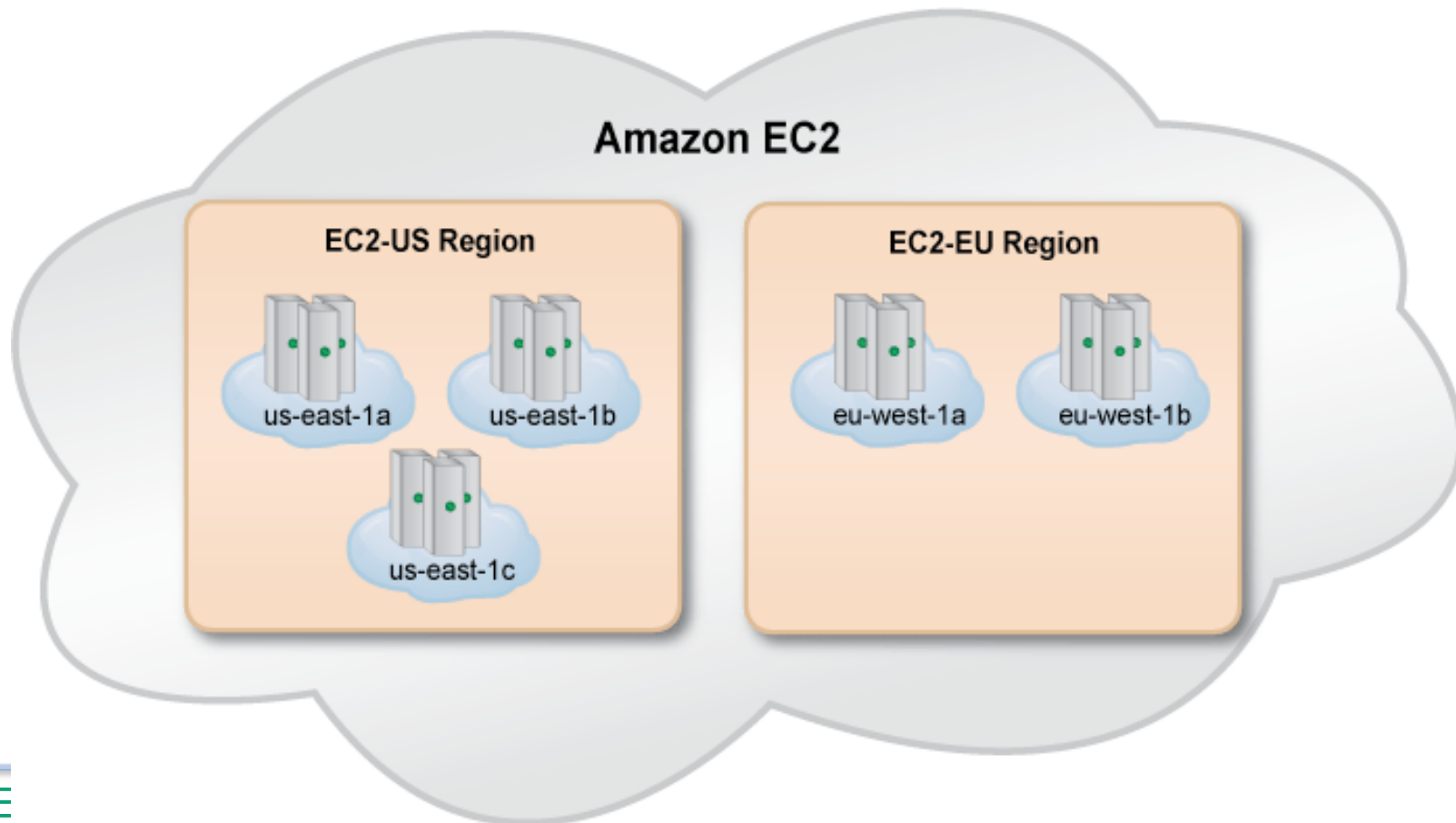


The Pieces (that we will touch)..

- EC2
- S3
- SQS
- DevPay
- What we ignore:
 - SimpleDB
 - Elastic IP
 - CloudFront
 - Elastic MapReduce
 - Mechanical Turk

EC2

Root access to a Linux machine in seconds..
Scalable costs..



S3

Manage Accounts | aws1@sensepost.com | Synchronize Folders | AWS Import/Export | Preferences

File Name | File Size(KB) | Modified Time

06/02/2009 09:42 PM	0	
06/13/2009 07:00 PM	13	.DS_Store
04/14/2008 04:59 PM	0	.Spotlight-V100
04/14/2008 04:36 PM	0	.Trashes

File Name | File Size(KB) | Upload Time

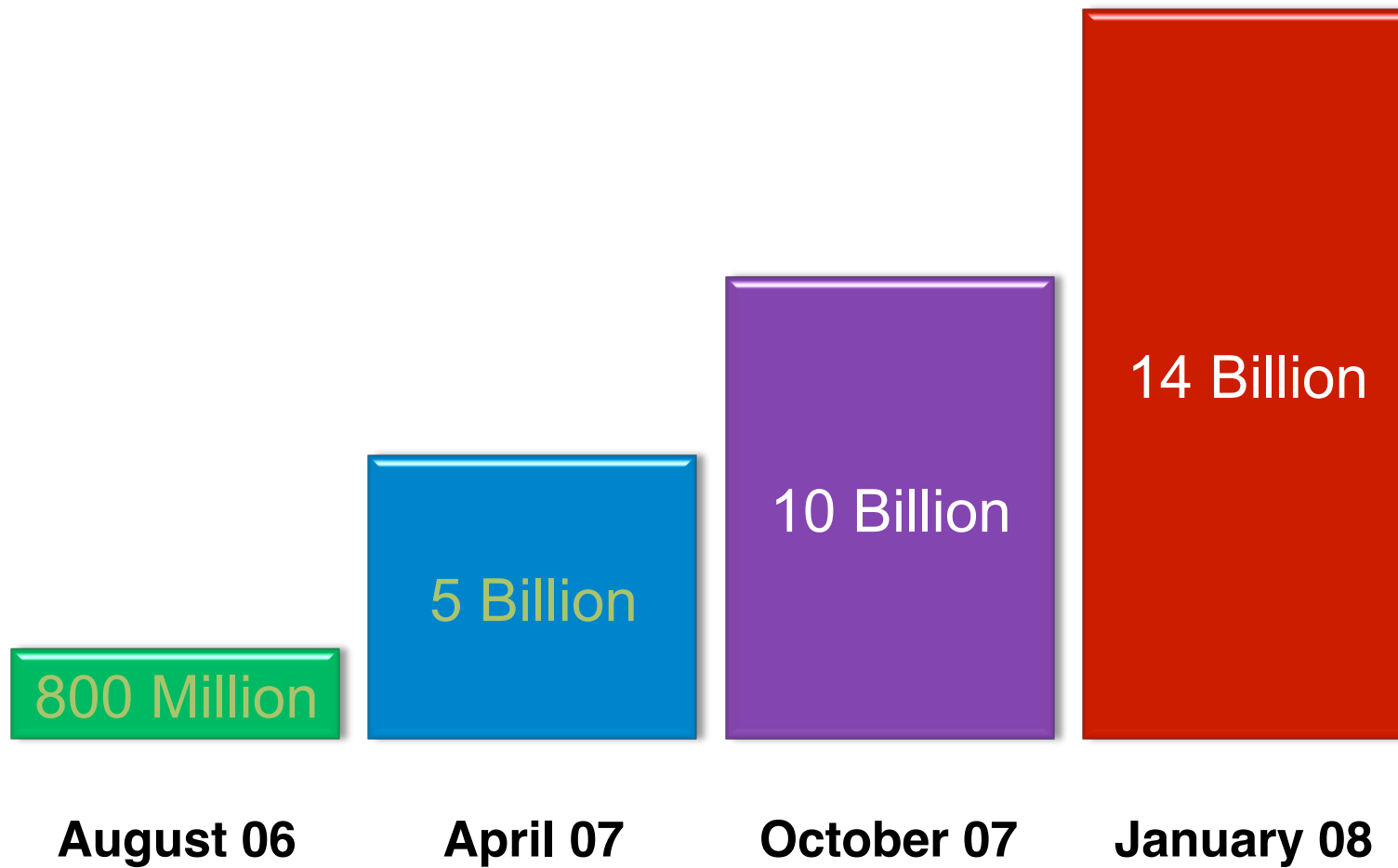
05/17/2009 10:29 PM	0	spscan4
05/17/2009 02:11 PM	0	spscan3
05/17/2009 00:48 AM	0	spscan2
05/16/2009 01:36 PM	0	spscan
05/19/2009 04:57 AM	0	splogs
05/16/2009 11:43 AM	0	sp1
05/18/2009 06:28 PM	0	qscan
07/15/2009 03:34 PM	0	fedora_11_full
07/20/2009 10:44 PM	0	copy-2
07/20/2009 10:11 PM	0	copy-1
07/15/2009 02:25 PM	0	amazon_fedora_8

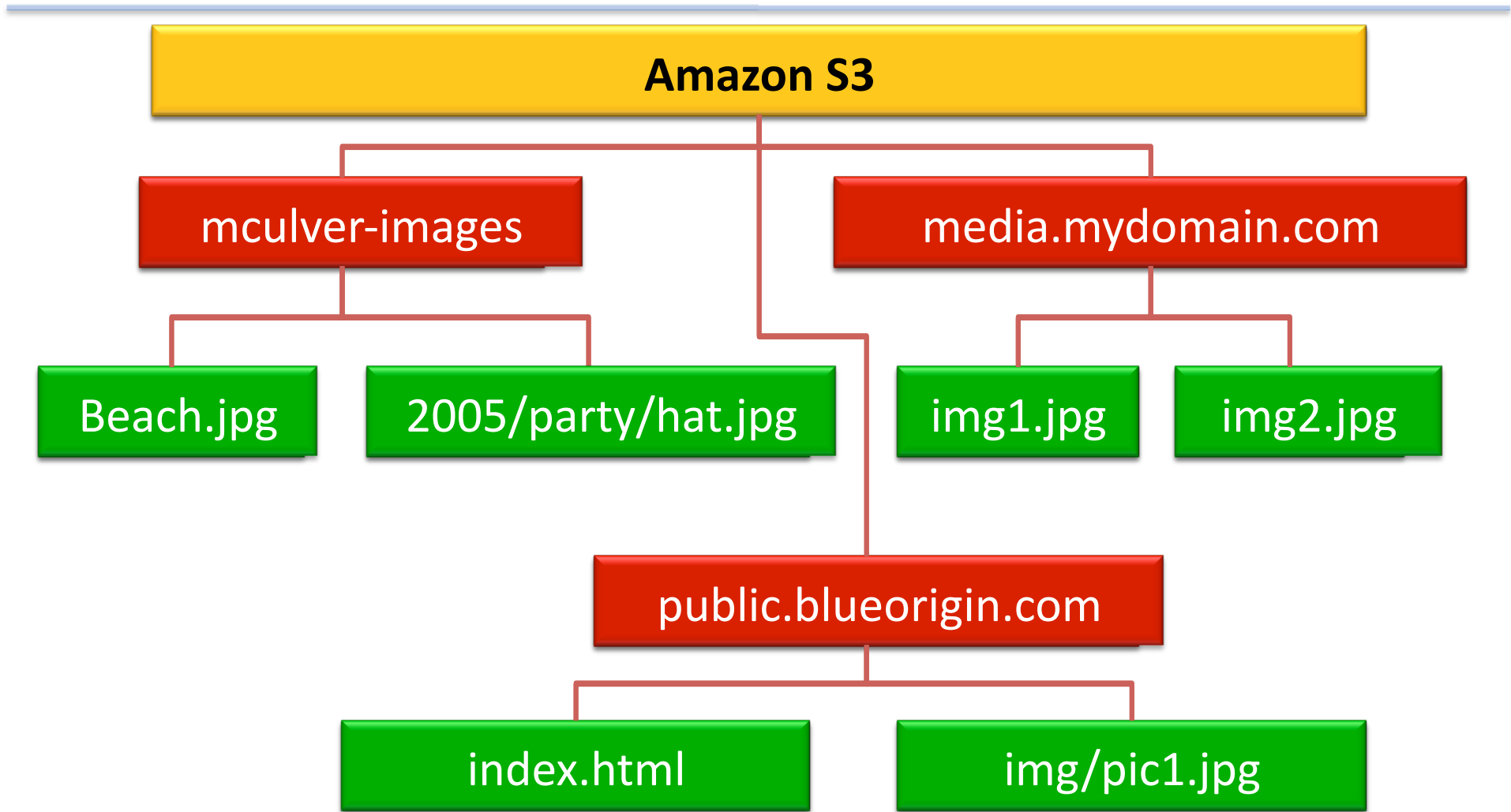
Current Tasks:

Regular Transfer | Synchronized Folders Transfer | Log

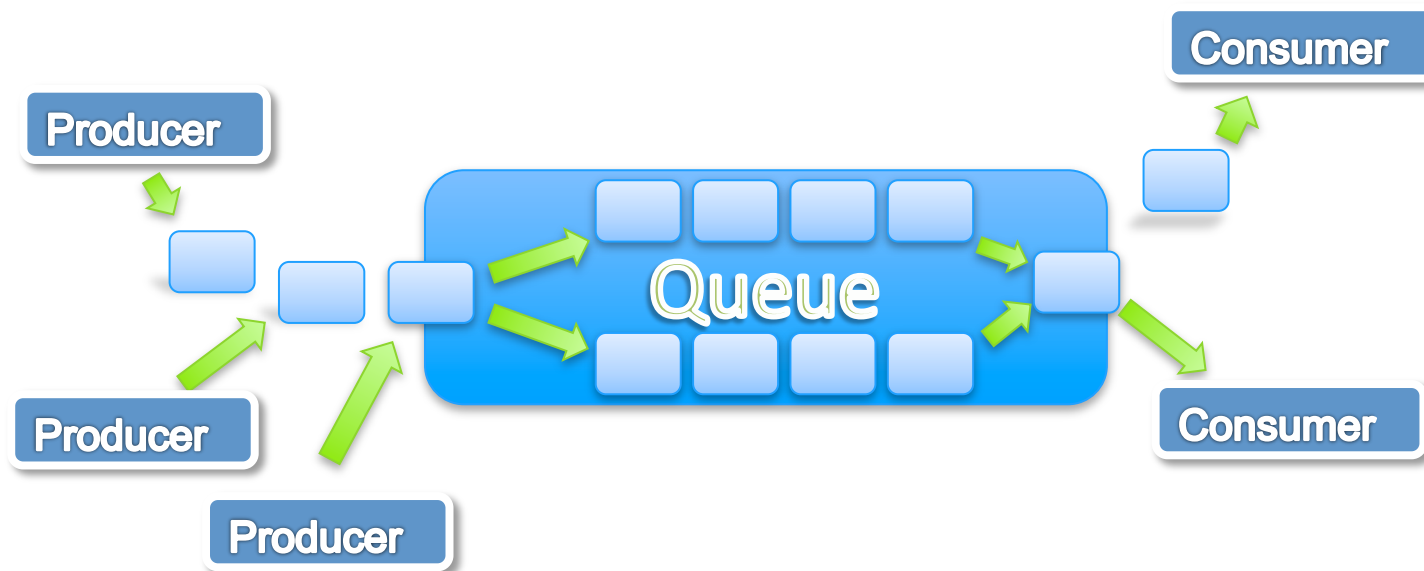
Clear | Pause | Clear Completed | Retry Failed Tasks

File Name	From	To	Type	Progress	Status
-----------	------	----	------	----------	--------





SQS



When in doubt..

Rinse... repeat!

Can we steal computing resources from
Amazon (or Amazon users?)

Sure we can..

Breakdown

Amazon provide 47 machine images that they built themselves..

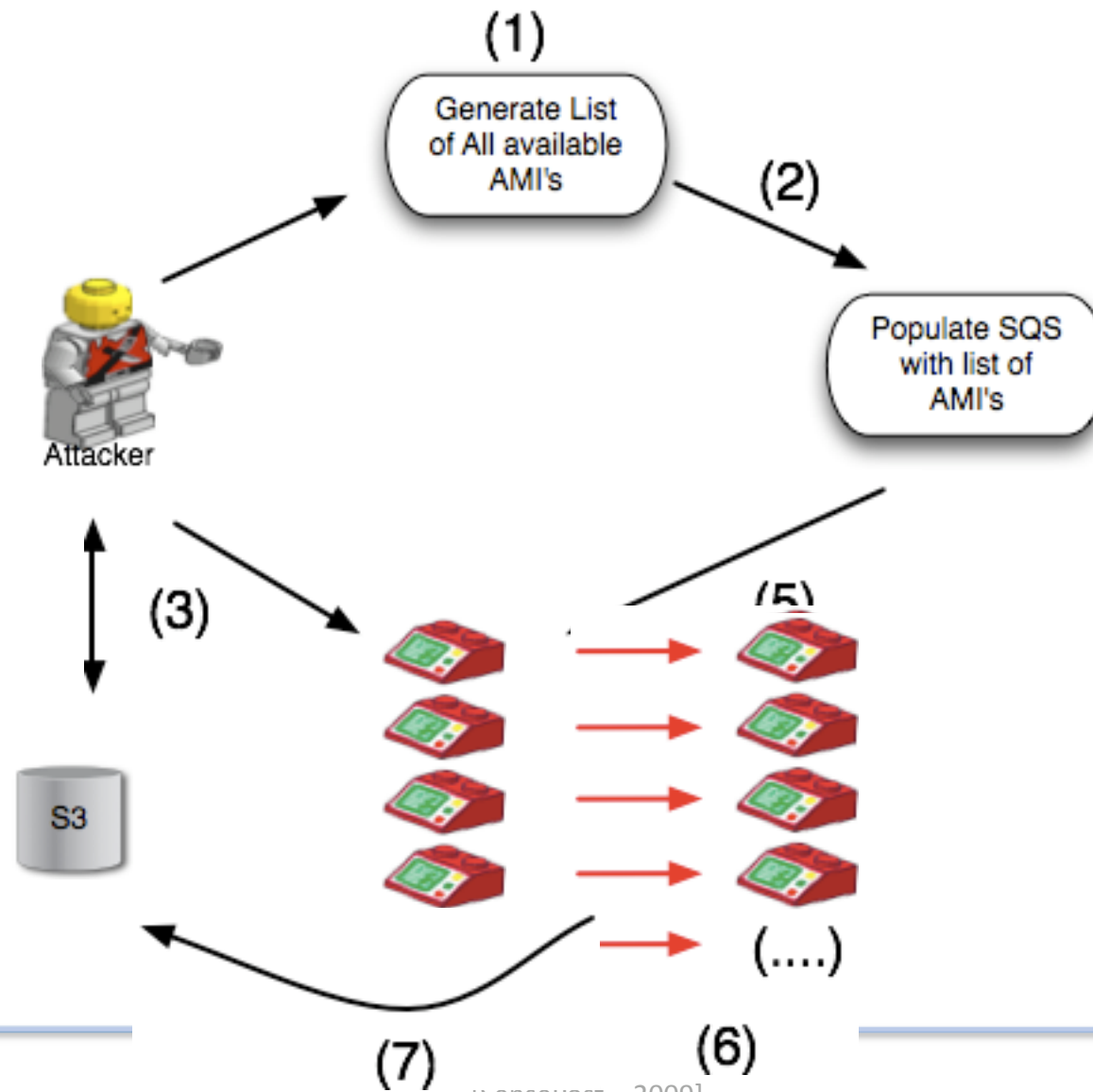
The screenshot shows the Amazon EC2 console interface. At the top, there are tabs for "Amazon EC2", "Amazon Elastic MapReduce", and "Amazon CloudFront". The "Amazon EC2" tab is active. On the left, there is a "Navigation" sidebar with a "Region:" dropdown set to "US-East". Below the sidebar, there are links for "EC2 Dashboard", "INSTANCES", "Images", "AMIs", and "Bundle Tasks". The main content area is titled "Amazon Machine Images" and contains a toolbar with "Launch", "Register New AMI", "De-register", and "Permissions" buttons. There are also "Show/Hide", "Refresh", and "Help" buttons. Below the toolbar, there are filters for "Viewing:" (set to "All Images") and "All Platforms". A pagination bar shows "1 to 50 of 2768 AMIs". The main table has the following data:

	AMI ID	Manifest	Visibility	Platform
<input type="checkbox"/>	ami-0022c769	level22-ec2-images/ubuntu-7.04-feisty-base-20071225a.manifest.xml	Public	Ubuntu
<input type="checkbox"/>	ami-005db969	alestic-64/ubuntu-8.04-hardy-base-64-20081222.manifest.xml	Public	Ubuntu
<input type="checkbox"/>	ami-005dba69	rbuilder-online/new-example-1-x86_64_20133.img.manifest.xml	Public	Other Linux
<input type="checkbox"/>	ami-005eba69	kaavo-ntier-db/imod-ntier-32bit-FC-DB.manifest.xml	Public	Other Linux

Shared AMI gifts FTW!

- Bundled AMI's + Forum Posts
- Vulnerable servers? Set_slice? SSHD?
- Scanning gets you booted.. We needed an alternative..

GhettoScan



[sensePost - 2009]

Results

```
ami-805eba09.files: > /mnt/cert.pem
ami-832b0c6a.files: -rw-r--r-- 1 root root 916 2009-03-11 11:21 cert-I652RSE2RKXY4ZLP7D7DUTY7V2J00WBU.pem
ami-832b0c6a.files: -rw-r--r-- 1 root root 916 2009-03-11 11:16 cert-I652RSE2RKXY4ZLP7D7DUTY7V2J00WBU.pem
ami-135fb87a.files: mv cert-GAZG6MLHP5G7ZLG3IH2FVBY623CLSDZC.pem /mnt
ami-135fb87a.files: ec2-bundle-vol -d /mnt -k /mnt/pk-GAZG6MLHP5G7ZLG3IH2FVBY623CLSDZC.pem -c /mnt/cert-GAZG6MLHP5G7ZLG3IH2FVBY623CLSDZC.pem -u 614613661965 -r 3386 -p dcm4chee_01
ami-135fb87a.files: ec2-bun
ami-135fb87a.files: ec2-bun /root/ec2:
ami-135fb87a.files: ./ec2-b
ami-2545a04c.files: total 32
ami-2545a04c.files: -rw-r--
ami-2545a04c.files: ec2-bun
ami-2545a04c.files: ec2-bun drwxr-xr-x 3 root root 4096 2009-03-11 11:21 .
ami-2545a04c.files: ec2-
ami-28ac4a41.files: ec2-
ami-2ca04645.files: -rw-
ami-2ca04645.files: mv c
ami-2ca04645.files: ec2-
ami-2ca04645.files: ec2-
ami-2ca04645.files: -rw-
ami-362acd5f.files: mv c
ami-362acd5f.files: ec2-
ami-362acd5f.files: ec2-
ami-362acd5f.files: ec2-
ami-362acd5f.files: ./ec
ami-399d7a50.files: ec2-
ami-399d7a50.files: ec2-
ami-399d7a50.files: ec2-
ami-399d7a50.files: ec2-
ami-399d7a50.files: ec2-
ami-399d7a50.files: ./ec
ami-399d7a50.files: ./ec
ami-399d7a50.files: ec2-
ami-399d7a50.files: ec2-
ami-399d7a50.files: ./ec
ami-399d7a50.files: ./ec
ami-399d7a50.files: ./ec
ami-399d7a50.files: ./ec
ami-399d7a50.files: ./ec
ami-443bde2d.files: -rw----- 1 root root 1755 2009-03-11 11:16 id_gsg-keypair
ami-460dea2f.files: -rw----- 1 root root 1676 2009-03-11 11:16 id-mypairselastic
ami-460dea2f.files: ec2-bun
ami-460dea2f.files: ec2-bun -rw-r--r-- 1 root root 926 2009-03-11 11:16 pk-I652RSE2RKXY4ZLP7D7DUTY7V2J00WBU.pem
ami-460dea2f.files: ec2-bun
ami-460dea2f.files: ec2-bun
ami-460dea2f.files: ec2-bundle-vol -d /mnt -k /mnt/pk-F227ID6GTZCJWI74BPL4XFPY3CFA33AX.pem -c /mnt/cert-F227ID6GTZCJWI74BPL4XFPY3CFA33AX.pem -u 956543411044 -r i386 -p bioceppimage
ami-47a6412e.files: ec2-bundle-vol -d /mnt -k /mnt/pk-L5G166YFD14D76IGMCWUDBGDAGK3P7XK.pem -c /mnt/cert-L5G166YFD14D76IGMCWUDBGDAGK3P7XK.pem -u 936750502090 -r i386 -p image
```

s3 haroon\$ grep High *.nsr | wc -l

1293


s3 haroon\$ grep Critical *.nsr | wc -l

646

fest.xml
fest.xml
ifest.xml
ifest.xml
ifest.xml
ifest.xml
7J.pem
AZ7J.pem
up all
roup all

License Stealing






Windows Update

Windows Family | Windows


Windows Update Home

 Install Updates (50)

Options

- Review your update history
- Restore hidden updates
- Change settings
- FAQ
- Get help and support
- Use administrator options

Installing Updates

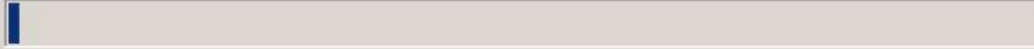


The updates are being downloaded and installed

Installation status:

- Downloading Security Update for Windows Server 2003 (KB924667) (update 4 of 50)... done!
- Downloading Cumulative Security Update for Outlook Express for Windows Server 2003 (KB929123) (update 5 of 50)... done!
- Downloading Security Update for Windows Media Player 6.4 (KB925398) (update 6 of 50)... done!
- Downloading Security Update for Windows Server 2003 (KB926122) (update 7 of 50)... |

Verifying the download:



Cancel

Why stop there?



-
- Video of neek steal:
 - <file:///localhost/Users/marco/Desktop/troopers10/6-steal-neek.mp4>

AWS as a single point of failure

- Availability is a huge selling point
- Some DoS attacks cant be stopped.. It's simply using the service..
- But it does need to be considered..

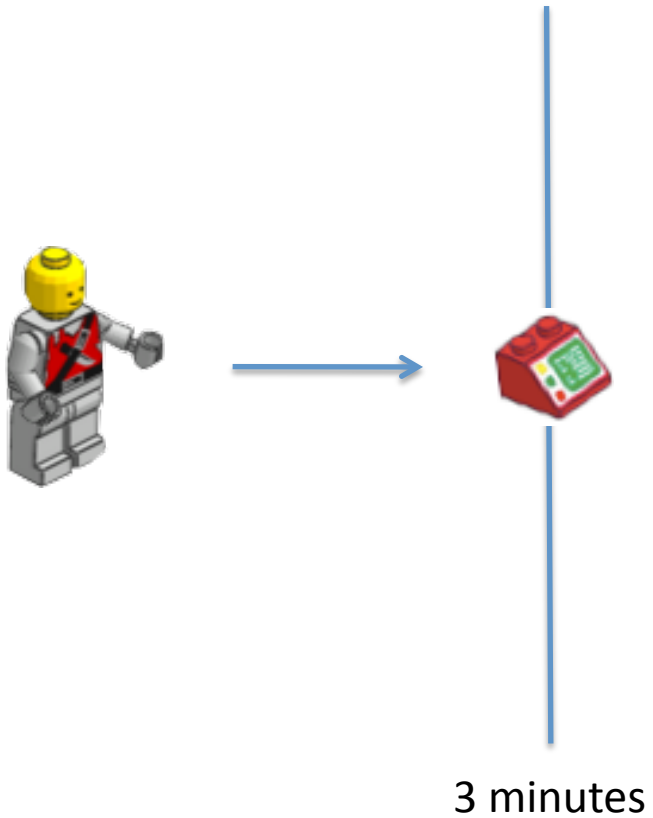
But it is Amazon!!

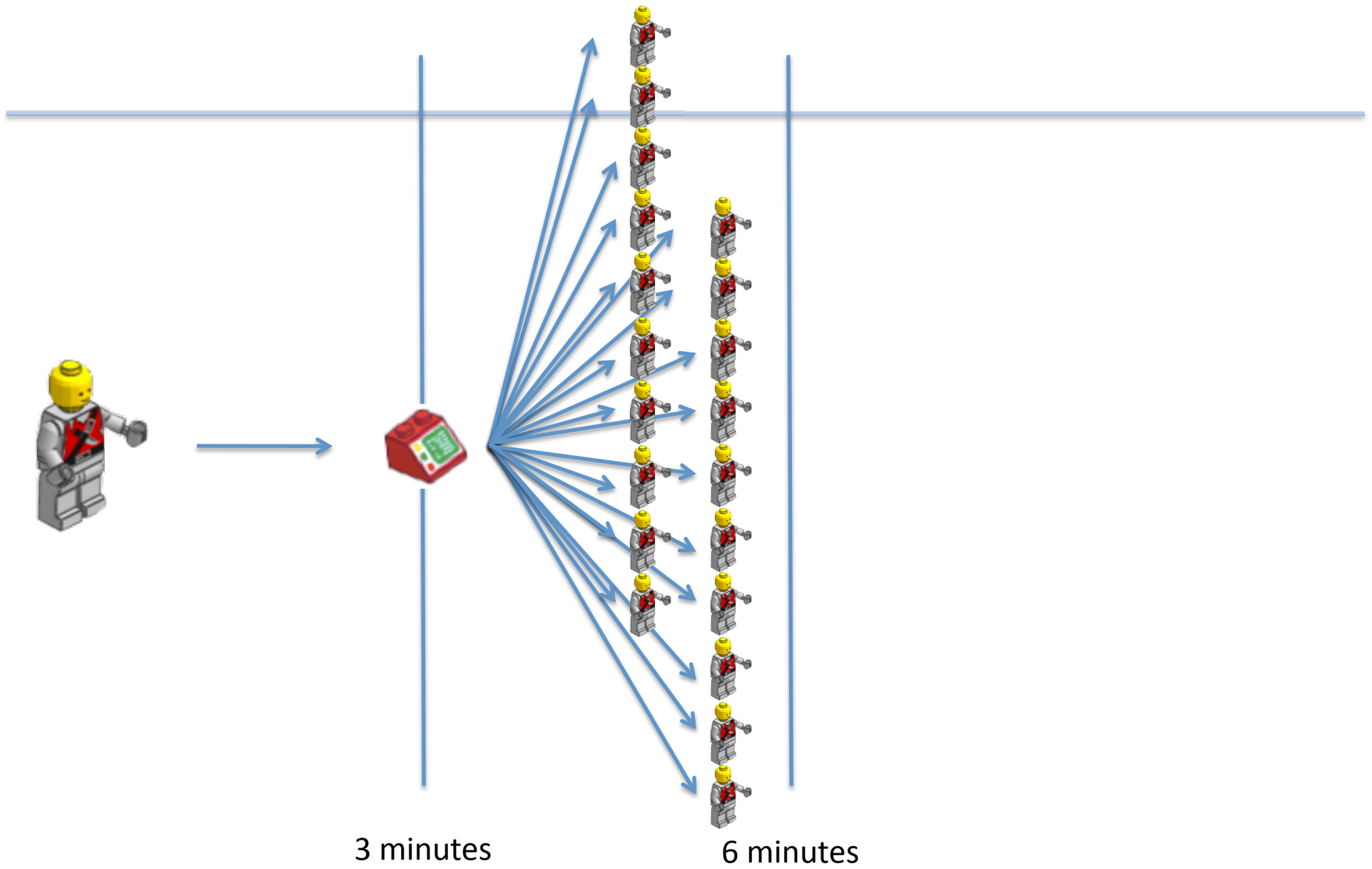
- **Distributed Denial Of Service (DDoS) Attacks:** AWS API endpoints are hosted on the same Internet-scale, world class infrastructure that supports the Amazon.com retail site. Standard DDoS mitigation techniques such as syn cookies and connection limiting are used. To further mitigate the effect of potential DDoS attacks, Amazon maintains internal bandwidth which exceeds its provider-supplied Internet bandwidth.

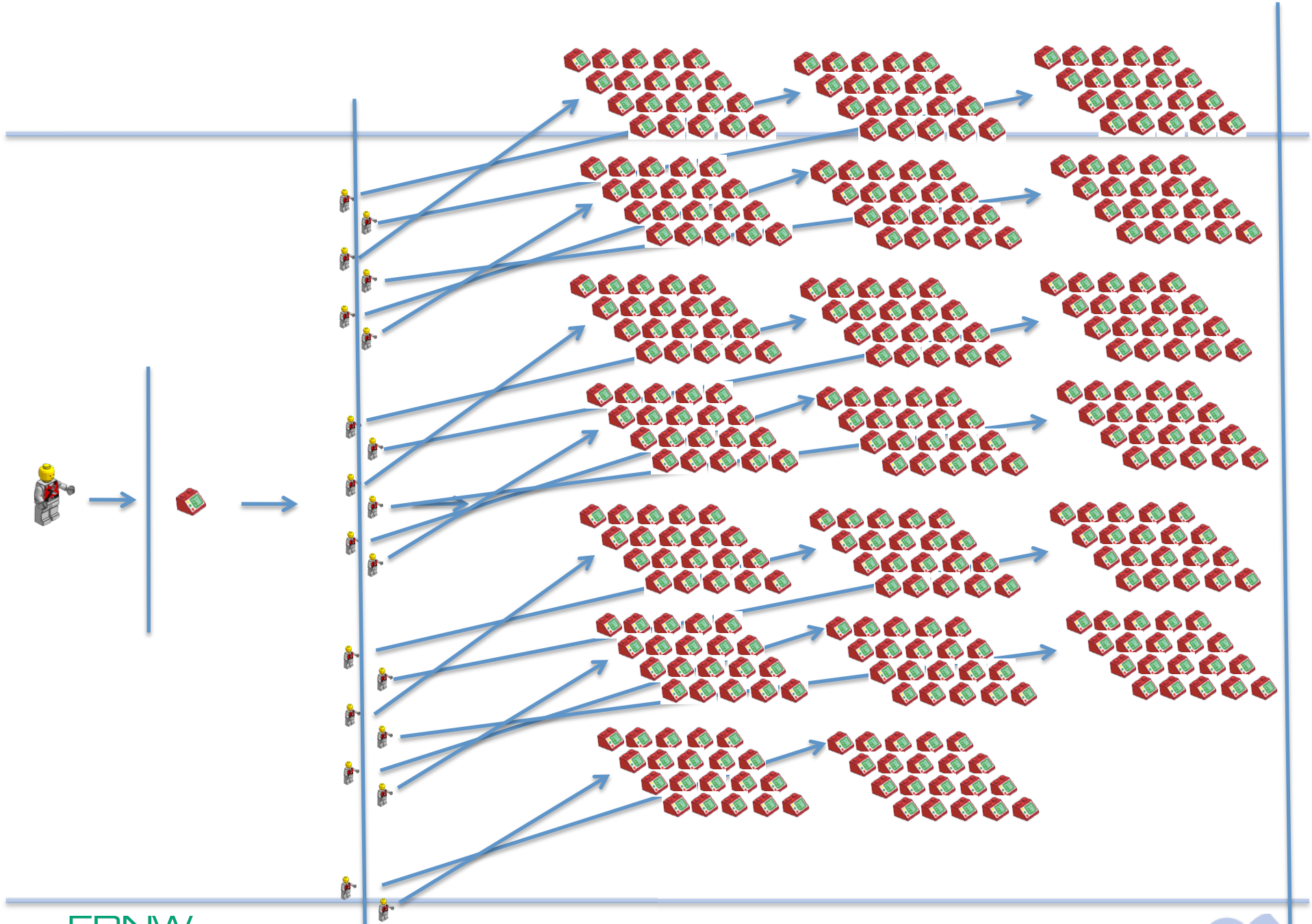
DDoS ? Really?



Scaling Registration?





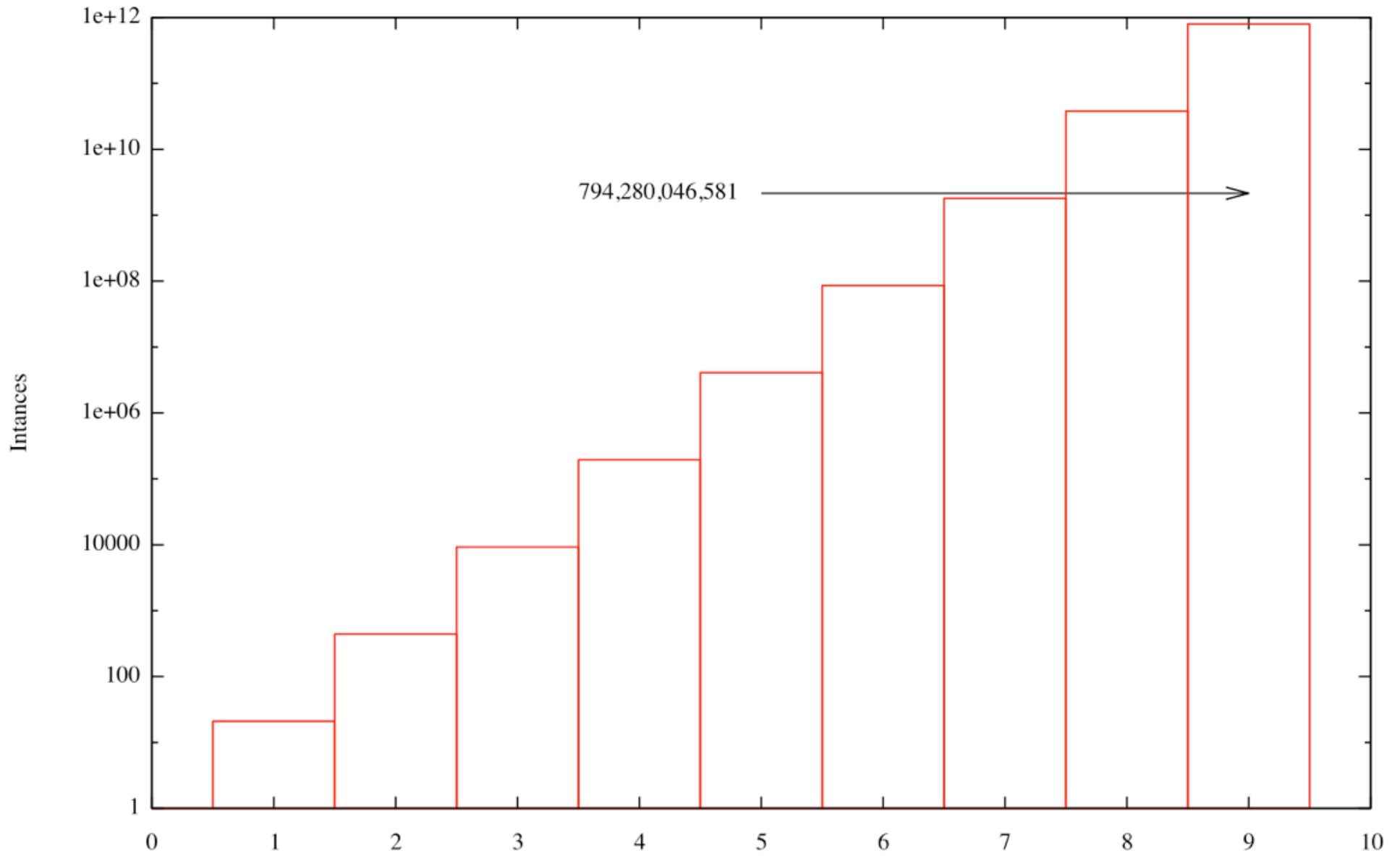


Twill Loving!

and

- <file:///localhost/Users/marco/Desktop/troopers10/7-ec2-create-20-proj.mp4>

Booting EC2 Instances Exponentially



Another way to steal machine time



If you plan to use a shared AMI, review the following table to confirm the AMI is not doing anything malicious.

Launch Confirmation Process

1	Check the ssh authorized keys file. The only key in the file should be the key you used to launch the AMI.
2	Check open ports and running services.
3	Change the root password if is not randomized on startup. For more information on randomizing the root password on startup, see Disable Password-Based Logins for Root .
4	Check if ssh allows root password logins. See Disable Password-Based Logins for Root for more information on disabling root based password logins.
5	Check whether there are any other user accounts that might allow backdoor entry to your instance. Accounts with super user privileges are particularly dangerous.
6	Verify that all cron jobs are legitimate.



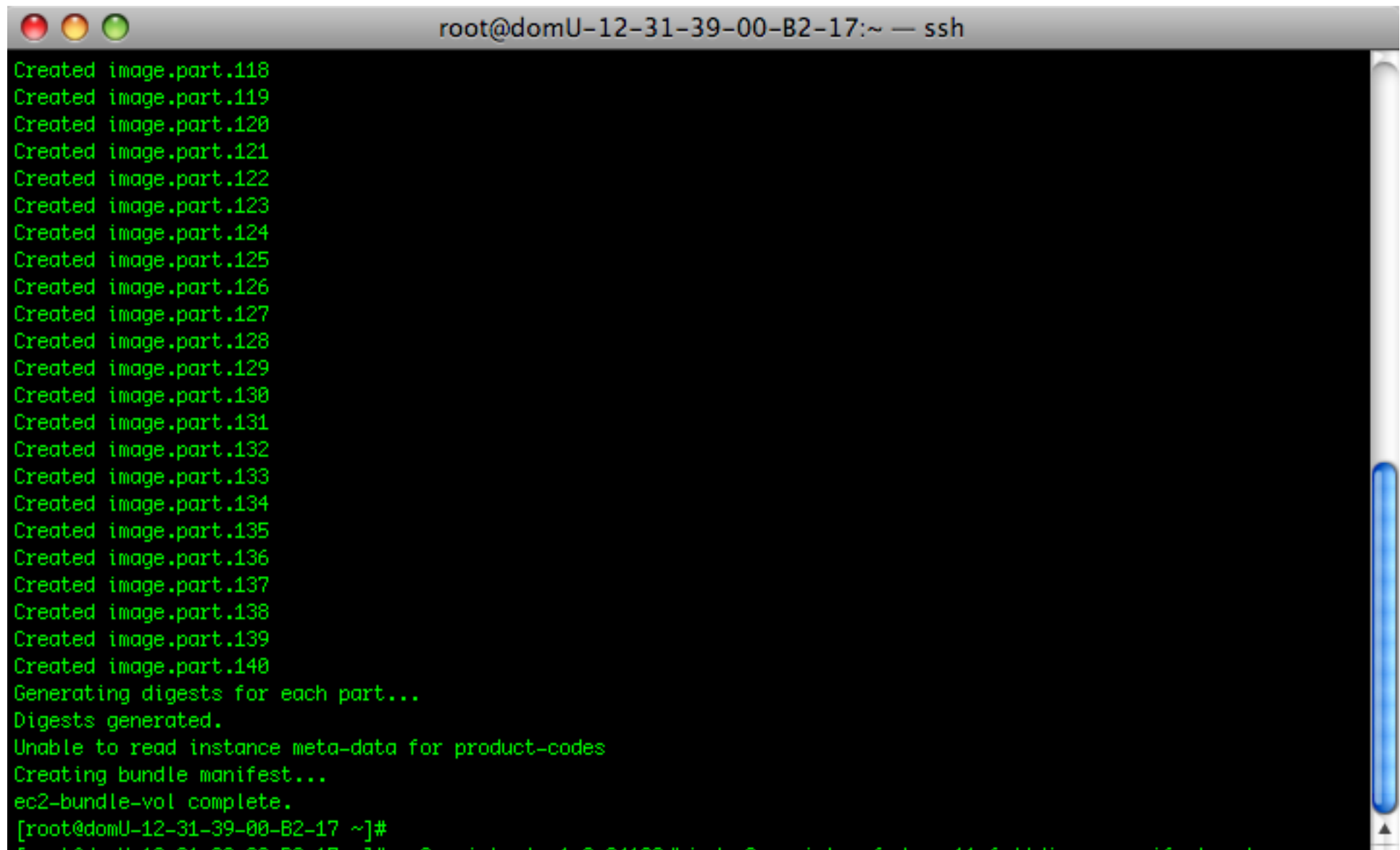
Really ?



Can we get people to run our image?

- Bundle an image
- Register the image (Amazon assigns it an AMI-ID)
- Wait for someone to run it
- Profit!
- Alas..

Can we get people to run our image?



```
root@domU-12-31-39-00-B2-17:~ — ssh
Created image.part.118
Created image.part.119
Created image.part.120
Created image.part.121
Created image.part.122
Created image.part.123
Created image.part.124
Created image.part.125
Created image.part.126
Created image.part.127
Created image.part.128
Created image.part.129
Created image.part.130
Created image.part.131
Created image.part.132
Created image.part.133
Created image.part.134
Created image.part.135
Created image.part.136
Created image.part.137
Created image.part.138
Created image.part.139
Created image.part.140
Generating digests for each part...
Digests generated.
Unable to read instance meta-data for product-codes
Creating bundle manifest...
ec2-bundle-vol complete.
[root@domU-12-31-39-00-B2-17 ~]#
```

Can we get people to run our image?

- Bundle an image
- Register the image (Amazon assigns it an AMI-ID)
- Wait for someone to run it
- Profit!
- Alas..

Register image, too high, race, top5

<file:///localhost/Users/marco/Desktop/troopers10/8-aws-race-proj.mp4>



-
- S3 + Image names are going to set off another name grab!
 - Register image as Fedora ?

```
[root@ec2box] # ec2-upload-bundle -b Fedora -  
m /tmp/image.manifest.xml -a secret -s  
secret
```

```
ERROR: Error talking to S3:  
Server.AccessDenied(403): Only the bucket owner  
can access this property
```

```
[root@ec2box] # ec2-upload-bundle -b  
  fedora_core -m /tmp/image.manifest.xml -a  
  secret -s secret
```

```
ERROR: Error talking to S3:  
  Server.AccessDenied(403): Only the bucket owner  
  can access this property
```

```
[root@ec2box] # ec2-upload-bundle -b redhat -  
m /tmp/image.manifest.xml -a secret -s  
secret
```

```
ERROR: Error talking to S3:  
Server.AccessDenied(403): Only the bucket owner  
can access this property
```

```
[root@ec2box] # ec2-upload-bundle -b  
  fedora_core_11 -m /tmp/image.manifest.xml  
  -a secret -s secret
```

```
Creating Bucket...
```

Amazon EC2

Amazon Elastic MapReduce

Amazon CloudFront

Navigation

Region: US-East

EC2 Dashboard

INSTANCES

Instances

IMAGES

AMIs

Bundle Tasks

ELASTIC BLOCK STORE

Volumes

Snapshots

NETWORKING & SECURITY

Elastic IPs

Security Groups

Key Pairs

Amazon Machine Images

Launch Register New AMI De-register Permissions

Show/Hide Refresh Help

Viewing: All Images All Platforms 1 to 50 of 2767 AMIs

AMI ID	Manifest	Visibility	Platform
ami-0022c769	level22-ec2-images/ubuntu-7.04-feisty-base-20071225a.manifest.xml	Public	Ubuntu
ami-005db969	alestic-64/ubuntu-8.04-hardy-base-64-20081222.manifest.xml	Public	Ubuntu
ami-005dba69	rbuilder-online/new-example-1-x86_64_20133.img.manifest.xml	Public	Other Linux
ami-005eba69	kaavo-ntier-db/imod-ntier-32bit-FC-DB.manifest.xml	Public	Other Linux
ami-00e70069	abami/image.manifest.xml	Public	Other Linux
ami-0111f068	prod-ec2-images/private_install-Jul24-2009.manifest.xml	Public	Other Linux
ami-0111f768	yale-vldb/hadoop-0.19.1-x86_64.manifest.xml	Public	Other Linux
ami-0118fe68	citrix-c3-lab/XenApp5.0_32bit_v1.1.manifest.xml	Public	Windows
ami-0121c068	qscan/image.manifest.xml	Private	Other Linux
ami-0123c268	fedora_11_full/image.manifest.xml	Public	Fedora
ami-0129cc68	cer-64-centos5_10-1/image.manifest.xml	Public	Cent OS
ami-014da868	ami.alurium.com/image_bundles/Fedora6_Jetty_OpenBD/image.manife	Public	Fedora
ami-015abc68	jumpbox-cloud-gear/wordpress-1.1.5.manifest.xml	Public	Other Linux
ami-015cba68	jumpbox-cloud-gear/drupal-1.1.12.manifest.xml	Public	Other Linux
ami-015db968	alestic-64/ubuntu-8.04-hardy-rightsacle-64-20081222.manifest.xml	Public	Ubuntu
ami-015dba68	rbuilder-online/new-example-1-x86_64_20134.img.manifest.xml	Public	Other Linux
ami-01648368	rbuilder-online/dj-flatpress-1-x86_64_19855.img.manifest.xml	Public	Other Linux
ami-01729468	alestic/ubuntu-8.10-intrepid-desktop-20090614.manifest.xml	Public	Ubuntu
ami-01749368	sixsq-slipstream-images/Examples/Apache/apache/cd4ae856-27b1-4	Public	Other Linux

```
[haroon@blowfish ~]$ tail -f /var/log/httpd-ssl_error.log
[Wed Jul 15 15:02:09 2009] [client 75.101.178.184] /usr/local/www/data-ssl/EC2_IMAGE_BOOTED
[Wed Jul 15 15:04:47 2009] [client 75.101.178.184] /usr/local/www/data-ssl/EC2_IMAGE_BOOTED
[Wed Jul 15 15:04:56 2009] [client 75.101.178.184] /usr/local/www/data-ssl/EC2_IMAGE_KILLED
```

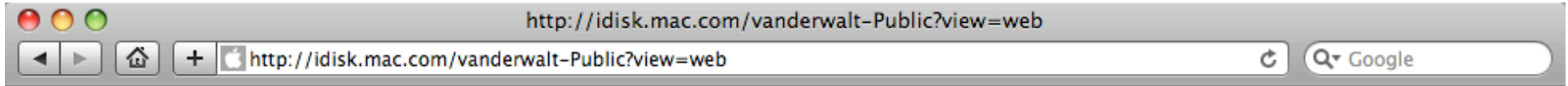

New Mistake, Old Mistake

Amazon Web Services Security		Thread Tools ▾	Display Modes ▾
<p>10-07-2008, 11:30 AM</p> <p>celeduc Junior Member Fog</p> <p>Blocking outbound connections</p> <p>Is there a way to block outgoing connections that can be blocked except those specifically needed for the application?</p> <p>I've looked over the (scanty) EC2 documentation and am concerned only with incoming traffic. Thanks.</p>	<p>administer EC2 hosts, their privileges on and access to the bastion hosts are revoked.</p> <ul style="list-style-type: none">• Guest Operating System: Virtual instances are completely controlled by the customer. They have full root access and all administrative control over additional accounts, services, and applications. AWS administrators do not have access to customer instances, and cannot log into the guest OS. Customers should disable password-based access to their hosts and utilize token or key-based authentication to gain access to unprivileged accounts. Further, customers should employ a privilege escalation mechanism with logging on a per-user basis. For example, if the guest OS is Linux, utilize SSH with keys to access the virtual instance, enable shell command-line logging, and use the 'sudo' utility for privilege escalation. Customers should generate their own key pairs in order to guarantee that they are unique, and not shared with other customers or with AWS.• Firewall: Amazon EC2 provides a complete firewall solution; this mandatory inbound firewall is configured in a default deny mode and the Amazon EC2 customer must explicitly open any ports to allow inbound traffic. The traffic may be restricted by protocol, by service port, as well as by source IP address (individual IP or CIDR block).	<p>#1</p> <p>Join Date: Sep 2008 Location: Vancouver, BC Canada Posts: 5</p> <p></p> <p>its that all outbound ports</p> <p>groups seem to be</p> <p> Quote</p>	
<p>10-07-2008, 11:59 AM</p> <p>Eddyys Member Stratocumulus</p> <p></p> <p>Why are you trying to block outbound connections? The only reason I could think of off the top of my head is that I don't quite know the answer.</p> <p>- Eddyys</p>		<p>#2</p> <p>Join Date: Oct 2008 Posts: 45</p> <p>to do this. The only reason I don't do this, I am sorry I don't</p> <p> Quote</p>	

Mobile me

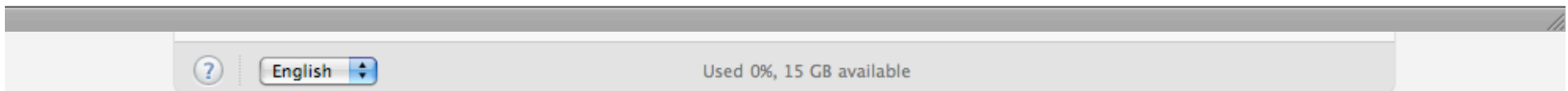
- Apple sneaks into the cloud
- Makes sense long term, your music, video, * are belong to Steve Jobs
- Insidious
- iDisk, iMail, iCal, findmyPhone

Hacked by..



Account Error: Nonexistent

- Mike Arrington! (Techcrunch)
- Account name leakage
- Not the end of the world.. but





http://idisk.mac.com/steve-Public?view=web

Google



Back/Forward iDisk Home

iDisk



New Folder Upload

steve's Public Folder

Name	Date Modified	Size
------	---------------	------

--	--	--

English

Used 0%, 75 GB available

Account password reset

- A hard problem to solve in the cloud..
- Forgot password → Nick
- <file:///localhost/Users/marco/Desktop/troopers10/9-mobileme-1.mp4>
- All dressed up and nowhere to go?
- Is everyone as “easy” as Nick?

and so?

- Told ya it was insidious..
- We have been going lower and lower with trojans now living in firmware
- Will we notice the trojans so high up in the stack that follow us everywhere?
- We all looked down on XSS initially
- <file:///localhost/Users/marco/Desktop/troopers10/10-mobileme-2.mp4>
- Finally, for fun:
- <file:///localhost/Users/marco/Desktop/troopers10/11-mobileme-3.mp4>



Conclusions #1

- There are new problems to be solved (and some new solutions to old problems) with computing power on tap.
- Marrying infrastructure to web applications means that your enterprise now faces risks from both infrastructure dodgyness and bad web application code.
- Even if marrying *aaS to web applications makes sense, tying them to Web2.0 seems like a bad idea.

Conclusions #2

- Auditors need to start considering the new risks the new paradigm brings:
 - (negative) One more set of problems scanners cant find
 - (positive) job security++
- Computationally difficult is easily within reach of anyone with a Credit Card. Tech skills not required
- We are getting moved into the cloud even if we don't know it. (Making us vulnerable to the “lame attacks” even if we don't rate them)
- Transparency and testing are going to be key..
- WOZ is cool...

Questions ?

(Videos/Slides/Tools)

<http://www.sensepost.com/blog/>
research@sensepost.com