"Get Off of My Cloud": Cloud Credential Compromise and Exposure

Ben Feinstein & Jeff Jarmoc

Dell SecureWorks Counter Threat Unit℠

Get Off Of My Cloud
DL. 25205
I'm Free
THE ROLLING STONES
DECCA

The Public Cloud

Brief Introduction to the Amazon Cloud

- First, some terminology and definitions…

amazon webservices™

- Amazon Web Services (AWS)
- Elastic Compute Cloud (EC2)
- Amazon Machine Image (AMI)
- Simple Storage Service (S3)
- Elastic Block Store (EBS)

BusinessWeek

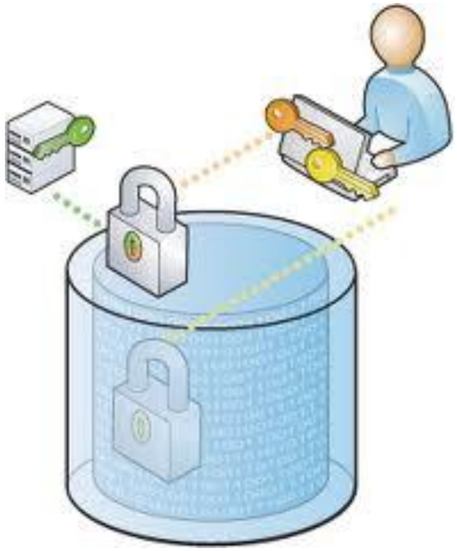
Amazon's Risky Bet

CEO Jeff Bezos wants to run your business with his Web technology. Wall Street wishes he would just mind the store.

BY ROBERT D. HOF (P.52)

AWS Security Credentials

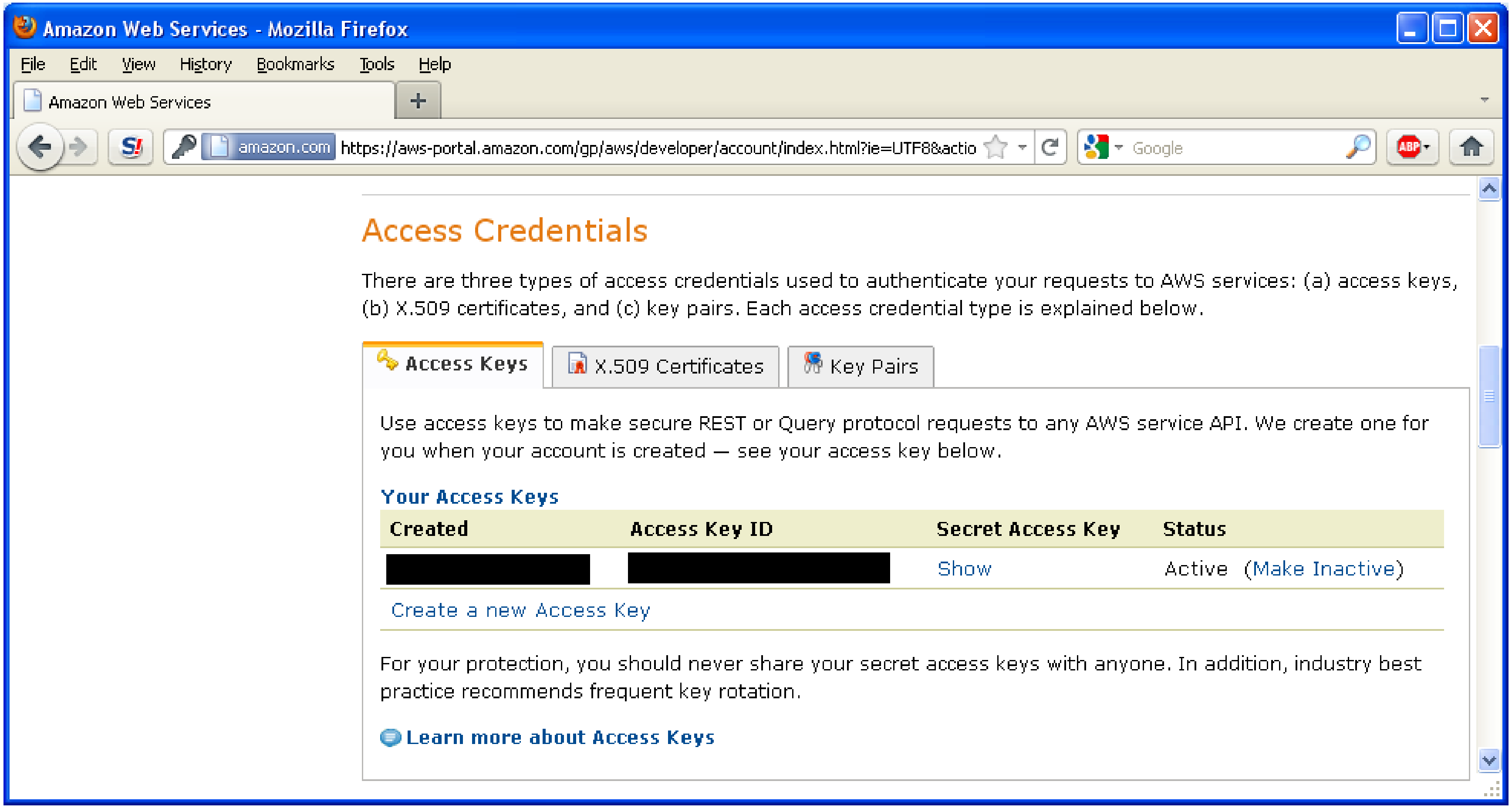
- Access Credentials
  - Access Keys
  - X.509 Certificates
  - Amazon EC2 Key Pairs
  - Amazon CloudFront Key Pairs
- Sign-In Credentials
  - Email Address & Password
  - AWS Multi-Factor Authentication Device (optional)
- Account Identifiers
  - AWS Account ID
  - Canonical User ID



AWS Access Credentials: Access Keys

- Each Access Key has a public and a secret part
  - Access Key ID
    - Unique identifier, Included in each API request
  - Secret Access Key
    - Used to calculate a digital signature included in each API request
    - Amazon validates digital signature to ensure authenticity of each API request
- Managed via "Access Keys" tab of "AWS Security Credentials" page
  - [screenshot]
- Used for making requests to AWS product REST or Query APIs
- Used for SOAP APIs of Amazon S3 and Amazon Mechanical Turk
- Used for making requests to Amazon CloudFront control API
- For security purposes, Amazon recommends rotating Access Keys every 90 days

Managing Access Keys


Amazon Web Services - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Amazon Web Services
amazon.com
https://aws-portal.amazon.com/gp/aws/developer/account/index.html?ie=UTF8&actio
Google

Access Credentials

There are three types of access credentials used to authenticate your requests to AWS services: (a) access keys, (b) X.509 certificates, and (c) key pairs. Each access credential type is explained below.

Access Keys
X.509 Certificates
Key Pairs

Use access keys to make secure REST or Query protocol requests to any AWS service API. We create one for you when your account is created — see your access key below.

Your Access Keys

Created	Access Key ID	Secret Access Key	Status
[redacted]	[redacted]	Show	Active (Make Inactive)

Create a new Access Key

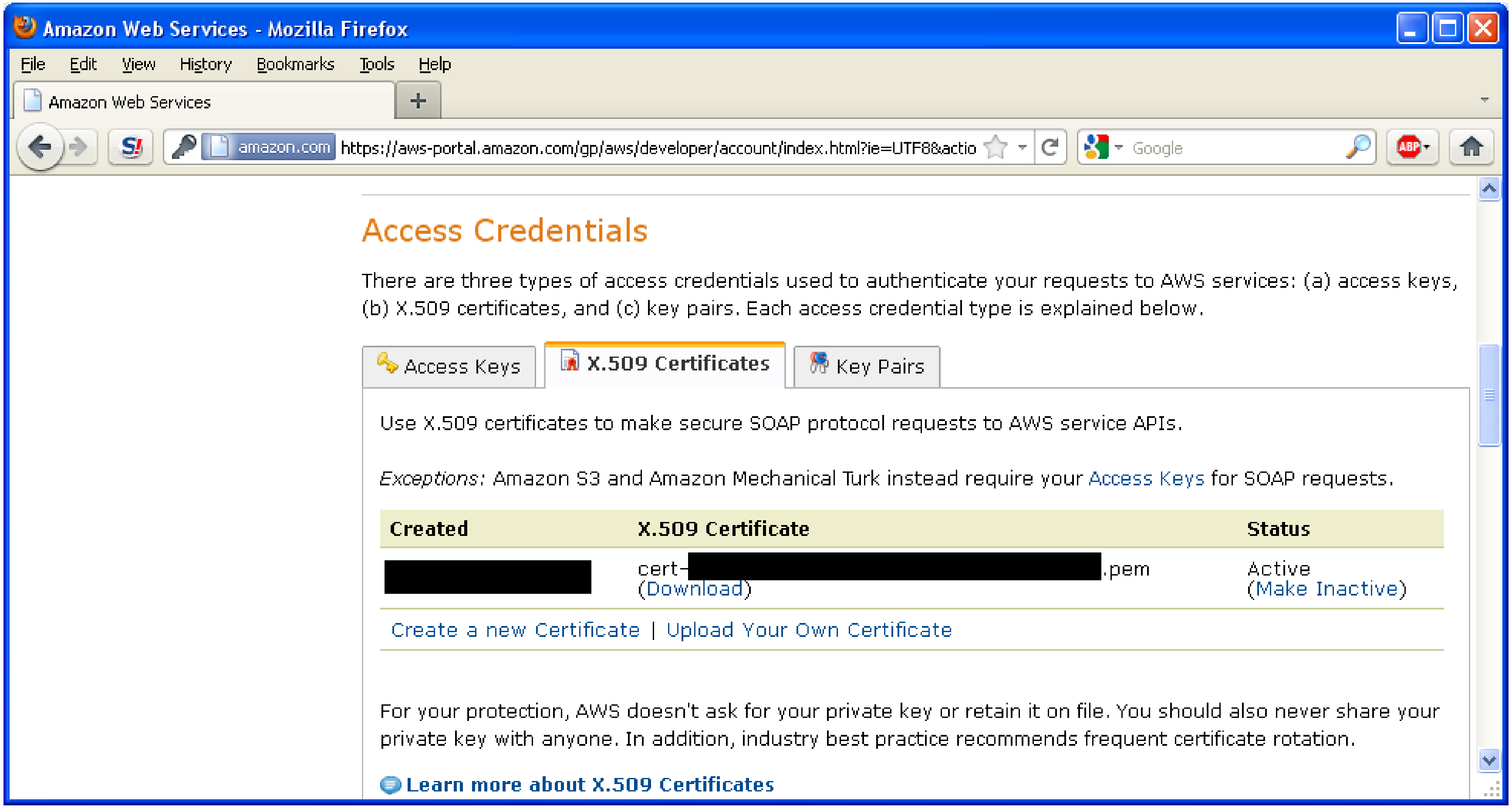
For your protection, you should never share your secret access keys with anyone. In addition, industry best practice recommends frequent key rotation.

Learn more about Access Keys

AWS Access Credentials: X.509 Certificates

- AWS can generate certificate and private key files, or user can provide their own certificate
  - Trade-off of convenience versus security
- Managed via “X.509 Certificates” tab of “AWS Security Credentials” page
  - [screenshot]
- Used for making requests to AWS product SOAP APIs
  - … with the exception of Amazon S3 and Amazon Mechanical Turk
- Also used for “bundling” AMIs, which are encrypted and signed using user’s certificate and private key
- For security purposes, Amazon recommends replacing X.509 Certificates every 90 days

Managing X.509 Certificates



Amazon Web Services - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Amazon Web Services
amazon.com https://aws-portal.amazon.com/gp/aws/developer/account/index.html?ie=UTF8&actio
Google

Access Credentials

There are three types of access credentials used to authenticate your requests to AWS services: (a) access keys, (b) X.509 certificates, and (c) key pairs. Each access credential type is explained below.

Access Keys | X.509 Certificates | Key Pairs

Use X.509 certificates to make secure SOAP protocol requests to AWS service APIs.

Exceptions: Amazon S3 and Amazon Mechanical Turk instead require your Access Keys for SOAP requests.

Created	X.509 Certificate	Status
[redacted]	cert-[redacted].pem (Download)	Active (Make Inactive)

Create a new Certificate | Upload Your Own Certificate

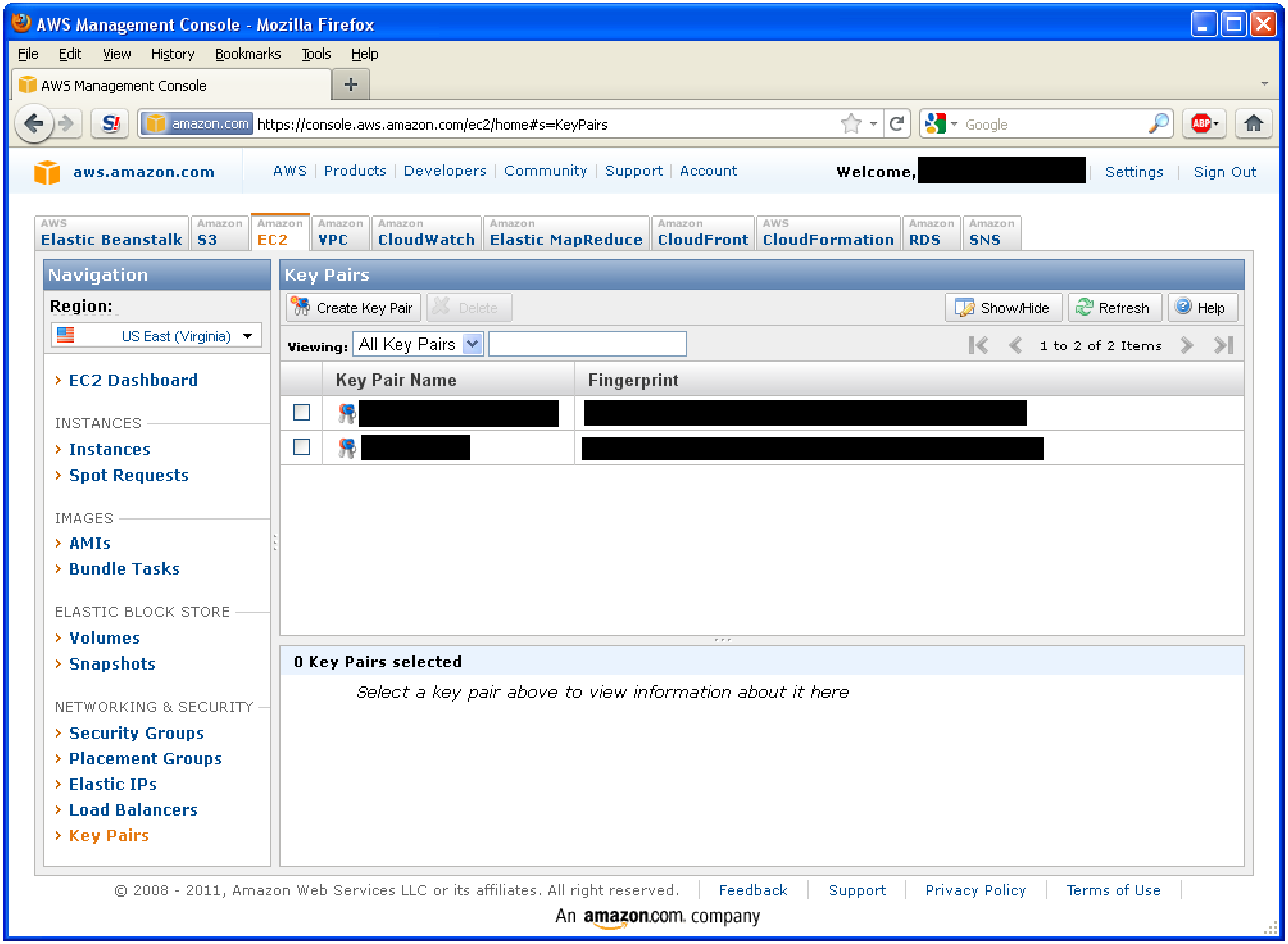
For your protection, AWS doesn't ask for your private key or retain it on file. You should also never share your private key with anyone. In addition, industry best practice recommends frequent certificate rotation.

Learn more about X.509 Certificates

AWS Access Credentials: EC2 Key Pairs

- Created and managed with Amazon EC2 API, or any interface or tool using the API
  - e.g., AWS Management Console
  - [screenshot]
- Comprised of a private key, public key and a key pair name
- Used for launching and connecting to Amazon EC2 instances
  - For Linux/UNIX EC2 instances, used for root SSH access
  - For administrative Remote Desktop access to Windows instances, private key is used in API call to retrieve and decrypt the administrator password
- No explicit security recommendations from Amazon about key pair rotation

AWS Management Console: Key Pairs



□	Key Pair Name	Fingerprint
□	[redacted]	[redacted]
□	[redacted]	[redacted]

0 Key Pairs selected

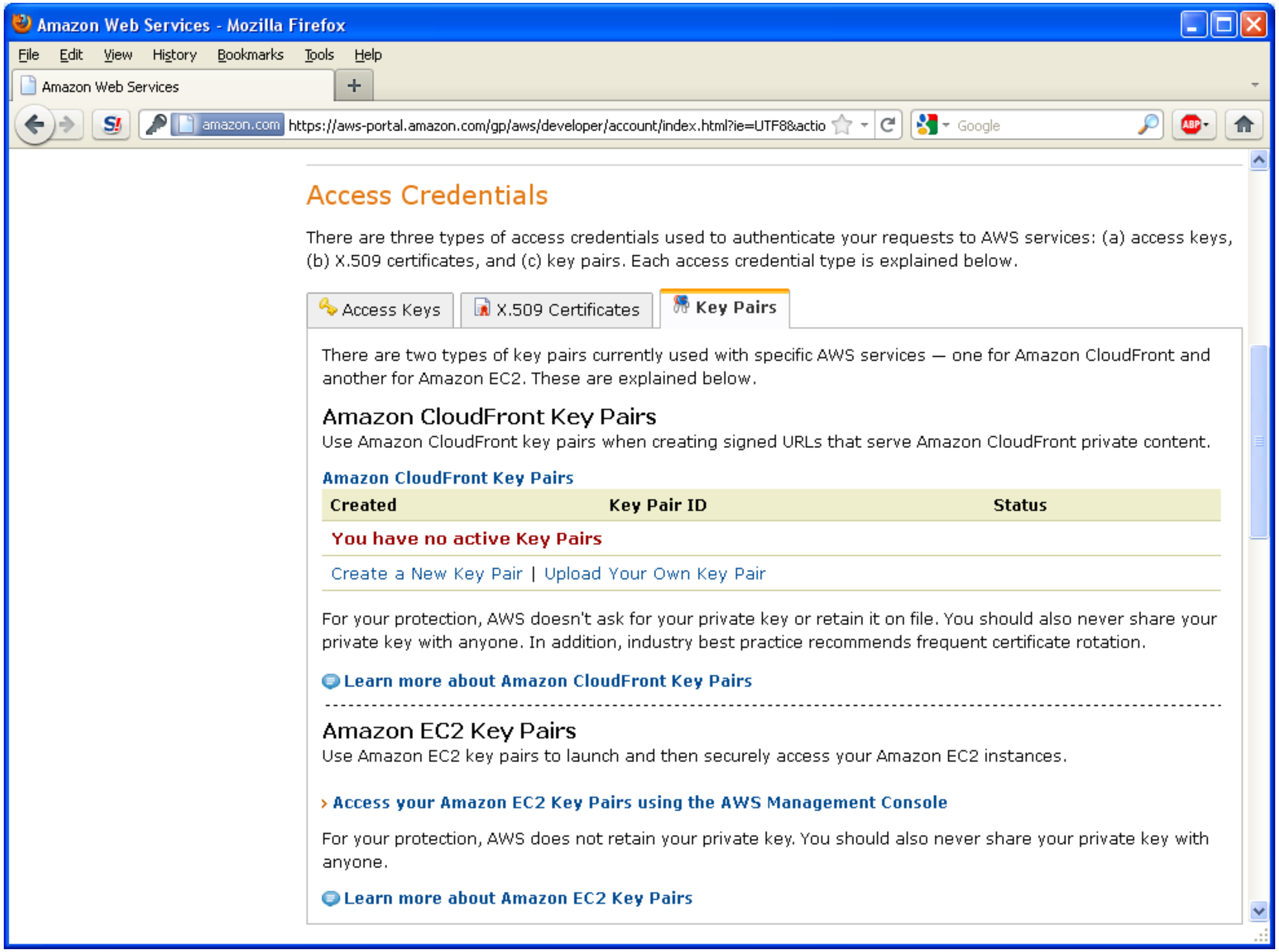
Select a key pair above to view information about it here

© 2008 - 2011, Amazon Web Services LLC or its affiliates. All right reserved. | Feedback | Support | Privacy Policy | Terms of Use
An amazon.com. company

AWS Access Credentials: CloudFront Key Pairs

- AWS can generate the key pair for you, or user can provide their own
  - Trade-off of convenience versus security
  - Amazon states that while they generate the private key on user's behalf, they do not store it anywhere
- Comprised of a private key, public key and a key pair name
- Used to generate signed URLs for access to private Amazon CloudFront content
- For security purposes, Amazon recommends rotating Amazon CloudFront key pairs every 90 days
- CloudFront also uses Access Keys to authenticate requests to CloudFront control API

Managing Amazon CloudFront Key Pairs



Amazon Web Services - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Amazon Web Services
amazon.com https://aws-portal.amazon.com/gp/aws/developer/account/index.html?ie=UTF8&actio
Google

Access Credentials

There are three types of access credentials used to authenticate your requests to AWS services: (a) access keys, (b) X.509 certificates, and (c) key pairs. Each access credential type is explained below.

Access Keys
X.509 Certificates
Key Pairs

There are two types of key pairs currently used with specific AWS services — one for Amazon CloudFront and another for Amazon EC2. These are explained below.

Amazon CloudFront Key Pairs

Use Amazon CloudFront key pairs when creating signed URLs that serve Amazon CloudFront private content.

Amazon CloudFront Key Pairs

Created	Key Pair ID	Status
You have no active Key Pairs		
Create a New Key Pair | Upload Your Own Key Pair		

For your protection, AWS doesn't ask for your private key or retain it on file. You should also never share your private key with anyone. In addition, industry best practice recommends frequent certificate rotation.

Learn more about Amazon CloudFront Key Pairs

Amazon EC2 Key Pairs

Use Amazon EC2 key pairs to launch and then securely access your Amazon EC2 instances.

› **Access your Amazon EC2 Key Pairs using the AWS Management Console**

For your protection, AWS does not retain your private key. You should also never share your private key with anyone.

Learn more about Amazon EC2 Key Pairs

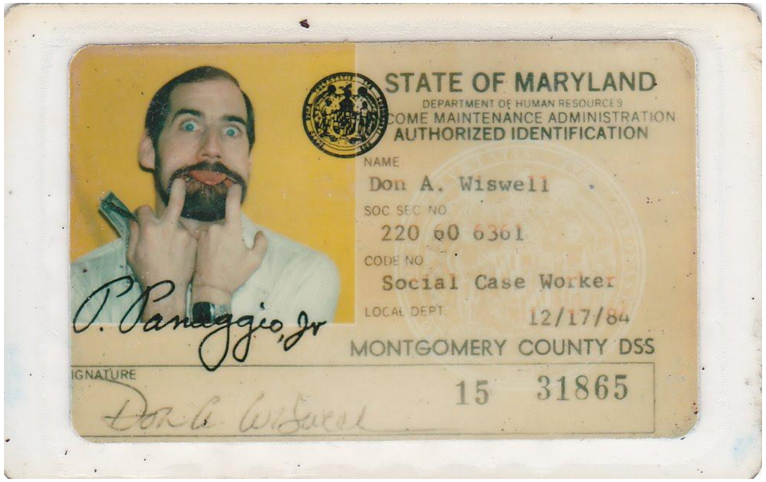
AWS Sign-In Credentials:
E-mail Address and Password

- Simply an Amazon.com account that is activated for AWS services
- Used for access to secure areas of AWS web site
- Used to access AWS Management Console
- Used to access AWS Discussion Forums and AWS Premium Support
- Amazon's recommended password complexity
  - Minimum of 8 characters
  - Include both uppercase and lowercase letters
  - Include at least 1 numeric digit
  - Include at least one special character
- AWS Multi-Factor Authentication is recommended for additional protection
- Does not appear password complexity is enforced

AWS Sign-In Credentials: Multi-Factor Authentication

- Optional AWS account feature recommended for additional security
- Second factor is a six-digit code generated by user's authentication device
- Currently supports Gemalto Ezio Time Token
  - Available for $12.99 in the "Gemalto Webstore for AWS Users"
- Only protects some Amazon web properties
  - Secure pages on the AWS Portal
  - AWS Management Console
  - Notably, does not protect AWS Premium Support site
- Does not protect AWS service APIs

AWS Account Identifiers



STATE OF MARYLAND
DEPARTMENT OF HUMAN RESOURCES
COME MAINTENANCE ADMINISTRATION
AUTHORIZED IDENTIFICATION

NAME
Don A. Wiswell

SOC SEC NO
220 60 6361

CODE NO
Social Case Worker

LOCAL DEPT
12/17/84

MONTGOMERY COUNTY DSS

P. Panaggio, Jr

IGNATURE

15 31865

- Each AWS account has two unique IDs
  - (why have one when you can have two, twice as good!)

- AWS Account ID
  - 12 digit number (AWS Account ID without the hyphens)
  - Used to bundle Linux/UNIX AMIs
  - Used to share AWS resources with other AWS accounts
    - Amazon EC2 AMI
    - Amazon EBS snapshot
    - Amazon SQS queue

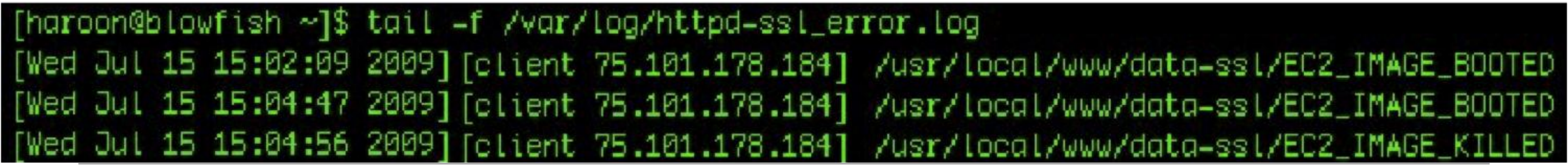
- Canonical User ID
  - Used to share Amazon S3 resources with other AWS accounts

Prior Research

- "Cloud Computing Models and Vulnerabilities: Raining on the Trendy New Parade", Alex Stamos, Andrew Becherer, Nathan Wilcox,
  Black Hat USA 2009 / DEF CON 17
  http://www.sensepost.com/blog/3797.html
  https://www.blackhat.com/html/bh-usa-09/bh-usa-09-speakers.html#Stamos

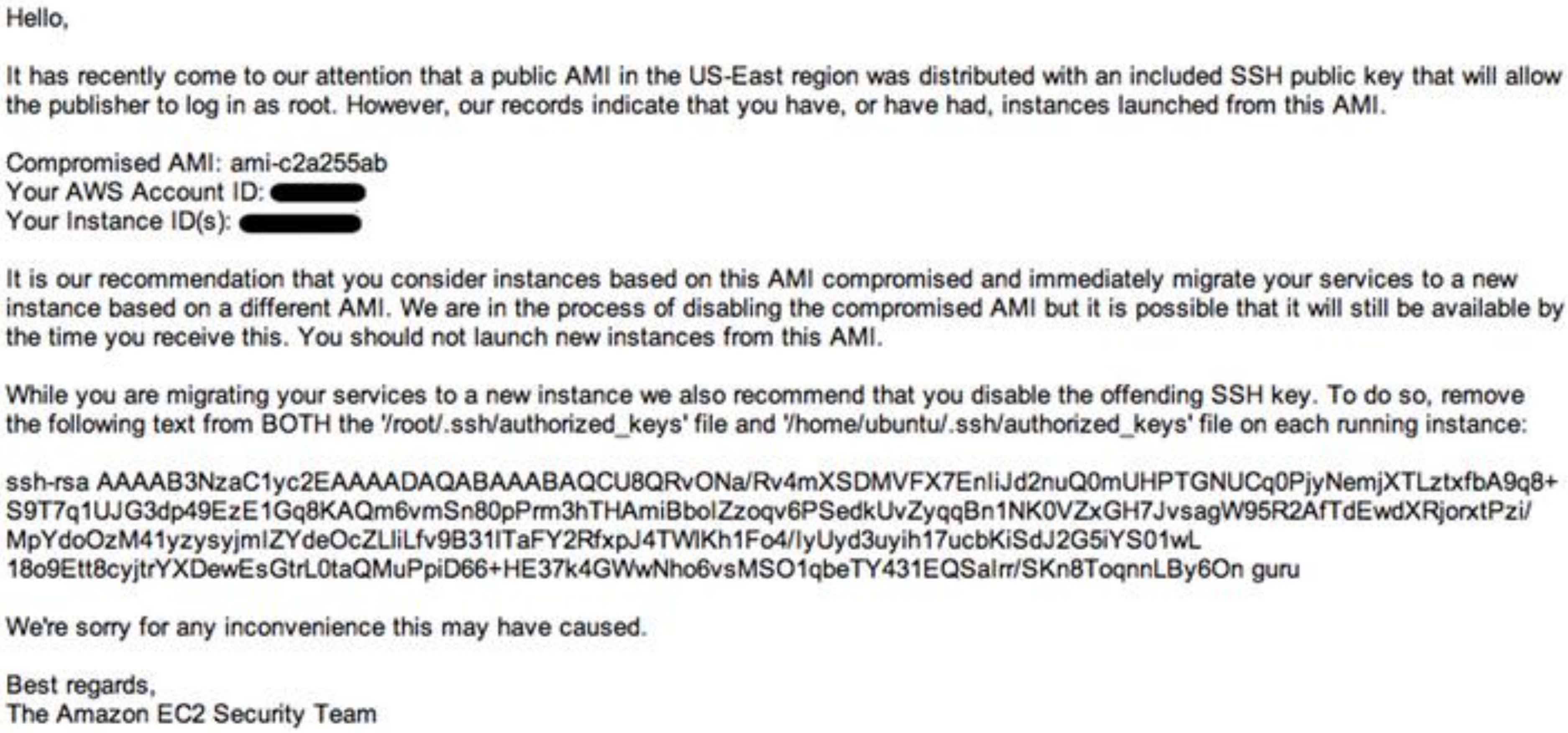
- Demonstrated method to get prime placement in AWS list of available AMIs

- Demonstrated ease of getting users to run an untrustworthy AMI



```
[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
```

Precendent



Hello,

It has recently come to our attention that a public AMI in the US-East region was distributed with an included SSH public key that will allow the publisher to log in as root. However, our records indicate that you have, or have had, instances launched from this AMI.

Compromised AMI: ami-c2a255ab
Your AWS Account ID: [redacted]
Your Instance ID(s): [redacted]

It is our recommendation that you consider instances based on this AMI compromised and immediately migrate your services to a new instance based on a different AMI. We are in the process of disabling the compromised AMI but it is possible that it will still be available by the time you receive this. You should not launch new instances from this AMI.

While you are migrating your services to a new instance we also recommend that you disable the offending SSH key. To do so, remove the following text from BOTH the '/root/.ssh/authorized_keys' file and '/home/ubuntu/.ssh/authorized_keys' file on each running instance:

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCU8QRvONa/Rv4mXSDMVFX7EnliJd2nuQ0mUHPTGNUCq0PjyNemjXTLztxfbA9q8+
S9T7q1UJG3dp49EzE1Gq8KAQm6vmSn80pPrm3hTHAmiBbolZzoqv6PSedkUvZyqqBn1NK0VZxGH7JvsagW95R2AfTdEwdXRjorxtPzi/
MpYdoOzM41yzysyjmlZYdeOcZLliLfv9B31lTaFY2RfxpJ4TWlKh1Fo4/lyUyd3uyih17ucbKiSdJ2G5iYS01wL
18o9Ett8cyjtrYXDewEsGtrL0taQMuPpiD66+HE37k4GWwNho6vsMSO1qbeTY431EQSalrr/SKn8ToqnnLBy6On guru
```

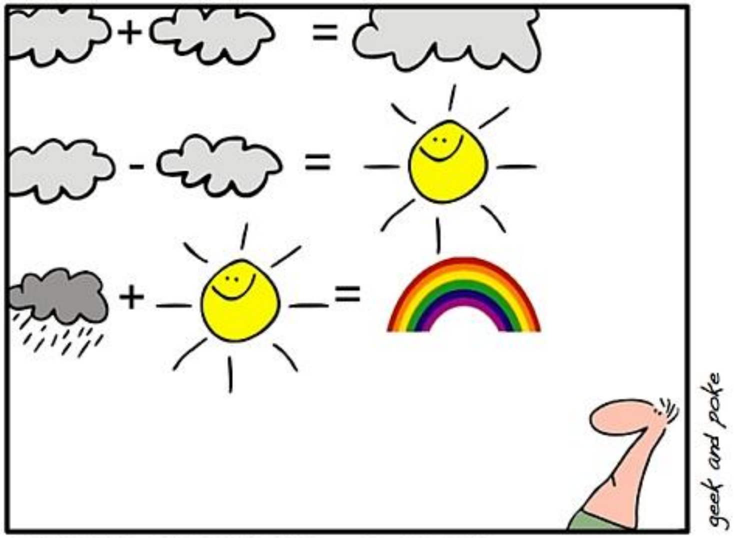
We're sorry for any inconvenience this may have caused.

Best regards,
The Amazon EC2 Security Team

"Cloud Security: Amazon's EC2 serves up 'certified pre-owned' server images", April 11th, 2011, Alen Puzic, TippingPoint DVLabs http://dvlabs.tippingpoint.com/blog/2011/04/11/cloud-security-amazons-ec2-serves-up-certified-pre-owned-server-images

Our Work

- Understanding of AWS credential types and their "order of precedence"
- Understanding of common mistakes / pitfalls
- Tools to detect credential exposure within images



SIMPLY EXPLAINED – PART 17:
CLOUD COMPUTING

- Tools to detect malicious images / backdoor'd images
- Experiment to quantify scale of potential victims of a malicious AMI
- Consistent with our reading of the "Amazon Web Services Customer Agreement" and the "Amazon Web Services Terms of Use"

Related Research

- Apparently, we weren't the only ones working on this problem!

- Center for Advanced Security Research Darmstadt
  - Prof. Dr.-Ing. Ahmad-Reza Sadeghi, Dr.-Ing. Thomas Schneider, Sven Bugiel, Stefan Nürnberger, and Thomas Pöppelmann
  - http://trust.cased.de/AMID

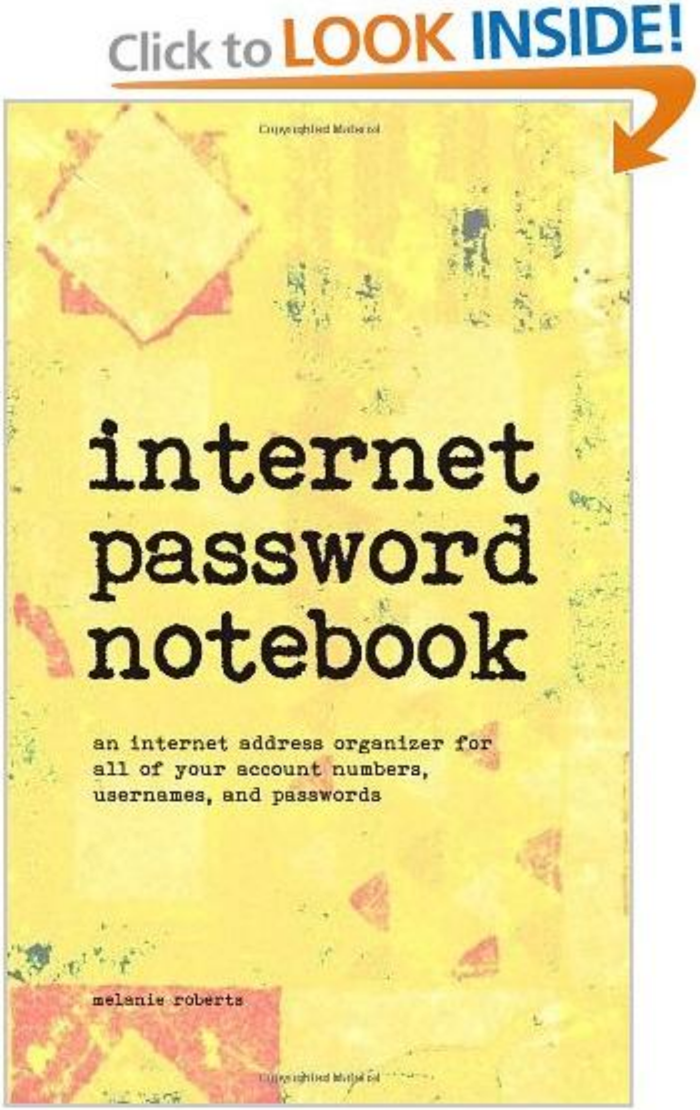
- AMI aiD (AMID) tool released on Google Code
  - http://code.google.com/p/amid/

Sir Isaac Newton (left) and Gottfried Wilhelm von Leibniz (right)

Mistakes When Creating a Public or Shared AMI

- AMI filesystem
  - AWS Cert + Private Key
  - SSH Key Pairs
  - SSL certs and private keys

- Bash history files containing environmental variable exports or command-line usage of credentials (e.g., Secret Access Key)
- Bash profile (e.g., .bashrc, .bash_profile) containing environmental variable exports
- Contents of .viminfo files



Copyrighted Material

internet password notebook

an internet address organizer for all of your account numbers, usernames, and passwords

melanie roberts

Copyrighted Material

Signs of a Compromised / Malicious AMI

- SSH authorized keys
- Rootkits
- Trojaned binaries (e.g., sshd)
- Open sockets (e.g., reverse shell / connect back)
- Trojaned custom Xen kernel

Expanding upon prior work on “Evil AMIs”

- Black Hat USA 2009 / DEF CON 17, Stamos et. al.

- We know victims are easy to find, but lets quantify this with data

- What size of instances?
- How many instances being launched in tandem?
- What AWS Regions and Availability Zones being launched in?

- **Would the instance’s AWS Security Group (i.e., EC2 firewall policy) have prevented remote SSH access, in case of a SSH authorized key?**

AMIexposed tool

- An extensible framework for scanning AMIs for common credential leakage and security problems

- Uses Amazon's APIs to automate
  - Generation of a list of images within scope
  - Launch instances of each image
  - Run tests via SSH session
  - Record findings to a database

AMIexposed: Test Modules

- Presence of SSH authorized_keys
  - Potential backdoor
- Presence of SSH identity keys
  - Can be used to gain illicit access to other hosts
- Presence of AWS x.509 certificate (.pem) files
  - Can be used to tamper with publisher's EC2 account
- Active connections to other hosts
  - Potential backdoors
- SSH Password authentication enabled

Tests Against Discovered System Files

- .bash_history, .vim_info, .bash_profile, .bashrc (in any path) and
- Anything found under Bash /etc/profile.d

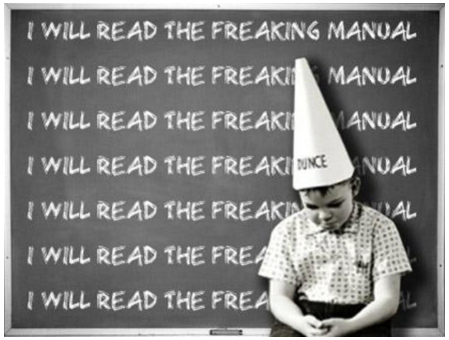
- AWS Access Key or Secret Key strings
  - Can be used to gain full access to owner's EC2 account

- Canonical ID
  - Identifies an AWS account for use with S3
- AWS Account ID
  - Identifies an AWS account
- Environment variable names which commonly point to these values

Results and Findings

- Findings being coordinated with Amazon Web Services security team
- To be presented during DEF CON presentation, with updated slides available online after presentation

New Guidance from Amazon


I WILL READ THE FREAKING MANUAL
I WILL READ THE FREAKI MANUAL
I WILL READ THE FREAKI ANUAL
I WILL READ THE FREAKI NUAL
I WILL READ THE FREAKI AL
I WILL READ THE FREA
I WILL READ THE FREA
DUNCE

- Amazon EC2 User Guide: “Sharing AMIs Safely”
  - http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/index.html?AESDG-chapter-sharingamis.html

- AWS Security Bulletin: “Reminder about Safely Sharing and Using Public AMIs”, 2011-06-04
  - http://aws.amazon.com/security/security-bulletins/reminder-about-safely-sharing-and-using-public-amis/

- AWS Tutorial: “How To Share and Use Public AMIs in A Secure Manner”, 2011-06-07
  - http://aws.amazon.com/articles/0155828273219400

Obtaining Trustworthy Amazon Machine Images?

- Amazon Web Services provides supported and maintained images
  - Support available with subscription to AWS Premium Support service
  - Security updates available via AWS package repositories
  - Predictable and documented Product Lifecycle and AMI updates
  - http://aws.amazon.com/amis

- A number of 3rd party vendors also provide their own images

- Organizations can use AWS supported and maintained images as a foundation for their own customized images

The Good, The Bad and the Suicidal

Q & A