



A Topology of Cloud Threats and Attacks

Making Sense of Risk

23rd September 2010

Hackers love the Cloud!



Agenda

- What is the Cloud?
- Attacking the Cloud
- Attacking from the Cloud
- Defending the Cloud

What is the Cloud?

The Marketing

- A game changing revolution in computing?



The Marketing

- The cloud, now with “magic pixie dust for crypto and security”



The Reality

- Is it just a mainframe?



The Reality

- The ultimate outsource?



Copyright © 2004 Stephen E. Gideon

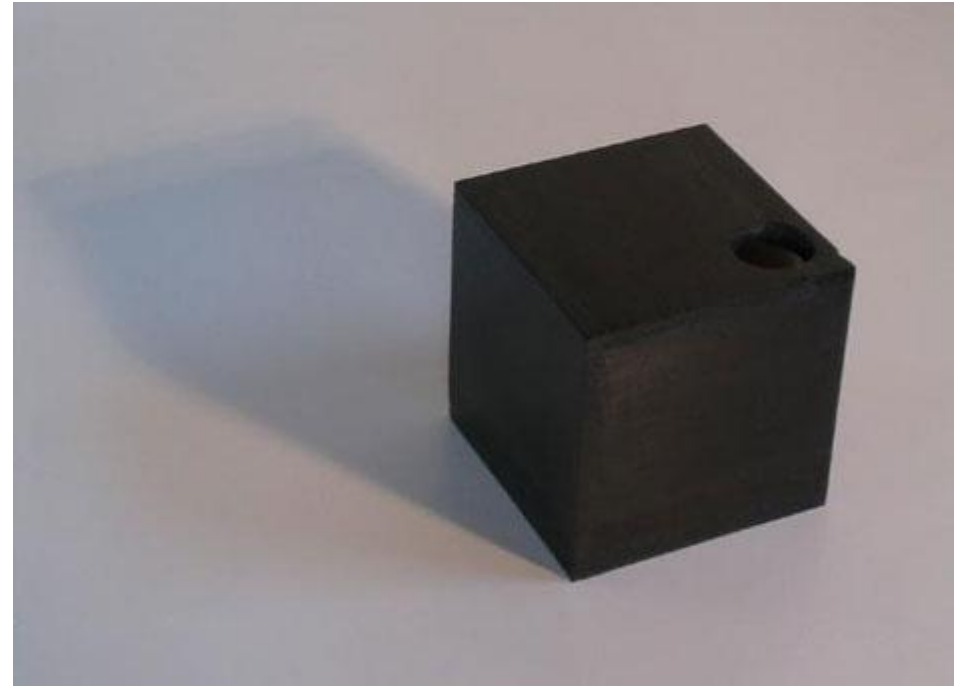
The Reality

- Just an extension of virtualisation?



The Reality

- The ultimate black box?



The Reality

- What about an attackers view?

Attacking the Cloud

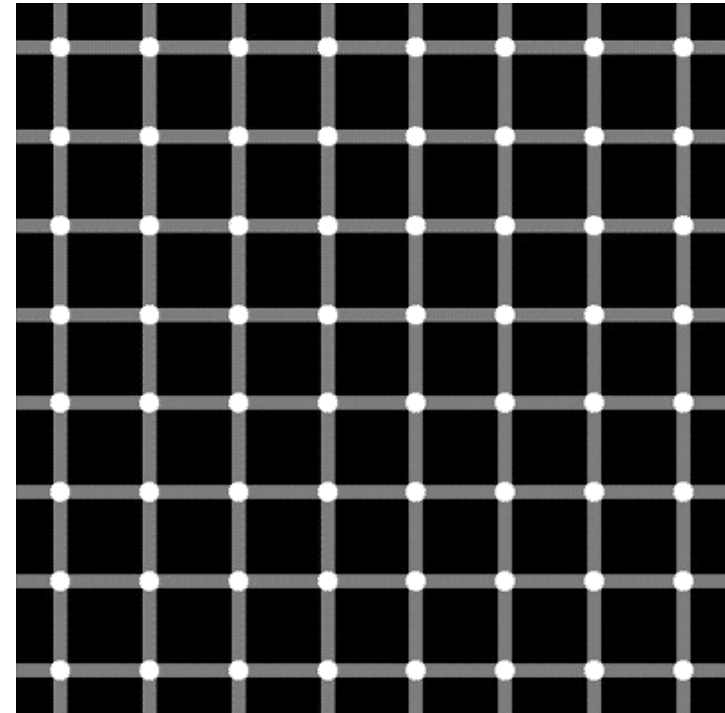


Attacking from the Cloud

Questions to Ask

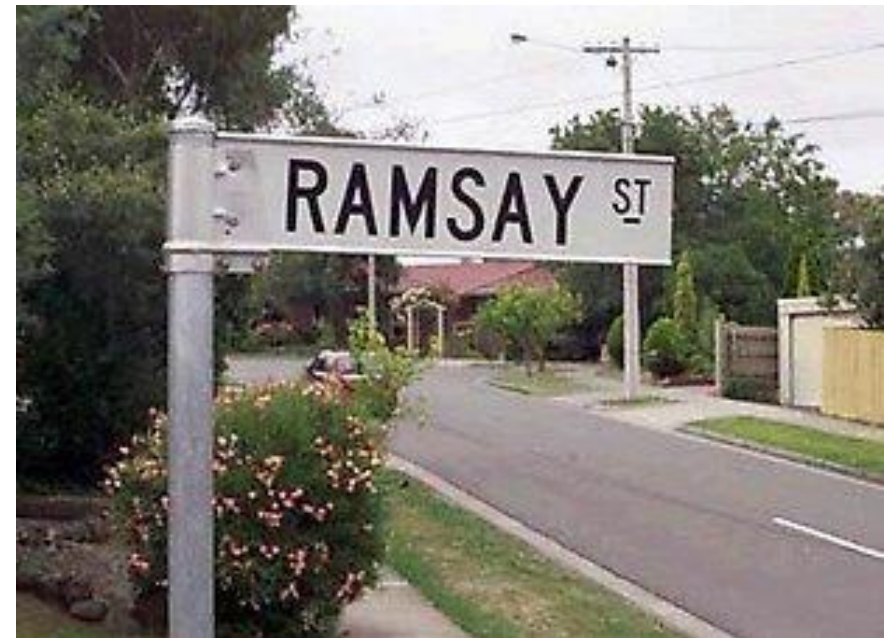
Does Location Matter?

- Is any point in the cloud the same as any other?



Your Location

- Can you choose your neighbours and can they see you?



The Provider

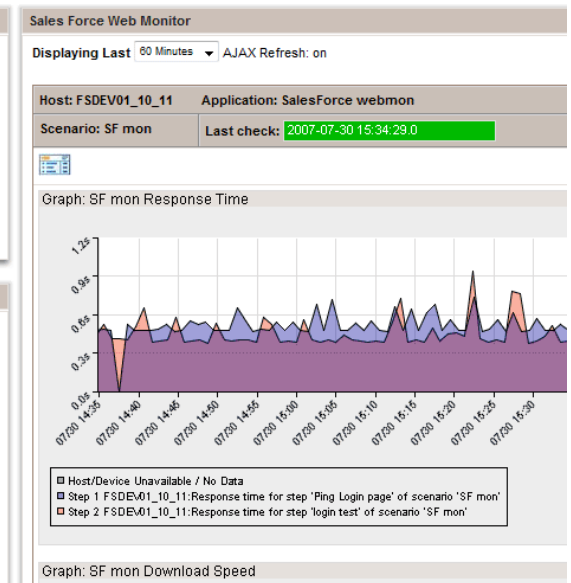
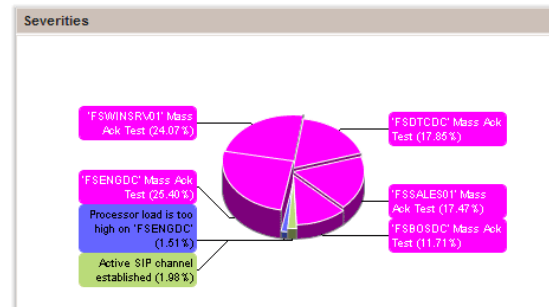
- How do you measure how good your provider is?

System Group Status Overview

(A) Availability (P) Performance (S) Security

Group	A	P	S
FS_California	Red	Green	Green
FS_Dallas_Group	Red	Red	Red
FS_Demo_Group	Red	Red	Red
FS_Dev	Red	Red	Red

Displaying last 7 DAY (Unacknowledged Only)



The Provider

- Do you audit them, test them or trust them?



Attacker's Kit

- Internet Connection
- Credit Card Number
- Mobile Phone

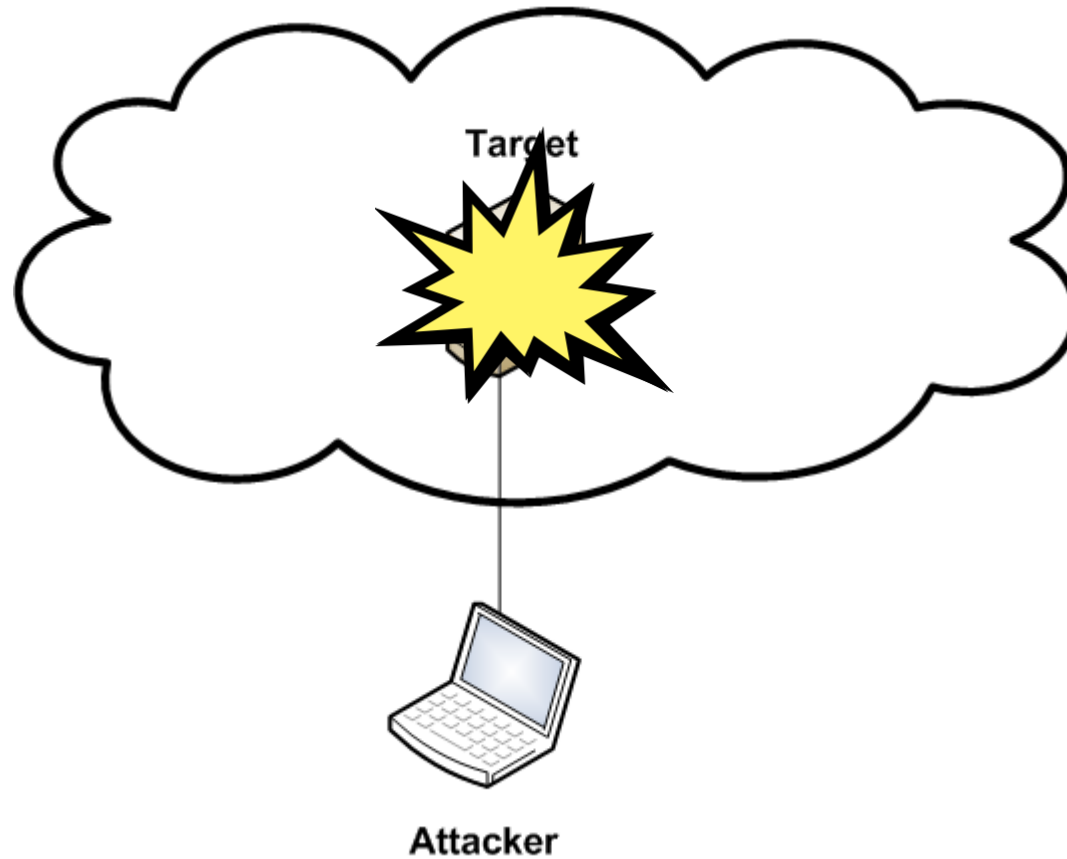


Valid Attack Vectors

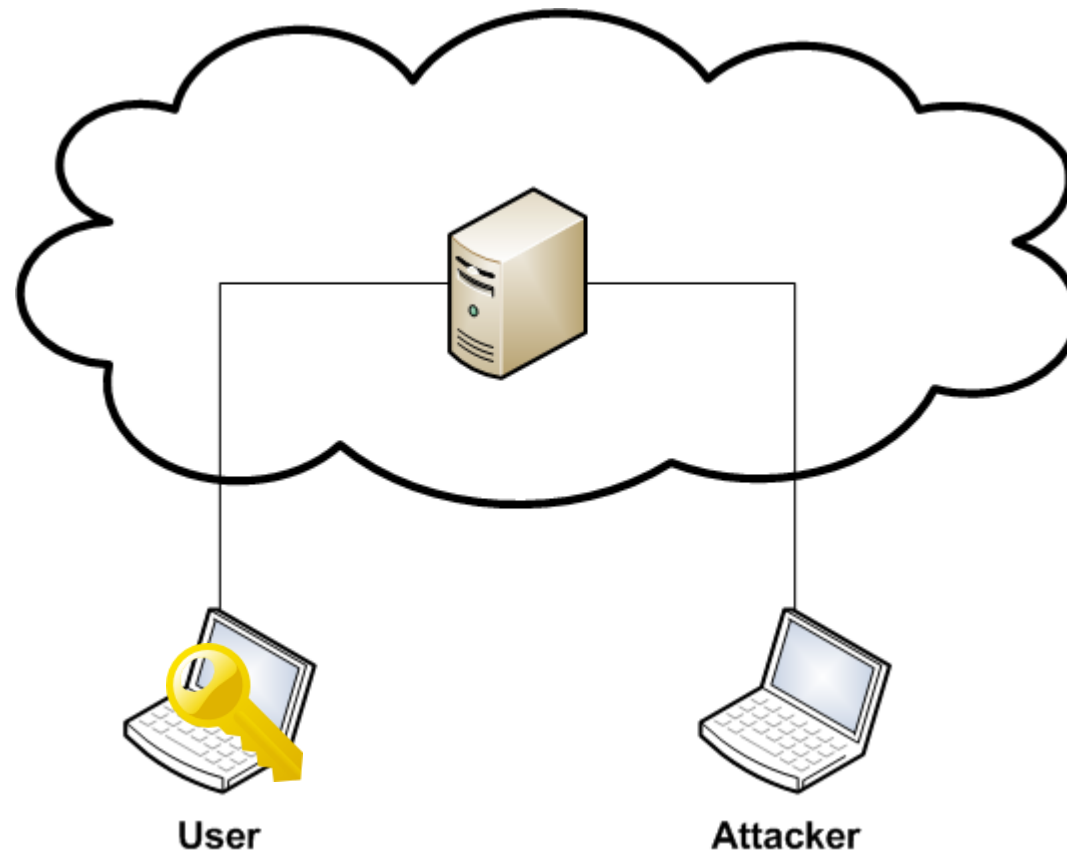
- The Management Interface
- Virtualisation/Sandboxing
- System Builds
- Operational Behaviour
- Other “Traditional” Attacks

Attacking the Cloud

Attacking the Cloud

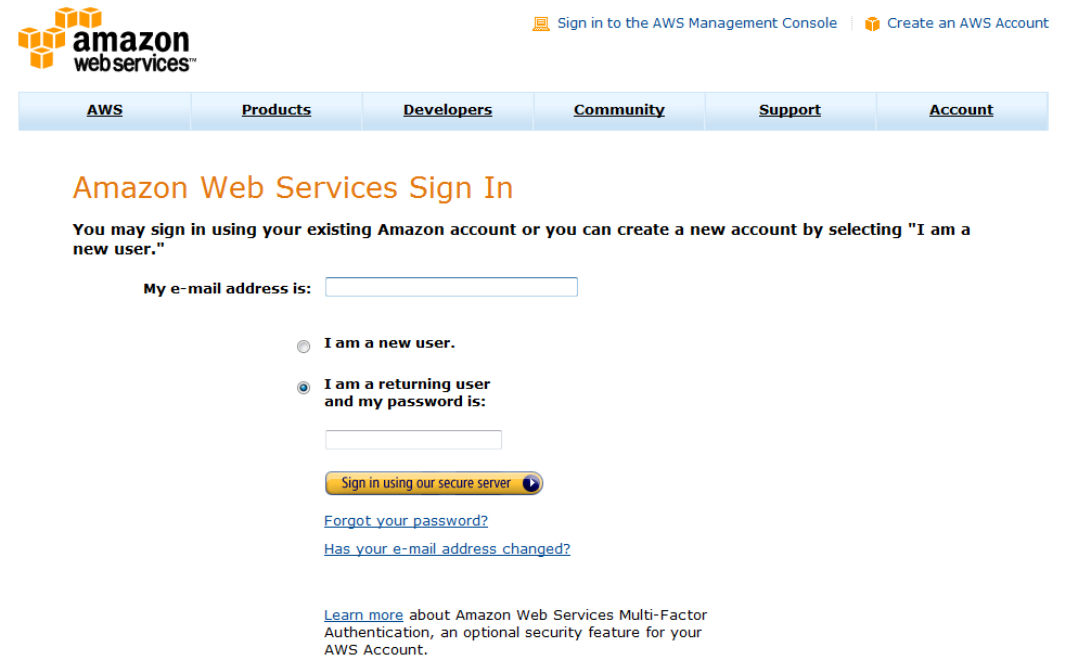


Steal or Guess Credentials



Password Policy

- How do you control it for your Amazon account?



The screenshot shows the AWS sign-in interface. At the top right, there are links for "Sign in to the AWS Management Console" and "Create an AWS Account". Below this is a navigation bar with tabs for "AWS", "Products", "Developers", "Community", "Support", and "Account". The main heading is "Amazon Web Services Sign In". Below the heading, a message states: "You may sign in using your existing Amazon account or you can create a new account by selecting 'I am a new user.'" The form includes a text input for "My e-mail address is:", followed by two radio button options: "I am a new user." and "I am a returning user and my password is:". The "I am a returning user" option is selected, and there is a password input field below it. A "Sign in using our secure server" button is located below the password field. At the bottom, there are links for "Forgot your password?" and "Has your e-mail address changed?". A footer note mentions "Learn more about Amazon Web Services Multi-Factor Authentication, an optional security feature for your AWS Account."

Password Distribution

- How are passwords distributed to the user?

From: Rackspace Cloud Support
Sent: 03 September 2010 13:49
To: MWR
Subject: Cloud Server Notification

Your Cloud Server build is complete.

IP: xxx.106.243.122
root/Administrator password: **PASSWORD**

XSS Attack



XSS Attacks


- With Amazon EC2 your password is decrypted using JavaScript



Retrieve Default Windows Administrator Password Cancel

To access this instance remotely (e.g., Remote Desktop Connection), you will need your Windows Administrator password. A default password was created when the instance was launched and is available encrypted in the system log.

To decrypt your password, you will need your key pair for this instance. Simply copy & paste the contents of your private key file into the text box below, then click **Decrypt Password**.

 Instance: i-95ccb5e2

* Required field

Encrypted Password: NLIg6MjvZUhl1Emzwb86103/l/mNkr5H0y8d1+6Tih86...

Key Pair: ec2key.pem
Note: You were prompted to download and save this when you created your key pair.

Private Key*:

Please include the entire text, including the Begin and End lines (Ex: "-----BEGIN RSA PRIVATE KEY-----")

Decrypt Password

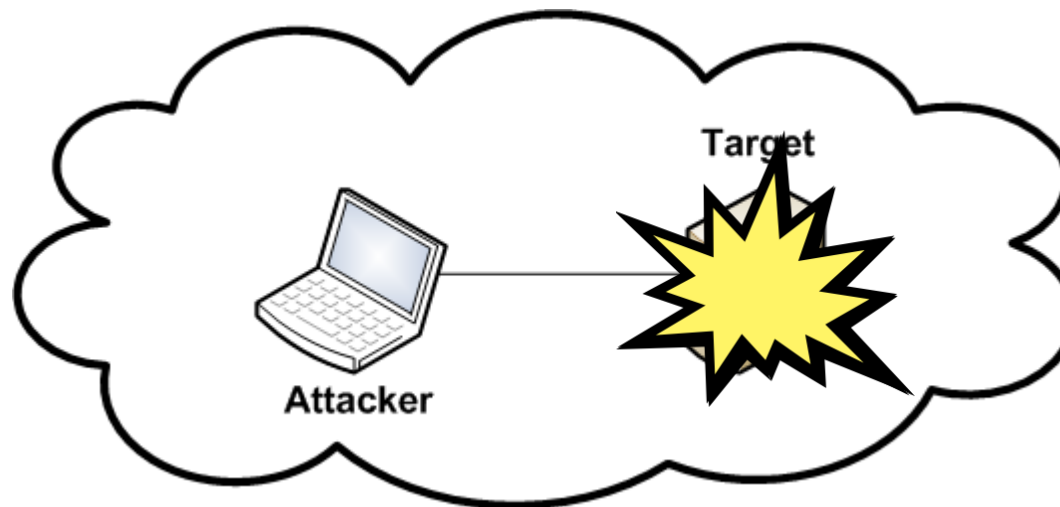
Social Engineering

- Cloud providers are no less vulnerable

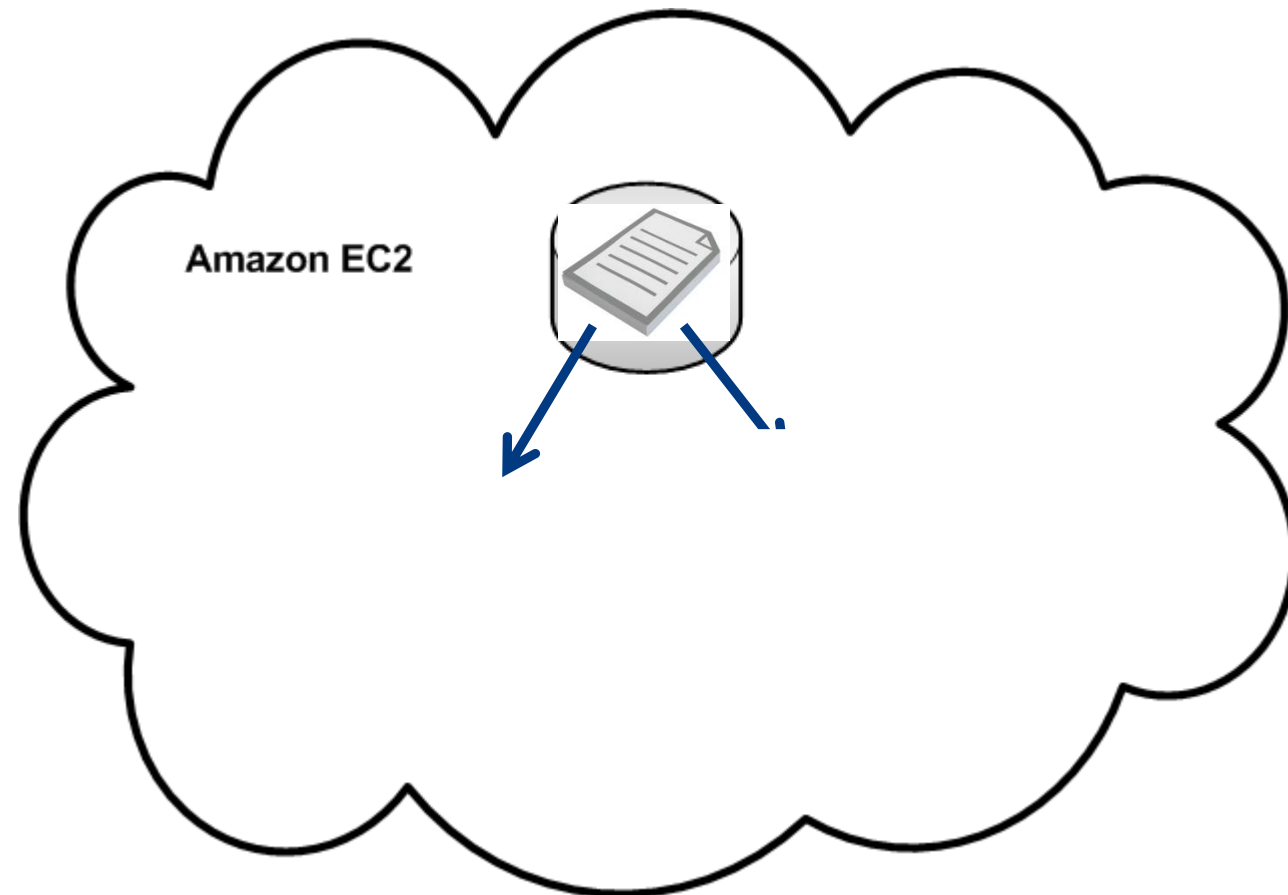


Attacking Within the Cloud

Attacking Within the Cloud



Recovering Data



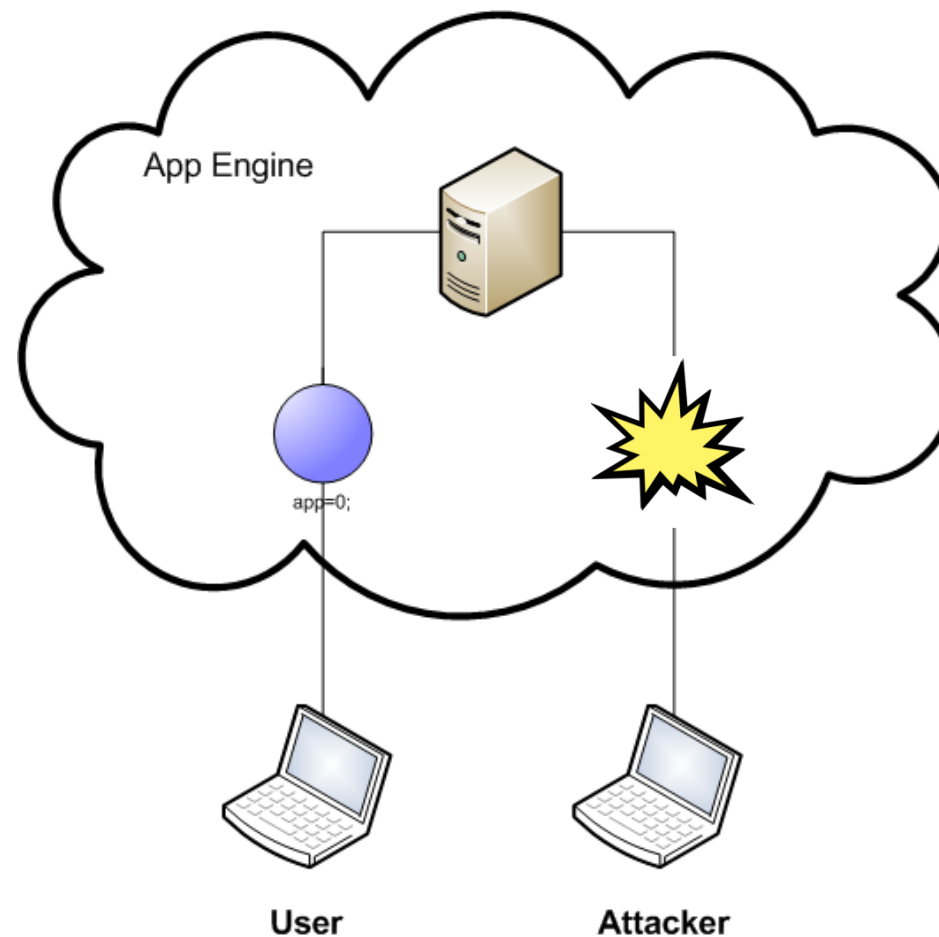
Temporary Storage

- Reading data from your temporary storage

```
root@host:/# df -h
```

Filesystem	Size	Used	Avail	Use%	Mounted on
/dev/sda1	15G	712M	14G	5%	/
devtmpfs	834M	116K	834M	1%	/dev
none	851M	0	851M	0%	/dev/shm
none	851M	48K	851M	1%	/var/run
none	851M	0	851M	0%	/var/lock
none	851M	0	851M	0%	/lib/init/rw
/dev/sda2	147G	188M	140G	1%	/mnt

Breaking the Sandbox



Jailbreaking

Google App Engine



- Does the provider allow you to run your own code?

W 09-06 02:50AM 44.424

```
A serious problem was encountered with the process that handled this request, causing it to exit.  
process to be used for the next request to your application. If you see this message frequently,  
Engine team. (Error code 204)
```

Private Clouds

- Many of the same risks are still present

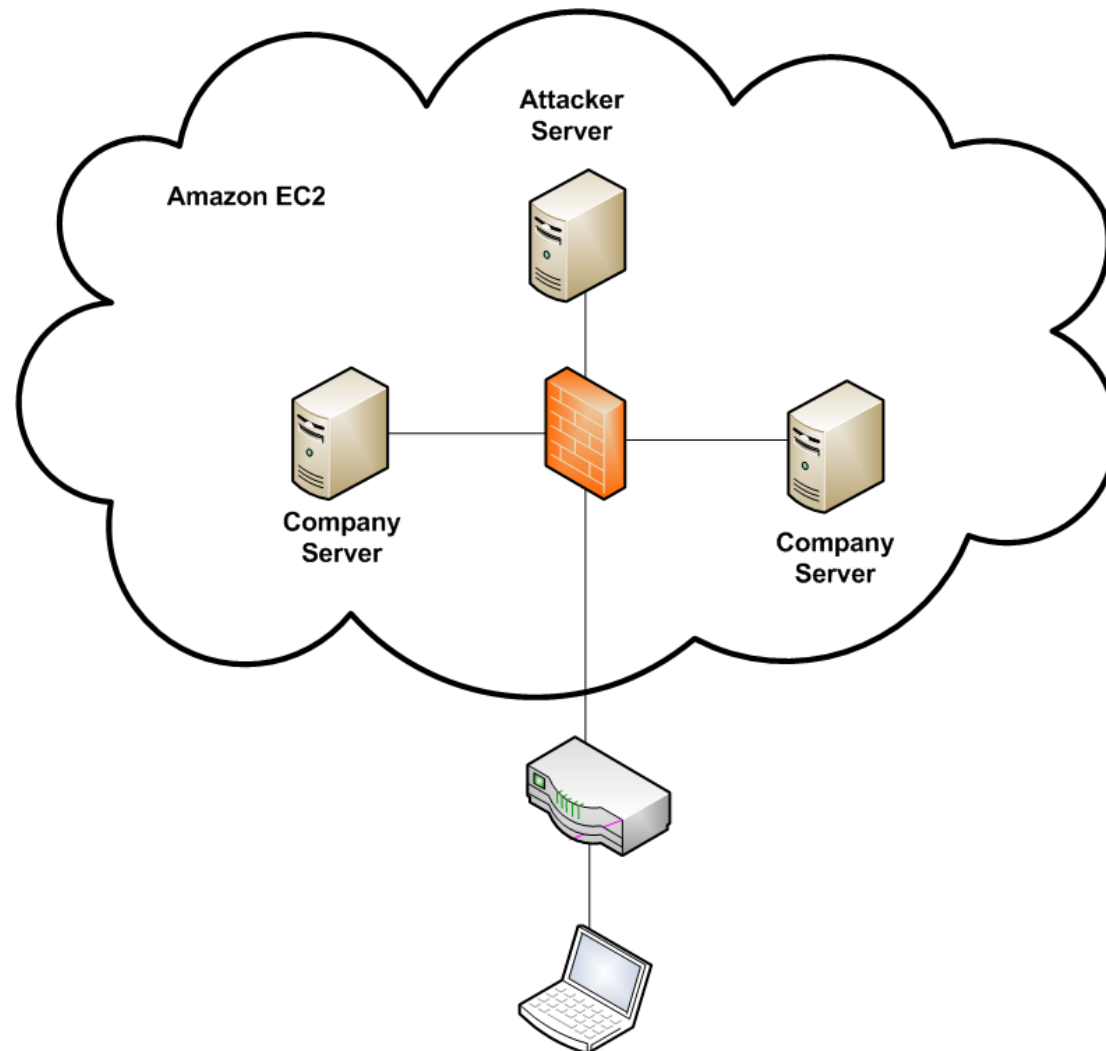


Network Architecture

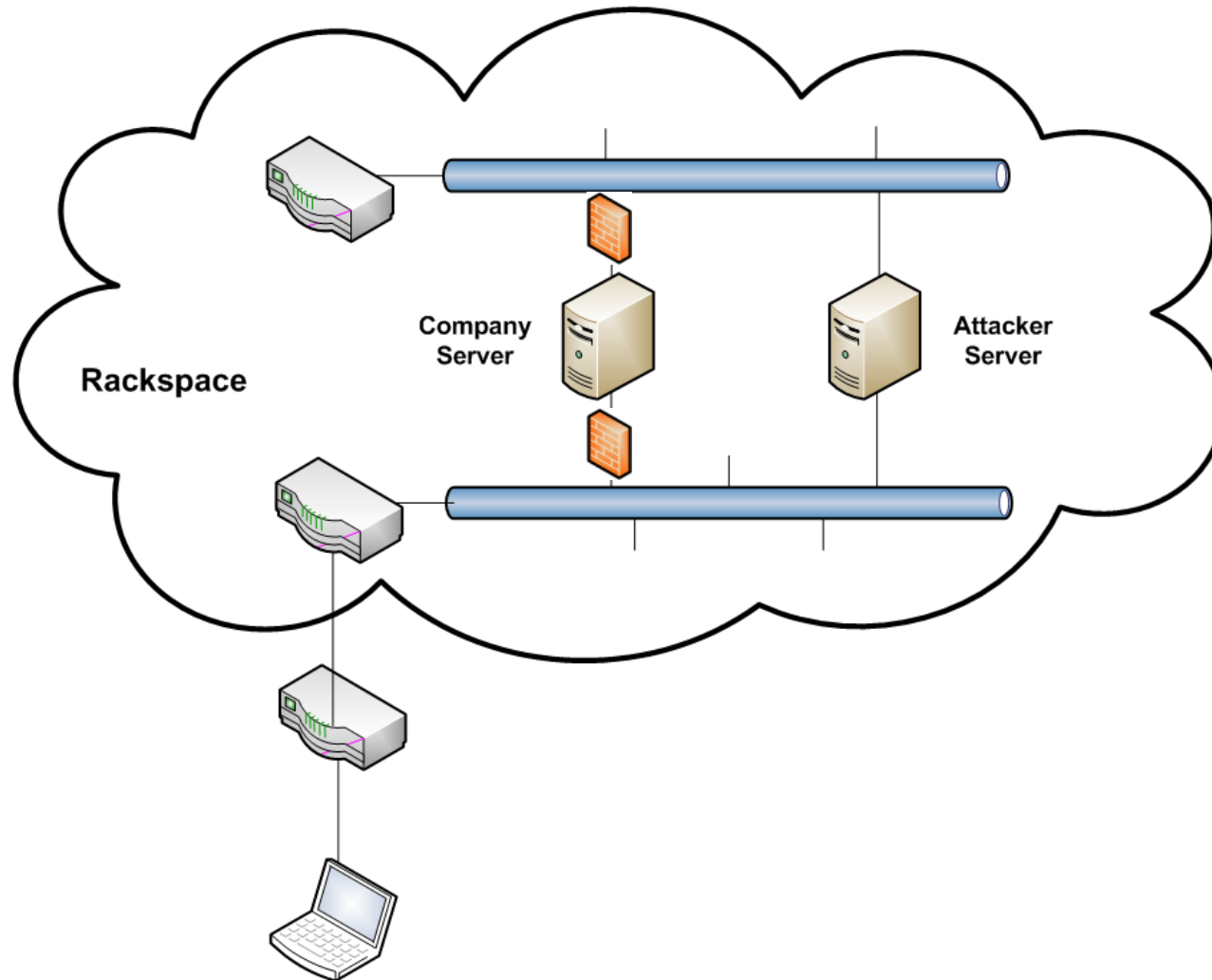
- How does firewalling work within the cloud?



Firewall Architecture



Firewall Architecture

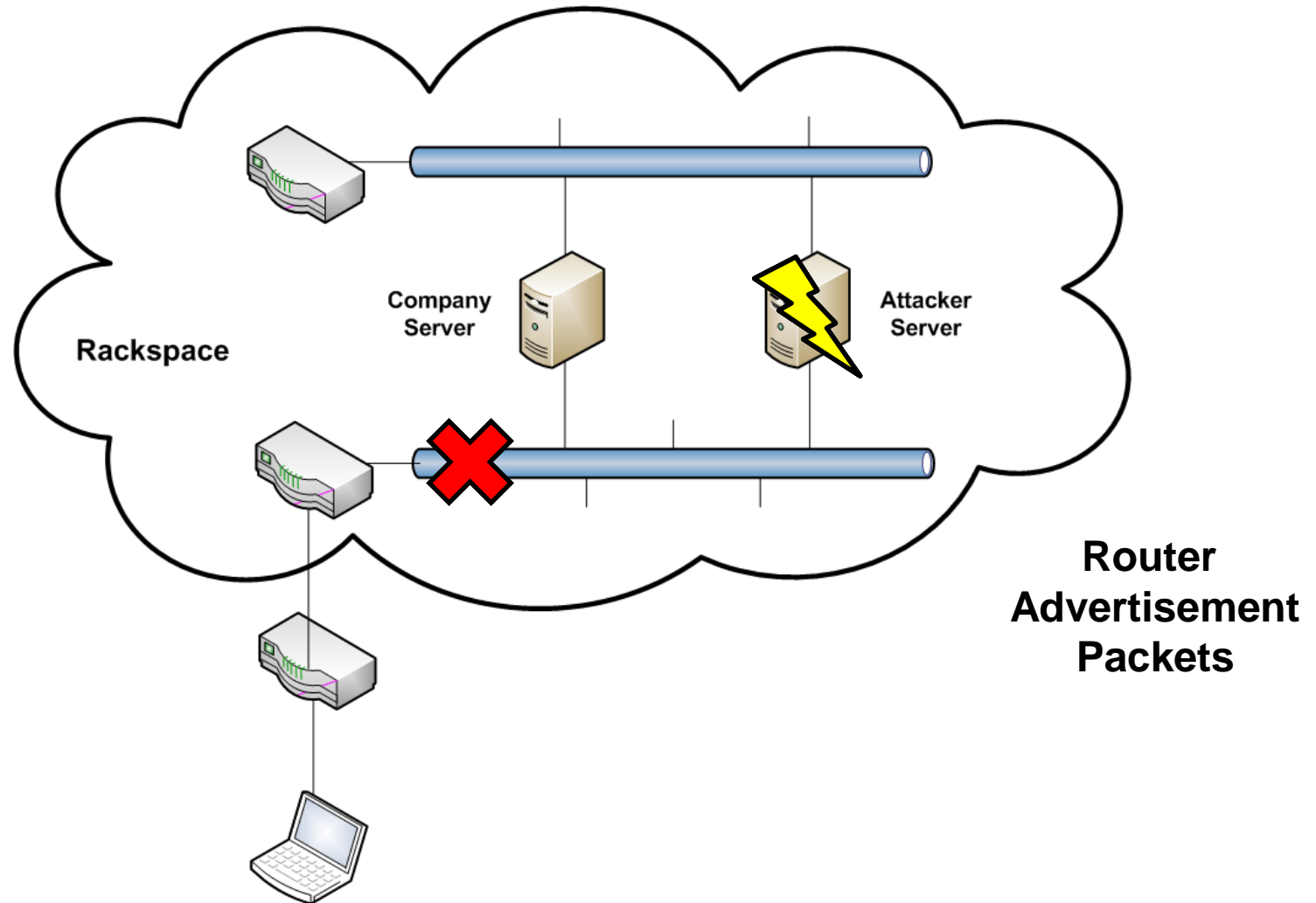


IPv6 Support

- Is IPv6 supported within the cloud?



IPv6 DoS



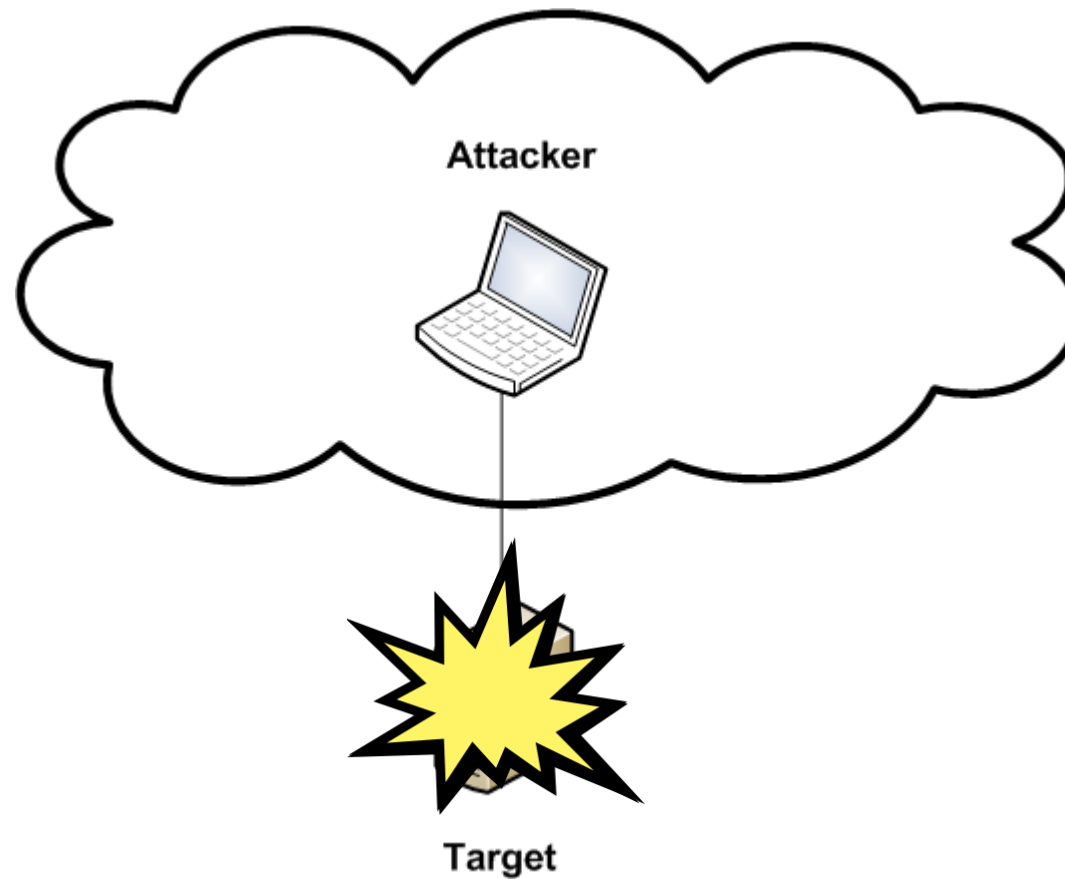
IPv6 Connectivity

- Not officially supported by Amazon but servers still respond!



Attacking From the Cloud

Attacking from the Cloud

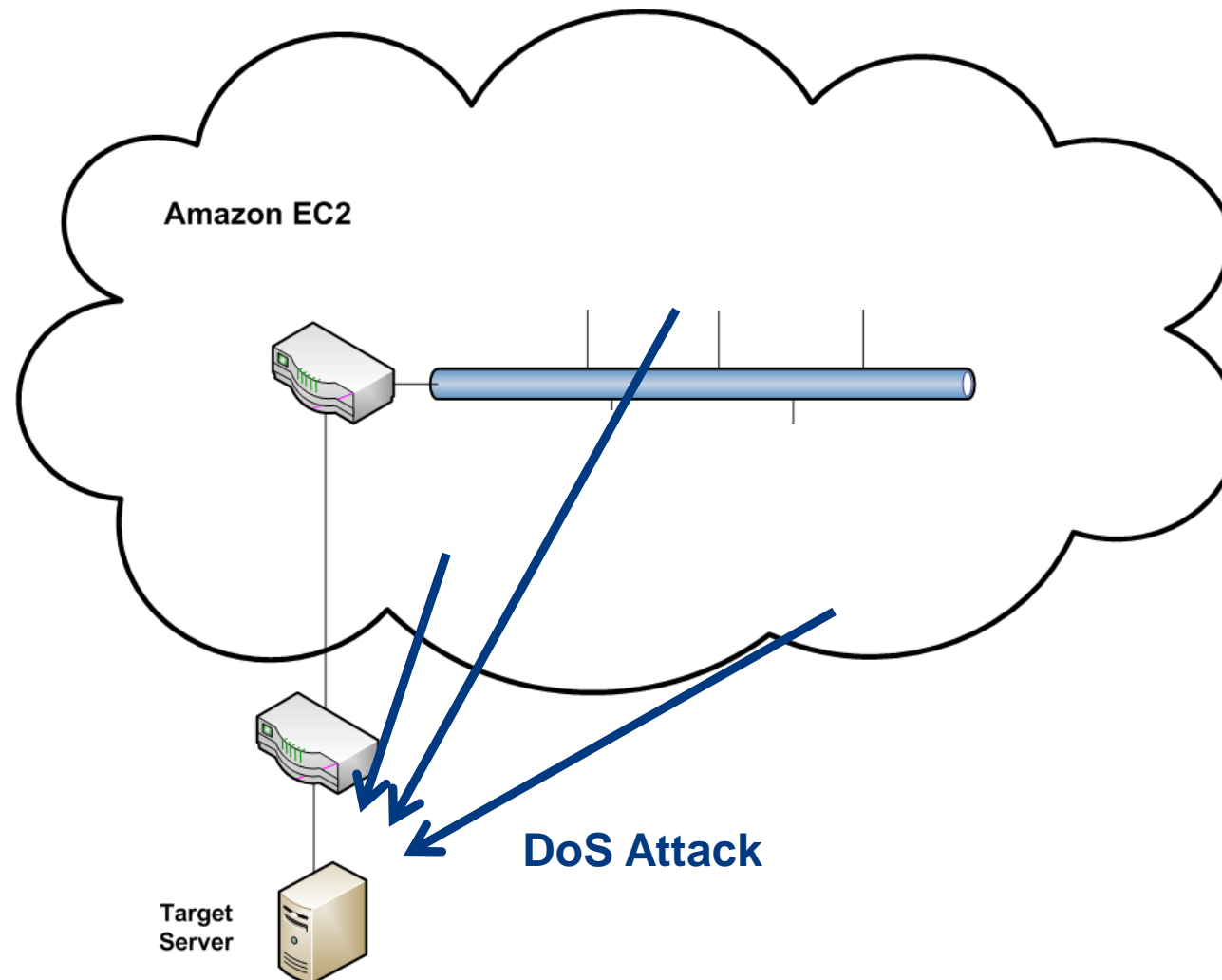


Denial of Service

- Sites have been taken down without intervention from the provider



DoS Example

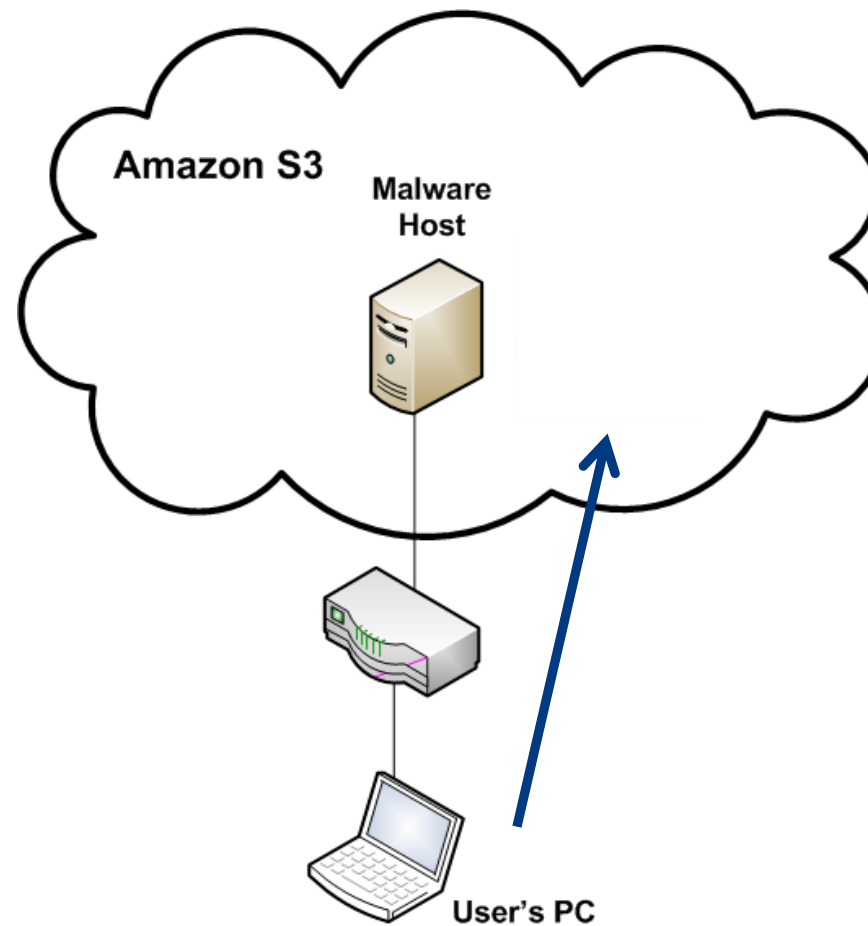


Malware Hosting

- Why run your own server containing exploits and malware?



Malware Hosting Example

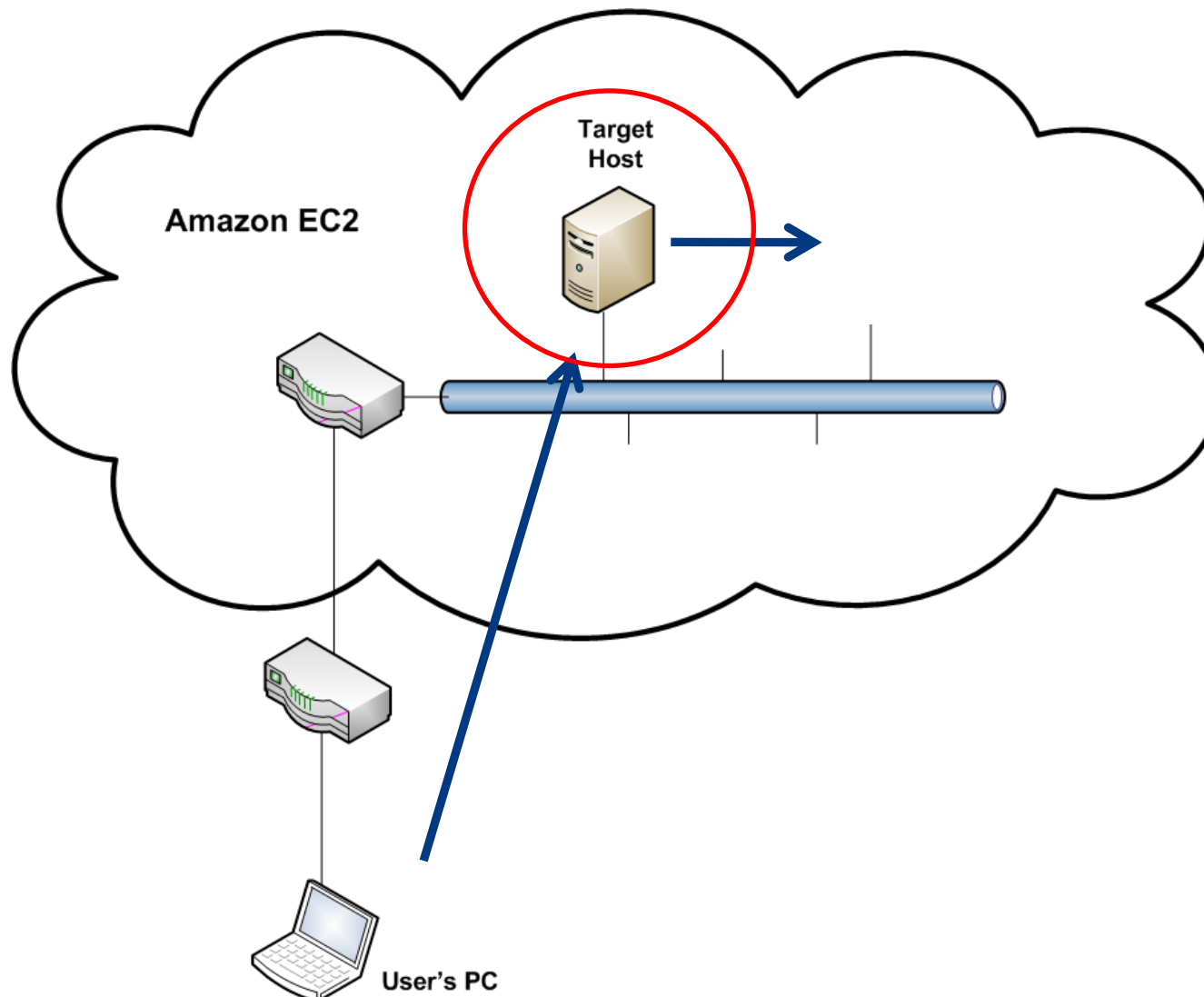


Malware Hosting

- Does the architecture facilitate the hiding of attacks



Malware Hosting Example



Other Attacks

- Can you steal Licence Keys from systems?



Defending the Cloud

Knowledge is Power

- Understand your use of the cloud and the risks



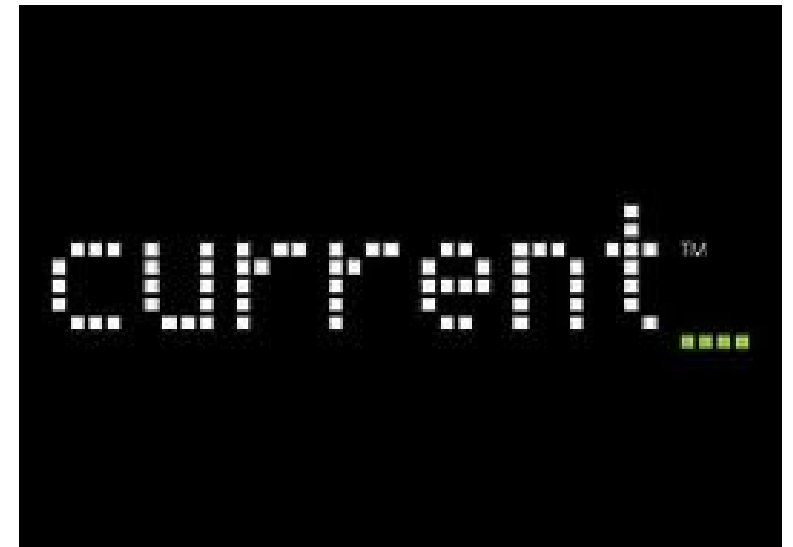
Gain Assurance

- Ask for assurances the same as with any other 3rd party



Nothing New

- Use the processes you already understand for working with the technologies in question



Hostile Territory

- Treat the cloud the same as any other potentially hostile source



Limitations

- Accept the limits of security assurance within the cloud



Summary

- Play safely



Questions