Security Challenges Operating a Public Cloud Service

Charlie Kaufman
charlie.kaufman@dell.com

What do I mean by “Public Cloud”

- Computation and Storage service where multiple customers share the physical hardware and pay proportional to the resources they use
  - Vendor gets economies of scale and more predictable aggregate demand
  - Anyone with a credit card (or perhaps some BitCoins) can become a customer
- If a company runs its own data center and shares the hardware among various “departments” of the company, that’s called a “Private Cloud”
- A cloud providing services to a small number of carefully vetted customers is somewhere in between

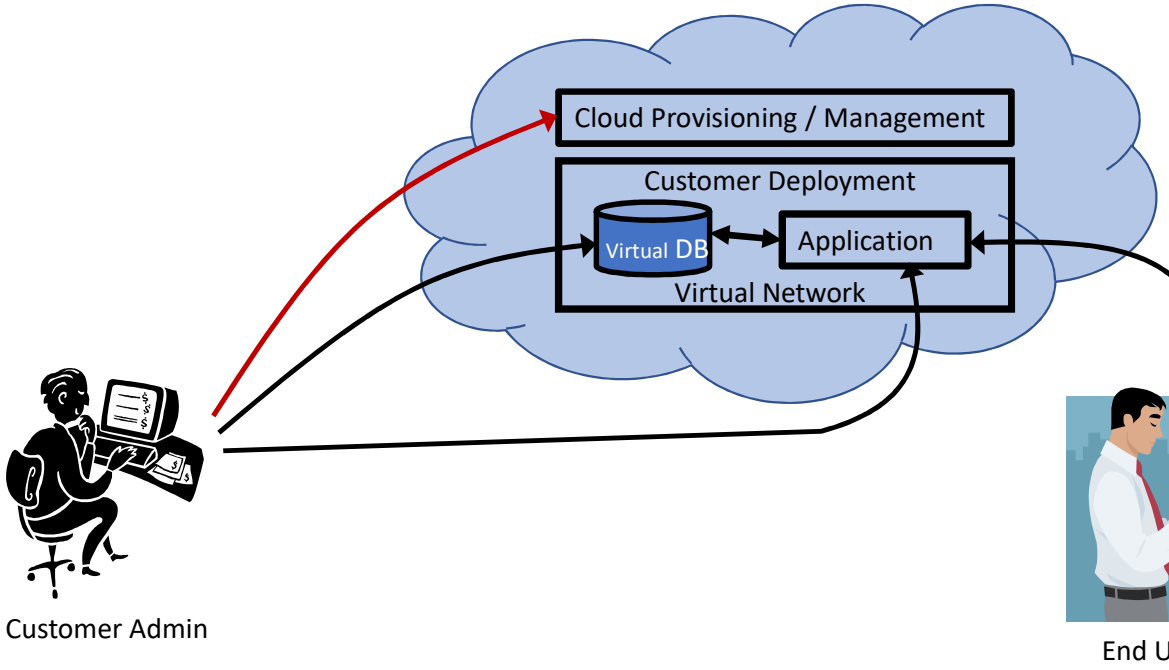
What's different when securing a public cloud vs. your own datacenter

- The stakes are higher
- The customers are less trusted…
  - Must be treated as hostile
- The customers' data must be protected from system admins
  - What's only good practice within an enterprise is a contractual guarantee in a public cloud

What's the Same?

- Detecting and preventing intrusions
- Mitigating DDoS attacks
- Protecting services from one another
  - Including fair allocation of shared resources
- Keeping patches up to date
- Focus on minimizing the attack surface

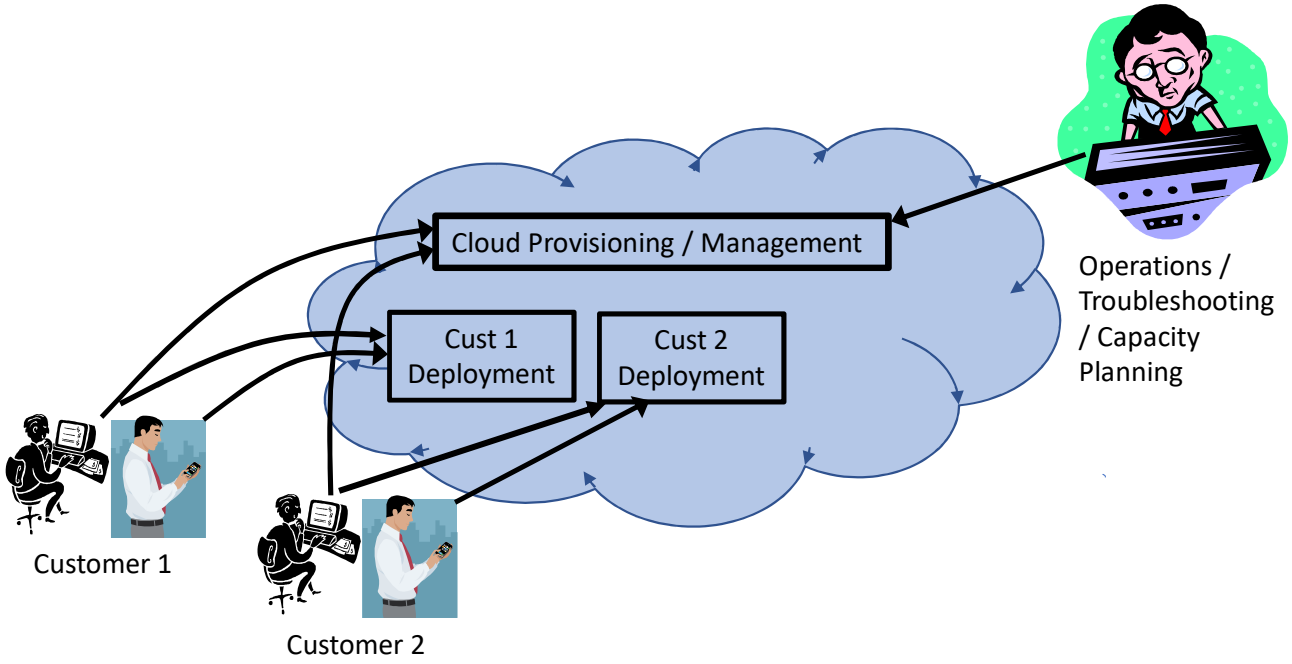
Customer's View of Public Cloud



Interacts with Provisioning App instead of installing physical servers

Doesn't know or care that application is in the cloud

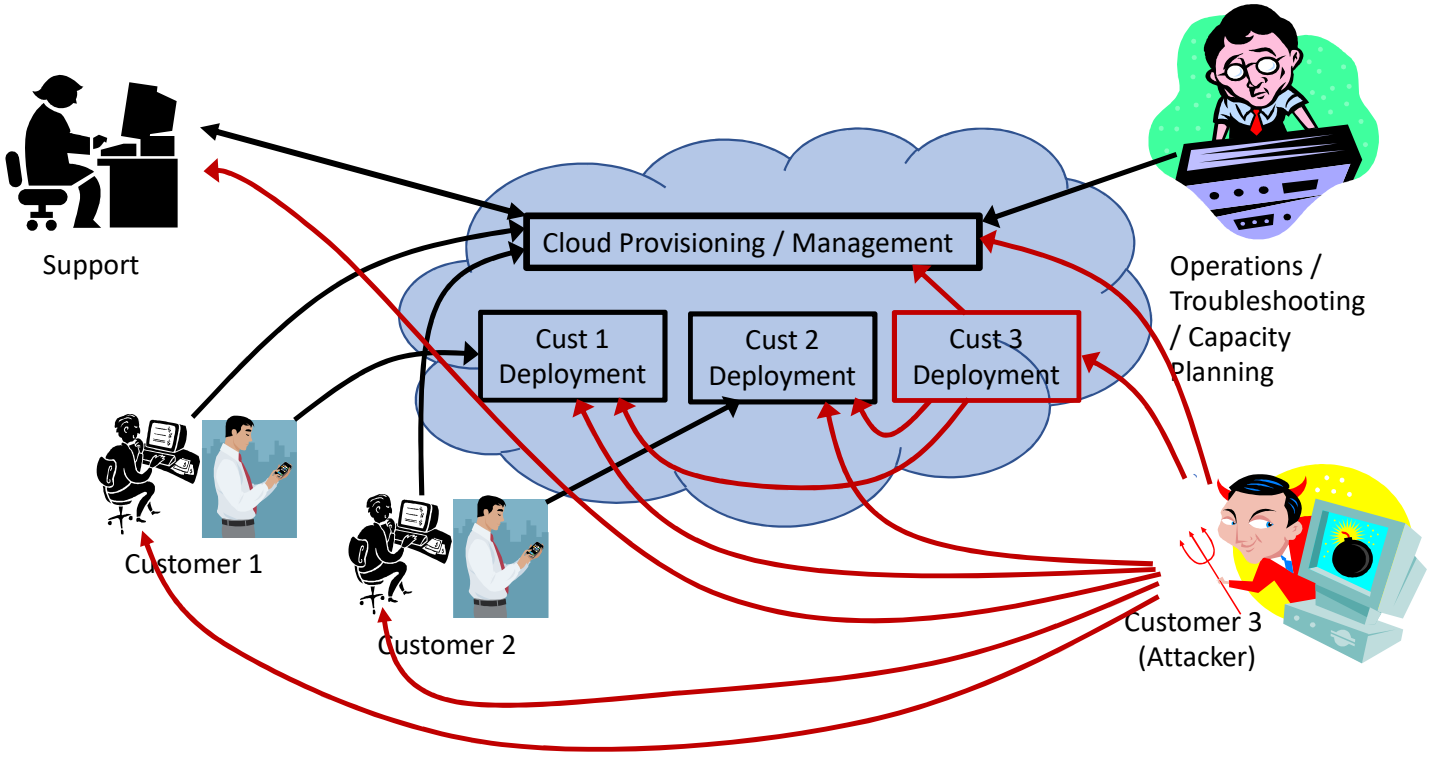
Provider's View of Public Cloud



Job of Cloud Infrastructure it to prevent Customers from being aware they share the same cloud using Virtual Machines and Virtual Networks

Attacker's View of Public Cloud

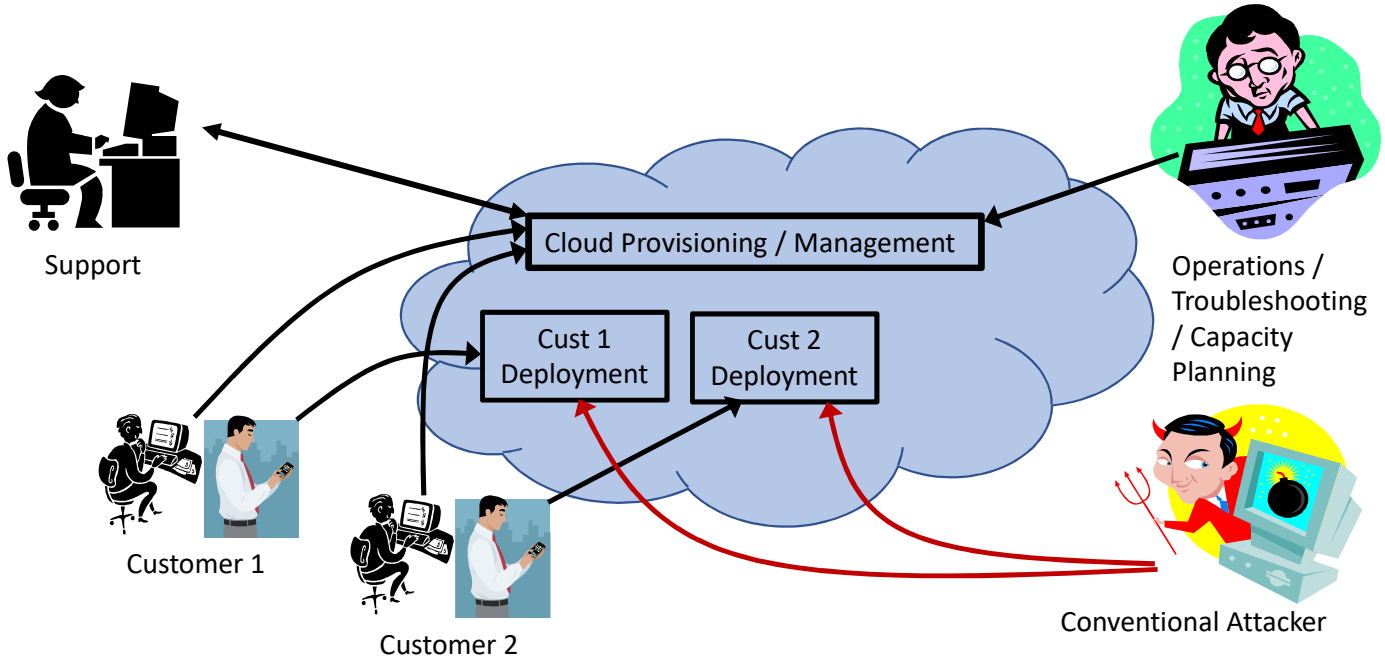
Lots of interesting new attack surfaces!



Security Basics: Keeping the Bad Guys Out

- A lot like the challenges with a conventional data center:
  - Firewalls can help
  - Authenticate your customers
  - Authenticate your administrators
  - Good coding practices to minimize bugs
  - Intrusion Detection
  - Anti-malware
  - Defense in Depth

Protecting Applications is now a shared responsibility



Helping Customers to protect themselves from outside attackers

- Defense becomes a shared responsibility
  - Network based defenses are shared resources
  - Only the customer understands the application
  - Only the cloud provider understands what is going on with the network
- Responsibilities need to be split clearly to assure nothing sneaks through the cracks!

Helping Customers to protect themselves from outside attackers

- Typical datacenters don't expose their servers to the full onslaught of the Internet
  - Datacenter firewalls
  - Intrusion detection hardware/software
  - DDoS mitigation systems
  - SSL accelerators
- Often these require considerable expertise to configure optimally
- Outside the cloud, there is genetic diversity forcing attackers to work on each target individually
- Diagnosing problems involves looking at lots of data (e.g. network and system logs)

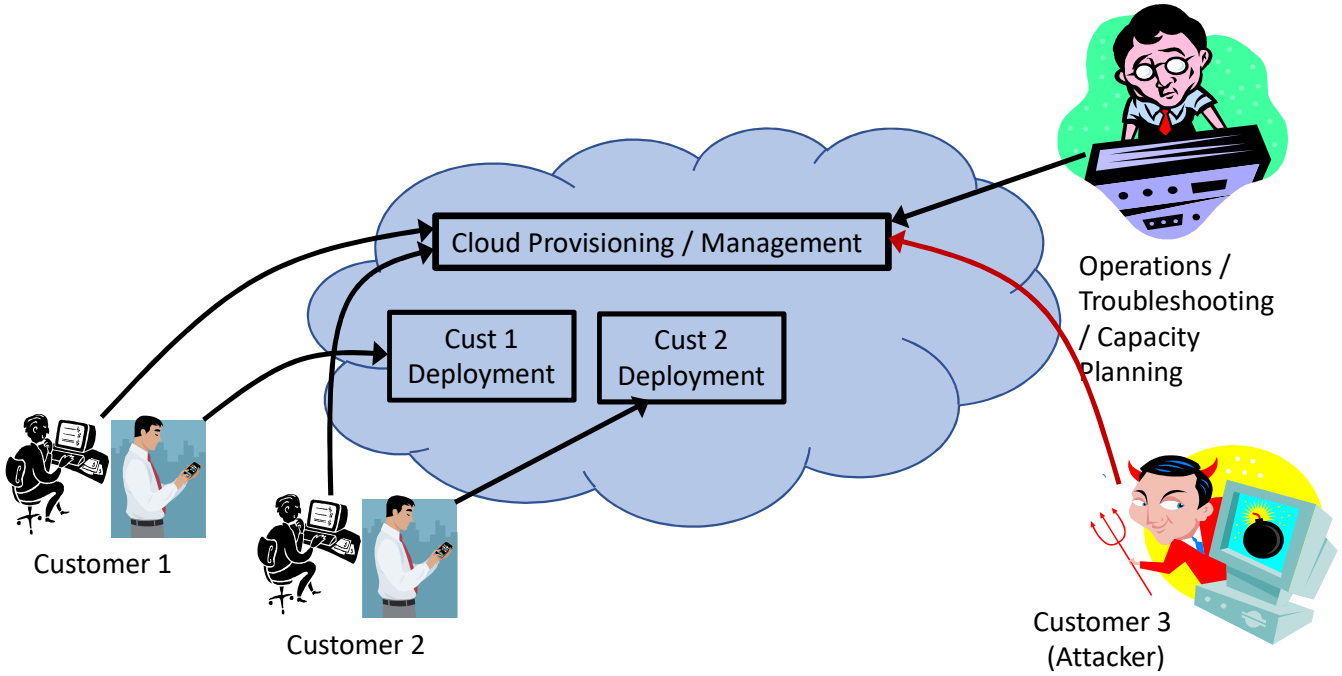
Public Cloud Limitations

- Customers typically can't choose their own firewalls and access network statistics
  - Unless the firewall vendors have ported their software to run on VMs so they can run within the cloud
  - Network statistics cover data from multiple customers
  - Cloud vendors need to provide equivalent tools and entice firewall vendors to support their platform
- Customers can't bring diagnostic hardware into the datacenter to diagnose tricky situations
- Attacks may be coming from inside the cloud over extremely high speed links

Public Cloud Advantages

- Cloud providers can afford to hire security experts to deal with problems that would rarely affect any given customer
- Cloud providers can detect port scans and block them before they have gotten to probe most customers
- Could providers can build databases of IP addresses and characteristics of DDoS attacks and then block them for all customers
- Just as customers can scale up processing capacity on demand, they can deploy DDoS defense firewalls only when under attack – this makes rarely needed defenses cost effective

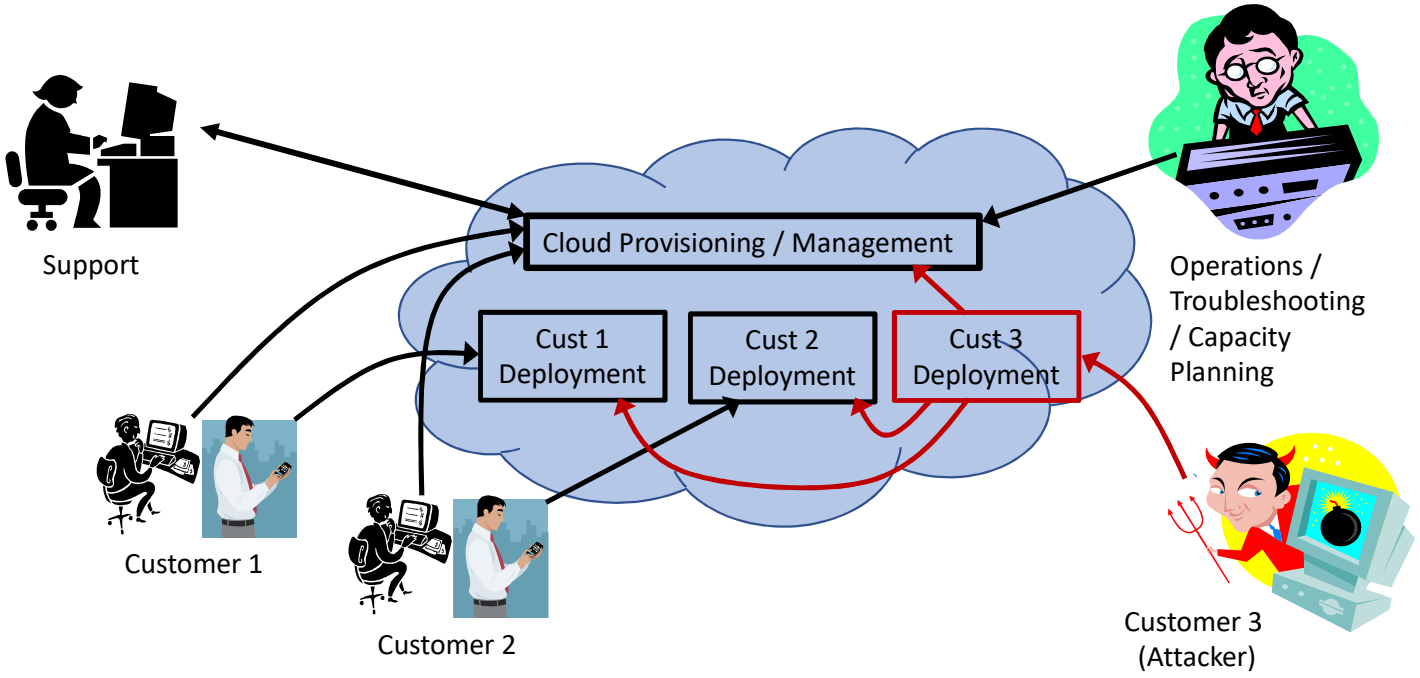
New Attack Surface: Attacking the provisioning system



The Cloud Provisioning System

- It's a web application like any other, subject to all the same attacks
- Replaces data center controls often requiring physical access to the room and locked cages within the room
- Provider must make it rock solid, including against DDoS attacks
- ***Should*** provide (optionally) strong forms of administrator authentication:
  - ***Smart Cards***
  - ***Integration with Biometric Authentication***
  - ***Locked down to accessibility only from protected locations***
  - ***Dual-authorization where sensitive requests must be made by one person and approved by another***

New Attack Surface: Attacking using a hosted server



New Cloud Security Challenge: Keeping the Bad Guys In

- In a public cloud, you have to assume your customers are not just incompetent… they are malicious
- You must defend against customer code as carefully as you defend against external attacks
- In theory, an OS could be secure enough to protect processes running under different identities from one another, but today's popular OSes do not
  - If you built a new OS with perfect security, no one would want it… it's not backward compatible

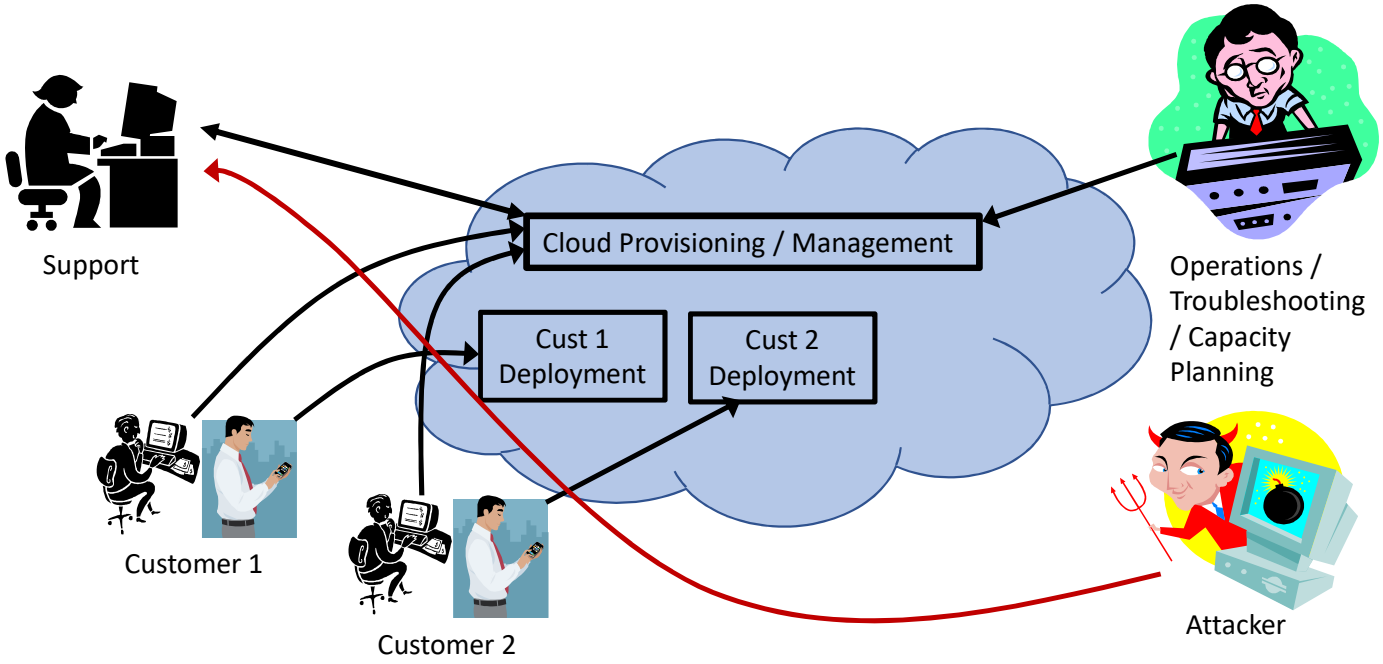
What to use for an application sandbox?

- AWS and Azure chose to use VMs over a hypervisor
- Could have used processes or containers within an OS
- Could have used managed code isolation within a process (Java, C#)
- Could have used physical machines isolated by VLANs
- VMs have the advantage of being new, without a lot of time to introduce performance features that weaken security

Creating the illusion that the customer is isolated

- Not just a matter of access controls
  - Resource quotas so response times unaffected by other customers
  - CPU capacity / Network Bandwidth / Storage Bandwidth
  - **Tough Call:** Provide only guarantees or allow customers to exceed guarantees if resources are idle
- Hyper-threading a serious problem
- Speculative Execution attacks a growing nightmare (e.g., Spectre and Meltdown)

New Attack Surface: Social Engineering Support People



What do you do when the customer really did forget his password?

Protecting the customers from cloud admins

- There is always a way to bypass the automatic access controls
  - To recover from bad situations
  - The automatic mechanisms have to be updateable
- Cloud developers and operators might be tempted
  - Individuals might profit from corporate espionage
  - Providers have to make it hard for our developers and operators to misbehave without getting caught – sometimes auditing is sufficient
  - Customers want to know how the internal controls work
  - Compliance auditors want to know how the internal controls work

Protecting the customers from governments

- Providers will comply with valid subpoenas
- Some laws provide less privacy protection to data held by a 3rd party
- Harder to detect surveillance when it is not your own data center
- Legal battles over various obligations are being fought
- There are technologies that make it impossible for providers to access customer data (e.g., Intel's SGX)

Are these subpoena-proof, or are they a way to get arrested?

So those were the attacks we prepared for…

What did we actually see?

Bots establishing accounts with stolen credit cards and exhausting our resources

- We thought about this threat, but could not see any way attackers could make money doing it
- This was just as BitCoin was taking off!

Credit Cards don't work the way you might think!

- Because of PCI (Payment Card Industry) regulations, only very well protected computers can handle credit card numbers
- Most vendors don't do this work themselves, they outsource it to a company that takes the credit card information and gives you a reference number
- There is no way to know you are getting thousands or requests to establish accounts that are supplying the same (stolen) credit card!

Credit Cards don't work the way you might think!

- With Card-Not-Present transactions (i.e., Internet Transactions), the credit card companies take no responsibility for fraud. If the customer denies the charge, you have to give back the money.
- Even if the customer does not report the bad transaction until months after it is made!

When our customers attack the Internet!

- Cloud providers don't want to provide a safe haven for criminals
  - Spammers
  - Scanners
  - Illegal distributors of copyrighted materials
  - DDoS bots
  - Bot Army rendezvous points
  - Phishing sites
- Being a good citizen and avoiding bad press are not the only incentives!
- Cloud providers sell with greater anonymity than most ISPs
  - Comcast knows where you live!

Automated Systems will punish you for bad behavior

- IP addresses that are the source of spam or malware get blacklisted
- IP addresses that are the source of DoS or probing attacks are blocked and reported to their owners for corrective actions
- If someone rents an IP address and a gigabit of bandwidth for 15 minutes, the reaction hurts the next tenant
  - If many IP addresses in a cloud provider's block are abusive, the entire block may be blacklisted

How do you define bad behavior?

- How do you distinguish a spam engine from a mail agent relay distributing mail to a mailing list?
- How many failed DNS queries are allowed before it constitutes an exhaustive search through a namespace?
- What looks like an attack could be someone testing the security of their own system

How do you handle complaints?

- Forward them to the customer responsible?
  - Customer contact information could be fake
  - Distinguish a hostile customer from a customer whose services were hacked
- Forward customer contact information to the complainant?
- The complainant could be complaining as a form of DoS attack on the customer

How do you handle complaints?

- There are laws governing “take down notices” alleging redistribution of copyrighted material
  - They are inflexible
  - If you can’t quickly figure out whether they are legitimate, you can end up with a large lawsuit or a very unhappy customer

Parting Thoughts…

- You won’t be attacked until it really matters
- You won’t be attacked at the interface you focused so hard on securing
- DDoS is the last attack you’ll think about and the first attack you’ll see

Parting Thoughts…

- The fun part of security is coming up with clever solutions to hard problems
- The hard part is knowing when something is secure enough – there are two ways to fail:
  - Deploying something that will lead to disaster
  - Not deploying anything until it is provably secure against any conceivable threat

Questions?