Detecting and Preventing Abuse of Resources in IaaS Cloud Computing

Jens Lindemann
Introduction

- Cloud computing becoming more and more popular
- Cloud resources may be abused by customers
- Negative consequences for Cloud Service Provider may ensue
- Infrastructure-as-a-Service (IaaS)
  - e.g. Amazon EC2, Google Compute Engine
  - customer has full control of the VM and OS
  - relatively hard to detect/prevent abuse
- So far, even commercial cloud offerings are insufficiently protected
Introduction

- Cloud computing becoming more and more popular
- Cloud resources may be abused by customers
- New issue
- Introduction

Amazon EC2 Used as Botnet Command and Control
By Brian Prince | Posted 2009-12-11

Trend Micro released a report Dec. 9 highlighting what it expects to see as far as security threats in 2010. Among the more interesting predictions -- attacks on cloud infrastructures will increase.

Almost as if on cue, a report surfaced the same day that the Zeus Trojan was observed abusing the Amazon EC2 (Elastic Compute Cloud) for its command and control needs. According to Don DeBolt, CA’s director of threat research for its Internet Security Business unit, a server within the Amazon EC2 network was compromised by unknown means and used as the command and control server. Files were placed on the server that bots were programmed to access from across the Internet, he said.

"Zeus Bots would call to the compromised server inside of EC2 to download instructions inside the 'config.bin' file," DeBolt explained. "The Zeus Bot then will post bank account data back to the C&C ... located inside of Amazon ... This shows how aggressive the groups behind malware are today."

This isn’t the first time attackers have used an unconventional means of controlling their bots. Earlier in 2009.
Introduction

- Cloud computing becoming more and more popular
- Cloud resources may be abused by customers
- Negative consequences for Cloud Service Provider may ensue
- Infrastructure-as-a-Service (IaaS)
  - e.g. Amazon EC2, Google Compute Engine
  - customer has full control of the VM and OS
  - relatively hard to detect/prevent abuse
- So far, even commercial cloud offerings are insufficiently protected
What constitutes abuse in an IaaS context?

Google Cloud Platform Acceptable Use Policy

Use of the Services is subject to this Acceptable Use Policy.

Capitalized terms have the meaning stated in the applicable agreement between Customer and Google.

Customer agrees not to, and not to allow third parties (including End Users) to use the Services:

- to violate, or encourage the violation of, the legal rights of others (for example, this may include allowing End Users to infringe or misappropriate the intellectual property rights of others in violation of the Digital Millennium Copyright Act);
- to engage in, promote or encourage illegal activity;
- for any unlawful, invasive, infringing, defamatory or fraudulent purpose (for example, this may include phishing, creating a pyramid scheme or mirroring a website);
- to intentionally distribute viruses, worms, Trojan horses, corrupted files, hoaxes, or other items of a destructive or deceptive nature;
- to interfere with the use of the Services, or the equipment used to provide the Services, by customers, authorized resellers, or other authorized users;
- to disable, interfere with or circumvent any aspect of the Services;
- to generate, distribute, publish or facilitate unsolicited mass email, promotions, advertisements or other solicitations ("spam"); or
- to use the Services, or any interfaces provided with the Services, to access any other Google product or service in a manner that violates the terms of service of such other Google product or service.

Offensive Content

You may not publish, transmit or store on or via the Services any content or links to any content that Rackspace reasonably believes:

- Constitutes, depicts, fosters, promotes or relates in any manner to child pornography, bestiality, non-consensual sex acts, or otherwise unlawfully exploits persons under 18 years of age;
- Publish, transmit or store any content or links to any content that is excessively violent, incites violence, threatens violence, contains harassing content or hate speech, creates a risk to a person's safety or health, or public safety or health, compromises national security or interferes with an investigation by law enforcement;
- Is unfair or deceptive under the consumer protection laws of any jurisdiction, including chain letters and pyramid schemes;
- Is defamatory or violates a person's privacy; or
What constitutes abuse in an IaaS context?

- Based on a survey of Acceptable Use Policies of large CSPs
  - Portscanning
  - Distribution of malware
  - (Distributed) Denial of Service
  - Sending unsolicited e-mail
  - Forged headers
  - Exploiting security vulnerabilities
  - Botnets

How to detect abuse?
How Where to detect abuse?
Option 1: Network-based sensors

- Best compromise between visibility and ease of deployment: customer VLAN ↔ shared LAN
- Need relatively few sensors
- Can observe traffic between customers
- Cannot observe internal traffic of customers
- Problem: How to evaluate detection techniques?
  - Available network traces old and captured in different environments
Option 2: Virtual Machine Introspection

- Traditional host-based sensors problematic
  - Customer would have full control over OS (and sensor)
  - If VM is compromised, attacker could tamper with sensor

- Possible solution: Virtual Machine Introspection
Option 3: VMM-based sensors

• The Virtual Machine Monitor (VMM) can also provide data that can be used for detecting abuse, such as
  - Creation and deletion time of VMs
  - Resource utilisation
How could abuse be prevented automatically?

- Technical measures
  - Abuse Prevention System
  - Logging
- Non-technical measures
  - Acceptable Use Policies (AUPs)
  - Account verification
  - Financial incentivisation
How should the security status of cloud resources be reported?

- Not all abuse can be prevented automatically
- Manual examination of each suspicious event too costly
- Reports should be aggregated
- Could be achieved by assigning reputations
  - Event very likely to be abuse → higher impact
  - Reputation of individual VM
  - Reputation of user
    - Aggregated over all of a user's VMs
What impact does abuse detection have on customer privacy?

- Providers may process confidential customer data
- Violates privacy laws if customer did not explicitly agree
- Avenue of research: Is it possible to detect abuse in a privacy-friendly way?
- Surveyed providers do not give much information on what types of data they currently process for abuse/intrusion detection
  - HP and Amazon reserve the right to investigate any suspected violation of their AUPs (no more detail given)
- Privacy policies not specific to cloud offerings
Conclusion

- **Problem**
  - IaaS cloud resources can be abused by customers
  - May lead to negative consequences for provider
  - No sufficient protection measures so far

- **Research questions**
  - What safeguards are currently in place to protect cloud resources from abuse?
  - How can abuse of cloud resources be detected automatically?
  - How can abuse of cloud resources be prevented automatically?
  - How should the security status of cloud resources be reported?
  - What impact do abuse detection and prevention have on user privacy?