

▶ IaaS Threats In The Cloud – Part 3

Tech Tip
by Philip Cox

© Copyright 2010 SystemExperts Corporation. All rights reserved.

► IaaS Threats In The Cloud – Part 3

How to use Infrastructure as a Service securely

This tip will focus on exposures in the Domain Name System (DNS) and how this affects Infrastructure as a Service.

A Quick DNS primer

DNS translates names in to IP addresses. In order to get to a server on the Internet, you need to know its IP address, and it is easier for humans to remember a name (i.e., www.techtarget.com) than an IP address (i.e., 192.168.134.235). The DNS infrastructure provides that translation. It does so using a hierarchy of servers, with Domain owners (i.e., those that own the DNS names) providing “authoritative” mapping of those names to IP addresses. As part of the system, there are secondary and caching servers that help in distributing the load of answering the request for name translations that occur.

Another point of note is that the main query-response request is done using the User Datagram Protocol (UDP) and is by default insecure, stateless, and unreliable.

What are the DNS threats that affect IaaS?

Since we rely on DNS to tell us the IP address of the name we are trying to reach, anything that can be used to block the translation or return erroneous data are things we must be aware of and mitigate if at all possible. Arguably the latter, bad data, is the biggest threat we need to address. Let’s look at a scenario.

You want to manage your IaaS server, whose DNS name is server.example.com. You open your remote management tool and initiate a session. Your client queries a DNS server to “resolve” the name server.example.com to the IP. At the same time, an attacker has setup a malicious DNS server to look for DNS queries and respond with an IP of a system he controls. Your client then connects to the IP address returned (the malicious server), and now the

attacker can attempt a “man-in-the-middle” attack on your client.

At the current time, there are four main threats associated with DNS that are most applicable to IaaS services, and should be addressed:

- **Cache Poisoning:** When a DNS server does not have information on a name to IP mapping, it must ask another DNS server that does. When it receives the answer it typically caches it for later use (there are timeouts and limitations, but they have limited effect). Cache poisoning is when the server receives an answer that has incorrect information. Malicious cache poisoning is also referred to as DNS spoofing.
- **Insecure dynamic updates:** This is another mechanism to get malicious data into a DNS server, which would then be returned for any query for that information. A similar effect as cache poisoning.
- **Information leakage:** An attacker performs a DNS zone transfer to gather DNS domain names, computer names, and IP addresses in hopes of identifying sensitive network resources.
- **Denial-of-service:** An attacker floods DNS servers with recursive queries in hopes of making them unavailable to answer legitimate queries. Without a name to IP translation, you will not be able to access your IaaS resource.

So what do you do?

So we know there are problems you need to mitigate them. This may be something you actually do, if you control the DNS servers, or something you will need addressed by your provider. Here are my recommendations for mitigation:

1. **Use IP addresses only or a local host file:** If you never need to use DNS to make name to IP translations, then all the DNS issues described above are totally mitigated. While this may seem impractical, if you have a limited number of IaaS instances, and are able to assign static IPs, this is a realistic solution.

► IaaS Threats In The Cloud – Part 3

- 2. Random transaction IDs:** Ensure DNS servers have a properly randomized transaction ID (most current DNS server do this). Each DNS query is assigned an ID, and randomizing the value makes the attack harder to perform.
- 3. Source port randomization:** Configure your DNS server to use “query source port randomization”. Now the attacker needs to know/guess the transaction ID, as well as the port from which the transaction was sent (i.e., a random source port other than 53). Note that it may affect firewall rules.
- 4. Secure dynamic updated:** Configure your DNS server and clients to only accept secure dynamic updates. You can also limit the IP address range that dynamic updates can originate from.
- 5. Limit zone transfers:** This will prevent an attacker from being able to easily gather information on IPs and hostnames of your IaaS instances.

In closing

DNS is a foundational service/protocol of the Internet. The Internet, and any service exiting on it, could not function adequately without DNS. However, like electricity, people do not seem to think about it until it breaks. I hope this Tip got you thinking about one of, if not THE, most important services that you rely on, and some of the security issues surrounding it.

Author Information

Philip Cox
CISSP, CISM, PCI QSA, NSA IAM/IEM
Principle Consultant
SystemExperts Corporation
Email: phil.cox@systemexperts.com
Phone: (530) 887-9251