# Securing the Other Side of the Cloud

**Lori MacVittie, 2009-01-09**

*Why would miscreants bother with other routes when they can go straight to the source?*

People concerned with security of the cloud are generally worried about illegitimate access of the applications and data they may deploy in the cloud. That's a valid concern given the needs of certain vertical industries to comply with privacy-focused regulations like HIPAA and PCI DSS. It's an extremely valid concern given research and studies showing just how vulnerable most web sites and applications are. Hint: it's more than you probably think it is, and it's likely your application is vulnerable to exploitation.

Moving an application from your environment to the cloud doesn't make it any less or more vulnerable to exploitation. The same code and platforms that made it vulnerable ***inside*** your data center make it vulnerable ***outside*** your data center.

But those same platforms and languages and environments are used to build the management systems through which you control your little piece of the cloud and one ***has*** to wonder how vulnerable ***those*** applications might be. It's a question that needs to be more well considered given the financial implications of someone with ill intent gaining control over your cloud deployment.

## APPLICATIONS ARE APPLICATIONS ARE APPLICATIONS

A web-based application is a web-based application no matter what its function may be. That may seem obvious to some folks but all too often it seems that we forget to include them as a potential avenue of entry. If a cloud provider offers up a web-based management console for use to provision and manage resources inside their cloud, then that's a potential point of exploitation and, methinks, quite a dangerous one.

Those old "u has been hax0red" pages that replaced the index files of web sites and applications might be more easily manipulated through the management console, replacing entire images instead of simply pages. A DoS against a particular site or application might be so easily carried out by compromising the management application and simply shutting down (and perhaps deleting!) instances. No bot-net necessary; just a few clicks on a web page and you are offline.

Go ahead and say it, I know you want to. "***But they use SSL to secure the management application!"***

Anyone who was thinking that will now go to the blackboard and write 1000 times, "SSL is not application security." In hex.

SSL is a mechanisms for securing conversation and data ***in flight.*** It does not stop vulnerabilities from being exploited, nor does it guarantee that the client attempting to access the application is legitimate – unless the application ***requires*** client certificates, and we know that almost never happens. If you still don't believe me, please see this site and this site for more detail on Google GMail and SSL and vulnerabilities.

SSL is not enough to secure ***any*** application and certainly should not be the only security (aside from requiring authentication) that is protecting a cloud management web application. SSL should be only one part of a more comprehensive application security strategy.

## WHAT ELSE IS THERE?

Securing any web-based application requires a two-pronged approach: access control and application security. The former ensures that only those legitimately authorized to access the application are allowed to do so, and the latter protects the application and its underlying platforms from myriad attacks – from XSS to session hijacking to parameter tainting to cookie poisoning to SQLi.

Access control can be as simple as IP-based restrictions – allowing access only to a specified IP or range of IP addresses. Or it can be more sophisticated using secure remote access technologies that can not only restrict based on IP (simple) but on type of client or version of client or the existence (or non-existence) of specified applications running on the client machine. Secure remote access uses SSL, so the conversation and data in-flight is protected, but it goes far beyond simple transport-layer security and provides a variety of methods for ensuring that only legitimate users are allowed to access the management application. Doing so reduces the possibility that someone can access the application and begin poking around to find a vulnerability to exploit in the first place.

Application security ensures that the management application is protected against all the standard web-based exploits out there, and further provides the means by which the application can be protected on a moment's notice through the implementation of scripting-based security solutions. Application security solutions, when coupled with a vulnerability assessment solution, can provide virtual-patching to prevent exploitation of discovered vulnerabilities while developers address – or administrators' patch – the problem.

There is no reason to ***not*** employ every means necessary to protect this most critical application and, given the potential impact on not just one but multiple customers from a single successful attack, there is no reason for customers not to ***demand*** that cloud management applications are properly insulated from illegitimate access and potential exploitation.

So if you're using a cloud solution today, how secure are its management applications? Do you know? Have you asked what solutions are in place to ensure the security of those applications?

- Researcher: Google Mail vulnerable to sidejacking despite SSL
- Incomplete List of Alleged Vulnerable Sites
- Check SSL Certificates for the Vulnerable MD5 Algorithm
- [PDF] **XSS** Evasion—Trying to hide in the all-concealing torchlight
- Amazon Compliance Confession About Customers, Not Itself
- Amazon Web Services Developer Community: Does Amazon EC2 meet PCI Compliance
- How to secure virtualized applications against the unknown
- Cloud Changes Cost of Attacks
- An Unhackable Server is Still Vulnerable

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

| | | | |
|---|---|---|---|
| F5 Networks, Inc.<br>Corporate Headquarters<br>info@f5.com | F5 Networks<br>Asia-Pacific<br>apacinfo@f5.com | F5 Networks Ltd.<br>Europe/Middle-East/Africa<br>emeainfo@f5.com | F5 Networks<br>Japan K.K.<br>f5j-info@f5.com |