Brad Semrad
SE-4930
February 6, 2012
Article Review 4

The article is titled Security and Privacy Challenges in Cloud Computing Environments and was written by Hassan Takabi, James B.D. Joshi, and Gail-Joon Ahn. It was in the November / December 2010 edition of the IEEE Security and Privacy magazine.

The article begins by discussing what Cloud Computing is and they define cloud as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction." In addition they discuss the five key characteristics of cloud computing. The first is rapid elasticity which allows the dynamic change of resources to scale up or down based on demand. The next is measured services which is the measure and optimization of the shared resources for the environments. The other characteristics are on-demand self-services, ubiquitous network, and location-independent resource pooling. In addition, there are three delivery methods. The first is Infrastructure as a service (IaaS) which is a set of virtualized infrastructural components. The next delivery model is Platform as a service (PaaS) which enables programming environments to access the underlying building blocks of the hardware. The final delivery model is Software as a Service (SaaS), which is the cloud service itself.

After the definitions, the article discusses the unique issues in security and privacy. One of the biggest issues is outsourcing the information to third parties. This requires appropriate mechanisms to prevent unauthorized people including the provider from viewing the data. When talking about cloud models there are different security concerns related to them. In Software as a Service, the providers are responsible for the application services that they provide. In Platform as Service, the customers are responsible for protecting the application that they run. However, the providers are responsible for isolating each application and the resources that are used by the application. In the Infrastructure as a Service, the customer must secure the application and data that are used. In addition the article discusses that the customers cannot simply rely on the provider to have security. Another item that was brought up is the use of virtualization and the communication between this virtualization. This requires that each virtualization to have strong isolations and any communication between the virtual machines has to be secured. One of the problems that exist is that Compliance and Regulations may not allow cloud computing to be used. This would require the cloud service to be validated in addition to any applications. The article continues to discuss other issues to securing the cloud such as authentication, access control, trust management, and secure-services. The article discusses a few guidelines for these but no good proven or accepted methodology.

From the article I learned a few things about the securing the cloud. The first item is that there are really not any know secure controls or methodologies to secure the cloud. This may be due to the article not covering this, but there are still many issues to be addressed. The other item learned was that the cloud service would have to be validated for compliance and regulations in order for an application to be created with the service. The final item was the idea of securing the communication between the resources. Even though these live within the network or devices, they each need to be secured individually. This provides extra layers of security in the environment.

When developing secure software, I should keep in mind that with new technologies or third-party technologies, you have to make sure that they follow all compliance and regulations that are required. The other lesson is to make sure that all layers and all portions are secured. Also, when developing a cloud or shared resource system, a developer should create isolation for each component. This can help prevent other applications from being infected or comprised due to other less secure applications.

The questions from the article are what are a lot of the concrete solutions to the problems suggested? The article only discusses a few solutions to the issues addressed. They seem to leave out any possible practices or ideas to address these issues. The biggest question about how to address is the issues that seemed to pop up the most. This was how to keep the data and applications separated?

Article can be accessed as a PDF here:
http://csdl.computer.org/dl/mags/sp/2010/06/msp2010060024.pdf