The Podcast was the 43rd episode from the Silver bullet series by Gary McGraw, which was recorded on October 21, 2009. It featured Christopher Hoff and can be found at http://www.cigital.com/silver-bullet/show-043/.

The Podcast’s main topic was What is Cloud Computing? and How to Secure the Cloud? It first defined what Cloud Computing was. There are two different perspectives for this term, one from the provider’s or vendor’s point of view and one from the consumer. From the provider’s point of view, it is the technology on how to create a product that involves key technology terminology like elasticity and scalability. From the consumer’s point of view, it is any service, technology, or anything else that allows them to take their content and data and place it or connect to store or process the data. It also discusses that cloud computing is really something that we have been doing forever with a different spin. Cloud computing is really just an operation model to make more effective and efficient way of using computing resources.

In cloud computing there are three different service models that create the cloud. These are called SIP stack or Software as a Service, Infrastructure as Service, and Platform as a Service. Software as a Service is the application and content for the developer. Platform as a Service is the integration and middleware. Finally, Infrastructure as a Service is the hardware and the virtualization. It is also considered the nuts and bolts of the system.

When discussing security for SIP, each level has a ways of looking at it. When discussing security the farther down on the stack you go, the more responsible that model is for security. For Software as a Service, security is really built in or contracted in by the provider. This is due to the fact that you are running on their platform and only really have control of your application. In discussing Platform as a Service, there is some security because it is the hooks into the infrastructure but yet the developer is still responsible for the security of the data passed in. This is one of the problems that people do not focus on. They typically focus on the application of Software as a Service or the Infrastructure as a Service, the network security type of layers. Finally for Infrastructure as a Service it has the security built in as this is the lowest level. It has to validate the data and responses.

After discussing how SIP has security, they go one step further and discuss an abstracted security model. This model also has three layers. The bottom most is the Hardware with involves the nuts and bolts such as routers, switches, and servers. This is essentially the network security. The next layer is the Meta-structure which the glue between the hardware and the next layer, the top layer, the Information structure. The Meta-structure is the APIs and protocols used to create this operational environment. The Information structure which is the application data, services, definitions, etc... As discussed earlier there is the focus on securing the Information structure or the applications and the network, or the hardware layer. The current problem is that not looking at the Meta-structure layer. Most of the energy is focused on the other two ends.
In reading the article, I learned about the definitions of cloud computing from the different perspectives. In addition, it was interesting to see at a high level of how the Cloud is broken down into different layers and what each layer is responsible for. In addition to this, I learned about the area of security that the providers focus on. It was interesting to see how security with cloud computing is not just a one stop area. It involves all levels and different trust boundaries.

In helping me develop software, in general, there is one lesson that I got out of this. There is not just one area to secure but multiple levels to secure. It is also noteworthy to say that you cannot just secure one layer on your stack but all layers equal. This was a lesson that was not learned by current providers. All layers have to be secure otherwise it can compromise the whole system. This is the Platform as a Service. In addition, when choosing or developing a cloud platform, it is good to keep in mind these security related issues.

The questions that I have are is there any big difference in securing the cloud in comparison to the standard methodology that has been used? The next question is that are there any different security patterns or methodology that needs to be used when looking at cloud computing or is it the combination of already know methodologies or patterns?