Best Practices for Security in Cloud Computing

featuring Don Faatz and Tim Morrow as interviewed by Eileen Wrubel

Eileen Wrubel: Welcome to the SEI Podcast Series, a production of Carnegie Mellon University's Software Engineering Institute. The SEI is a federally-funded research and development center sponsored by the Department of Defense and operated at Carnegie Mellon. A transcript of today's podcast is available at sei.cmu.edu/podcasts.

My name is Eileen Wrubel, and I am the initiative lead for the Agile-in-Government practice here at the SEI. Joining me today are Tim Morrow and Don Faatz who are both researchers here at the SEI. Today, they are here to talk about best practices for security in cloud computing. This is the second of a two-part podcast focused on their work in cloud computing. Welcome, Don and Tim.

Tim Morrow: Thank you very much, Eileen, for having us here.

Don Faatz: Yes, thank you, Eileen**.**

Eileen: I am glad you could join me. I would like to start by having each of you talk briefly about your backgrounds. What have you done here at the SEI, at CMU, and prior to your arrival with us.

Tim: Well I have been here 15 years now at the SEI. This is Tim. I have focused mostly on systems-of-systems type of work. I am an architect, and I try to get an early impact on the lifecycle programs where we can make an impact. Before I came to the SEI, I worked as a hardware/software engineer where I did a lot of work working with nuclear reactors for the Navy.

Don: Hi, this is Don. Before joining the SEI, I spent about 20 years as a cybersecurity architect helping U.S. government organizations address their cybersecurity challenges. Just before coming to the SEI, I was at the National Cybersecurity Center of Excellence developing security solutions for industrial control systems that are used by electric utilities.

Eileen: Today we are here to talk about best practices in cloud computing. In our earlier podcast, we talked about risks, threats and vulnerabilities in moving to the cloud. What is the current state of cloud computing, and why is this an interest for you both right now?

Tim: Well, it is changing a lot. We have a lot of interaction with customers now where they are moving to the cloud, but we are seeing also that it is a very dynamic area. So we are seeing new features being added to the cloud, specifically in areas like AI [artificial intelligence] and machine learning, the assistants, like Alexa, different things with IoT, and serverless computing. So there are a lot of new services and features coming along that we need to help our customers with.

Another thing that is why we are developing these papers is to help IT staff that are typically very small with these organizations, so you want to provide some guidance. We are not seeing very clear guidance out there in the market. The last thing from my point of view is we always run into where customers just get so overwhelmed with these problems. We want to provide a way to help them understand how to get started in this. What is a good way to do that?

Eileen: OK, Don?

Don: I think cloud computing provides an enormous opportunity for businesses and governments. It is a demonstration of the economic principle of specialization. Somebody takes over a function. So the cloud-service provider focuses on one aspect of something running information technology. So now your business doesn’t have to stand up the data center, buy hardware, and configure it. You buy that as a service, and you can focus more on running your business or your mission, which is really what it is all about.

The downside to this is that you are trusting business assets to some other entity, the cloud service provider. People have a difficult time overcoming the trust barrier with respect to handing over that information, since it could conceivably damage your business if it was lost. Large organizations seem to have done a good job. They have a lot of resources to apply, but small and mid-size organizations seem to struggle. The best practices paper is targeted at helping these organizations understand the things they can do to address risks and threats and develop trust in outsourcing parts of their IT operations to cloud-service providers.

Eileen: In a recent SEI blog post you outlined some of these best practices that organizations should be using. Can you talk a little bit more about them?

Tim: One of the first ones we talk about is performing due diligence. We mentioned that in the earlier podcast that we did that we were going to highlight four areas here in this discussion. One is to make use of a cloud adoption framework. There are so many different cloud providers out there if you are a government organization. They have FedRAMP that gives them a list of 100 different ones they could choose from. So it is hard to figure out which one. But we found that if you go with one of the big three, they have a lot of extensive documentation for how to do adoption into the cloud.

As well as, there is a number of good third parties out there. So developing a framework kind of leads you to understand what all you need to do to move to the cloud. Your transition is important, so we recommend that.

I think the training is a big one. A lot of times people think, I have IT staff that I can develop. I do VMs, and I can set them up in my network. When you put that up in the cloud, the security is very different. You need to have the training for your staff to understand what it takes to do it safely. I think that is a key part of that.

The security is not the same in terms of a perimeter for your network. A lot of times people are slow catching on to that, *It is not a fence up protecting me. Especially when I go to the cloud everything is accessible via the Internet.* You need to understand how to do that securely.

A third point I would like to do under due diligence is that in the past when you had your on-premise data centers, you had to go out and physically do that inventory. It wasn’t very easy to understand, *What version of software do I have? What version of hardware is out there*? When you are in the cloud, you can allocate what you want to spin up for servers, what you are running. So it is very easy to have a blueprint of what exactly you have at this moment in time. That is something that we are seeing that people need to take advantage of in their security concerns too.

The last thing I want to bring up under this one is—we talked about this a little bit in the previous podcast too—about getting your data out. You spend a lot of effort to get your features, your assets up into that cloud, but you need to be concerned that they are a business too. They can fail. They can have problems with losing data due to power or something. So you have to have a plan in place to figure out whether I need to have a backup, multiple cloud providers, duplicating your services, or having a way that you need to have data on-premise. That is part of the planning that you need to do. It is part of your due diligence here.

Eileen: OK, Don?

Don: The second area for best practices is to manage access to your data resources. The very first thing you should do is you should adopt multi-factor authentication. This is just generally good advice whether you are doing cloud or not, but as we mentioned in the threats and vulnerabilities, cloud management APIs are accessible over the Internet. Password credentials are easily compromised, and you have no indication they have been compromised until such time as they have been used. Adding a second factor, especially for your privileged users who do management is critically important.

On a side note and personal advice, if you use things like Gmail or [Microsoft] OneDrive or even Facebook, you are using the cloud. All of these services offer multi-factor authentication to you personally. So not only should you do this in your business, you should also consider doing it personally.

The next area is to implement a good collection of roles that provide separation of duties for managing all of your cloud resources. This sounds like straightforward everyday advice you would do in your IT data center, but you should be careful not to just replicate the roles that you have internally because the services are different. It is not unusual for people to have network admins and operating system admins and application admins. You could try to translate those to the cloud, but in the cloud everything is virtual. It is just a matter of writing a line of code to change your networking or your hardware or whatever. You should look across the new environment and understand what roles are appropriate. The big three cloud service providers offer advice. Amazon has a publication on roles and responsibilities. Look at that in the line of doing due diligence, understand those, and then define your own set of roles and responsibilities.

The last area for managing access will seem kind of again like a normal thing you would do. Correctly configure and manage access on all of the services. The single largest cloud-related incident over the last year was people misconfiguring Amazon S3 buckets and leaving them publicly accessible on the Internet. Every cloud service has a unique set of permissions that have to be correctly configured. You need to understand them and configure them correctly, so that you don't accidentally leave a collection of your data exposed to the Internet. Tim?

Tim: The third area is protect data. Following along with what Don had just spoken about was the data that you have in your system, you have to worry about the encryption of it. The data you transmit into the network—that is, getting it in so that you have it in there securely—needs to be encrypted.

Once it is on the system, you want to make sure that it is encrypted. Then, when it is in use by the applications, encryption is important. These are options that you have to select when you are putting your assets and your applications in place in the cloud. You have to physically choose to do that encryption. That is something that is a very good, safe thing to do because if someone would accidentally get access to your credentials and be able to access that data. If they don't have the keys for it, then you are protected. It just gives you a little bit better protection. So encryption is very important for that.

The next one was dealing with the availability of your data. So I mentioned that earlier, doing due diligence, but just understanding where your data is in your configuration, how you are using it, and what would happen if you would lose some service availability. It is very important to understand how your cloud service provider implements their systems. They understand how it works. You need to have that same capability to make sure that you can always get at your data or if you need to come up with alternates to do that.

The last part is dealing with deleted data. Don did a very nice diagram in the blog post that provides an example of*, Oh I put data up here. I put it in, and I need to have it archived, and it is backed up*. But that data also goes to multiple other places in your network if you are delivering content. The concern is being able to know where it is, and if I want to get that out and removed, you will have to work with that cloud service provider to have a very good understanding of how they implement things, so that you are assured that you can get that date out.

Don: The last area of practice is to monitor and defend the resources that you have deployed to the cloud. A lot of people are used to having their own instrumentation on-prem, and they know the data that comes from there, and they know how to use it. A first pass for most people is to say, *OK, I'm just going to take all my on-prem monitoring, and I'm going to put it out in the cloud*. Well, remember we said that you gave up some responsibility to the cloud service provider. You no longer have physical visibility of what's on the physical network. You are looking at something on a virtual network.

Our advice is don't start with the premise that you are just going to move all of your other stuff, despite the fact that over 70 percent of people who go to the cloud do exactly that. We think you should start by understanding the monitoring that the cloud service provider offers. One of the fundamental principles of cloud computing is metered service. To have metered service you have to have instrumentation. Cloud service providers have vast instrumentation, and most of them make available to their customers all kinds of data. Look at that data and understand how to use the cloud service provider's monitoring and augment it only in places where you think you have a blind spot that you need to.

The next challenge is your security situational awareness is not just your cloud infrastructure. It is all of the IT assets, no matter where they are. The next thing you are going to have to do is find a way to combine the information you get in the cloud with the information that you gather on-prem, recognizing that it may not be an apples-to-apples comparison because you are using someone else's monitoring. When you do combine them, you again need to look at *What is the best place to do that combination? Should I move my on-prem data to the cloud, or should I move the cloud data back out to on-prem*?

We have talked to some cloud service providers, and they suggest that you might actually be better off moving your on-prem data into the cloud. Tim had mentioned earlier that there is a cost to moving data in and taking out, and it is often asymmetric, meaning it is cheaper to move it in than it is to move it out, for somewhat obvious reasons. So with the service providers you might pay less moving your on-prem data into the cloud. Also you have elastic capabilities in the cloud. You can spin up all kinds of resources to do analysis and then shut them down. So it might actually be cheaper to do your analysis in combination in the cloud.

Lastly, I mentioned the cloud service provider gives you this advice. The cloud service provider is monitoring the underlying infrastructure. Whenever you have an incident, it is important to know how to collaborate and work with the cloud service provider to investigate that incident. They have more information than you do. They can help you. Before you have an incident, you should work with them to understand how that incident response is going to go.

Eileen: If a member of our audience wants to learn more about these best practices, what resources are available to them?

Tim: One good search that we have used a lot is the Cloud Security Alliance. Also, ENESA [European Union Agency for Network and Information Security] is another good search that is European, so it gives you a different perspective. We have learned and more recently appreciate the data privacy. They have always been very much in that. So now the U.S. is starting to catch on to that and we have this. So we found their website was very good with that. I like looking at the SANS Reading Room. It is one that has always been very educational to help me understand what people are running into. I know, Don, you have a couple that you like to look at too.

Don: Yes. Tim mentioned using a cloud adoption framework. Amazon has actually a very general-purpose, cloud-adoption framework. They obviously published it, to use with their service, but it is in no way vendor specific. Using that is a good way to do things. From a managed-access perspective, most of the large vendors have elaborate identity and access management capabilities. You should look at the documentation for those. Lastly, we have a paper Best Practices in Cloud Security that will be released soon. You can take a look at that and it will have more detail on the things we have discussed here.

Eileen: What is next for both of you? What is the next collaboration I am going to talk to you about?

Tim: We are looking into applying security in the hybrid multi-cloud environment. There are a lot of new services that we mentioned earlier coming out by these cloud service providers. They are not provided at all the different data security levels. So there are different services at different levels and that's one thing that we want to look at, to identify, *What type of security is appropriate for this level of data*? And, Don.

Don: The other thing that we have started to look at is security related to the Internet of Things, specifically use the Internet of Things within enterprises, *What happens when people bring their personal Internet of Things stuff into the enterprise environment, and how can industrial control systems be adversely affected*? There is a natural synergy here because a lot of Internet of Things stuff depends on back-end cloud services to work. The sharing of information from those personal sensors or other sensors out to the cloud creates an interesting challenge. We have just begun looking into this area.

Eileen: I look forward to having both of you back some time to talk about those topics once you have done some more work. I would like to thank both of you for joining me today to talk about this work.

Tim and Don recently co-authored a blog post outlining best practices in cloud security. You can read that at insights.sei.cmu.edu. Click on the author tab and search under Faatz F-A-A-T-Z. Also, please know that we will provide links to all of the resources mentioned in today's podcast in the transcript.

This podcast is available on the SEI website at sei.cmu.edu/podcasts, on Carnegie Mellon University's iTunes U site, and the SEI's YouTube channel and [SoundCloud]. As always, if you have any questions, please feel free to reach out to us at info@sei.cmu.edu. Thank you.