Applying Best Practices in Network Traffic Analysis

featuring Tim Shimeall and Timur Snoke as Interviewed by Suzanne Miller

---

Welcome to the SEI podcast series, a production of the Carnegie Mellon University Software Engineering Institute. The SEI is a federally funded research and development center sponsored by the U.S. Department of Defense. A transcript of today's podcast is posted on the SEI website at sei.cmu.edu/podcasts.

Suzanne Miller: My name is Suzanne Miller. I am a principal researcher here at the SEI in the Agile-in-Government group. And I am very pleased to introduce to you again—they have been here before—Tim Shimeall, Timur Snoke. They are going to tell us today about best practices in network traffic analysis.

So for those that have not met you before with us, could you give us a little bit of background as to how you both got into this sort of best practices thing? Because that's a thing. And what drew you to doing that, that kind of work?

Tim Shimeall: Well I started out as an academic, a professor working for the Navy out in Monterey, California which is…

Suzanne: It's as good as duty as you can get.

Tim: Yes. And then I really became interested in network security when I was kind of a sideline on the Morris worm incident. I actually had an administrator rush into my office. And that started me being interested in tracking down network problems and network issues. Particularly human-caused ones. That eventually led me here to the SEI, and I decided to shift out here and swap Monterey for Pittsburgh, which I've never regretted except in Februarys. I have been an active member of the group for the last 20 years. A lot of that experience has been working with departments and agencies and companies and special events. Over that time, a lot of the common practices emerged and some of the best of breed filtered to the top.

Suzanne: If you see enough problems, you start to build, *Here is the common solution pattern for this*. You and I are of an age where, yes.

Tim: Principles emerged, yes.

Suzanne: Yes, cool. Timur?

Timur Snoke: I kind of started in the trenches. First, as a high school teacher in a classroom with a bunch of computers that didn't work and then ending up working for consultants in a variety of different industries. I saw that there were common problems across all the different places that I went to, but there wasn't really a unified vision as to how we solve them. A lot of vendors have their own solutions, but they did not have vendor agnostic solutions that explained why we do what we do. When I ended up here, the ball started rolling in a positive direction.

Suzanne: I have done best practices work in process improvement in some of those areas. In the network analysis area, what are some of the things that distinguish a best practice from *almost good enough* and from, *Oh, please don't do that*? How can you characterize best practices?

Timur: Or even aspirational practices.

Suzanne: Aspirational practices is another one, yes.

Timur: There is a limit to how much you really want to do and how much you really want to invest in it because, as most businesses will recognize, their network is not a profit center. It doesn't earn revenue for the organization. The money that you spend on defending the network is really money that you are taking away from something else. You have to be intelligent about how you are spending your money and try to get the biggest return on your investment. That is where I think the best practices come in.

Suzanne: So the best practices are the ones that you can identify: *What is the return on investment if we do this or what is the risk if you don't do this?* Because that is the other side of this*; if we don't do those things, then we run risks that may be sort of out of bed with how much it costs to defend against them, right?* That is the thing you are trying to mitigate.

Tim: But without competing against the activities that support your profit centers. It is easy to forbid things which you need just because they are risky.

Suzanne: Yes. We have that eternal conflict between usability and security. The usability is one of the things that accelerates our ability to deliver our capability profit center, and the security is often the slowing down of our ability to deliver that.

Tim: In terms of network traffic, one very common question becomes: *OK, do we encrypt the traffic on our network*? If we encrypt the traffic on the network, it is improving the data security because it has got a lot more privacy associated with it, particularly if we go end to end. On the other hand, if you are looking to see whether or not Joe is emailing out the company secrets and the traffic stream is encrypted, you don't have that capability.

Suzanne: Sometimes the things that you think are best practices might be best practice for one vulnerability, but may actually reduce your ability to address some other kind of vulnerability. There is that sort of multilayered aspect as well.

Timur: Absolutely, I would also add that I think that it is important to recognize that although we are talking about network security best practices, really the overarching goal is to defend whatever the mission is of the applications that are running on the network. Although we could secure everything in every dimension, we end up with a bunch of machines that can't talk to each other. The things that we are supposed to do, we are unable to do. We have to weigh all of that.

Suzanne: When you express best practices, how do you help analysts understand some of that context?

Tim: Part of it is expressing things in terms of trade-offs. You get into a dialogue with the analysts, *Look, this is what you want to do*. But there is this other side about it. *Are we trading off this to that? Are we spending the time analyzing network traffic rather than spending the time extending the network, dealing with things like that? When we are deploying things like network firewalls, to what degree does that segmentation of the network make things more complicated to support integrated applications, for example?*

Suzanne: Right. End-to-end, how does it reduce the flow of data that is needed in a timely fashion, whatever that timely aspect is?

Tim: Right, and often this is very key with respect to traffic analysis because what analysis you are able to do depends on the infrastructure of your network and the architecture of your network. Where you are able to see the traffic, where you are able to make sense of the traffic.

Timur: That is really a key component to all the best practices is understanding what it is that you are defending, understanding what the perimeter looks like. *Where are the gaps in defenses? Where are the gaps in security? And where are the gaps in your understanding about how the applications work in the network?*

Tim: Understand also—and I hate to put it this way—understand what you are looking for. I have seen analysts that spend their time looking at DNS [domain name system] data not because DNS is particularly key to their application, but because the analyst just happens to be interested in abuses of DNS, and he is hunting to see whether there's any abuses of DNS occurring within his organization.

Suzanne: And that may not contribute to their mission in a way...

Tim: And it doesn't contribute to the mission...

Suzanne: ...that is substantive...

Tim: ...it doesn't reduce their risk. It doesn't give you more awareness of the organization. He is just hunting for weird little artifacts in the DNS queries and responses. Do you really need somebody to do that? The obvious answer is probably not.

Instead you want to focus the analyst and say: L*ook, this is what we are really concerned about. You are interested in DNS. Wonderful. We want to see whether or not any of these particular domains or any significant shift in resolutions is occurring. Those are things we want to track but not these weird little artifacts;* that is, *Is there any voice-over DNS occurring?* It may not be relevant to us.

Suzanne: Right. Depending on the context. So context is everything, just like every other aspect of technology. It also sounds like there is a need for an understanding between the business element of the business, the mission element of the business, and the technical, the technology element of the business. The example you gave, the guy looking at the DNS stuff, probably hasn't been connected enough to the business to really understand what it is that gives value back to them in terms of network analysis. How are you dealing with that translation between the things you would tell a technical analyst and the things you would say to the business people that are essentially paying for these best practices to be implemented?

Timur: Interestingly enough, this all boils down to communications, right? We are talking about network traffic analysis, and the really integral part of it is having effective communications, so the institutional knowledge of the business owners can be translated into actionable intelligence that the network defenders can use to support the business owner's mission.

Suzanne: How are we making that happen? What I am looking at is, what are the mechanisms that you guys are using to make sure that that communication occurs not just that we have published another set of best practices?

Tim: We focus on awareness rather than on instant response or security. The aspect of awareness is an understanding of: *OK, what knowledge do your decision-makers need to do to make appropriate security decisions for your organization, and how do we derive that knowledge from the network?* That is where network situational awareness comes in.

A classical model of situational awareness is, *How do you perceive now? How do you understand where things are shifting towards, and where do you predict things are going to shift into the future?* Looking at things in that way tends to put it in a technical perspective.

Where things are now, the key parts of where things are now are business things. A*re you protecting engineering? Are you protecting finance? Are you protecting HR? Are you protecting*

parts logistics? *Are you protecting contracting*? Those are key business functions that every business needs to have in order to survive. If you don't protect those, it doesn't matter how good you are at protecting the router. Yes, a router is important. It provides connectivity, but is not more important than getting paid.

Suzanne: Right. We will all agree on that.

Timur: It is important to identify security practices that support the nature of the business, because if flexibility is a key component in the business, coming up with a workflow that requires an extended period of time before executing a new application or something like that is going to be causing pain for the business. Again, those trade-offs need to be identified, but understanding a good baseline and communicating what the current state is and maintaining awareness of how that is evolving and preparing for the big changes that are coming are all things that we have to pay attention to.

Suzanne: We recently held our annual research review at the SEI. I would say this review had more content related to Internet of Things and machine learning than I have ever seen. That big shift is one where network traffic…There is a lot of situational awareness that going to be affected. Having best practices in place so that you actually can start to look beyond the mechanical things, down in the weeds things, to some of the more situational things, the more business things, I think that's going to become more and more important as we move forward with these things.

So I am a network traffic analyst, and I want to be better at doing my work. I want to use your best practices, but I also want to communicate with my management about them. Where do I go? What resources do we have to help somebody that actually wants to do this better to be able to improve their practices?

Tim: One of the key resources that you have is. one, communicating with other analysts. The SEI does have an annual conference where analysts gather together and talk as analysts. It is a very geek-heavy, very nerd-heavy fest.

Suzanne: My brother goes.

Tim: And it is called FloCon. The next one will be in New Orleans in January, early January. We are in the ramp up to that right now. The basic theme of this FloCon is using data to defend, particularly using data to defend large-scale networks. There are a bunch of people there that have a lot of experience in pulling apart various sorts of data, not just network flow data, but log data, packet data, routing data things like that. You hear and talk with, *What works well for you? Well, what works well for us? Well we ran into this kind of an issue. Well, we dealt with that kind*

of an issue by going this way. Being able to exchange practices and get a feel for how other people are doing it is a very, very big advantage to learning more.

For those coming in new, there is training going on. One training that we are going to be doing is actually being taught by some people that probably should be more modest, but anyway, it is on thinking like an analyst.

Suzanne: That was...we did that podcast earlier...

Tim: *What is a model of network activity, and what are some of the common thinking fallacies you fall into? And how do you defeat those fallacies? How do you deal with some of those kinds of concerns*? That is material that we introduced last FloCon and have improved upon for this coming FloCon. That is moving forward there.

In terms of the analytical resources, there is also the forthcoming SiLK Analyst Handbook, which is really much more focused on the analysis process. We are looking at analyzing things in terms of more or less a reactive model. You have an event. You want to understand what is going on around this event. It may be something where a piece of equipment failed. It may be that you got hacked. It may be that there was an unexpected drop or boost in network traffic. How do you figure out what is going on? *How do I support a multi-threaded analysis approach where there are several different pools of data that may appeal there? I want to be able to analyze those in parallel and then integrate.*

Suzanne: Right, and figure out which ones are the meaningful ones.

Tim: And how do I work in a more exploratory manner? The key thing there is where do you stop exploring and say, *This is the conclusion*. You are working in a more iterative fashion of exploring, testing, and defending on that. The handbook really gets into that in some depth.

Timur: Admittedly, it is 250 pages long. As a resource for really digging into it with examples, that is a resource that is coming out very soon now. We are still in the process of getting the final release approval, but it is coming out.

Suzanne: Sometimes it takes a while for that. We always say it's worth waiting for.

I am also guessing that FloCon is one of the sources for some of your best practices from the viewpoint of being able to look at what kinds of conversations are going on. *Everybody is talking about this. Oh, we don't have that in our list of best practices but that is emerging*. I guess what I am saying is I am intuiting that this is not a static set of best practices. This set of best practices is meant to evolve, and that it's meant to be updated. So people shouldn't just look at it once and say, *OK, I'm done now*. *It's something that we need to keep track of over time because the world changes.*

Tim: That, in fact, itself is a best practice. You want to have some mechanism for keeping current. You want to know, *OK, the kinds of technologies that we are fielding today are not the kind we fielded 10 years ago; 10 years ago the big question was, Do we want to go wireless or not*?

Suzanne: That is not really a question anymore.

Timur: The idea that we export things into the cloud and we are doing cloud integration and supporting multi-cloud integration and those kinds of things are really something that wasn't on the radar 10 years ago. It is very current today.

The types of risks that we are facing. Ten years ago the big risk was botnets. They have people that are herding together large numbers of compromised machines and focusing on it. APT hadn't even been composed 10 years ago. That's an acronym. And today it's a very concerning threat and a very impactful threat. The idea of spearfishing and whaling as attack methods really emerges a much more serious threat over the last decade. And …

Suzanne: And so that's going to continue?

Tim: Yes.

Suzanne: That is really the point is what happened in the last 10 years. We don't know what's going to happen in the next 10 years. But we know that we're going to have to evolve and that we're going to have to be responsive and be able to continue looking at these issues as they emerge. So we need communities like FloCon. We need people like yourselves that keep watching this part of the technology to see what are the new things? We need people to respond to do things differently. Those are all, I think, things that we want to make sure our listeners take home.

Tim: Something like FloCon also gives you an opportunity to see what solutions work and what solutions are really kind of problematic. There is an awful lot of tendency to follow, *Ooh, there's a nice shiny thing. I want that*. Rather than look at, *OK, what does this really provide in terms of capability that my organization truly needs*?

Suzanne: And benefit and risk. What risk does bringing that technology in really mean for our defense? Both sides of that so…

Timur: Just because something is popular or being much discussed, does not mean it is universally needed. Some of it comes with quite high price tags both in terms of knowledge required by the users and in terms of acquisition and fielding costs.

Timur: This is actually a really big component in the best practices where the cost of maintaining the resources to support the acquisition of data for making decisions about defending the network: *How much is enough? How much is too much? Do you really want to store and maintain that? What kind of liability issues are you getting into as you start looking at collecting information on your network?* If you are a private enterprise or a publicly traded company, all kinds of things that we need to be aware of.

Suzanne: Many of those, again, are things we didn't think about as clearly 10 years ago. We have got to evolve our way of looking at these things.

I am going to suggest to our listeners that they stay in touch with you guys, and watch for your blog posts, and watch for future podcasts. Look for you at FloCon. I am assuming you will both be there since you will be teaching. New Orleans in January, not quite Monterey, but, you know, it's not bad.

Tim: It's not bad.

Suzanne: It is not bad. I want to thank you again for spending the time with me today to talk about this. I think this idea of understanding what is the balance of how much to invest in the best practice versus be aware of how it actually affects your business, that is a key element that it is easy to let go of if you really are just in the weeds of whether it is network traffic analysis or other kinds of data analysis. I think that message is one that everybody appreciates. Thank you again. FloCon. Go to flocon.org. Is that correct?

Tim: FloCon without a W. F-L-O-C-O-N.

Suzanne: Yes, I automatically think of that now, but I know it is not automatic for everyone. And I also want to mention that you co-authored with Angela Horneman an SEI Blog on this topic, so there is a blog post out there. All of the resources we have talked about will be available in the transcript that goes along with this podcast. I want to thank you both for joining us, and I want to thank our listeners for joining us as well.

Tim: Thank you, Suzanne.

Timur: Thank you very much.

Thank you for joining us. Links to resources mentioned in this podcast are available in our transcript. This podcast is available on the SEI website at sei.cmu.edu/podcasts and on Carnegie Mellon University's iTunes U site on the SEI's YouTube channel. As always, if you have any questions, please not hesitate to email us at info@sei.cmu.edu. Thank you.