NTP Best Practices

featuring Timur Snoke as Interviewed by Suzanne Miller

Suzanne Miller: Welcome to the SEI Podcast Series. A production of Carnegie Mellon University Software Engineering Institute. The SEI is a federally funded research and development center operated by Carnegie Mellon University and funded by the U.S. Department of Defense. Today's podcast is available on the SEI website at www.sei.cmu.edu/podcasts.

My name is Suzanne Miller, and today I am very pleased to introduce you to Timur Snoke. It is my first time meeting him. The first thing I would like to do is ask you about why are you here at the SEI? You have not been here that long, and so, what do you do, and why would you come here?

Timur Snoke: I am one of the newer additions to the SEI. I have only been here for seven years.

Suzanne: I know. That is new here.

Timur: Originally, I went into the world of work as a high school teacher and found that I could not stop tinkering with computers. One thing led to another, and I eventually ended up as a consultant. Then I ended up here.

Suzanne: What brought you to the SEI as opposed to all the other things you could be doing?

Timur: I went back to school, and one of the people that I was in school with was a visiting scientist at the SEI. He told me about a job in his department. I applied for it but I did not get it. Eventually I found another position over with the Network Situational Awareness team.

Suzanne: Let's turn our attention to Network Time Protocol. What is it? Why is it important? And what are best practices for that.

Timur: NTP or the Network Time Protocol is the way in which devices identify what time it is. So, when one device communicates with another device, it establishes when the communication started. The expectation on the other side is that they are going to be able to identify that they received the communication in a timely fashion.

This becomes a problem when the time does not quite line up. If you send something, and you are expecting a response that comes back within a certain time period, but the response is 15 minutes off, it can cause problems in general network communications.

It also becomes a problem when you are trying to troubleshoot what is happening on your network. So if you have a computer that says that it is 4 o'clock and a router that says that it is 2 o'clock, and you have an event that crosses by both of them, how are you going to correlate the events?

Suzanne: I can imagine there are things like delays that become suspicious. Could it have gone somewhere else before it got to us? If there is an expectation that it will be within this time boundary, or if there could be a problem with one of the parties having some kind of a power issue or other kinds of things. I can see that this is an important way of establishing everything is OK on both sides.

Timur: Right. One of the concerns that people have a lot is the threat of a man-in-the-middle attack. To make sure that communications have not been co-opted in route. So making sure that things show up when you think they are supposed to, is really kind of important. NTP is one of the ways that we are able to assure that the stuff was sent and received at the time it was expected to be.

Suzanne: This is a protocol, so we embed it into different kinds of devices and into different kinds of software for troubleshooting and things like that. What are some of the things that people want to make sure they are doing if they are trying to make best use of NTP in the way that it is intended?

Timur: Essentially, NTP has been around for a long time. It is one of the foundational services. They first started working on it in 1980 or something like that. It is something that is publicly available on the Internet where you can query a public NTP server to figure out what time it is. People do this and people have set up services where they are dependent upon those time services to coordinate activities or events or things like that.

Kind of the best practices that we are working towards is saying that *If you are going to be doing stuff that requires time, which is essentially anything on the Internet, you [should] be a conscientious user of the services and do not expose yourself to any of the risks that are incumbent with public services on the Internet.*

So, if, for example, you wanted to set up an NTP service and contribute to the masses where NTP originally was set up in a time where people trusted each other; and they would expose their NTP services. So if somebody wanted to figure out if their time was good, they would make a request to somebody else's NTP server and say, *Do we have consensus on what time it is*? And over time, people have found ways to abuse that.

And so, we talk about how in, I think it was in 2015, there was this huge uptick of abuse of NTP servers where people were able to take a vulnerable NTP server of which I think there were like seven million vulnerable NTP servers, and send a single bad packet and just generate a huge response. You can send a lot of these bad packets and be able to generate a DDoS attack against other machines…

Suzanne: Distributed a Denial of Service attack.

Timur: Right. Keeping in mind that at the time, there were like seven million that were vulnerable to this, and only 5000 could generate somewhere between 30 and 400 gigs of data. So, they made some patches. They distributed them out to the community in 2016. They were able to knock that number from seven million down to eighty thousand.

But there are still vulnerable things out there. But knowing that it is out there, knowing that it is available, people use it. If you are in an enterprise of any substance, you probably need to have an NTP service that you set up inside so you are not…

Suzanne: For internal use.

Timur: Right, and you are not dependent upon external sources. So we talked a little bit in the blog post about standing up in NTP hierarchy that is available and provides a robust solution. So everywhere you are in your network, you are pretty confident that you know what time it is.

We talked about setting up multiple time servers because as Segal's Law states, *A person with one clock knows what time it is, but a person with two can never really be sure*. The whole basis of NTP is generating a consensus among multiple clocks. You get some really, really accurate clocks that could be atomic clocks or radio clocks or GPS clocks, and then you have others that hang off of them that distribute and can redistribute with reasonably certainty that they have got an accurate time. That is kind of the upshot of what we are looking towards.

Suzanne: Part of this is also understanding the risks that are inherent in these kinds of services. That is the other piece of the best practices is understanding what the risks catalog essentially is for that. What are some of the risks that people may not be as aware of that come along with these kinds of services? We have talked about man-in-the-middle already.

Timur: Timing is really important for a lot of different things. There is a lot of stuff like high-speed financial transactions that are really dependent upon timing. There are other activities like sharing credentials, signed certificates that are valid for a very, very short windows.

A lot of the banking applications that we are using now are using one-time passwords that are only valid for a very distinct period of time. If you can mess with what the computer thinks the time is, then you might be able to set up a window of opportunity.

Suzanne: You can extend the time to be long enough that you can actually figure out what the password is, as one of the scenarios that my evil mind can create.

Timur: And there is loss of opportunities for abuse. The system itself is still very trustworthy, and they try to put cryptographic capabilities in there. But when you do that you add…

Suzanne: You affect the time.

Timur: You affect the time. You do. It becomes more computationally expensive. So the response to a query now has to deal with unencrypting the communications and re-encrypting it. It just adds another layer of complexity. It is best that we work in a world where we have control, and that we have trust. But if you are a vendor that is producing products that are going out into the world, like toasters that want to have the right time, so people do not have to worry about fiddling with that, set up an NTP service on there that pulls things out in the real world but recognize that everybody who is setting up something is doing that as a public service. If you want to have your toasters for GE connecting to an NTP time source, contact NTP.org and say, *Hey, we would like to do this. Can you set up our own pool that we can have access to so we are not competing with other people's resources*? That way, we can all kind of share this utopian commodity together.

Suzanne: And it is a very useful commodity. Because I would really like my coffeemaker to have the right time on it when it produces the coffee because cold coffee in the morning does not do a thing.

Timur: Every time there is a power outage, you have to go through the house and touch every device.

Suzanne: That is a very mundane aspect of this, but we can also think of… My father has a pacemaker, so I think about timing because he's always sending data back to a server. If that time is disrupted in some way, that could be devastating to him.

Timur: Absolutely. If you think about multi-national companies, having an event that happens across multiple segments, to figure out what actually happened. To come up with a chain of events.

If somebody were to rob a bank via communication channels within the infrastructure and went from the United States to France from France to the Cayman Islands, being able to synchronize the time of all those different events requires that they have some external verifiable time source.

Suzanne: Verifiable because if you cannot establish that frame, then you cannot find anything.

Timur: Absolutely. And that's the value proposition that the NTP is providing for everyone.

Suzanne: This is very educational for me. This is an area I have never really worked in, but as I said, my dad has a pacemaker so I am going to start paying closer attention to this and make sure that the pacemaker company uses the right NTP service. I am sure when they ask them that question on the website though, they will respond right away.

I do want to mention this is the latest in our series on our best practices. We have already had a best practice podcast on Distributed Denial of Service, which we mentioned as one of the attack forms, by Rachel Kartch. [We also published a podcast] on best practices for prevention and response which she dealt with that also. Mark Langston sat down with us to discuss Domain Name Systems (DNS) best practices. We are getting through all the acronyms now. We have got NTP in the box.

I thank you very much for joining us today and talking about this.

This podcast is available at the SEI website at www.sei.cmu.edu/podcasts, and it is available on the SEI's YouTube channel, and on Carnegie Mellon University's iTunes U site. As always, if you have any questions please don't hesitate to contact us at info@sei.cmu.edu. Thanks for joining us today, Timur. Thanks for listening and viewing.