Best Practices for Trust in the Wireless Emergency Alerts Service

featuring Robert Ellison and Carol Woody interviewed by Suzanne Miller

---

Suzanne Miller: Welcome to the SEI podcast series, a production of the Carnegie Mellon University [CMU] Software Engineering Institute. The SEI is a federally funded research and development center on CMU's campus in Pittsburgh, Pennsylvania. A transcript of today's podcast is posted on the SEI website at sei.cmu.edu/podcasts.

My name is Suzanne Miller. I am a principal researcher here at the SEI. Today, I am very pleased to introduce you to Dr. Carol Woody and Dr. Robert Ellison. Today, we are going to be talking about the wireless emergency alert service and the importance of trust for its use--for its *safe* use I might add. First, a little bit about our guests.

Carol has been a senior member of the technical staff since 2001 and currently she is the technical lead of the survivability analysis team, whose research focuses on cyber security engineering, building capabilities, and defining, acquiring, developing, measuring, managing, and sustaining secure software for highly complex network systems as well as systems of systems. I have to tell you she's a very collaborative member of our staff. I have worked on several projects with her on different aspects of this.

As a member of the cyber security engineering group within the SEI CERT program, Robert has served in a number of technical and management roles. He was a project leader for the evaluation of software engineering development environments and associated software development tools. He's also a very special person in that he was also a member of the Carnegie Mellon University team that wrote the actual proposal for the SEI to be convened. He joined this new FFRDC in 1985 as a founding member. This is the first time I've ever gotten to interview a founding member of the SEI. Thank you for coming here, Robert and Carol.

Carol Woody: Good to be here.

Robert Ellison: Thank you.

Suzanne: All right. Well, let's start off by having you give us some background about the Wireless Emergency Alerts system and how it works, and how did the SEI get involved in this research?

Carol: You want me to take that one?

Robert: Yes.

Carol: The wireless emergency alerting system is a capability that's been added to the general public alerting system that's been in existence, I think, since television was started. What this allows to happen is that emergency alerts now can come directly to your cell phone.

Suzanne: We've seen that with some of the polar vortex kinds of things that have happened.

Carol: Weather alerts. Amber Alerts are another one that comes through that process. What this also allows to happen is, if you and your cell phone are in the geographic area where an alert is issued, you'll receive the notification. You don't have to sign up for it in advance.

Suzanne: And, it doesn't matter what service you are part of. Anybody that has that wireless capability will receive that notice.

Carol: All the major services are distributing these notices, but it is restricted to the newer telephones. The newer cell phones have the capability to pick up this particular communication capability because it's using a very low bandwidth distribution, so that even if the service was degraded during an emergency, you would still be able to get that information.

Suzanne: Which is important because often in these emergency situations, we do lose the typical kinds of communication services.

Carol: When the weather takes out the towers, you still want to be able to get some level of communication.

Robert: And, on purpose, it's a very short message too.

Suzanne: Which we all appreciate.

Robert: So, well it goes in those conditions.

Suzanne: Excellent. So, how did you get involved in this research?

Carol: The SEI was asked to work with the Department of Homeland Security because they're supporting all of these alert originators—and there are thousands of them—to help them figure out how to stand up this new capability. The capability itself just went live last April, and all of these alert originators are now adding this to their systems to try and understand what capability they need, and how they can integrate it with what they're already using. So, in some sense, they're struggling with all of the typical system expansion capabilities that we would think of with any software effort.

Robert: An originator can be very small, a two- or three-person office, it can be a whole county facility in Texas, or a state.

Carol: Or, national for the weather.

Robert: Or, national, so a very significant range of capabilities. You have to manage all of them.

Suzanne: So, you need to be able to understand the trust issues related to the alert originators: *Am I a real alert originator or am I somebody who wants to try to spoof the world with some alert that is not official, is not something that's real*. You have got to be able to deal with all the service providers. You have got to be able to deal with all the government agencies that are related to all these. So, this idea…

Robert: And who do you buy your software from?

Suzanne: So, all of these things come into this idea of trust issues.

Carol: And, trust is two-sided. One side of it is, *I'm putting an alert into the system as the originator*; but the other side of it is, *I'm receiving an alert. Am I going to act on it?* So, we have to look at it from both sides, and that's not typically done in a software process.

Suzanne: The originator needs to trust that when I put an alert out, the people that are meant to get it are going to actually get it. When I get an alert, I need to trust that it is something valid and it's something that I should act upon.

Robert: The alert originator also needs to say, *If I put the message in this form, they will read it, and they will know what to do*. So, it's a case of they have to understand what kind of trust are they expecting of the people who receive the message.

Suzanne: Right. So, with an AMBER Alert, you are going to expect different kinds of action than another alert, for example. So, they need to be specific about what's the expected action. So, all of these kinds of things go into that communication.

Robert: *How do I encourage that they receive or trust my message?*

Suzanne: So, you've got alert originators--FEMA, the Federal Emergency Management Agency, commercial mobile service providers, suppliers of methods-generation software--I mean all of these are elements that contribute to that trust. You have written a technical report that starts to provide recommendations related to all of those different stakeholders. Why don't you tell us a little bit about, sort of, what is in that report and what is important for people that want to know more about both the Wireless Emergency Alert system and the kind of work you're doing with it?

Carol: Well, let me talk a little bit about how we factored in the right information to describe trust, because there are lots of things that could influence trust. But, the question is, in this particular case, what does?

We started with public alerting experts--people that have been working in this field for a long time--and interviewed them in terms of characteristics of what works and what doesn't work. Remember, we are building on the legacy system, so there's a lot of data to mine from that side. Then, we also did surveys of the typical alerting population so we could get their feedback. These are the cellphone users and the cell-message distributors. So, those people would have an understanding of how they would react. We also talked with the vendors, as well, to get a sense of how they're supporting the system and the kind of qualities that they are attempting to build into their software. All of these provided a big range of factors, but they are plus factors and negative factors. How do you figure out which ones are influencing?

Suzanne: Right, because, for example, you don't want to scare the public and create a panic reaction with a certain type of message. Certain events you need to communicate about carefully. I'm also assuming that someone that is a digital native, who grew up with computers and cell phones and smart phones, is going to react differently to some kinds of messages than digital immigrants that, maybe, some of us are more reflecting, that didn't have a computer available to us until we were almost adults.

Carol: Well, we're also a multi-lingual environment. So, the factor of the content that appears on the phone will also be a motivator in terms of whether you trust the information or not.

Suzanne: So, how do you describe this? How do you help the alert originators and the message providers understand where they might be contributing to not getting their message across as well as ways that they can actually get their message across in productive ways?

Carol: We built a series of scenarios, and from those scenarios did a lot of surveys of data. That gave us reactions to different scenarios that we then assembled in a model. It is a Bayesian Belief Network Model that allows us to simulate a whole lot of factors in terms of determining their importance.

Suzanne: Right, and that [the Bayesian Belief Network Model] is a statistical method that is used frequently for setting up the boundaries of reasonableness for different kinds of factor analysis.

Robert: We had something like 60 or 80 factors. You have say, *Only a few of these you can deal with, which ones were important?* or, *Which ones shouldn't you do*? So, it was a combination of what was really good and *no don't do this*, so we had to identify out of that whole collection a few they could pay attention to.

Carol: Well, many of them were conflicting factors, too. You're not going to be able to maximize everything. So, you are playing trade-offs between these. The question is: *What are the important trade-offs*?

Suzanne: That's really the key to some of why this research is important, because if people don't understand where there are inherent conflicts between different factors that they might want to maximize, they may go off in a direction that is counter-productive.

Robert: You could rush an alert, but then you would have misspellings and misplaced words. That will [have an effect of message recipients deciding], *I'm not sure I'm going to pay attention to this. I'm not sure it's from a good source.*

Suzanne: If you can't even spell the words right, how do I know...

Robert: Or, if I can't really tell you what to do that could also affect it. Both sides have to understand what the relationships are.

Suzanne: OK. So, where are you in the progress of this work, and what comes next?

Carol: What we've done at this point is assemble a range of recommendations: recommendations for the alert originator as well as recommendations to them about the recipients so that they can factor these into their choices of systems and [decide] how they proceed to set up the capability. I think it would be useful for us to give you a quick rundown of those recommendations, because they start to give you a sense of the kind of factors that are involved.

If you look at it from an alert-originator's perspective, they are going to be focusing only on the very-high-urgency, severe events, because this is something that's going to be massively distributed and quickly available. So, it has got to be something that is sufficiently important for that distribution mechanism. It is also recommended that they seriously look at matching the footprint of the distribution as closely to the alert problem as possible.

That is one of the challenges to the way the system is currently set up: it is based on county boundaries. On county distributions in the east coast, that might be fine; but on the west coast, you're talking about massive geographic distribution that may be way far away from the alert. If people get enough noise, so to speak, of unexpected alerts or *useless* alerts (I think is a better word to say), they're going to start to ignore them, and that's a concern.

Suzanne: Basically, what we call "alert fatigue," which you have to deal with in lots of situations where you have a lot of data coming in.

Carol: Right. We don't want to compete with the email spam by any means. They also have to be very comfortable that it is an authorized alert. They have to be comfortable that the security is

working. They have to be comfortable, from an alert originator-perspective, that the system itself is accessible, that they can get it out quickly and efficiently, that the system is going to perform well. All of these are your typical software system results.

Suzanne: Often, things that have to be accounted for in degraded-environment kinds of emergencies.

Robert: These folks are not necessarily in their office during an emergency, so they have to be able to do this from other locations, from mobile devices, and yet it has to be done securely.

Carol: There are some real challenges.

Robert: These are things that these alert originators, smaller ones, hadn't really thought of. So, these are some new things to consider.

Carol: They are also challenged with integrating this capability with their existing structure, which is quite archaic and, in many cases, relies on telephone service. So, they have got some real challenges with integrating wireless in that environment.

Robert: It is particularly a problem with the smaller organizations who did not have the funding to do major upgrades.

Suzanne: That's right.

Robert: So, we had to offer advice for how they could they approach that.

Suzanne: *How can you do the business case for this and get your constituents to help to fund this?* Yes.

Carol: The speed at which they can generate the message is important. They are going to be under time pressure, and they are going to be under a lot of concern to get the information correct. And, they are confined to 90 characters. So, how do you pack as much information as possible in there as quickly as possible.

They also need to ensure that the alert will be issued appropriately, that the accuracy is going to carry through from what they enter to what the person actually receives on the cell phone. So, that's reliance on the system itself.

One other thing that generates trust is some sort of feedback mechanism because they are sending information out, but they don't really see the actual recipient process.

Suzanne: If they have a neighborhood that needs to evacuate in a fire, they need to know that people have received that [alert] and are acting on it.

Carol: Right.

Suzanne: That is a piece that I haven't really seen in the alerts that I've received, is any kind of way to do that kind of feedback. That is an interesting point.

Robert: It is also feedback after the fact: *What could we have done better?* On that message, the person who receives it needs to be able to understand it and say, *I accept that this is important* and then be able to act. It is a combination that those things have to come together for it to be a successful alert.

Suzanne: Exactly.

Carol: Did you want to go over the ones for the recipient because I think those are equally as important?

Robert: For the recipient, we were again looking at this model that said, *If you're looking at an alert, you want to be able to answer the phone*. That is, if they see who it is from, and they immediately ignore it, that is not going to be a success. They have to understand that message. They have to accept that it was from an authorized source and then have enough information to act. As we looked through there, the things that we actually came up with was a combination of things to do and not to do.

Certainly *to do* was clarity of the message, spelling. We ignore messages from our bank that are misspelled, is certainly part of the problem. Ask me, *Why do I want to do this? Why is it important?* Clearly define what are they supposed to do. The issue that came up in terms of languages, it was important that the alert be in the primary language of the recipient.

Then there are things not to do: As we said earlier, too many alerts that are not applicable, they will be ignored. If there is confusion or insufficient information, that is also going to be a significant problem. If you have an alert that simply comes in 10 minutes late or worse--yes, you will lose confidence in that alert very quickly.

Suzanne: *Evacuate now. Yes, I can see that. My house is burning down*.

Robert: Certainly, a security compromise with bogus alerts is going to be a significant problem. One that is harder to control is that these areas will have a city, they may have a county, multiple [agencies] could issue alerts.

Suzanne: I was thinking about that.

Robert: If they all start doing it and no coordination, it could be very confusing.

Suzanne: There are situations like fire, [which is] is a situation that I know a little bit about. There are many, many stakeholders that have different parts of the information landscape in a

fire situation. So, making sure that you do not overload people with that conflicting information from different places.

Robert: Since these are only 90-character messages, you also typically want to say: *More information?* Give them a pointer, some other place they can go. Because, you can't include everything, [alerts need] just enough to get their attention.

Carol: What I think you are sensing, too, here in these recommendations is that not all of them are things that can be implemented easily. Some of them are going to require governance changes with this coordination effort. Some of them are going to require improved technology and follow-up with the feedback because they have never looked at feedback for the public emergency alerts. Televisions don't mine feedback on that. All of these—as we are personalizing things more and more—we have to build a way to know that the message is getting through to the right people.

Suzanne: Sure.

Carol: So, all of these become additional requirements that get layered on in terms of the capability that aren't usually thought of originally when people are saying, *Oh, that would be a great idea.*

Suzanne: Well, people that have in their minds the precedence of the emergency alert system—the noise that comes on the radio and that as your frame of reference—they don't think about that level of personalization and the possibilities. So, when you are building the systems, you may not even include the possibility in your architecture that you can actually accommodate some of those things.

Robert: I think in these organizations, with this, there is a high risk that you don't do it right in terms of damage or loss of life. So, that is increased stress that they probably haven't...They are getting immediate actions for something that normally it will be a half hour later. Now you are looking at things five minutes from now.

Suzanne: Well, and what that also tends to generate is some risk aversion. If I'm at risk financially or somebody is going to complain to the government, sue the provider, or whatever, then actually getting people to put this out there is an issue in and of itself.

Robert: For an organization it turns out even that decision, who makes the decision within an agency or local alert, who makes [the decision] that [alert] can go. In one case it had to go to a county executive who had to be able to reach them in order to get approval to send it out.

Suzanne: So, there are both social factors here and technical factors. It's not just one or the other. So what are you doing now, what comes next?

Carol: Well, at this point we are supporting the group [DHS and alert originators] in terms of thinking about the security more in depth. That, of course, is one of the major issues to make sure that [trust is built into the capability].

Suzanne: That's one of the expertise areas of your group and CERT in general.

Carol: So that we can help them understand *What are the kind of risks that they may be facing?* and *How can they then evaluate their particular situation and systems and vendor choices and integration choices?* to make sure that they are maximizing security appropriately.

Suzanne: Okay, well as someone who hates getting things on my cell phone that I'm not sure I trust, I applaud that focus on security. I'm sure many other people appreciate the fact that your team is working on this.

Well, I want to thank both of you very much for joining us today. Robert, I've known you for a long time, and I love to see the different things that you get involved in. Carol you've just been a breath of fresh air ever since you got here at the SEI in terms of collaboration across boundaries, so I'm thrilled you guys are doing this.

Thank you so much for joining us today. If our listeners would like to download their technical report on this topic, or any recent SEI technical reports, go to resources.sei.cmu.edu/library. In the bottom left-hand corner, under SEI links, click on the Author A-to-Z index and find either Carol Woody or Robert Ellison.

For visual diagrams for key concepts associated with the recommendations that Carol and Robert have put together, please see the transcript that goes along with this audio podcast.

This podcast is available on the SEI website at sei.cmu.edu/podcasts and on Carnegie Mellon University iTunes U site. As always, if you have any question please do not hesitate to email us at info@sei.cmu.edu. Thank you.