Security and Wireless Emergency Alerts

featuring Carol Woody and Christopher Alberts interviewed by Suzanne Miller

---

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 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 Christopher Alberts. Today, we are going to talk with them about Security and the Wireless Emergency Alerts Service, but first a little bit about our guests.

Carol has been a senior member of the CERT technical staff since 2001. Currently she is manager of the Cyber Security Engineering team whose research focuses on 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 had the pleasure of working with Carol on several things, not on all of these areas, but in some of them.

Christopher, Chris, is a principal engineer in the CERT Program where he leads applied research and development projects in software assurance and cyber security. He has also co-authored two books, "Managing Information Security Risks: The OCTAVE Approach" and "The Continuous Risk Management Guide Book." I have also had the pleasure of working with Chris on OCTAVE a little ways back. So, welcome both of you. I'm really happy to talk to you about this topic today.

Christopher Alberts: Thanks, great to be here.

Carol Woody: Thanks for having us.

Suzanne: Okay, so we covered some things about the Wireless Emergency Alerts Service in a previous podcast. Chris, you weren't with us on that one. So, let's start by having you remind our listeners about the Wireless Emergency Alerts Service and how it works.

Carol: Wireless emergency alerting is a capability that has just been publicly made available in the United States. It is provided so that emergency alerters—which would be your firefighters, your weather, the AMBER alerts that are following the missing children—those are all setup in a way that they can send messages to the wireless phones.

Suzanne: I've received some of those I think all of us have received various of those over the last six months.

Carol: It's actually integrated into the capability that also feeds messages to the Public Broadcasting System, so it's in essence enhancing the capabilities that they have got to do that. But, what it is doing is bringing a larger group of people into this process and also connecting not just to the televisions and radio, but now to wireless carriers and then on down to individuals that receive things on their cell phones.

Suzanne: So, it's really about integrating a lot of different sources of information and a lot of different pathways of getting information out to the public and integrating all that together in the wireless environment, so that we can all get information that we need that is relevant, current…

Carol: And quickly.

Suzanne: And quickly but also trying to keep the noise down. So, it is that balance of getting the right information to the right stakeholders while keeping the noise down, so that you don't get alert fatigue or you know so that you don't stop listening to what's going on.

Carol: Well, it's setup to really be used for imminent crisis. So, you'll be getting the tornado alerts when the tornado is right in your area. It is focused on specific areas, so the alerts can come out by county. It is not limited. You don't sign up for this. If you and your cell phone are in the area where the alert is going out then it will come to you.

Suzanne: It is really the providers that sign up and commit to being part of the network.

Carol: Right. Exactly.

Suzanne: OK, all right. I think that gives people and idea of what we're talking about. So, I can imagine that security is kind of important for this kind of a system. You don't want people to be hacking in and sending out spurious alerts. You don't want denial service kinds of things happening where you can't get the messages out all those sorts of things.

Carol: It's critical to get them out timely.

Suzanne: Yes, and you don't want responsiveness to be degraded. So, security kind of gets into all that and you've got some methods for now analyzing the security in this alert system. From

what I understand this starts with an aspect of research that you're working on that's called Mission Thread Analysis. Is that correct?

Carol: Exactly. What we're starting with is portraying how all the connections need to work together.

Suzanne: So, kind of a desired statement.

Carol: If it functions as intended what is supposed to happen? The alert will start from the alert originator submitting it into the central system as I said it was riding on the Public Broadcasting System. So, there is an existing system there that FEMA supports. From there it goes into the alert carriers and then down to the cell phone. If you think about it, it is quite a range of technology that we expect all work together.

Suzanne: You mentioned FEMA, that's the Federal Emergency Management Agency.

Carol: Right.

Suzanne: Who are some of the critical players in sort of getting the security issues, the Mission Threads analyzed for this?

Christopher: So, when you take a look at the wireless emergency alert pipeline or what we refer to as the WEA pipeline, the starting point is with the first responders. These might be law enforcement or people who are first on the scene if it is an accident-type situation, the National Weather Service if it's a weather alert. Then, that goes to the alert originators who enter the alert into the system. Then, the alerts go into the systems owned by the Federal Emergency Management Agency. Then, after they process it, they send it to the carriers, which are AT&T, Verizon, and the others who are the interfaces to the recipients' cell phones. Then, the messages go to cell phones. That's kind of how the pipeline works.

Suzanne: So, all along that threat of stakeholders, there are potential vulnerabilities in their individual security systems and there are also potential vulnerabilities in their individual security systems and there are vulnerabilities in how they interact with each other.

Christopher: Sure in what you're, what we just talked about is the groups that are part of the pipeline and then there's technologies supporting those groups. As part of our analysis, the second step then is start saying which technologies support each part of the pipeline? [We then] identify those technologies, then how they're interconnected: where the data flows. Then, you are starting to get into how does the technology actually work. Then, we can start getting into the security risk analysis.

Suzanne: So, the mission thread gives you a way of communicating about all these different aspects.

Chris: Yes, it is the anchor or the foundation.

Carol: Each alert originator has their own way of doing alert submissions.

Suzanne: I am so surprised by that.

Carol: I know. There are thousands of them. So, what we've been focused on is how do we provide them with guidance that will allow them to work with their providers to understand their security issues. Security is certainly not the top thing that a firefighter is worried about when they are out there fighting the fire. But, they need to have enough concern about it to make sure that all of the pieces are set up right so that the messages they are trying to get through quickly do get to the right people.

Suzanne: You've given me kind of an abstract scenario moving from one stage to another. When I think about that in a more concrete way—so, let's say a tornado alert—what are some of the vulnerabilities that you've discovered so far that you can talk about that might come in to the thread of going from the National Weather Service out to people in the public like myself?

Carol: I think the first one that immediately comes to mind is that someone can create a fake alert but make it look legitimate. There are real challenges with that in terms of the mechanisms that are controlling authenticity. So, those are pieces that we've been working with alert originators to help them understand and figure out how to control.

Suzanne: Any that come to mind for you Chris?

Chris: Well, I think that a lot of the standard types of attacks that you read about in the newspaper everyday apply here as well. It can be as simple as people not resetting default passwords in their systems and someone exploiting that [or] people breaking into the network in general or coming into a third party and inserting malicious code that eats up bandwidth and creates a denial of service. There are lots of different ways that things can be exploited. In terms of this particular project, because this is public information, confidentiality is not as important as the other security attributes of integrity and availability. What we are really looking at, as Carol was saying, the spoofing alerts, getting false messages into the system was something of concern and anything that would affect the timeliness of getting an alert to the recipients is another thing that we would look at.

Suzanne: OK. All right. I think that gives our listeners an idea of some of the work that you're doing. Where are you in the work and what comes next in your research in this area?

Carol: Well, we have completed the guidance in terms of support for alert originators. That material has actually been published by the Department of Homeland Security.

Suzanne: We'll provide the link for our listeners for that document.

Carol: In terms of what comes next, we are discussing how we can go about basically bringing the same level of guidance to other groups that are a part of the pipeline.

Suzanne: Oh, OK. All right.

Carol: And, at a minimum, at least provide some expanded training for those groups.

Suzanne: It sounds like awareness of this as an issue is one of the big barriers that you're dealing with. As you say, firefighters don't think of security as the first thing when they get to a site, but if they don't have some awareness of security as an issue then they may contribute unintentionally to a vulnerability.

Chris: The other thing that we're doing is we are now enhancing our whole risk analysis approach with a research project currently that we've started this past year where, in addition to doing mission threads, we are doing other types of modeling techniques to get a more systematic and more thorough characterization of the operational environment. Then, we are doing our security risk analysis in relation to those models that we are developing.

Suzanne: We'll have to talk to you about that some other time Chris.

Christopher: That sounds great.

Suzanne: All right. Well, I do want to thank both of you for joining us today. I would like our listeners to know that if they'd like to download the technical report on this topic or any recent SEI technical reports please go to resources.sei.cmu.edu/library. In the bottom left-hand corner, under SEI links, click on the Author A-Z index and find either Carol Woody or Christopher Alberts. This is the second post in our series on Security and Wireless Emergency Alerts.

The first podcast in this series, "Best Practices for Trust in the Wireless Emergency Alerts Service" and all of our podcasts can be found on the SEI website at sei.cmu.edu/podcasts and on Carnegie Mellon University's iTunesU site. As always, if you have any questions, please don't hesitate to email us at info@sei.cmu.edu. Thank you for listening.