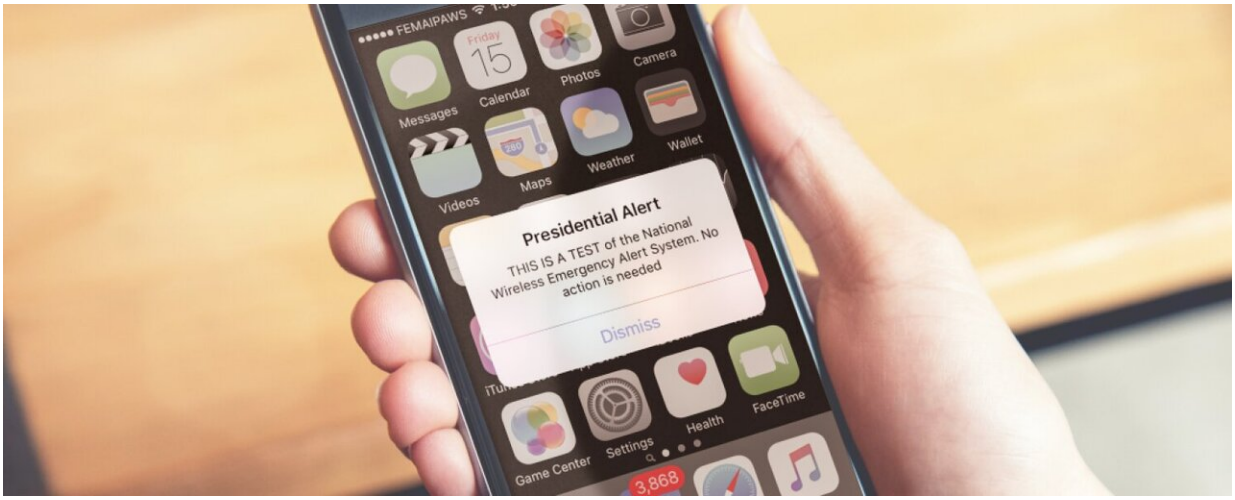
National emergency alerts potentially vulnerable to attack

June 21 2019, by Daniel Strain



Credit: FEMA

On October 3, 2018, cell phones across the United States received a text message labeled "Presidential Alert." The message read: "THIS IS A TEST of the National Wireless Emergency Alert System. No action is needed."

It was the first trial run for a new national alert system, developed by several U.S. government agencies as a way to warn as many people across the United States as possible if a disaster was imminent.

Now, a new study by researchers at the University of Colorado Boulder raises a red flag around these alerts—namely, that such emergency alerts authorized by the President of the United States can, theoretically, be spoofed.

The team, including faculty from CU Engineering's Department of Computer Science (CS), Department of Electrical, Computer and Energy Engineering (ECEE) and the Technology, Cybersecurity and Policy (TCP) program discovered a back door through which hackers might mimic those alerts, blasting fake messages to people in a confined area, such as a sports arena or a dense city block.

The researchers, who have already reported their results to U.S. government officials, say that the goal of their study is to work with relevant authorities to prevent such an attack in the future.

"We think this is something the public should be aware of to encourage cell carriers and standards bodies to correct this problem," said Eric Wustrow, a co-author of the study and an assistant professor in ECEE. "In the meantime, people should probably still trust the emergency alerts they see on their phones."

The researchers reported their results at the 2019 International Conference on Mobile Systems, Applications and Services (MobiSys) in Seoul, South Korea, where their study won the award for "best paper."

Wustrow said that he and colleagues Sangtae Ha and Dirk Grunwald decided to pursue the project, in part, because of a real-life event.

In January 2018, months before the first presidential alert test went out, millions of Hawaiians received a similar, but seemingly genuine, message on their phones: someone had launched a ballistic missile attack on the state.

It was, of course, a mistake, but that event made the CU Boulder team wonder: How secure are such emergency alerts?

The answer, at least for presidentially-authorized alerts, hinges on where you look.

"Sending the emergency alert from the government to the cell towers is reasonably secure," said co-author Sangtae Ha, an assistant professor in the Department of Computer Science. "But there are huge vulnerabilities between the cell tower and the users."

Ha explained that because the government wants presidential alerts to reach as many cell phones as possible, it takes a broad approach to broadcasting these alerts—sending messages through a distinct channel to every device in range of a cell tower.

He and his colleagues discovered that hackers could exploit that loophole by creating their own, black market cell towers. First, the team, working in a secured lab, developed software that could mimic the format of a presidential alert.

"We only need to broadcast that message into the right channel, and the smartphone will pick it up and display it," Ha said.

And, he said, the team found that such messages could be sent out using commercially-available wireless transmitters with a high success rate—or roughly hitting 90 percent of phones in an area the size of CU Boulder's Folsom Field, potentially sending malicious warnings to tens of thousands of people.

It's a potentially major threat to public safety, said Grunwald, a professor in computer science.

"We think it is concerning, which is why we went through a responsible disclosure process with different government agencies and carriers," he said.

The team has already come up with a few ways to thwart such an attack and are working with partners in industry and government to determine which mechanisms are most effective.

More information: Gyuhong Lee et al, This is Your President Speaking, *Proceedings of the 17th Annual International Conference on Mobile Systems, Applications, and Services - MobiSys '19* (2019). DOI: 10.1145/3307334.3326082

systems.cs.colorado.edu/headlines/cmas.html

Provided by University of Colorado at Boulder