Do Emergency Text Messaging Systems Put Students in More Danger?

The rush to use text messaging as an emergency notification system fails to consider the weaknesses and potential hazards of this solution

By **John Bambenek** and **Agnieszka Klus**

Cell phones have become prevalent on college campuses. Most students use them as their primary phone to avoid changing phone service every year or dealing with university–based long-distance charges. In the wake of recent college shootings and threats of violence on campus, administrators have begun to deploy cell phone solutions to send emergency messages to students. Many believe that emergency text messaging systems will minimize the damage (specifically loss of life or injuries) in an emergency situation, including natural disasters.

Despite the speed with which such systems are being deployed (some even mandated by law), little attention has been given to the efficacy and implications of such technologies. Crisis communication services must demonstrate several characteristics to meet the requirements for emergency operation:

- Extremely high reliability
- Excellent access control
- High-speed delivery

Does text messaging meet these requirements? No.

Short Message Service Text Messaging

Among different messaging options, short message service (SMS) has become very popular. A key design feature is its relative simplicity. The downside? The SMS protocol is not only insecure but can't be made secure. The protocol handles only the bare necessities of getting messages of no more than 160 characters from one device to another. Among the features SMS generally does *not* include are error checking, guaranteed delivery, and speed of delivery. In normal situations, this does not matter.

While e-mail and Internet services have defenses such as virus scanners to provide security against attacks, the SMS messaging protocol does not. Additionally, cell phones cannot perform the complex tasks of security and authentication. As a result, false messages to cell phones are extremely difficult to prevent, and more people are seeing spam SMS messages on their cell phones, especially as more services support the technology.

SMS messages do not require the sender to use a cell phone. Most cell phone providers offer an SMS gateway, however, so each phone has an e-mail address. For instance, a Verizon Wireless customer with a cell phone number of 312-555-1212 would have a phone e-mail address of 3125551212@vtext.com. Cellular providers also provide web interfaces so that individuals can send SMS messages using a web-based form. Both these tools allow people anywhere in the world to send an SMS message to any cell phone user without authenticating the sender.

An additional vulnerability with SMS messaging was recently discovered. Researchers from Pennsylvania State University demonstrated the possibility of overwhelming a cellular network by sending a flood of SMS messages to users in the same geographical area. A successful attack would effectively shut down not only the ability to send SMS messages but also the ability to make normal cell phone calls (denial of voice service, or DoVS).[1]

Clearly, SMS messaging lacks reliability, access control, and speed of delivery (when the number of messages is high). SMS messaging simply does not meet the requirements of crisis communications systems because it was never designed for high-stakes communication.

Emergency Text Messaging Services

The main driver for formal adoption of text messaging technology is its use in crisis situations. Even the label "emergency text messaging systems" presupposes and reinforces the idea that these systems primarily target emergencies. For instance, stated uses of the service at the University of Illinois at Urbana-Champaign include pandemics, floods, school closings, and active threats. The university answers the question "What is an active threat?" as follows:

> An "active threat" is defined as any incident which by its deliberate nature creates an immediate threat or presents an imminent danger to the campus community. In addition to offenders armed with firearms (active shooters), obviously, it is possible for other types of weapons or instruments to be used by offenders who want to cause harm.[2]

Emergency text messaging services were being considered before the Virginia Tech shooting, but the move to adopt such systems took on much greater urgency after that event under the assumption that they could have reduced the loss of life. The accelerated adoption of text messaging technology for emergency communications unfortunately has limited consideration of its usefulness and weaknesses.

The service itself is straightforward. In most cases, students and staff register to participate in the system by giving the university their cell phone numbers. The emergency text messaging application converts the numbers to e-mail addresses and then applies standard bulk e-mailing techniques to send out a large body of SMS messages as quickly as possible.

To initiate an emergency message, a dispatcher or other authorized person enters a message within the 160-character limit and sends it off. The time it takes for messages to be received depends largely on the number of users in the list. Anecdotally, technologists who have tested the system for colleges and universities report a 15–60 minute range for receipt of messages. This delay is on top of the time it takes for a 911 call to be initiated, for a dispatcher to gather information, and for the appropriate decision maker to authorize sending the message.

Note that the DoVS vulnerability mentioned above would come into play here. A successful DoVS attack concentrates on victims who communicate through the same cellular tower. In this case, an emergency text message would be sent to users in a tightly defined geographic area (on and around the campus) and would likely be associated with the same few cellular towers. As a result, an emergency text message could interfere with normal voice communications. This is especially true during an "active threat" scenario when people are trying to ascertain if their loved ones are safe. Emergency text messages are thus a one-shot technology: Once a message has been sent, the cellular networks in the area become saturated, meaning it will be some time before a follow-on message could be sent.

In analyzing the efficacy of these systems, it is necessary to put oneself "in the moment" of an active threat. Hindsight is 20/20, and administrators do not have it when making emergency decisions. Using recent school shootings and threats as examples, we can analyze emergency text messaging in light of a school shooting or active threat.

Northern Illinois University Shooting

Shortly after 3 p.m. on February 14, 2008, Steven Kazmierczak emerged from behind a curtain in a Northern Illinois University lecture hall and fired over 30 rounds. Five people were killed and 18 wounded. The campus was ordered into lockdown very quickly, and emergency messages were posted on the main website about 20 minutes after the initial report of the shooting. The shooter did not roam through Cole Hall or the campus; he fired into the lecture hall and then killed himself.[3]

It took about 70 minutes for police to ascertain that the shooter was dead and the area was clear. It is important to ensure that a situation is secure before announcing it, but in a crisis, civilians tend not to communicate clearly, and even trained professionals can suffer from garbled communication. In this situation, those in danger knew what was happening before the police did. Because the shooter made no attempt to find more victims and the shooting was over rather quickly, messaging those outside the classroom would not have affected the outcome. Further, the information gaps combined with the time needed to send text message alerts made them infeasible.

Virginia Tech Shooting

The Virginia Tech shooting was the catalytic event for emergency text messaging systems. In this case, the timline[4] of events on April 16, 2007, is important:

7:15 a.m.—Report of shooting in West Ambler Johnston Hall with two victims killed (male and female)

9:26 a.m.—University sends out e-mail notifying the campus of the shooting and urging caution

9:45 a.m.—Shooting at Norris Hall begins

11:53 a.m.—After several prior e-mails, another e-mail is sent saying the shooter "is in custody"

Roughly two and a half hours separated the first and second shootings. In theory, the university had time to send out an emergency text message and close down the campus. The question is whether that would have been prudent.

The belief among the authorities who responded to the 7:15 a.m. shooting was that they were dealing with an isolated incident, probably a domestic dispute. At the time, no descriptions of the shooter were available, although they had identified a "person of interest." They identified the female victim's boyfriend as the potential shooter and detained him around 9:24 a.m. that day. The reports after the fact concluded that this line of investigation was reasonable, albeit ultimately wrong.

At 9:45 a.m., reports of shootings were coming in to 911, and police responded to the event in Norris Hall. After initial difficultly gaining entrance to the building, they found the gunman had shot himself after killing 31 people. Later investigation found no connection between shooter Cho Seung-Hui and the individuals in West Ambler Johnston Hall or any indication that Cho had planned an attack on Norris Hall specifically.

The Virginia Tech Review Panel specifically cited the police as having erred in not considering other scenarios than a domestic dispute for the first shooting. This charge was repeated in the media and campus community. The problem with this line of thinking is that it assumes a finite number of possibilities. In reality, the Virginia Tech incident was unique in the sparse history of college campus shootings. At that moment, the police had no historical frame of reference to make the leap between a seemingly isolated shooting to a mass casualty incident.[5]

This analysis of incident response has important implications for emergency text messaging systems. Administrators in future will err on the side of extreme caution because "another Virginia Tech" may happen, and this mentality is also present among the staff and students of other universities. They insist on being notified of any violent incident or threat of a violent incident so that they can protect themselves. This all but ensures over-utilization of emergency communication systems in general. More importantly, it creates a cultural mindset that will respond immediately and unquestioningly to emergency text messages (or other emergency communication) as if another Virginia Tech–like incident were imminent. Fear-based responses make people more likely to trust authentic looking communication without analysis, a potential hazard discussed below.

The review panel also found miscommunications during the response to the shooting that could have complicated an effective response. The first problem was that when the initial call to 911 came in, the dispatcher had a difficult time understanding exactly where the shooting was taking place.[6] It takes time to communicate a report to police so that they have enough information to respond.

The shooting in Norris Hall lasted approximately 11 minutes. Given the time it took to communicate to dispatchers the location of the shooting, an emergency text message would have started being received minutes after the shooting ended. This delay further encourages administrators to warn the campus community and lock down the campus at the first indication of trouble—and the campus communities demand as much.

St. Xavier University Closing

The presumed purpose of a text messaging system is to alert individuals to an active threat. The institution thus obligates itself to send SMS alerts over any significant act of violence, regardless of circumstances. In many cases, this would result in a lockdown of the campus.

With such a low threshold for sending out alerts, the probability that people will recklessly abuse the system and cause a lockdown rises. In the cases of Oakland University[7] and St. Xavier University,[8] threatening graffiti in campus buildings forced the schools to shut down completely. In the case of St. Xavier, four schools surrounding the university were closed as well.

St. Xavier remained closed for eight days while the threat was investigated. Because only graffiti was involved, the forensic evidence available was minimal. With such a low threshold to shut down not only a college but also surrounding institutions, it is entirely plausible that a student who wants to shut down a campus might turn to graffiti or other pranks.

While this scenario does not directly bear on emergency text messages, it does illustrate a sociological consequence of adopting such systems; namely, administrators must respond as if they were facing the absolute worst-case scenario. The cultural reaction to alerting systems all but forces their overuse by administrators and unquestioning compliance with emergency instructions by recipients.

Leading Victims to the Threat

While the possibility of using false text messages is not inconsequential, there is a more significant risk: A hostile entity could use a forged emergency text message to lead victims to the threat instead of away from it. This scenario is not hard to imagine—it has happened before.

In 1998, the Real IRA (an Irish Republican Army splinter group) phoned in a bomb threat indicating a courthouse in Omagh, Northern Ireland, was the target. There is some debate whether the confusion was intended or accidental. Unfortunately, the lack of prosecution of those responsible means we may never know.

The car bomb was not at the courthouse, however, but in the city center. As part of the standard bomb threat response procedures in Northern Ireland, the area around the courthouse was secured and bystanders were moved to the city center—a safe distance. The city center and the associated businesses stayed open while police investigated the threat. The bomb in the city center exploded, killing dozens of people. The destruction and loss of life was more severe because of the confusion over the actual target.

With the deployment of emergency text messaging systems using an insecure protocol, it becomes possible for a malicious individual to use such technology to achieve the same result. Any notification system could be misused this way, but emergency text messaging systems are particularly vulnerable and easier to exploit.

False Text Messaging

Every moment, thousands of spam e-mail messages clog inboxes and mail servers. Most of these messages are forged to varying extents. More malicious e-mails, such as phishing attacks, purposely try to appear as if they come from legitimate sources. The more legitimate looking the e-mail, the more likely a phishing attack will succeed.

Because emergency text messaging systems often rely on e-mail to deliver messages, a malicious individual halfway around the world could send a fake emergency text message without difficulty. The method for sending forged e-mail is well known and trivial—every e-mail client can be set to send e-mail that appears to come from someone else. While any communication system can be compromised, e-mail is inherently insecure and easy to forge.

Figure 1

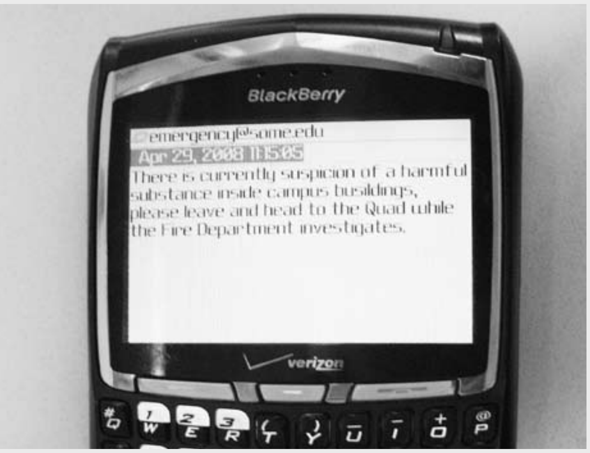
Example of Forged Emergency Text Message

```
user@mailhost% telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 mailhost.com ESMTP Sendmail; Fri, 11 Apr 2008 14:41:47
  -0500 (CDT)
helo localhost
250 mailhost.com Hello localhost [127.0.0.1], pleased to meet
  you
mail from: emergency@some.edu
250 2.1.0 emergency@some.edu... Sender ok
rcpt to: XXXXXXXXXX@vtext.com
250 2.1.5 XXXXXXXXXX@vtext.com... Recipient ok
data
354 Enter mail, end with "." on a line by itself
From: emergency@some.edu

  There is currently suspicion of a harmful substance inside
campus buildings, please leave and head to the Quad while
the Fire Department investigates.
  .
  250 2.0.0 m3BJflfi018046 Message accepted for delivery
```

Figure 2

Phone Display of Forged Text Message



emergency@some.edu
Apr 29, 2008 11:15:05
There is currently suspicion of a harmful substance inside campus buildings, please leave and head to the Quad while the Fire Department investigates.

The example in Figure 1 shows it only takes a few keystrokes and no real technological effort to send a fake emergency text message. The recipient of the message will see a message similar to Figure 2, which proves how hard it is to distinguish a real alert from a falsified one.

With e-mail, an experienced system administrator has a variety of tools and information to discern real messages from forged ones. No such information is available with text messages to make a determination, even for experienced technologists. Unfortunately, the source e-mail address is often published on campus websites discussing the university's emergency text messaging system. The purpose, of course, is to help people recognize emergency messages. The consequence is that an attacker has almost all the information needed to send a false text message. All that's missing is target phone numbers.

Unfortunately, many campuses publish student phone numbers on the web. Additionally, many people put their phone numbers on social networking pages such as Facebook or MySpace. Spidering these websites takes some effort, but tools already exist that can accomplish the task in an automated fashion. Or, an attacker could use the area code and the first three numbers of the exchange of cellular providers in a given area. For a ten-digit phone number, the first three numbers are the area code (publicly known), the next three are the "exchange" (unique by carrier and geographical area, usually city), and the last four are unique to create an individual number. An attacker could simply send text messages to every number in a relevant area code and exchange. All that's necessary is to get one or two students in every classroom and you've got a campus population following the same instructions.

The danger is that people will immediately and unquestioningly obey the instructions provided in a forged emergency text message. Calls to 911 will start coming in, with nervous individuals looking for clarification or administrators wanting to know what is going on. Discovering that an unauthorized text message went out takes little time; sending a follow-up corrective text message would still have a 15–60 minute delay at best.

The lack of authentication seriously undermines the system. A malicious individual who wanted to cause a mass panic from halfway around the globe could fairly easily send false text messages to a good portion of a campus and accomplish that goal. Even worse, an attacker (or group of attackers) could plan an Omagh-style attack to lead students and staff out of buildings and direct them toward a threat. In the case of explosions, walls and the building structure absorb some energy from a blast. In the open, people have no protection, and it is easier to pack more people in a smaller space.

Other methods of attack could exploit the ability to lead victims to a target area. Falsifying an emergency message is possible in any type of emergency communication. Text messaging systems, however, make it absolutely trivial to send a false message with no physical connection and little forensic evidence to track afterwards. If an attack is timed carefully, it will cause a far greater casualty count than would be possible otherwise. Administrators would simply have no time to countermand a false message to prevent it.

Conclusion

The question remains, can text messaging systems protect a campus population? Or do they put people at more risk? Any emergency communication system must be reliable, with controlled access and fast delivery. Not only does text messaging fall short in all three areas, recent campus shooting incidents demonstrate that these systems would not have helped during the emergencies, only supporting supplemental crowd control afterwards.

Any form of communication has benefits and costs. Despite the apparent advantages of text messaging as an emergency service, opportunities abound for overuse, and the possible hazards are exacerbated by the common willingness of people to comply promptly with emergency messages. In addition, the potential for abuse is high, especially since trivial incidents can lock down an institution. The use of such systems would all but paralyze normal voice communications, increasing anxiety—and perhaps danger—in a heightened threat environment. Finally, because of the triviality of sending a fake text message, the sender could not only shut down a campus but actually lead students and staff toward a threat instead of away from one.

Emergency text messaging can be useful in announcing school closings or facilitating crowd control. Given the sociological context in which these systems are implemented and the perceptions surrounding them, however, it is possible to manipulate a campus population for malicious purposes from anywhere in the world. We can only conclude that the use of text messaging tools is woefully insufficient and dangerous for use in emergencies.

Endnotes

[1] William Enck, Patrick Traynor, Patrick McDaniel, and Thomas La Porta, "Exploiting Open Functionality in SMS-Capable Cellular Networks," presented at the 12th ACM Conference on Computer and Communications Security 2005, Alexandria, Virginia, November 8–10, 2005, http://www.smsanalysis.org/smsanalysis.pdf.

[2] "Active Threat Information," Division of Public Safety, University of Illinois at Urbana-Champaign, http://www.dps.uiuc.edu/activethreat.htm.

[3] See the news story "6 Shot Dead, Including Gunman, at Northern Illinois University," CNN, February 14, 2008, http://edition.cnn.com/2008/US/02/14/university.shooting.

[4] See the news story "Virginia Tech Shootings Timeline," CNN, April 17, 2007, http://edition.cnn.com/2007/US/04/17/timeline.text/index.html.

[5] Virginia Tech Review Panel, "Report of the Review Panel," August 2007, http://www.governor.virginia.gov/TempContent/techpanelreport.cfm.

[6] Ibid.

[7] Jesse Dunsmore, "Multiple Threats Close Campus," *The Oakland Post*, April 16, 2008, http://www.oaklandpostonline.com/read_article.php?id=297.

[8] CBS News, "4 Local Schools Close Due to Threats at St. Xavier," CBS 2 Chicago, April 14, 2008, http://cbs2chicago.com/local/saint.xavier.threats.2.699041.html.

John Bambenek (bambenek@control.csl.uiuc.edu) is a Research Programmer and Agnieszka Klus (aklus2@csl.uiuc.edu) is a graduate student in Accounting at the University of Illinois at Urbana-Champaign.