Alert Notification Systems

Alert notification systems are tools by which information is disseminated to groups of people through mobile devices. The information can be critical or routine, depending on the needs of the user. Alert notification systems can be used by first responders to enhance situational awareness and to notify of any potential threats in the area. Using these tools can decrease emergency response times and increase awareness and efficiency.

Technology Description

Alert notification systems can be used to disperse messages to a group of devices through Short Message Service (SMS), Multimedia Messaging Service (MMS), or e-mail. Standardized text messages can be built into the system, allowing the administrator to quickly send out a pre-defined text message to groups of contacts, including other responders and the public. The system administrator can also send out a customized text message. Custom text can provide more accurate and relevant information, but is marginally slower to distribute than standardized messages. MMS messages can contain photos, audio, or video, allowing the administrator to convey information that is not feasible to send through a text message. While e-mail is not the fastest communications option when using an alert notification system, it still plays an important role. E-mails can be used to disseminate low priority information that may not need to be acted upon immediately.

Alert notification systems utilize current hardware and software, making them both lightweight and adaptable. The system has three components: a computer, a database, and the mobile devices used to receive messages. The software is installed onto the computer, which can then be used to send messages to smartphones, pagers, or any number of devices that have messaging capabilities. The database is used to store contact information, allowing the software to send messages to the designated devices. In order to quickly send messages to certain groups of individuals, the system administrator can designate contact groups within the database.

Security risks are an issue when using alert notification systems. An intruder can intercept the administrator’s password with a phishing attack. These attacks occur when an individual sends a communication (usually an e-mail) to a target in an attempt to acquire sensitive information. For example, if the intruder sends an e-mail to the system administrator claiming to be an employee of the alert system software company, the administrator may surrender his password. Once a security breach has occurred, the intruder would then have access to the entire system and would be able to send bogus notifications, which could delay response times for real emergencies.
It is relatively simple to combat potential intruders using two-factor authentication. Along with a password, the system would require another form of identification in order to log in. SMS authentication codes are easy to implement and create a much more secure alert notification system. Every time system administrators try to log in, they would receive a text message containing a code. The system would require both this code and the correct password in order to log in. An alternative to SMS codes is biometrics. Using biometrics, the system would require some type of measurement from the administrator’s body in order to log in. Fingerprint and retinal scanners are commonly used and would greatly decrease the effectiveness of phishing attacks.

**Pricing Models**

There are a variety of pricing models available for alert notification systems. Subscription-based models exist wherein users of the service pay a fee based on the model that they choose to purchase. The most basic form of a subscription-based model is the per-use charge. Simply put, users are charged a fee every time they send out an alert. This model may be useful for responder organizations that plan to use the system only for emergency situations; however, the per-use model may become costly if the system has a large database of contacts or if it is frequently used. Another form of subscription model is time based, which involves a monthly or annual fee. Users can select the most optimal plan based on their usage and capacity needs. With both the per-use and time-based fee models, the software and hardware are maintained by the licensing company, allowing responder time and resources to be allocated elsewhere. Because the system is hosted in a remote location, it is less susceptible to natural disasters or malicious attacks that can otherwise cripple the alert service.

If the subscription-based model does not make sense for an emergency responder organization, the organization can simply buy the software license and maintain the software themselves. When the license for the software is owned, the alert notification system may be customized to the specific needs of the organization. Agency-owned systems can utilize existing hardware such as smart phones, computers, and servers. These types of systems have some drawbacks, however. Upgrades may be necessary in order to fix any bugs or increase the database capacity. Depending on the magnitude of the upgrade, this may be costly. Agency-owned systems are vulnerable to natural disasters or terrorist attacks. Responders may not be able to send or receive during these emergency events. To avoid this, it may be useful to host the system in a remote location. It is important to consider the required functionality and capacity of the system when choosing a pricing model.

**Applications**

Alert notification systems are widely used to disseminate relevant information to groups of people. Colleges and universities across the globe use these systems to notify students of school closings and events of interest. Severe weather alerts are sent through smartphones based on location data, informing people of adverse and potentially dangerous weather conditions in their area.

These technologies are important and have several applications in a first responder environment. Responders can receive valuable information that enables them to perform their duties more effectively. For example, maps and blueprints can be distributed to firefighters, enabling them to perform more efficient searches and avoid any potential dangers. Briefings can be sent to police officers through audio messages, allowing them to receive information while on patrol.

Message receipt acknowledgement can be built into the system, allowing responders to press a button to confirm that they have received an alert. System administrators can utilize this functionality to keep track of responder assignments and availability. If the administrator chooses to limit the number of alert confirmations, this system can be used to form teams for smaller emergency events.

Using global positioning system capabilities in mobile devices, the alert notification system can target specific responders and inform them about emergency events near their location. An algorithm can be developed to find the most optimal responder for any given event. Specific responder groups may receive an alert based on the geographic location of their agency. This feature provides a distinct advantage over conventional systems that send messages to all responders over a large area, including responders located far from the incident site.

**References and Resources**
