Aiding First Responders

April 2015

Resilient Network Systems

100 Pine St, Suite 700
San Francisco, CA 94111
Telephone: (415) 291-9600
www.resilient-networks.com

Aiding First Responders

The Challenge

In the aftermath of a major disaster or terrorist event, recovery teams face a dangerous environment. Power lines may be down. Water, sewer, and gas lines could be ruptured. Communication systems may not be fully operational. Continuity of state and local government may be at risk in the affected area. Providing "Survivor Centric" services such as medical aid, water, food, and blankets to citizens, as well as providing fuel and supplies to hospitals, police stations, and critical infrastructure sites may be hindered by damaged roads and collapsed buildings. Organizing effective rescue and recovery efforts may be further complicated by the need to differentiate between incoming volunteers and potential looters.

As rescue and recovery teams are assembled and deployed, information sharing between federal, state, local, critical infrastructure partners, and volunteer organizations becomes critical. Real-time validation of identities, capabilities, and the location of assets could greatly speed response times. A series of enhancements utilizing existing technologies can be made to first responder organizations at the federal, state, and local level. For instance, the integration of commercially-available mobile infrastructure can enable FEMA to quickly gain situational awareness, rapidly assess damage, identify the most critical needs, and execute rescue and recovery plans in conjunction with state, local and volunteer organizations. This solution can also assist in documenting actions, coordinating continuing logistics, resolving incidents, and reporting progress.

Solution Overview

Over the past five years, mobile-based technologies and capabilities have progressed enormously. Through the deployment of these commercially available technologies along with the use of a new enabling technology for securing cross-organization information sharing called a Trust Network, government agencies and private sector relief organizations are in a position to provide significantly

improved communications capabilities, applications, and situational awareness for first responders at a disaster area.

For instance, to restore communications quickly and provide situational awareness, deployable cellular base stations can provide high data-rate cellular connectivity to smart phones. Portable aerostat, drone, or balloon based multi-spectral camera systems can provide images of conditions on the ground.

Through the use of a Trust Network, authentication and authorization of individuals moves beyond traditional methods of mobile device security. Not only does the Trust Network validate the mobile user's identity, the network can incorporate other context and the use of data access credentials in addition to the device's identity. It can allow full mobile device functionality while ensuring that devices can be shared between responders. Mobile devices can be protected from theft or misappropriation by access validation in the network. With this enabling technology, additional capabilities can be easily added to responder's mobile devices. These capabilities allow first responders to quickly identify other legitimate first responders, direct their teams, coordinate aid, and publish damage assessments from the field. It allows responders to populate XML reports in real-time, and record video and audio of events for later review and collaboration. The solution enables rapid retrieval and sharing of critical event-related data between FEMA and other DHS components or with law enforcement agencies as needed.

Solution Detail

Since first responders provide aid and conduct damage assessments on foot, combining both agency and personal needs on a single mobile device minimizes the weight of carried electronics. The solution supports shared and interchangeable devices among responders on rotating shifts, and the use of personal mobile devices. It addresses the organization data security needs while delivering the personalization that responders have come to expect with their own devices. This solution utilizes a new method of authentication and authorization that validates individuals separately from their mobile devices.

In previous data security models, the device identification was directly tied to the identity of the device owner making device sharing, or the use of personal devices a challenge. Likewise, data access policies were developed as part of the

applications. This approach poses several limitations to information sharing. Multiple applications on the same device had differing policies for data access. As circumstances on the ground changed, hard-coded data access policies in the applications required application updates and testing which limited the speed at which policies could be updated.

Validating the individual separately from the mobile device requires a network-based identity attestation process. As responders initialize the mobile equipment for use during their shift, the authentication process could include multi-factor authentication, to include checks against the responder's home identity directory (e.g., an Active Directory), along with use of biometrics (e.g., voice or finger print), and geo-location coordinates. This process can dynamically associate the equipment with a particular responder and initiate a secure deployable communications link. Then the responder's agency applications that have already been security screened are loaded on the mobile device as a thin client. The applications are specific for each responder, as permitted by their mobile device manager. Upon completion of the shift, the thin client applications disappear from the mobile device as soon as the responder logs off. All of the collected data from the responder's session is stored by the agency for review and use. As the subsequent responders initialize the equipment, their unique applications can be loaded into the device and new user sessions of data collection would be initiated.

For responders at a disaster area, it can be advantageous to integrate smart glasses. The smart glasses capture facial images to provide real-time, low-resolution, non- cooperative face matching in a hands-free environment as the responder approaches individuals in the disaster area. Incorporating voice recognition technology allows digital voice samples to be collected while an individual is engaged in conversation. The face matching and voice samples can be compared to databases containing the biometric data of known first responders to rapidly validate identities and capabilities. The biometric data can also be used to identify known criminals or terrorists. First responders can be alerted in seconds to dangerous situations. These technologies help clear the "Fog of Triage".

Operation Centers can utilize multi-spectral, time-lapse camera systems to identify the position, proximity, and travel history of response teams to better coordinate action. Aerial photos or infrared images can be sent to an application on the first responder's smart phone in real-time. The aerial images provide improved situational awareness and identify dangers such as arcing power lines

or fuel spills. A voice response application on the smart phone automatically engages aerial camera systems and the audio-visual recording of events through microphones and smart glasses if additional resources are urgently needed.

As injured persons are triaged and prepared for transport, hand scans or facial scans can be performed to provide additional biometric information. This information can be validated against digital health records to avoid allergic reactions or adverse drug interactions. GPS location data and speech-to-text capability allow the automatic, hands-free creation of treatment reports by populating XML documents in real-time as each person is being aided by the first responder. At the end of the shift, the responder can review the XML documents for accuracy. Imbedded links to biometric databases in the document allow the responder or other authorized personnel to review the biometric data for each person and the voice and video capture of the event to verify the content of the report. The XML documents utilize embedded security tags for dissemination control that check with security policies in the network prior to permitting access. The audio and video recordings along with remote participation by the Operations Center personnel protect the responder and agency against false claims by persons in the disaster area and reduce the time consumed by legal defense. After-action review of the audio and video recordings can be used to improve training and operational tactics.

Since first response agencies need to transition survivors to subsequent government agencies for continuing aid, there is a need to share the survivor's biometric information and the video and audio recordings of the engagement. Instead of replicating data between agencies, FEMA, for instance, may want to share links to the biometric data with credentialed users in other federal, state, and local agencies. The information can be accessed when it is needed if the requestors meet the access credentials defined by the data owners. This design approach minimizes the transmission and replication of data across multiple databases. It saves on transmission, storage, administration, and synchronization costs between databases. Security is also enhanced since the biometric data obtained by first responders can remain at rest in the biometric database.

About Resilient Network Systems, Inc.

Resilient Network Systems makes adaptive access management software for identities you don't (or can't) manage. Our network-based, distributed

architecture is highly flexible and scalable, allowing customers in government and enterprises to safeguard their data and applications, while enabling more collaboration and information sharing with their entire ecosystem. We make it simple to leverage existing identity and security products, or add external identity sources and services, with easy-to-implement, predefined and custom policies. Resilient Network Systems is a privately held, venture-backed company based in San Francisco.