Securing a public safety broadband network with identity management

April 15 2015, by Evelyn Brown

The First Responder Network Authority (FirstNet), part of the National Telecommunications and Information Administration (NTIA), is building a nationwide public safety broadband network to provide first responders with access to 21st century communication technology that improves safety and security. But how do you make sure the network only helps the good guys? The National Institute of Standards and Technology (NIST) has published an analysis of how a public safety broadband network can be secured so that only approved first responders and public safety personnel can access it.

The planned broadband network will offer emergency and law enforcement personnel many advantages, including audio, video and real-time information sharing via broadband cellular technologies to mobile devices. In the past, for example, firefighters from different jurisdictions teaming up to fight a major fire have had communications problems because their systems use different radio frequencies or encryption technologies. A nationwide wireless broadband network would provide a mechanism not only to integrate those systems, but also to provide layers of advanced support. It could, for example, integrate a live video feed from a robot sent into a fire to search for people or let chiefs located at different points around a fire see a live feed on their mobile devices. This stands to improve situational awareness and enable incident commanders make more informed decisions.

But such a network also comes with challenges. Not just ensuring that only authorized people can use it, but also ensuring that sensitive information, such as a criminal record, is shared only with sanctioned people that have a "need to know."

NIST's analysis draws on its expertise in identity management for mobile devices. Considerations for Identity Management in Public Safety Networks provides background information on identity management and a review of applicable federal and industry guidance for using next generation networks with a number of options for policy makers to consider. Topics include selecting identity credentials and the authentication process. It also includes analysis of possible identity management technologies that could be used.

The NIST analysis on securing first responder communications may be applicable to local public safety networks, private sector communities and public safety applications that leverage identity management services, including criminal justice information and records management systems.

More information: "Considerations for Identity Management in Public Safety Networks" (NISTIR 8014) is available at DOI: dx.doi.org/10.6028/NIST.IR.8014.

Provided by National Institute of Standards and Technology

Citation: Securing a public safety broadband network with identity management (2015, April 15) retrieved 19 April 2024 from https://phys.org/news/2015-04-safety-broadband-network-identity.html