Pipeline
Technology for Service Providers.
www.pipelinepub.com Volume 9, Issue 6

Securing Next Gen 9-1-1

By Jesse Cryderman

Few telecommunications systems are as important as the emergency response platform that effects everyone in the U.S., 9-1-1. This analog system is comprised of public-safety answering points (PSAPs) and relies on telco billing-system data to provide location information for first responders. The faster this data can be pulled and distributed to the appropriate teams, the better: swift palliative care following a serious injury improves survival rates, and fires that are suppressed early cause less personal and property damage. Simply put, speed saves lives, so how can emergency response systems benefit from the speed advantages offered by digital automation?

Like many other systems that are undergoing evolution, 9-1-1 is being overhauled as well, and the result is Next Generation 9-1-1 (NG9-1-1). By moving to the IP realm and relying on several informational databases, NG9-1-1 not only dramatically shortens response times but improves location accuracy and can be provisioned to distribute additional pertinent information to emergency response teams. While 9-1-1 was designed for landline communications and tweaked to support cellular, NG9-1-1 is engineered from the ground up to accommodate the many different ways people communicate now, including VoIP, cellular and text messaging. Transitioning to an IP-based system increases security risks, however, and since 9-1-1 is such a critical system, a fortified security platform must be applied to ensure uptime, resiliency and dependability.

This Isn't Your Father's 9-1-1 Service

While NG9-1-1 is an IP-based system, it has a unique set of features that pose some different challenges from a security perspective. Unlike traditional computing systems, where security patches and upgrades are regularly applied and the system is subsequently rebooted, NG9-1-1 systems must avoid downtime at all costs. Also, data protection and network requirements are significantly higher in these systems than in traditional peer-to-peer IP networks. "An NG9-1-1 system must deliver a secure, resilient and redundant IP-enabled network with 99.999 percent uptime," writes top NG9-1-1 consultancy firm L.R. Kimball.

At the same time, NG9-1-1 shares many of the same challenges that face all IP-based platforms. Transitioning from relatively discrete analog systems to interconnected IP-based systems dramatically increases the number of entry points — and therefore exposure risk — and human security compromise, whether intentional or by mistake, represents a significant threat. In addition NG9-1-1 systems must implement physical security and redundancy similar to that of data centers and cloud providers, including redundant power, anti-flammable and anti-static surfaces, intrusion detection, physical access monitoring and logging, and more.

NG9-1-1 requires "a foundation of cyber security hardware and software measures to protect the network from being checkmated by malicious opponents or accidentally taken down by users," writes L.R. Kimball. Current 9-1-1 systems, although slower and analog based, aren't vulnerable to denial-of-service attacks, MAC address spoofs or internationally distributed malicious viruses. Without an exhaustive cybersecurity framework for NG9-1-1, public safety is at risk.

Another point to consider is that cybersecurity is a specialized expertise that falls under the realm of IT. Some PSAPs don't employ an IT security expert with the experience to build a secure Emergency Service IP Network (ESInet); for these 9-1-1 centers, engaging with a third-party consultant would be a wise move.

Making Your List and Checking It Twice

The National Emergency Number Association (NENA) has been leading the charge toward a national, interoperable NG9-1-1 network for more than a decade. NENA drives the development and standardization of NG9-1-1, and it takes security very seriously. In fact the organization created NG-SEC (Security for Next Generation 9-1-1) to specifically address NG9-1-1 security. To get an idea of just how extensive its recommended security measures are, take a look at the NENA Security Audit Checklist. The 396-item list is nearly 100 pages long and is regularly updated to address new and future security issues. It's also probably the best and most thorough document to review if an organization is considering moving emergency response systems to NG9-1-1.

NG-SEC breaks the checklist down into 14 sections that address every possible security concern. Significant focus is given to authentication and password processes, which address the problem of human security compromise. The 59 steps ensure that password protection policies are established, enforced, logged, and regularly reviewed and updated. Other mandates include:

- Authenticated credentials must be encrypted if stored, and must be obscured on the screen when entered;
- Workers in an NG9-1-1 environment should never use personal storage (USB thumb drives, for instance) with NG9-1-1 computers;
- Passwords used to access public safety systems must never be used outside for personal computing or Web-based services;
- Two-factor authentication schemes must be created in such a manner that the compromise of one factor doesn't enable that of another.

An essential component of data protection in the NG9-1-1 environment is keeping its networks totally separate from other IP networks. "NG9-1-1 IP-enabled networks should not completely mirror the peer-to-peer connectivity that the Internet provides," writes NENA, but "operate over IP with clearly defined redundancy and resiliency." This extends to wireless networks within a building: NG-SEC requires that Wi-Fi LANs be dedicated to the NG9-1-1 system and separate from other networks.

Without an exhaustive cyber security framework in place for NG9-1-1, public safety is at risk.

Are You Ready?

As any telecom engineer will attest, the lab and the wild are two very different environments. Following a checklist is important, but testing a system after it's built is even more important. Following an established framework for a security-readiness assessment is essential and includes vulnerability testing, VoIP-initiated denial-of-service attack modeling and system testing for penetrability and compromise by various other hacks. Again, if a PSAP doesn't have IT security expertise in-house, the services of a third-party NG9-1-1 security consultant are highly recommended.

Enabling the Future

Preparing operators for the future of emergency response is a level of security in and of itself, as the reliability of the system doesn't end in the ESInet but in the operator's chair. Operators at PSAPs will have much more information at their fingertips, and contact might be in the form of a text message rather than a phone call. Beyond NG9-1-1 platforms from companies like Motorola and Synergem, the NG9-1-1 evolution will require training. Most solution providers can supply it, but NENA's Education Program is probably the best bet: it provides more than two dozen industry-best offerings that span the width and breadth of 9-1-1 technology and PSAP operations topics.

Whenever public interest, private business and global connectivity intersect, solutions that seem simple at first glance become complex. Next-generation emergency services are especially complex because the security and reliability of the system are the definition of "mission critical." Creating an interoperable network that functions the same way in Andover, Massachusetts, as it does in Chico, California, is not an easy task, but it's under way. No matter who the providers, partners and PSAPs are in each unique situation, security must be a foundational pillar of the NG9-1-1 solution.

The most costly cybercrimes continue to be those caused by malicious code, denial of service, stolen or hijacked devices, and malevolent insiders.

“You are going to see entirely new systems, tools and support solutions come out of this.”