

Data

Threats



## Wireless broadband advancements force network administrators to rethink data-security tools.

By Rory Conaway

**M**ission-critical data networks are a little different than most government-based networks, not only because of the type of data stored, but the integration into bigger government databases. Historically, that integration was only a problem at a central command center. With the ability to deliver broadband to vehicles and devices over virtual private network (VPN) tunnels, through cell phones, and via other channels, the number of gates that have to be watched increases exponentially. In addition, many governments, both friendly and unfriendly, have coordinated efforts to breach data in the United States at many levels. Criminal organizations have now moved into Internet fraud and data acquisition that they sell to other criminal groups. The effort to get information is directly related to the value of the information.

Law-enforcement databases are a tempting target. Even the smallest law-enforcement agencies with the smallest technical staffs have access to some of the biggest criminal databases in the world. The most common operating systems and network hardware currently used are also the source of the most easily compromised points of entry. Smaller agencies typically don't have the manpower or the expertise to keep up with weaknesses or to implement proper procedures to ensure that vulnerability on a local level doesn't give

someone access to state or federal information.

The tools that make law enforcement more effective are the same tools that make security that much tougher. Multiuse, citywide Wi-Fi networks used by police, fire, city inspectors, and others such as public Internet users greatly improve efficiency. These systems can also add a force multiplier with the addition of cameras, gunshot monitors, real-time vehicle video, and other monitoring technologies.

Many law-enforcement agencies have networks separate from other city networks. They generally have dedicated terminals in vehicles, which use licensed spectrum usually with low speeds such as 9.6, 19.2, and 33.4 kilobits per second (kbps). However, that is nowhere near the bandwidth needed for real-time video, facial-recognition systems, graphics-based database information, relational database processing, and other applica-

tions. Although the technology exists to deploy higher speed bandwidth to vehicles, more thought needs to be applied to the security of this capability.

Tell a law-enforcement network administrator to integrate an internal network with a public Wi-Fi mesh network, and watch him cringe. If an administrator has any security experience, he knows that giving someone a high-bandwidth pipe or multiple high-bandwidth pipes to the

exterior of a network only invites trouble. Good administrators know that point of entry must be extremely secure and closely monitored.

Taking this issue to the next level, the Department of Homeland Security (DHS) requires integrated radio systems that allow multiple agencies to share equipment and communicate among government agencies in times of emergencies. The next step is an integrated data system, such as a city-wide mesh network. However, municipal mesh networks are designed to operate within city limits. It's now possible to create an integrated multi-jurisdictional infrastructure that can be separated for normal use and integrated in times of crisis.

### Security Standards

Given these types of scenarios, can network administrators provide a reasonable level of security with a dynamic, changing environment where the numbers of gates to the

**Although the technology exists to deploy high-speed bandwidth to vehicles, more thought needs to be applied to the security of this capability.**

network are growing daily? Most network administrators already employ the easiest lines of defense, which include a basic firewall, anti-virus at desktop and server levels, some type of password policy for the users, and anti-spam filtering and Web site protection software. However, the only secure network is one without outside CD-ROMs, floppy disks, or USB keys; that doesn't allow laptops to connect to other networks; has no outside e-mail or Internet connection; and isn't connected to any other network with the same limitations. This world simply doesn't exist.

It's time for mission-critical network administrators to start using a common standard in network security. Aside from the above-mentioned security measures, additional security processes — both human and computer — need to be implemented. Although the human security methods are the easiest to define, they are often the hardest to implement. Let's start with the most basic security protections: the user name and password. User names must never be a first initial, a first or last name, or three initials. User names should be randomly chosen by a user or generated by a computer and shouldn't be any combination of a user's name. Administrators should disable or rename the administrative account on any server, router, or switch. They should disable the default local accounts on all PCs on a network.

The password for any computer network should be eight characters or more and a mixture of letters and numbers. The system should have the ability to compare a password to commonly used dictionaries to ensure the password isn't easy to guess. The password should be changed every 60

days at a maximum. Administrators should periodically do a physical audit of all user work areas to see which users put sticky notes under their keyboards, inside their desk drawers, or even on the front of their monitors. When changing passwords often, many users forget their passwords and thus write them down where they can easily find them.

Although firewalls protect the exterior of a network, few tools pro-

## 8 Basic Security Precautions

- 1 User names must never be a first initial, a first or last name, or three initials.
- 2 User names should be randomly chosen by a user or generated by a computer, and shouldn't be any combination of a user's name.
- 3 Administrators should disable or rename the administrative account on any server, router, or switch.
- 4 Administrators should disable the default local accounts on all PCs on a network.
- 5 The password for any computer network should be eight characters or more and a mixture of letters and numbers.
- 6 The system should have the ability to compare a password to commonly used dictionaries to ensure that the password isn't easy to guess.
- 7 A password should be changed every 60 days at a maximum.
- 8 Administrators should periodically do a physical audit of all desk areas of users, to see who puts sticky notes around their work areas.

tect the interior. Microsoft, Cisco, Enterasys, and other vendors are aware of this and are implementing new procedures and security protocols such as 802.1x, internal VPN tunneling, network access protection (NAP), and network access control (NAC). Network companies are integrating their hardware, switches, routers, and other equipment with Windows so they work hand in hand, not separately. The only problem with these new features is that they are implemented with new operating systems from Microsoft and new hardware and firmware from network hardware manufacturers. Their implementation requires either significant investments or additional training of current network administrators.

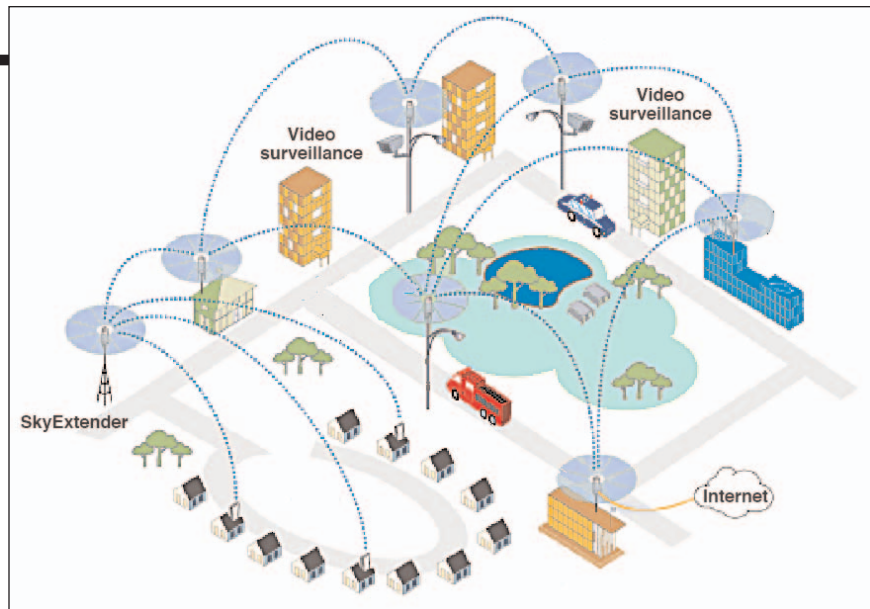
Administrators also need to start looking at more proactive tools such as intrusion detection systems (IDS) and intrusion protection systems (IPS). An IDS will monitor all packets within a network for threat signatures such as viruses, worms, and spam. An IDS should be integrated with some type of network-management tool. Policies are created in advance on how to deal with threats and stored within a network-management tool, so they can be implemented when threats are identified. A network-management tool can reprogram a hardware network device on the fly and apply or modify a policy on a device to handle a threat.

For example, the IDS is physically attached to the central switch of a network. A laptop that just connected to a wireless access point on a network has been infected with a Trojan virus that is probing computers all over the network. Even worse, the virus is changing its own IP address when it runs into conflicts. The IDS immediately sees two things: IP address conflicts on the network and the Trojan virus. The problem is the Trojan is moving around in the IP address range. The IDS system notifies the network-management tool that it sees these two specific threats along with any other data it has collected.

In this case, it has captured the same media access control (MAC)

address in both categories. Even though it acted on both threats, the policy for these types of threats is the same, "Block the MAC address from getting on the network." That block is then applied at multiple levels. It notifies the switch to block any MAC address traffic from the offending computer, while the network-management tool simultaneously tells the wireless access point the same thing. The laptop can no longer get past the access point and is effectively disconnected. In addition, an administrator has been notified that this problem has occurred. Hopefully, the administrator can track down the offending party and fix the problem. This result could occur whether the user is wirelessly or physically connected.

For multiuse outdoor wireless networks, most cities are using wireless security methods such as MAC address authentication tables, which can be easily hacked by emulating a password; wired equivalent privacy (WEP), also easily hacked in minutes by good wireless hackers; Wi-Fi protected access (WPA) or WPA 2; tunneling; no broadcast service set identifier (SSID); VPN solutions; and advanced encryption standard (AES) encryption. Most of these are good and can't be cracked. However, nobody has addressed what happens when someone plugs directly into an access point that is on a network. Administrators don't disable the Cat-5 connector on an AP, and anybody with a \$10 hub can physically plug into one. This connects a user half-way across town to the network. A user can sniff all the traffic or



It's now possible to create an integrated multijurisdictional infrastructure that can be separated for normal use and integrated in times of crisis.

take whatever time is necessary to probe and gather all the information needed to get into a network. Because most cities don't employ an IDS or IPS system, this could occur for weeks before anyone has any idea what is going on. Wireless networks make protecting the system far more difficult than just locking the doors.

For wireless networks, most companies and agencies use a virtual connectivity middleware product from companies such as Radio Mobile, Radio IP Software, and Identiprise. These products also provide additional security features such as secure VPN tunneling. Multijurisdictional environments require additional server components, and some products such as Identiprise have basic IDS capabilities all the way to the clients.

Security of any network can be a daunting task. The level of security

elevates as the value of the data increases. To meet this challenge, manufacturers are implementing new protocols and products that additionally strain information technology (IT) staff. Mission-critical communications network managers have even more strain because of further security requirements that other groups may not be subjected to. Managers have to realize that though these implementations are not inexpensive, the cost of not implementing them could be significantly greater. ■

Rory Conaway is president and chief executive officer (CEO) of Triad Wireless, an engineering and design firm headquartered in Phoenix. Triad Wireless specializes in unique RF data and network designs for municipalities, public safety, and educational campuses. Contact him at [rconaway@triadwireless.net](mailto:rconaway@triadwireless.net).

**The only problem with new security features is that their implementation requires either significant investments or additional training of current network administrators.**

RadioResource *MissionCritical Communications* delivers wireless voice and data solutions for mobile and remote mission-critical operations. The magazine covers business, public safety, and regulatory news; case studies; in-depth features; innovative applications; product information and comparisons; emerging technologies; industry reports and trends; and technical tips. In addition, each issue contains *Public Safety Report*, a special section devoted solely to the needs of the public safety community. Editorial content targets organizations in the United States and Canada with mobile and remote communications needs, including public safety, government, transportation, manufacturing, utility/energy, business, and industrial entities. To request a FREE subscription or get more information, go to [www.mccmag.com](http://www.mccmag.com). RadioResource *MissionCritical Communications* is published by the RadioResource Media Group. Pandata Corp., 7108 S. Alton Way, Building H, Centennial, CO 80112, Tel: 303-792-2390, Fax: 303-792-2391, [www.rrmediagroup.com](http://www.rrmediagroup.com). Copyright 2007 Pandata Corp. All rights reserved. Reprinted from the June 2007 issue of RadioResource *MissionCritical Communications*. For more information about *MissionCritical Communications* and the RadioResource Media Group please call 303-792-2390 or visit [www.mccmag.com](http://www.mccmag.com)