

Secure Networks for First Responders and Special Forces

Originating Technology/ NASA Contribution

When NASA needed help better securing its communications with orbiting satellites, the Agency called on [Western DataCom Co., Inc.](#), to help develop a prototype Internet Protocol (IP) router.

Westlake, Ohio-based Western DataCom designs, develops, and manufactures hardware that secures voice, video, and data transmissions over any IP-based network. The technology that it jointly developed with NASA is now serving as a communications solution in military and first-response situations.

Partnership

In early 2000, Glenn Research Center approached Western DataCom to develop the prototype IP router. This was part of NASA's "IP in Space" initiative, which looked to employ commercial off-the-shelf products

to support reliable, fast, and secure communications between NASA and its orbiting satellites. The company signed a Space Act Agreement with Glenn and delivered a prototype device that met the three requirements set by the NASA research center, namely speed, security, and reliability. The router employed advanced data-compression techniques (to improve throughput and meet the speed requirement) and encryption (to meet the security requirement), and operated with commercial protocols (to meet the reliability requirement).

Because of the work it had done for Glenn, Western DataCom was approached by Cisco Systems, Inc., in 2001, to participate in the development of an IP encryptor for the Cisco Mobile Access Router (3200 Series), for military use. According to Western DataCom, it offered Cisco two distinct advantages: 1) Western DataCom had leading encryption and compression technologies, from working with NASA, as well as the National Security Agency; and 2) Western DataCom code developers

possessed the military clearances needed to perform the work required. Cisco created its "Advance Technology Partner" classification and named Western DataCom the first of such partners. Cisco also joined Western DataCom in working with Glenn to develop the reliable, fast, and secure mobile router system for military and first-response use.

The technology was not commercially available at the time that the September 11 attacks took place, but will prove invaluable to emergency and rescue personnel in averting any potential future threats.

Product Outcome

In the hours and days after September 11, communications between first responders and emergency-management officials from Federal, state, and local agencies were severely disrupted. New York City's Emergency Operations Center, designed to coordinate rescue efforts in a major terrorist attack, was housed in the 47-story "7 World Trade Center" building and destroyed.

The World Trade Center was a node of central communications for all forms of voice and data traffic and was utilized by business and private customers, as well as the city's first responder and emergency-management agencies. Communications systems for the police and fire departments were temporarily disabled as a result of the damage caused by the collapsing of the building and senior emergency-management officials were unable to contact first responders in the early hours of the tragedy.

Because police and firefighters could not communicate directly with each other, many firefighters within striking distance of safety never received a police warning on the impending collapse of the South Tower. A report from the University of New Hampshire* concluded that this lack of interoperability between the police and fire communications systems were "at least, partially responsible for the loss of 343 firefighters at the World Trade Center."



This van served as the mobile test bed when the IP router technology was field-tested at Glenn Research Center.

Much of New York City's landline and cell phone infrastructure was also damaged or destroyed during the attacks. Moreover, the disaster generated so much communications traffic in and around the city that the remaining intact landline, cellular, and two-way pager systems became too congested to be of use to first responders and emergency-management personnel.

The experiences of September 11 have driven many organizations and individuals to realize that new communications systems are needed to secure our country and improve our ability to respond to terrorist attacks. In addition, the ongoing conflicts in Afghanistan and Iraq have broadened the need to provide a mobile, interoperable, and secure communications system solution for the U.S. military and first responder personnel, such as U.S. Army

National Guard, firefighters, police, and emergency medical services (EMS).

In 2004, the secure mobile router system co-developed by Western DataCom and NASA was successfully used by the Army for an aerostat (balloon)-based radar, called the Persistent Threat Detection System, in Operation Iraqi Freedom. The system permits military technical operations centers (TOCs) in Iraq to send secure, high-speed voice, video, and data communications to the field through tactically deployed mobile units. This was the first use, during war, of technology enabling TOCs and mobile units to send secure voice, video, and data communications, according to Western DataCom.

First responders from Cook County, Illinois; the New York Port Authority; and the New Jersey Port

Authority are currently utilizing the company's secure system in preparation for natural or man-made disasters. Also, in 2004, Western DataCom developed a secure-communications modem to be utilized primarily by first responders for homeland defense operations. These products were successfully deployed during the Republican National Convention and the presidential inauguration.

Recently, Western DataCom received a \$100,000 Glenn Alliance for Technology Exchange (GATE) award from Glenn and Battelle, an organization that helps bring NASA technology to companies outside the traditional aerospace industry. The award, in the form of \$50,000 in cash and \$50,000 in Glenn engineering time, will be used to design a small personal computer encryptor card for commercial markets. This card is anticipated to act as a shield outside of a computer, protecting its hard drive from outside "attacks," such as worms and viruses, as well as "middle-man" and "spoofing" threats. (A "middle-man" is someone who unwittingly spreads a virus by simply opening or forwarding an e-mail, while "spoofing" is a technique used to gain unauthorized access to computers. A user receives e-mail that appears to have originated from one source when it actually was sent from another source, in an attempt to trick the user into releasing sensitive information.)

The two NASA engineers assigned to this project have experience with Western DataCom, in that they were involved with the 2000-2001 "space router" project that culminated in the basic technology platform utilized in the company's current encryptor product line.

Once the commercial personal computer card is operational, Western DataCom plans to design a top-secret military version. The company intends to have the commercial card designed and operating, and to have work started on the military version, by the end of 2005. ❖

*Lund, Donald A., *The Lessons of Non-Interoperability in Public Safety Communication Systems*. University of New Hampshire, April 2002.



Western DataCom Co., Inc.'s Executive Travel Case sets up connections automatically to the Internet, Secret Internet Protocol Router Networks (SIPRNETs), and Non-secure Internet Protocol Router Networks (NIPRNETs), for use by the U.S. Joint Forces Command.