



Case Study



No Strings Attached

As the Government of Canada moves to mobility, security is the number-one priority.

At the RCMP detachment in Surrey, B.C., officers are testing a new wireless solution that is, in the words of applications specialist Don Bandurka, “light years ahead of anything we’ve had up to this point.” The solution is called OnPatrol. It involves software developed specifically for police agencies, loaded onto Research in Motion (RIM) Wireless Handheld™ devices.

OnPatrol is just one example of how government organizations are adopting wireless technology—and addressing the security challenges that accompany it.

On the street

“This solution will enable our foot-patrol officers to securely query police databases, as well as send and receive digital messages,” says Bandurka. “Officers will no longer have to stop and write out details of a complaint, for instance; all the information will be contained in their handheld, ready to be accessed and relayed instantly.”

“The federal government is, to a great extent, like any large enterprise adopting technology. The government also, however, collects vast amounts of private information—and is obligated to protect that information.”

Lawrence Surtees,
Director, Telecom Research
IDC Canada

Equally enthusiastic about the solution, Raymond St-Jean of the RCMP's Mobile Communications Branch in Ottawa says testing will expand to several RCMP and non-RCMP detachments across Canada. Results will then be carefully monitored. “The officers are keen to try the handhelds,” he says, “but with the obvious security concerns associated with such small, portable devices, we must exercise caution—and be certain the solution is airtight.”

xwave, the organization responsible for creating OnPatrol, is an end-to-end IT-services provider that has worked for many years with public-sector organizations, garnering particular experience in sensitive areas involving public security and safety. The firm has built a secure directory for the Department of National Defence; it is currently developing an improved electronic-service-delivery platform for Canada Customs and Revenue Agency; it rebuilt the external website for the Communications Security Establishment; and it recently launched a web-based offender-management network—called the Client Information System (CIS)—for the Government of New Brunswick. Winner of two industry awards, the CIS has caught the attention of the State of Maine, whose Department of Corrections has now contracted xwave to build a similar system.

In the area of wireless technology, xwave has worked extensively with public-safety and police-related organizations. In addition to OnPatrol, the firm has developed a wireless solution called ROADS—the Remote Office And Dispatch System—currently installed in approximately 1,500 police vehicles across Canada.

Wireless applications are appearing with increasing frequency in most government organizations. And as many people in those organizations agree, we're all still in the very early stages of wireless—about the same stage the Internet was at in 1993. But it would seem we're not all jumping in with quite the same technological zeal we had in the 1990s. There was a time, for example, when the inclusion of the word 'Internet' in a venture-capital proposal meant funding was assured. Today, after both the demise of the dot-coms and the shock of 9/11, people are carefully weighing wireless benefits against security risks.

At the office

Mary Ann Bednar is an IT project manager with Environment Canada (EC). “Without a doubt, security is of critical importance to government organizations using wireless technology,” she says. “Employees here are eager to try new applications and devices, but we have to be careful about what people can and can't use.”

A keen adopter of handheld devices—there are a couple of hundred now in use by EC employees—the department recently enabled wireless access. Though the new network is still being tested, it will eventually allow visiting EC executives from across Canada to connect easily with their regional offices. It will also be used for presentations and training—situations in which a number of laptops need to be connected simultaneously. In developing the network, security has been a high priority.

“Which is why we've added a requirement for a Virtual Private Network,” says Bednar. “The VPN tunnel adds an extra layer which makes the network that much more difficult to break into.”

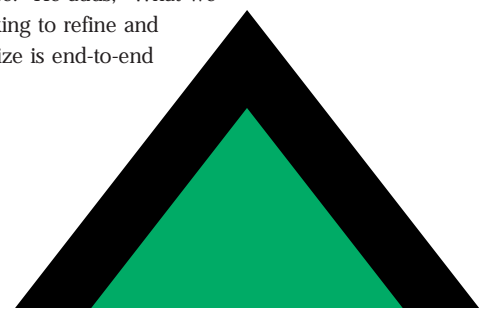
Developing strategies

As both users and legislators of wireless technology, government organizations are clearly in a unique position when it comes to security.

“The federal government is, to a great extent, like any large enterprise adopting technology,” says Lawrence Surtees, Director, Telecom Research at IDC Canada. “The government also, however, collects vast amounts of private information—and is obligated to protect that information.”

The Communications Security Establishment (CSE) advocates two key strategies to improve wireless-communication security: “We collaborate with the technology vendors to help make the products more secure, and we work with the users to ensure they're using the products properly,” says Bob Stevens, Chief of Staff for the Information Technology Security business line at the CSE.

“There is an inherent risk in transmitting information over a wireless network,” says Stevens matter-of-factly. “And while in the past, the rule was 'if it's not secure, you can't use it,' in today's world, that rule is simply not possible to enforce.” He adds, “What we are working to refine and standardize is end-to-end



encryption: from the moment the message leaves one device to the moment it is received by another, it is encrypted—and remains so while it's stored on the device.”

Unlocking potential

Security aside for a moment, government employees see great potential in wireless technology. Says Environment Canada's Mary Ann Bednar: “I equate it to the microwave oven—once you have it, you don't know how you got along without it. I see many uses for wireless: in satellite offices; for temporarily relocated employees; for training—and there, I see enormous possibilities. With wireless technology, you could set up a virtual classroom anywhere.”

Schools in remote communities have been doing exactly that for a number of years: interfacing satellite communications with wireless local-area networks (WLANs) to provide local high-speed Internet service—thereby opening the door to a world of educational opportunity.

WLANs can enable Internet-based communication in places where wires either don't exist, can't be installed—or need to be removed. That was the case a couple of years ago at a Department of Fisheries and Oceans (DFO) lab in B.C.: during four months of extensive renovations, communication at the lab continued uninterrupted thanks to wireless access.

The person who recommended the installation of that WLAN is Jeff Kingsley, a member of the Emerging Technologies sector in Government Telecommunications and Informatics Systems (GTIS).

Minimizing risk

“From a security perspective, there has been quite a learning curve in WLAN development,” says Kingsley. “Initially, people tended to just put it in and worry about it later. Then the road-rogue stories began to materialize: hackers sitting in parking lots with laptops, intercepting information being transmitted wirelessly in the building next door. And people began to stop and think about the technology they were using—and its level of security.”

Kingsley adds that improved technology, combined with improved planning, is making the newer wireless networks more difficult to

penetrate. “Most of the eavesdropping was done on open networks transmitting in the 900 Megahertz (Mhz) range,” he points out. “The newer WLANs operate in the ISM (Industrial, Scientific and Medical) range, in 2.4- and 5-Gigabit frequencies. There are ways to configure these newer networks to help prevent transmission bleedout, and lessen the chance of people breaking in.”

First off, he explains, activating certain security measures while deactivating others—all in a particular sequence—can be an effective means of mitigating the risk of eavesdropping. He advises turning the Wired Equivalent Privacy (WEP) encryption on, while turning off the Media Access Control (MAC) address transmission, and changing the Service Set ID (SSID). It is the combined simultaneous transmission of all three that enables a hacker to monitor and mirror the WEP algorithm—and ultimately break in.

To reduce transmission bleedout, Kingsley recommends a proper site survey for placing and calibrating the network's wireless transmitters, or access points. “For example, you can lower the power-transmission levels to suit a smaller space,” he says. “You can also increase attenuation—which means increasing the distance between the transmitter and the antenna.” In general, he says, planning is key; the more thought people put into wireless networks before installation, the more secure the networks will be when they're operational.

As both a wireless consultant with GTIS and a recently accredited Cisco Aironet site surveyor, Kingsley regularly advises government departments considering WLANs. He's also involved in mobile-wireless initiatives, such as the ongoing government-wide rollout of the RIM BlackBerry Enterprise Edition™. “The Enterprise Edition provides users with their own servers—extensions of the email applications on their desktops,” he explains. “So rather than have information sit on an outside server, waiting for transmittal, users have that extra security of knowing the information is always stored on their own server.”

New applications

While many of the government-issued handheld devices are still used primarily to send and receive email, an increasing number are being



Government On-Line Gouvernement en direct

**“Without a doubt,
security is of critical
importance to
government
organizations using
wireless
technology.”**

Mary Ann Bednar,
IT Project Manager,
Environment Canada



loaded with job-specific software – as is the case with xwave's OnPatrol.

"We're starting to see handheld applications tied in to back-end operational systems," says Anthony LeBlanc, Group Director of Government Solutions for RIM. "For example, in the U.S., the military is using BlackBerry handhelds for wireless management of inventory, and to help track medical records of forces personnel. Sky marshalls employed at airports since 9/11 are now using the technology to communicate both with one another and with other law-enforcement officers. And, of course, we're seeing widespread use of the devices among members of both the House of Commons and the House of Representatives—over 2,000 devices in the House of Reps alone." He adds, "These are people who spend a lot of time in chambers, yet must stay in touch." In Canada, Sheila Copps, Alan Rock and John Manley have all been seen using handhelds.

Anthony LeBlanc says security is the first word on everyone's lips. "The first questions people ask are, 'What encryption do you use? Are you FIPS-certified?'" LeBlanc is referring to the FIPS-140-1 certification granted to vendors that meet the security standards established by the U.S.-based National Institute of Standards and Technology (NIST).

In designing the OnPatrol and ROADS solutions, xwave has, for obvious reasons, paid close attention to security. Along with incorporating 128-bit encryption, OnPatrol, for example, makes use of a log-in screen, through which users sign on with a password. As well, the device includes both application-lock-out and remote-device-erasure capabilities: application lock-out essentially shuts the device down if the wrong person repeatedly—and incorrectly—tries to log onto it; remote-device-erasure allows a user to disable a lost or stolen device by erasing the information contained on it.

Continued growth

While security remains an ongoing concern for wireless users—both inside and outside government—many government employees feel that the cost-efficiency and convenience of wireless will continue to drive what Jeff Kingsley calls "phenomenal growth."

"You could set up a 10-meg WLAN connecting one building to another for about \$1,000—with no disruption, and you own the equipment; there are no monthly fees," Kingsley explains. "A wireline network will cost you somewhere between \$900 and \$4,000 per month—and that doesn't include installation, which can run anywhere from \$2,000 up to \$10,000."

The other driver is need. Mac Anderson, xwave's Program Manager, Wireless Applications, offers this observation: "There's no doubt that the newer WLANs are efficient and effective," he says, "though for the most part, people will only upgrade to wireless if the wiring doesn't exist." Regarding security, Anderson reiterates what Jeff Kingsley and others in government are saying: that technology and standards are improving. And Anderson points out that while people in general tend to be concerned about the impact technology will have on their privacy—and new technology in particular—they will use that technology if the benefits are significant enough.

It would appear that, so far, the benefits of wireless technology are significant indeed.

Contact us

xwave is a full-service business solutions provider with 1200 professionals in locations across North America.

xwave has three service lines: Integration, Infrastructure and Fulfillment solutions. We are focused on providing end-to-end solutions from systems integration and software engineering, right through to infrastructure services and product fulfillment.

For more information:

Visit our web site at www.xwave.com

Call toll free 1-877-449-9283

Email us at solutions@xwave.com

Or contact your local xwave office in Newfoundland, Nova Scotia, New Brunswick, PEI, Ontario, Quebec or the United States.



A DIVISION OF BELL ALIANT