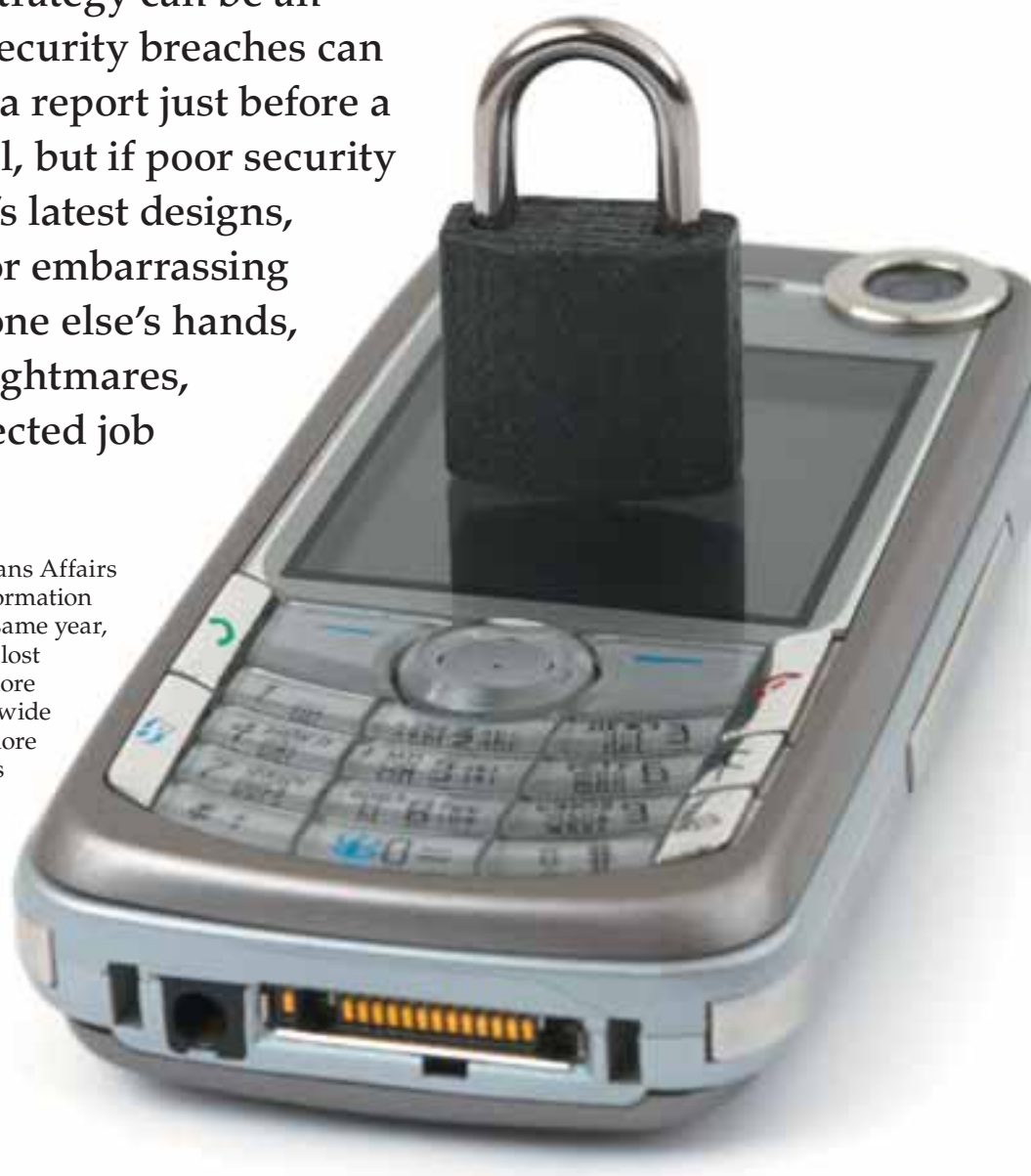
Wireless Security

In everyone's best interest

By David Crowe

Like back-ups, security tends to be what you remember when it is too late to undo the damage. Loss of data from a bad back-up strategy can be an expensive lesson, but security breaches can be devastating. Losing a report just before a deadline can be painful, but if poor security leads to your company's latest designs, unreleased financials or embarrassing e-mails being in someone else's hands, you have the stuff of nightmares, headlines or an unexpected job search (yours).



In 2006, the U.S. Department of Veterans Affairs lost one laptop containing personal information for more than 28.6 million people. The same year, a vendor of the clothing chain The Gap lost a laptop containing personal data for more than 800,000 job applicants. The Nationwide Building Society in the UK was fined more than $2 million in 2007 because of a loss of a single laptop containing information on their 11 million customers.

Not to be outdone, the British government lost CDs containing information about all families with a child under 16, or about 25 million people. They were forced to admit to a raucous parliament that this included name, address, date of birth, national insurance number (the UK's SIN equivalent) and, for some, banking details.

In Germany, in late 2008, a major newspaper received a box containing microfilmed credit card statements for tens of thousands of customers. Apparently, Landesbank Berlin, the nation's biggest issuer of cards, was still transferring data by mailing microfilm.

Canada is not immune, although our smaller population tends to make the breaches less dramatic. In 2004, data on about 1,400 Canadians was lost by credit-reporting agency Equifax Canada. Canadians were also affected when credit card databases of the U.S. parent company of retailers Winners and HomeSense were hacked. Our government is not immune either. In 2007, it was discovered that the Passport Canada Web site could be used to access personal data on applicants, merely by changing some characters in a URL.

It's not just important to think about security once in a while, but rather you have to think about it every day and through every aspect of your organization – including people. You can put the best possible technical security on all devices and communications links, but people, without any technology beyond their voice or a piece of paper, can still cause security breaches.

Security does have its limits, and one of those is a trade-off with usability. Luckily, the trade-off between security strength and usability is not linear. While you cannot get any reasonable level of security with no impact (such as needing to enter user names and passwords), and the absolutely highest level of security will have dramatic usability impacts (such as sealing all communications ports on laptops), it is possible to achieve high security with acceptable impacts on the usability of systems used by an organization's employees.

The need for security in wireless networks is not a new realization. It was back in the 1980s, when cell phones were either large bricks or embedded in cars, when operators realized that they had to secure access to their networks. U.S. carriers alone were losing well over half-a-billion dollars a year by the mid 1990s due to cloning fraud, where a mobile is covertly reprogrammed with the identity of another. This not only affected the operators, but also the subscribers who ended up absorbing the costs of fraud and who might also be distressed by a huge bill, even when it was later forgiven by the operator.

The method developed to protect the network by about 1990 was similar for all cellular technologies. The mobile device and the network both have a secret key, a methodology known as symmetric key encryption. The network can verify that the mobile possesses this secret indirectly (to pass the secret key over the radio interface would immediately render it un-secret) through a challenge-response mechanism. The network picks a large random number and sends it to the mobile which feeds it and the secret key into an algorithm. The result, another large number, is then returned across the radio interface.

Only if the mobile possesses the correct secret key can it generate the correct response. The method is still secure even though the challenge random number and the response are transmitted openly. If an intruder was to take the identity of another device it would be sent a new random number and it would be unable to produce the correct response. Cryptographic authentication essentially ended cloning fraud when it was widely implemented.

Authentication protects the right of access to networks, but it does not protect communications from interception. In fact, authentication was used to protect access to analog networks, meaning that only an authorized subscriber could make a call, even though anyone with an appropriate FM scanner could listen to it.

Digital cellular communications made eavesdropping more difficult, but public wireless has never been promoted as a secure means of communication. Even when radio communications are encrypted, it is only over the wireless portion of the interface. If law enforcement wanted to eavesdrop on your communications, they would likely do so at the mobile switching centre (MSC), the hub through which voice communications must flow openly. If you really want to be absolutely sure you can talk with only the person you have called listening, you will need

to establish end-to-end encryption through a data session (and never use your phone in a public space).

Network access authentication based on a challenge/response algorithm is simple and fast and has only one major flaw for other applications: The two entities participating in the security session must have previously established a secret key. This is easy for security between a wireless device and a cellular carrier's network because the manufacturer can embed a secret key in the device and make it available to the operator. Third parties, such as online vendors, will not have physical access to a mobile and thus do not have such a simple way to establish a key.

In this situation, a more sophisticated system is needed: public or asymmetric key encryption. This has the advantage that the two entities can start the session without a pre-established relationship and, through protocols like TLS (Transport Layer Security, used in HTTPS), still give assurance that their communications will be secure even if the underlying system is not. In the case of mCommerce, one entity will be the wireless device and the other will be the bank or online store. In the case of secure e-mail or Web communications with a private network, a VPN (virtual private network) may be established in a similar fashion between a mobile device and an organization's gateways.

The main disadvantage with this powerful security methodology is that public key cryptography is computationally intensive, although this can be limited to key establishment.

Protection of communications is important, but protecting the data on a phone is just as critical. Traditionally, there has been little such protection, but then before the era of PDAs there was little stored on phones that needed protecting except perhaps the address book and a few text messages. Now that the memory capacity of some phones is measured in gigabytes, it is possible for massive quantities of data to be stored, and some of that data could be private, highly confidential or perhaps even embarrassing if made public.

One way to avoid this problem is to ensure that nothing sensitive is stored on the device itself, but rather access such data quickly and securely via the increasingly ubiquitous high-speed public wireless network in a database client/server mode.

That is a good solution for some applications, but would it would be unsatisfactory for people who need data on airplanes, when the data is in a form unsuitable for remote access or when the quantity of data is simply too great to be efficiently transmitted. For these situations, encryption of the storage space on the device is necessary. The user will then need to enter a secret, such as a password, to unlock the storage.

Even more intelligent would be to combine these capabilities: to allow data that is being worked on to be downloaded to an encrypted storage area on a device, and then to be automatically resynchronized with the database later, if updates are made.

Another looming challenge is malware designed for mobile devices – viruses, Trojan horses and phishing attacks – that can be designed to extract private data such as e-mail

addresses of contacts or credit card numbers. So far this has not been a big problem, probably due to a number of factors, including mobile operating systems being newer than PC operating systems and thus designed with security in mind, the larger number of operating systems and OS configurations in use on mobile devices and the greater likelihood that use of the data link will be detected through unexpected data charges on phone bills. This is definitely an area to monitor and security characteristics should definitely be a consideration when determining which mobile device operating systems are acceptable.

Another capability that can be useful is the ability to remotely lock or erase the data on a device. A device can be programmed so that the first time it accesses a network after it has been reported stolen it can be sent a command to ensure that its data becomes completely inaccessible.

No matter how good technology is at securing devices and their communications links, security still always has a large human component. Human beings might have perfectly secure devices, yet still choose to discuss top secret information in loud voices in a hotel lobby or on an airplane. They might print a draft report from their wireless device and leave the printout in a hotel's business office. They might still reply-to-all with information that should be for-your-eyes only.

Employees need to be educated about the importance of security. They need to know that security is in their best interest and the best interest of their company. They need to know how to use the security tools that are provided and feel that they are listened to when new tools are chosen or designed. Tools need to be designed so, while maintaining a high level of security, they intrude as little as possible.

Security is a systems problem, and needs to be considered as that. It shouldn't be an afterthought (although if you didn't think of it then, it's never too late to start thinking about it). It is not something that can be bolted on to a system – by then your secure data may have bolted from the stable.

That does not mean that systems should never be changed. It just means that every change should be thoroughly analyzed. After all, wireless capabilities are often added on to mature systems because they simply weren't available when the systems were first designed. Stopping the addition of wireless capabilities is futile because the benefits are so compelling, and it would be counter-productive because users would just be driven into a wireless underground.

Organizations need to recognize that new wireless uses are evolving, and make sure that security is considered, whether that requires the purchase of new software for devices or simply better education of users about secure and insecure ways to use the devices. ■

David Crowe is a wireless standards, technology and numbering resource consultant based in Calgary. He can be reached at David.Crowe@cnp-wireless.com.

Buyers' Guide/Preferred Trade List