

# Strong authentication eliminates risks intrinsic to the use of wireless technology

by T. Kendall Hunt, CEO, VASCO Data Security

The increasing use of wireless technology enhances the risk of identity theft and needs to be effectively secured before it can be turned into a strategic advantage. The answer to these security challenges is strong authentication. Strong authentication allows identifying the person trying to access a corporate network or application, allowing only authorized users and keeping all the others out.



*T. Kendall Hunt is Founder, Chairman of the Board and CEO of VASCO Data Security International.*

*Mr Hunt holds an MBA from Pepperdine University, Malibu, California, and a BBA from the University of Miami, Florida.*

In today's world, fast technological progress and ICT-driven organizations have become the standard. We are accustomed to new technological developments being immediately converted into practical applications and implemented in the everyday functioning of an enterprise. This is not surprising, as new trends in ICT often offer new and exciting strategic opportunities. In the last few years, wireless technology has become one of those trends. Employees are increasingly using laptops, smartphones and other mobile devices, enabling them to work from home or while on the road.

The increasing availability of wireless technology offers enterprises many advantages too. The use of mobile devices such as netbooks and smartphones allows employees to connect to company systems, check their email and search the Internet anywhere and anytime. This means that almost any location can be turned into a productive environment: a remote office, a worker's home or simply a hotspot in an airport or a hotel - even Starbucks

offers free wireless access. This gives employees the opportunity to utilize their time effectively and to establish a work/life balance, resulting in more motivated staff and increased productivity. Being able to send and receive information on-the-go creates a fluid information loop, ensuring that staff are constantly up-to-date with important developments within the company. In other words, wireless technology enables very effective communication.

But increased mobility and flexibility come at a certain price. Despite all the benefits, the use of wireless technology involves many risks. Security has always been a very important issue for companies and organizations, but the increasing use of mobile devices such as laptops and smartphones has new challenges. One of the main problems is authentication. How can you make sure that the individual using the company laptop to log in to the corporate network is really the person that they claim to be? How do you know if it is one of your employees working from home or on the

road and not a hacker trying to access your system? How do you ensure that user names and passwords are not intercepted by Internet fraudsters? How do you know that a worker's netbook or BlackBerry have not been stolen and are now being abused to log on to the corporate network?

The authentication problem is inherent to the use of wireless technology. The physical absence of the person using the mobile device always implies the risk of identity theft. As an enterprise, you have to make sure that your staff dispose of the right infrastructure and the right solutions to eliminate that risk. Only then can your organization turn the use of wireless technology into a strategic advantage. If secured, remote access to the corporate network and the use of web-based corporate applications offer obvious advantages. If not, the consequences could be disastrous often having dire financial and brand impact. Imagine that unauthorized users are able to gain access to sensitive information such as financial data or client information. It is unnecessary to explain



that it is absolutely essential that this kind of information remains well protected.

The answer to security challenges created by the increased use of wireless technology is strong authentication. The use of strong authentication or two-factor authentication solutions allows identifying the person trying to access a corporate network or application, allowing only authorized users and keeping all the other ones out. The principle of strong authentication is quite simple. Classic log-on methods usually require only a username and a password to gain access to a network or application. Strong authentication always requires more than one factor to log on, which is why it is also called two-factor authentication. Usually, it is a combination of something you know, like a password or a PIN-code, and something you have, for instance a smart card or an authentication device. Most people are actually already familiar with the principle of two-factor authentication, without being aware of it. For instance, when you need to withdraw cash from an ATM, you use your bankcard (something you have) and your PIN-code (something you know). Suppose your bank card gets stolen, the thief would still need your code to gain access to your bank account. And if anyone was able to guess or to intercept your PIN, they would still need your bank card. It is obvious that the combination of the two factors ensures a much higher level of security than the use of only one factor.

The same principle can be applied in enterprise security. Today's enterprises often deal with similar authentication challenges, such as securing remote access. Remote access to company networks and applications goes hand in hand with the increased use of laptops and other mobile devices, and offers many advantages. Today's employees work from home, or on the road. Enterprises that are operating worldwide hire employees all over the world, allowing them to work from remote home offices while still being able to access all the necessary applications. But

they need to ensure that only authorized users are able to gain access to important data and corporate information; remote access needs to be effectively secured. If remote access is only secured with a weak static password, it becomes easy for fraudsters to intercept or simply to guess the password.

Most people tend to use easy to remember passwords, such as their pet's name or their children's birthday. This kind of information can be easily obtained, for instance from social network websites such as Facebook. Imposing a strict password policy rarely helps, as complex passwords and regular password changes tend to be confusing for many employees. This often results in the writing down of passwords, which is of course all but helpful in improving security.

Strong authentication drastically increases the security level of remote access solutions. Authentication devices are able to generate so called dynamic or one-time passwords (*OTPs*), which replace the use of static passwords. Dynamic passwords are valid for a limited amount of time and can be used only once. This means that even if a fraudster was able to intercept a password, they would not be able to use it again. The employee is only able to log on using something they know, for instance a username or a PIN-code, and something they own, meaning the authenticator used to generate the dynamic password. This solution is not only very effective, protecting the corporate resources from unauthorized access, but also very user friendly, as it becomes unnecessary to remember complex passwords or change them on a regular basis.

Strong authentication can be used not only to secure remote access, but also all other corporate applications. One of today's ICT trends is Software as a Service (*SaaS*), the use of web-based company applications hosted on external platforms. This trend also goes hand in hand with the flourishing of wireless technology, as you only need an Internet connection to be able to access your company's web-based applications. Having a laptop or a netbook, employees can work with these applications anywhere and anytime. The principle of strong two-factor authentication can be applied here as well. Employees will use an authenticator to generate a one-time password and log in safely, ensuring that only authorized users gain access to the application.

One of the big advantages of strong authentication devices is that they can take

the form of hardware as well as software authenticators. Hardware authenticators are usually little devices, which can be carried around easily in a pocket, a purse or even on a key ring. Software authenticators also come in different forms and can be installed on the user's computers, laptops and even mobile phones. In the context of the increasing use of wireless technology, this is a very important feature. Employees already equipped with laptops, smartphones or even regular mobile phones, can use these mobile devices to implement an authentication solution. This way, the same tools used to benefit from the advantages of wireless technology also become the carriers of the authentication solutions used to secure access to corporate networks and applications.

In today's enterprise context, wireless solutions offer many advantages. Both employees and companies benefit from the increased mobility and flexibility. Employees are able to work anywhere at anytime, allowing better time management and a better balance between work and private life. The company can manage the communication and information flow more effectively, keeping everyone constantly up to date. But wireless technology also brings along an increased risk of possible identity theft and abuse, and needs to be effectively secured before it can be turned into a strategic advantage. Strong authentication drastically decreases the risk of password abuse and allows employees and companies to fully benefit from the opportunities offered by the increasing use of wireless technology. ●

