



How safe is your mobile data?

Last month the Assistant Information Commissioner Mick Gorrill urged organisations to make sure they encrypted all mobile devices such as laptops and PDAs, to protect against the risk of data loss or theft. With the use of mobile data growing all the time, from in-vehicle solutions to smart phones, and the amount of data captured increasing too, the necessity to address the issue of data security is not going away, writes Dan Worth.

The Mobile ID Unit is proving very popular with Border and Port Authority Police, as well as the National Football Unit. It is set up to only hold a minimal amount of information before it is cleared.

Chris Paddock from Microbus, a supplier of both encrypted and unencrypted mobile data solutions, re-enforces the point that many vehicles used by the emergency services require access to confidential information, which is why it's vital this information can only be accessed by those who have the necessary permission to do so. What if the device storing this information (or the vehicle itself) was stolen?

Protecting data is done in three ways, outlines Paddock. "You can use software to encrypt the data on the storage medium, making it impossible to read unless you have code that unscrambles it. Secondly, the storage medium can be protected by additional hardware so only those with the necessary passwords and 'tokens' – such as a USB dongle – can access the information. And thirdly, the data can be sent and stored on remote hard-drives so no data is stored in the terminal that sends it, thus removing the risk of it being stolen."

Sending information to be stored remotely means technology can work independently of personnel in vehicles, increasing the scope of work the technology can offer. Technology like Automatic Number Plate Recognition (ANPR) can be programmed to record and send information back to a central, secure location without the need for officers to operate the technology. "This means if a vehicle is captured on ANPR that's of interest to the emergency services for reasons above the security

clearance level of the officers in the car, then the time, data, and location of where the data was recorded can be captured, and sent to a secure location, without the officers in the vehicle knowing it has happened and without retaining the data in the vehicle."

Microbus supplies a large number of police forces with mobile data units for installation in vehicles, and the Metropolitan Police use 1,700 of its units to allow officers access to the PNC. While Microbus supplies the units to the emergency services, the encryption technology itself is provided by Stonewood Group, whose products are used by central government, local governments and emergency service users.

Stonewood's Andy Donaghue observes that the need for encryption has risen for a number of reasons. Firstly, software that previously protected unencrypted data is now easily infiltrated by basic attack tools. Secondly, as the use of mobile data has risen so more emergency services personnel are working remotely from the main site – either in-vehicle, in shared offices with local authorities, or even from home. "This means information they access remotely must be encrypted." Finally, there are now far greater implications for lost data, as seen by the Cabinet Office's Directive to encrypt mobile data and devices, and supported by the Information Commissioner's Office. "The Information Commissioner has to be informed about any losses and this is invariably reported in the media. However,

if data is lost, or stolen from a vehicle, and it's encrypted, then the loss is negated because the data will not be accessible."

Stonewood supply a wide range of end users, and its encrypted hard drives are the preferred choice of NATO for use in regions such as Iraq and Afghanistan. "Since then we've expanded the use into areas such as emergency services. On the back of this we have recently launched a brand new range of encrypted hard-drives called Eclipt that offer additional benefits – such as multi-user access, 256-bit encryption and a two-level drop in the data's protective marking – and conform to all necessary encryption standards such as the American Federal Information Processing Standards (FIPS) and the British government's Communications-Electronics Security Group." Furthermore, Donaghue emphasises that this encryption is seamless when used with the Flagstone and Eclipt hard drives, as they operate independent of systems.

In the field – borders and ports

APD, a leading supplier of communication and control applications, recently introduced a new Mobile ID Unit that is proving very popular in particularly with Border and Port Authority police and the National Football Unit.

John Gwynne of APD explains that using the unit, officers can check a person's name, date of birth, gender, nationality and document information in just a few seconds. This information is then formatted into a Police National Computer (PNC) query and the results displayed on the device's screen and the information stored on the terminal. To avoid the potential data risk of too much information being stored on one piece of equipment, the device is set up to only hold a minimal amount of information before it is cleared; thus also removing the risk of too much information being lost.

Gwynne notes the importance of ensuring all elements of the data chain are protected: "These days, you have to assume that those you are encrypting against are also using high-level technology and that they could be trying to hack into your systems at any stage in the connections. It's therefore crucial to encrypt the end-user device as well as the back-end system it's connecting too. It may be the case that a hacker will try to trick, or 'spoof', a terminal into believing a connection is the correct one and so will transmit data direct to the hacker."

FireLink

The fire and rescue service is currently going through a massive overhaul of its mobile data systems as part of the



FireLink programme under which all vehicles are being upgraded with new in-vehicle terminals to offer a range of benefits, one of which is greater system resilience and security. The upgrade will bring all fire vehicles interoperability on Airwave to allow communication with the police and ambulance while also ensuring all fire vehicles are on a common equipment platform. The new mobile data terminals, being installed by telent and supplied by Motorola via Airwave, will offer increased levels of encryption. David King from telent comments that many fire vehicles require access to information that needs to be encrypted, such as layouts of government buildings, or where chemicals are stored, "so it's important information like this can't be stolen or intercepted. By providing high levels of encryption on the new terminals this risk will be removed and also with the encryption on radios the firefighters and command personnel can talk freely over the networks without fear of conversations being overheard."

Communities and Local Government adds that FireLink radios encrypt all their traffic, both voice and data, and the encryption of data storage devices is being considered (within the context of the sensitivity of the information to be handled), as part of a package of security measures to protect confidentiality, integrity and availability.

Additional BlackBerry security

As mobile data devices become smaller more information can be pushed to individual users (eg officers on the beat). Smartphones are increasingly being used by police forces to access the information when out on the beat. Graham Baker from Research in Motion (RIM), which provides BlackBerry smartphones to one in six UK police officers, highlights that all BlackBerry smartphones and the BlackBerry platform have been accredited up to 'restricted' level data by the Communications Electronics Security Group (CESG). "Therefore users can be assured that sensitive information can be accessed securely and if lost or stolen, devices can be instantly wiped and disabled over the air by an appointed administrator."

To offer further levels of protection, RIM has recently introduced a new smaller BlackBerry Smart Card Reader that offers proximity controlled access to a BlackBerry smartphone using AES-256 encryption. This means that a BlackBerry smartphone, or any other Bluetooth supported device, will automatically lock itself if it is moved a certain distance from the Smart Card Reader or if the card is removed from the reader itself, providing an extra level of security beyond those outlined above.

"These days you have to assume that those you are encrypting against are also using high-level technology and that they could be trying to hack into your systems at any stage in the connections."

John Gwynne,
Product Manager,
APD.

Stonewood's new Eclipt range of encrypted hard-drives offer multi-user access, 256-bit encryption and they conform to CESG standards.