Cyber fears? Go modular

Cyber security has become an increasingly important concern over the past year. David Rowe argues that embracing radically modular computer architecture is essential if we are to make real progress in meeting the challenge

As I write this, Edward Snowden's permit to remain in Russia as a refugee from US prosecution has been extended for three years. This is a reminder of two striking events in the past 14 months that have raised public awareness of cyber security as a growing risk management problem. The other was the data breach at Minnesota-based retailer Target Corporation, resulting in the theft of credit-card numbers and other personal details of some 110 million customers.

The massive release of sensitive documents by Snowden in June 2013, when he was a contractor for the US National Security Agency, showed how even the most secretive of organisations – with huge intellectual and financial resources – can fall victim to failures in cyber security.

The Target episode drove home the magnitude of the financial and reputational costs such lapses can cause. *Time* magazine reported in August that Target's latest estimate of its total costs related to the breach is upwards of $148 million, and this probably does not fully reflect the unknowable long-term impact of reduced sales due to the reputational damage it has suffered.

David Rowe is senior strategist for risk and regulation at Misys in London.
Email: david.rowe@misys.com

Despite the obvious need to enhance data security, progress continues to be slow. In part, this is because foolproof data security is a bit like a cure to the common cold – threats are as varied and capable of environmental adaptation as the multiple viruses that bring on a cold. Potential sources of unauthorised access to data range from hardware flaws and software bugs to lapses in human behaviour. For this reason, there is no silver bullet that will ensure data-security breaches never happen again, although more thorough application of encryption technology would be a huge step forward. During a recent interview, this point was emphasised by Snowden himself, and he should know.

In considering how to proceed, it is important to realise encryption is far more easily and effectively applied in some contexts than in others. One of the most widely discussed areas of application is email.

Public key encryption will allow a sender's system to retrieve the recipient's public key and use it to encrypt the outgoing message.[1] If sender verification is essential, the document can first be 'digitally signed' by including a string that is encrypted using the sender's private key. The recipient's system then decrypts the message using the recipient's private key to produce readable content, and it can also decrypt the signature string using the sender's public key to confirm the identity of the sender. This results in a communication that only the intended recipient can interpret and only the claimed sender could have created.[2]

Such a system is still potentially vulnerable to specific types of threats directed at individual communications or individual users. Assuming the resulting email files are stored in encrypted form, however, these tailored attacks do not allow wholesale capture of private correspondence or other documents through the interception of internet traffic or by gaining access to mail servers.[3]

One important reason why encryption is both highly effective and practical in the context of email is that an archive of such communications has an obvious modular structure. Far more awkward issues arise in the context of large, integrated relational databases. In general, such databases need to be fully decrypted for selected contents to be accessed efficiently. This lays them open to wholesale theft by an intruder who gains access to the servers where they reside.

There are emerging methods of homomorphic encryption that allow certain database tasks to be performed on encrypted data directly. The problem is that the choice of encryption method requires advance definition of the types of queries that will be supported, and these are generally more constrained than those possible when the unencrypted database is available.[4]

Modular data storage using self-describing documents is far more suitable for the application of encryption than a relational database environment. Individual information modules can be retrieved in a secure environment before being decrypted and analysed to update the central document index. This allows the effective search and identification of modules that are relevant to a given analytical task. These can then be retrieved and once again decrypted in a secure environment during the performance of the task in question.

In summary, modular self-describing documents lend themselves directly to the efficient application of encryption methods in a way large relational databases do not. The need to strengthen cyber security is yet another reason why companies must move beyond decades-old relational-database technology and towards a radically modular approach to data storage, executable code design and hardware configuration. **R**

[1] Underlying this is the assumption that an effective public key infrastructure is in place to ensure the correct association of public keys and their owners.
[2] An added level of security can be created by storing each person's private key on a portable device, such as a building access card, so these keys cannot be compromised by an attacker gaining access to them on a mail server's hard disk.
[3] It is important to recognise that 'encrypted email' may only mean that files are encrypted as they pass across the internet, but not when they are stored on the email servers of either the sender or recipient. In this case, they are still vulnerable to wholesale theft if an attacker gains access to these servers. They are also available to the operators of the mail service itself.
[4] This 15-minute video featuring Nickolai Zeldovich, an associate professor at MIT, gives a good, high-level view of homomorphic encryption: http://video.mit.edu/watch/panel-2-privacy-enhancing-technologies-nickolai-zeldovich-27326