Protecting the perimeter

Information security personnel are often too interested in what is happening within the perimeter of the network and defending it against the onslaught of the massed forces of evil on the internet.

In most organisations, there are large resources put into firewalls, content filters, intrusion detection and prevention systems and so on at the perimeter.

These are very important tools in the good fight to defend the network, but we must not believe that these alone are the answers. We must also ask is the network secure.

A common and popular method deployed today is that of the proximity card and reader. Traditionally, the access cards that most people had deployed were those based on magnetic strip information on the back of the card, much in the same way as a credit card used before chip and Pin.

The magnetic strips on these cards wore out over time, and other magnetic devices in people's pockets often damaged them. They have been superseded in many organisations by radio frequency identifier (RFID) based proximity cards. This is mainly down to their usability and reliability.

As the name suggests, you only have to have the card in proximity to the reader for the information to be read and authenticated. This can often be done without taking the card from its protective sleeve or wallet.

The RFID chips being used are similar to those that have gained notoriety recently as a result of being mandated for inclusion in electronic passports for countries wishing to continue their participation in the United States visa waiver programme.

One of the concerns that this type of access card raises is similar to that raised with the introduction of the new RFID-based ePassports, which is the ability to read the details from an RFID chip and clone them to a new one and impersonate the rightful owner.

In the case of the ePassport, there are a number of technical security controls in place based on the use of public key infrastructure (PKI) solutions.

These ensure that even if one were to clone a chip, it could not be altered to impersonate another. However, these sophisticated controls are not applied to access control system proximity card chips.

The impact of an unauthorised access attempt to the building could be devastating as it is not registered as a break-in by the other security controls such as burglar alarms.

Once inside, one's imagination can run riot as to the impact, but think about introducing a rogue wireless access point to the network so that further hacking can take place externally without risk of physical compromise. Imagine the scene from the film, Ocean's Eleven.

One of the simplest ways of preventing a breach of the physical perimeter, and many

other types of breach is to require users to enter a Pin as well as presenting the card.

In this instance, there is a Pin associated with every user and their proximity card; shared Pins are not permitted. This is slightly more cumbersome for users, but only needs to be implemented at the external perimeter access points or other controlled areas within a building.

If someone loses an access card (RFID or magnetic stripe), the requirement for an associated PIN ensures that the impact of this loss or cloning is minimal. This is a similar control to that implemented by the financial institutions to reduce fraud on credit and debit cards by requiring a Pin for authorisation, not just presentation of the card details.

This is a simple method of increasing the effectiveness of card-based perimeter access control systems without impacting users too much.

This could be extended to provide different colour badges for different people in the building and not given perimeter Pins to third parties or contractors.

A small risk analysis session on the implementation of perimeter access control systems should highlight most of these issues, and appropriate countermeasures and controls to limit the likelihood and impact of a breach can then be taken.

Rits Group Head Quarters
Information Security Centre
2052 Castle Drive
Citywest Business Campus
Co. Dublin
Ireland

Tel: +353 (0) 1 6420500
Fax: +353 (0) 1 4660468
Email: info@ritsgroup.com
Web: www.ritsgroup.com