Information Security Now – 37

John Mitchell

A question in a past CISA[1] examination was along the lines of 'what is the biggest threat presented by single sign-on'. The answer, of course, was 'maximum exposure if the sign-on credentials are compromised'. And herein lies the question of identity. With logical access control we rely on pre-programmed logic to authenticates the user's identity. Once authenticated the user receives pre-assigned privileges for access to and perhaps manipulation of: applications, data and commands. If we consider the confidentiality, integrity and availability aspects of security (CIA), then correct identification, coupled with associated privilege allocation is important for all three, but absolutely essential with regard to availability and confidentiality, as these aspects relate to availability of the service to those who should have it at the time of need. Integrity may also be compromised if an incorrect person receives privileges which would allow for an unauthorised change to either data, or software. So identity authentication, assuming correctly assigned privileges, is the key to the identity corundum. In itself this does not totally eradicate the risk of unauthorised manipulation, as an authorised person may abuse their privileges, but it does reduce some of the risk. We have many ways of authenticating the identity of a person, ranging from the physiological to the entirely logical, but they all come down to either something known, something possessed, or something you are, or a combination of all three. Control in-depth is required if we are to reduce the likelihood of maximum exposure if a single sign-on is compromised. So two, or even three factor identification has become *de rigour* for remote authentication. The UK border Agency is currently using facial recognition technology for entry to the UK. The entrant requires a passport (something possessed) the photographic details of which (encoded in a chip) is compared against the face (something you are) of the entrant as scanned by a camera. Effective, but expensive due the equipment required and it does require the physical presence of the entrant. Variations of this are now being tested by to remotely authenticate the user by using a local webcam for facial recognition, but this does require some pre-registration process. It also falls down if a camera is not available. The standard on-time password generator does require a pre-registration process, but does not require a camera, thus providing more access options for the user.

My car identifies its key by a handshake protocol which authenticates the key, but it does not identify me as being its owner. Whoever has the key is seen as being the owner, so there is a flaw in the authentication process in that it is authenticating the wrong thing, in much the same way that a swipe card can track the use of the card around a building, but does nothing to validate who possesses the card. So we have very effective control mechanisms which unfortunately do not achieve their real objective which should be 'who possesses the key, or card'? So our starting position on identification has to be a control objective which can be objectively verified. This is level 4 (Managed &

[1] Certified Information System Auditor

Measured/Predictable) on both the CMM[2] or ISO 15504[3] scales. If the control objective is simply to authenticate the key, or card, then we have achieved the objective. If however, it is too authenticate the owner, then we have failed miserably. So the only true identification mechanism is likely to be something characteristic (retina, fingerprint, etc.), but this almost certainly requires some form of pre-registration and a sophisticated scanning mechanism.. This package may be both cumbersome and expensive, but offers a high degree of effectiveness in meeting the control objective. Other processes may be cheaper, but less effective, so ultimately it comes down to the materiality of the asset we are trying to protect. Which brings me neatly to ISO 2700, the Information Security standard. ISO 27000 requires the identification and classification of assets as its starting position. People are assets and thus should be classified. Some people will be considered more 'important' than others and will therefore require a higher level of authentication prior to privilege allocation. In some instances we may wish to authenticate multiple users before we allow an action to take place, such as the launching of a nuclear tipped missile. The greater the privilege(s) the higher the identification requirement.

John is Managing Director of LHS Business Control, a corporate governance consultancy. He is a member of BCS Council and Chair of the Information Risk Management and Assurance (IRMA) specialist group. He can be contacted at: john@lhscontrol.com, www.lhscontrol.com, or on +44 (0)7774 145638

[2] Capability Maturity Model
[3] Process Capability standard