



NEEDED: IDENTIFICATION AND AUTHORISATION

Both authorisation and identification functions need to work together if an IT system is to stay secure, says Guus Leeuw jr, President and CEO of ITPassion Ltd

DEAR READER, I would like to thank you, first of all, for the ten minutes of your busy schedule that you are willing to spend with me by reading this editorial.

Reading the public news papers or watching the news in the evening is not always funny, especially when the government is blamed for IT mishaps or eavesdropping on the public. I see one common topic in most of these reports. That topic is Security.

Over the last few years, security has played a big role in the IT industry. Most, if not all computer systems nowadays require the user to log in to identify themselves. This defends computer systems from unauthorised usage - or so a popular warning goes.

IDENTIFICATION VS AUTHORISATION

"Wait a minute," I hear you say, "Identification is not the same as Authorisation." That is absolutely correct and Microsoft has understood this by allowing a whole slew of security policies to be applied to users and computer systems. This, for sure, is the right way going forward: If a computer system knows who you are, or in other words has identified you, it should certainly check that you are allowed to do what you are doing. This applies to starting or installing a program, as well as viewing online contents.

Most systems, however, do not cater for this type of fine-grained authorisation. Once you are connected to a website, that website does not check whether you are allowed to view certain parts of its contents. Worse still, once you are connected to a database system, that system does not check that you are allowed to view the data that is stored in that database system.

Some end-user applications do support systematic checking of authorisation. However, I believe this should be done for many more systems. In the light of recent events, should a member of the council staff really have the authorisation to view anti-terror CCTV footage? Or should a lost CD-ROM really be such a big hassle? I don't think so (in either case).

SECURITY IS KEY

Authorisation is what security in the IT industry needs to focus on; and not only on Windows™ Systems, but across the board. There is a wide variety of LDAP platforms out there: Microsoft Active Directory, Oracle Identity Manager, RedHat IPA, ITPassion Identity Server, SUN One Directory, and so forth.

All these systems provide for a number of

processes and functions that allow fine-grained identification and authorisation, but the big problem is that these platforms do not work well together.

Heterogeneous environments mostly have two enterprise directory services, one for Windows systems, and one for UNIX or database systems. These services share some information, such as user ID and password, but they often do not share security settings. The principle role of these systems, central user and account management, is thus easily defeated.

If there was a central location for all CCTV footage, viewing anti-terror footage should only be allowed for officers of Scotland Yard. A lost CD-ROM should not be readable unless an appropriate decryption key is applied to the contents of the CD-ROM. A stolen laptop should not reveal its contents to a clever hacker.

SAFEGUARDING DATA

At ITPassion, we take IT security very seriously. We have a number of users whose contact



“If one of our laptop or desktop systems were compromised, even when the third party knows the user password to access the laptop, he would not automatically be able to see the data stored on that laptop. This can be achieved for local or central government systems as easy as it has been achieved for ITPassion's systems”

details are kept in our systems. These details cannot be read unless the appropriate software is utilised, and the appropriate authorisation is granted to the identified user. If, for example, our sales database was compromised and published to unauthorised entities, these entities would most likely not be able to view the data that we hold in that database.

Equally, if one of our laptop or desktop systems were compromised, even when the third party knows the user password to access the laptop, he would not automatically be able to see the data stored on that laptop. This can be achieved for local or central government systems as easy as it has been achieved for ITPassion's systems. Without going into too much detail, for security reasons, the system basically works because of central identification

and authorisation management, which is needed for, but decoupled from a laptop system when that is not in the realms of our corporate network.

Equally, the online backups that are taken from our laptop and desktop systems, are encrypted and can only be accessed and decrypted by the user for whom these backups were created. A lost or stolen laptop or desktop system can then easily be replaced by brand new equipment.

The use of central authentication and authorisation management products enabled ITPassion to develop truly secure systems that can virtually not be broken into, even if the SHA1 protocol is apparently not so secure anymore.

FOR MORE INFORMATION

Please visit www.itpassion.com/gt/august2008