

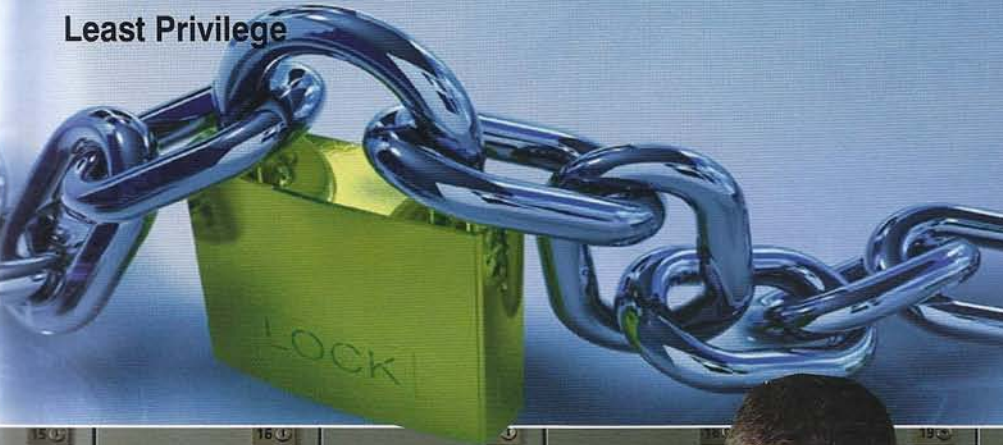
Computing Security

Secure systems, secure data, secure people, secure business

NEWS
OPINION
INDUSTRY
COMMENT
CASE STUDIES
PRODUCT REVIEWS

That's privileged!

The forgotten principle of
Least Privilege



Access all areas?

IT access management
tackles the enemy within



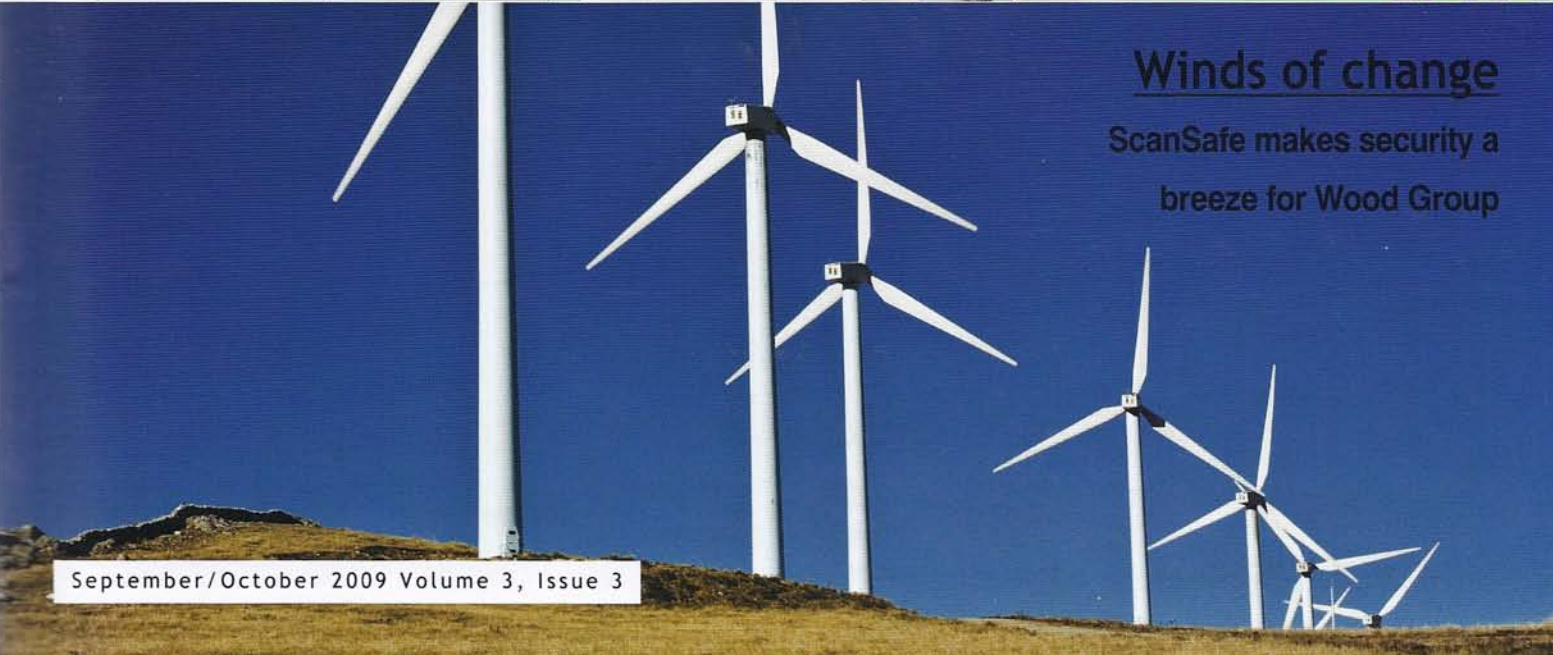
The removable threat

Securing removable storage



Winds of change

ScanSafe makes security a
breeze for Wood Group



CLICK CLICK - WHO'S THERE?

STEPHANE FYMAT, VP OF STRATEGY AND PRODUCT MANAGEMENT AT PASSLOGIX, WRESTLES WITH THE CHALLENGE OF SHARED ACCOUNT ACCESS



Failing to manage shared passwords adequately as part of an identity and access management policy, can expose organisations to serious vulnerabilities; particularly in the case of privileged accounts, where a disgruntled employee could potentially have the power to hold an entire network hostage.

Keeping track of privileged user and shared access accounts is also important for accountability. Unfortunately, however, many organisations simply don't know for sure who has access to shared passwords. Far too often the entire IT department knows the detail of what is supposed to be a limited-access password.

As a result of many high-profile incidents, legislation and industry regulations such as PCI DSS are increasingly prohibiting the sharing of accounts between users. But this causes big headaches for many IT managers in both the public and the private sector, as shared and privileged accounts have become a necessary component of today's enterprise IT infrastructure.

All kinds of employees, from office administrators and temporary workers, to nurses and civil servants, require access to shared account logons for enterprise applications and systems. IT managers therefore need to strike a balance between providing the flexibility required to meet end users' needs, and assure

security and compliance with corporate policy, and the latest industry regulations, and legislation.

So, how do they protect themselves from the risks in a cost-effective manner? To make certain of compliance - and to ensure that IT applications and systems are secure - organisations need to know who is using what shared account and when, so they can identify the culprit if data is stolen, changed, or deleted. They also need to be able to demonstrate this information in a clear audit trail.

The first step is to put in place a scalable and flexible method for regularly changing passwords, as well as a reliable way of ensuring that all passwords generated are unique on every system, and suitably complex.

The second step is to centralise shared account storage and control, so that a user must make a request to use a shared password. This can then be approved or denied based on pre-established policies, set by the organisation. This ensures that the organisation has visibility, and hence control, each time a privileged credential is used.

The more people who know a password, the greater the security threat it poses. So the next step is to ensure that all passwords for shared accounts are concealed. This prevents the inadvertent or malicious sharing of

passwords, as well as sabotage by rogue administrators. To facilitate regulatory compliance, it is also important to tie shared account usage to the user within the organisation's identity management system, so that the actual user of a shared password is known at all times.

For particularly sensitive accounts, organisations might also want to consider controlling the usage of privileged or shared passwords by policy. For example, by setting a limited time window for their use, or prescribing a maximum number of logons. A further security measure could be to introduce two-factor authentication at the point of logon, to ensure that the person using the account is actually the person authorised.

Solutions for managing shared credentials can provide a simple, secure and audit-ready approach to providing system and application access, for workers and others, who must share account passwords. They dramatically reduce the risk that enterprise systems will be compromised by the unauthorised use of privileged accounts.

Not only does this close the security gaps associated with shared password management, but it also provides a cost efficient way for organisations to comply with data protection and PCI DSS regulations that prohibit the sharing of accounts between users. CS