

Improving Windows[™] networks security with UserLock[®]

This document reviews how IS Decisions' UserLock[®] improves Windows[™] networks security by: limiting concurrent connections, restricting computers where users or groups can logon and tracking all logon/logoff activity.

Why concurrent connections are such a big deal?

Unlike most network administrators, the information security community has clearly identified threats posed by concurrent connections.

It goes without saying that the logon process is the first line of defence within the organization's network. Hence it is worth reviewing how this flaw might jeopardize the overall network security.

Generally speaking, one can come across three distinct situations:

1. *A user logs on at the same time on several workstations*
2. *A user shares his credentials with a non-authorized user, both log on at the same time*
3. *A cracker gets hold of a user's credentials, both log on at the same time.*

Here we have three different, specific threats:

- ▶ In the first situation, a single user can misuse his rights by logging simultaneously on several workstations. If another user needs one of those workstations, network administrators have to be disrupted to unlock the unattended workstation, while the careless user still uses another workstation. Network resources are unequally shared amongst users. Another possible issue is a situation where the same user might concurrently open the same file, and therefore could overwrite the wrong version of the file by accident.
- ▶ The second situation is the one where a user is irresponsible enough to share his credentials with people who belong to the same organization. A typical situation is the one found in universities where students share their username/password with friends, and let them log on at the same time on the computers of the campus. Even though this situation is common place, the threats posed are serious. Firstly it compromises the organization's confidentiality, as the illegitimate user has access to the organization's files and resources. Finally, the concurrent connection makes the legitimate user accountable for any action taken by his "friend".
- ▶ The last situation is by all means the worst case. Here we have made the assumption that the cracker has obtained a valid username/password. Then, to make things worst, he logs on at the same time as the legitimate user. This situation can happen more often than it is thought, since to improve security, users can often only log during office hours, hence for the cracker, connection is only possible while the legitimate user is already on-line. In the previous case, we naively assumed that credentials were shared with a friend/colleague. Here, we know in the first place what the cracker is up to. The legitimate user will be held responsible for all offences the cracker will commit, both within and outside the corporate network.

In short, concurrent connection introduces two major vulnerabilities.

Firstly, an unequal share of network resources which can end up in a Denial of Services for other legitimate users, and secondly, the inability to distinguish between actions taken by different individuals logged with the same credentials.

Countermeasures

To address these vulnerabilities major software editors provide their Operating Systems with some built-in capabilities to restrict concurrent connections. Novell Netware comes with this feature for years. All UNIX and Linux Operating Systems can boost their authentication features by adding PAM (Pluggable Authentication Module).

Oddly enough, Microsoft has forgotten to include this feature in its OSs (even Windows 2003 Server does not provide any means to restrict concurrent connection on workstations).

As an afterthought, Microsoft has shipped in its Resource Kit a buggy utility called CConnect, which actually introduces new serious vulnerabilities instead of mitigating the original ones.

UserLock® improves dramatically Windows™ security standards

Where Microsoft utterly fails, UserLock® succeeds.

It definitely plugs the security hole left by Microsoft: thanks to its exclusive technology, it is highly effective restricting connections.

Unlike in Microsoft CConnect, no session is opened during the authentication process, leaving no chances to eventual attacks.

The good news is that the effectiveness and robustness of UserLock® come with additional features that make the network administrator's life easier:

Connections restriction with high granularity

Based on usernames or groups, UserLock® enforces stricter logon policies:

- ▶ Sets the number of authorized simultaneous connections
- ▶ Restricts the computer(s) where users can logon, either by computer name(s) or IP range.

Rich auditing and monitoring capabilities

Real-time monitoring is a "must" for a sound network administration.

UserLock® notifies in real-time most sensitive logon/logoff events through pop-up or e-mail, and tracks all related logon/logoff activities through CSV log files for subsequent thorough analysis.

UserLock®'s focus on logon/logoff activities makes spotting suspicious logon attempts far easier than with Windows native Event Log Viewer: with such a powerful feature, network administrators can easily keep a watchful eye on all logon/logoff events that might happen on their networks.

Network administration made easier

Software deployment in distributed systems is a nightmare for administrators.

UserLock® spares administrator the pain of editing logon scripts or Active Directory group policies for software deployment.

Once installed on a server, UserLock® seamlessly deploys its agents on every single workstation.

All administration tasks are performed through an MMC (Microsoft Management Console) which makes UserLock® easy to integrate with other standard Windows administration tools.

Conclusion

Microsoft has neglected this security feature leaving Windows™ networks exposed to a number of attacks. Therefore, it appears mandatory to implement effective measures to enforce tighter logon policies.

UserLock® fulfils all these requirements and goes beyond: it educates end-users by forcing them to not share their credentials and/or use more than one workstation.

Furthermore, it provides administrators with an accurate, real-time picture of logon/logoff activities within their networks.