Subject:	Security Profiles
Date:	October 2001
Reference:	TA0152

What level of security is available on my SCO OpenServer 5.0.5-5.0.6?

Installation – Security Profiles *{Excerpt from Brian McBee of the SANS Institute}*

The choices for Security Profile are (in order of increasing security):

Low – Allows anything for a password, including a null password. Allows unlimited password failures. Default umask is 022. No C2 features. All users can schedule jobs. Home directory permissions are set to 755. 8 significant characters in password. Use of the su command is not logged. No use of shadow passwords.

Traditional – Same as Low, except: Minimum password length of 3 characters. Allows 99 failed login attempts and pauses 1 second between each attempt. Clears SUID/SGID bit on writing to a file. Logs use of the su command. Adds shadow passwords.

Improved – Same as Traditional, except: Expires passwords every 42 days. Password lifetime of 365 days. Minimum password length 5. Passwords are checked for triviality. Passwords are required for login. Maximum of 9 unsuccessful login attempts. Delay 2 seconds between attempts, default umask 027. User accounts cannot be deleted. All users are locked out if the security database is corrupted. Trusted Computing Base is used.

High – Same as Improved, except: Minimum time between password changes is 14. Password lifetime is 90 days. Passwords are generated, users cannot choose their own. Minimum password length is 8 characters. Strong password obviousness checks are in place. Maximum of 5 unsuccessful login attempts. Default umask is set to 077. All daemons must be run as a specific user.

"Improved" and "High" are intended to be C2 compliant. I would recommend setting it to "High". If your system is already up and running, you can still change this setting. Run scoadmin from the command line, select system, then security, the Security Profile Manager. It will take a reboot for any changes to take effect.