Authenticating Aptos Users Against LDAP
Some Benefits and Risks
SAM Nov 2005

Introduction

The University maintains an LDAP (Lightweight Directory Access Protocol) database which holds basic information about all individuals at the University (staff, students, associates etc). The key data held is username and password. This data is accessible to application software to allow authentication against the application. It is currently used by applications such as email, MeetingMaker, SITS eVision. It is also intended to be used by the University Portal currently in development.

It is possible to authenticate Aptos users against LDAP. This would mean that passwords would be held not in the Aptos application, but only in LDAP.

The benefits and risks of this approach are presented below:

Benefits

- The user would not have to remember multiple passwords. They are therefore less likely to write down the password and compromise security.
- Users may be less willing to share passwords which also give access to e-mail accounts (and hence personal data)
- There is less chance of fraudulent changes to passwords (currently changed by system administrator on request by phone or email)
- Much time is wasted across the University while users wait for forgotten or expired passwords to be reset
- Password administration consumes a large amount of system administrator effort across the University
- Maintenance of multiple passwords presents the risk that access to all systems may not be removed when a user leaves the organisation
- Single Sign On (SSO), via a common password will be the authentication method used by the University Portal. Any web-enabled application using LDAP authentication will be more easily integrated with the Portal.

Risks

- If the single user password is compromised then a hacker (internal or external) can gain access to multiple applications
- The current system does not enforce password ageing or formatting (this could be investigated further if required). This may not be acceptable to auditors