Minimum Standards for Security of Devices on UCInet

Appendix A - (DRAFT)

Summary: The following minimum standards are required for devices connected to UCInet.

1. **Software patch updates**
   Networked devices must run software for which security patches are available in a timely manner. They must also have all currently available security patches installed. Exceptions may be made for patches that affect the usability of the device, critical applications, or attached devices. See the **Exceptions** section of this policy for more information on how to get an exception.
2. **Anti-virus software**
   Anti-virus software available for any type of device must be installed, running and up-to-date on every device, including clients, file servers, mail servers, and other types of networked devices.
3. **Host-based firewall software**
   Host-based firewall software available for any type of device must be running and configured on every device, including clients, file servers, mail servers, and other types of networked devices. Departmental firewalls do not necessarily obviate the need for host-based firewalls.
4. **Passwords**
   Campus network service providers must have a suitable process for authorizing any use of shared services under their control. Most of the time this is referred to as an "account".
   - No user accounts shall exist without passwords or some other authentication system (e.g. smart cards). These measures must meet the minimum complexity requirements specified in the Implementation guidelines.
   - Where possible, devices must be configured to enforce the minimum password complexity requirements.
   - All default passwords for network - access able devices accounts must be modified.
   - Passwords used for privileged access must not be the same as those used for non- privileged access.
5. **No unencrypted authentication**
   Unencrypted authentication can be monitored across networks, and the information gathered can be used to gain access to services by unauthorized users. Therefore, all authentication over the network must be use only encrypted authentication mechanisms. Insecure services such as telnet, FTP, POP, and IMAP must be replaced by their encrypted equivalents.
6. **No unauthenticated mail relays**
   No devices on UCInet may provide SMTP service that allows unauthorized third parties to relay email messages (i.e. neither the sender or receiver is a local address). Authentication for use of the SMTP service must use an account and password; authentication via IP address or domain name is not sufficient to meet this standard.
7. **No unauthenticated proxy servers**
   Unauthenticated proxy servers may enable an attacker to use the proxy to attack devices on or off-campus, hiding their identity, and it may allow relaying of email spam. Therefore no unauthenticated proxy servers are allowed. Authentication for use of the proxy service must use an account and password; authentication via IP address or domain name is not sufficient to meet this standard.
8. **Physical security**
   Unauthorized physical access to an unattended device can result in any number of unauthorized actions such as sending of email, modification of data, etc. Where possible and appropriate, devices must be configured to "lock" and require a user to re-authenticate if left unattended for more than 20 minutes. Physical restraints or locking devices must be used on mobile computing devices (laptops, PDAs, etc) to prevent theft.
9. **Unnecessary services**
   If a service is not necessary for the intended purpose or operation of the device, that service shall not be running. This includes, but is not limited to, services such as echo, chargen, discard, and daytime.

Updated: February 17, 2010