

Cyber-safety Workgroup Report

June 2006

Background

The UC Davis Cyber-Safety Program policy (PPM 310-22) was adopted in May 2005. This policy established 14 computing security standards for UC Davis and an annual compliance reporting requirement for campus units. The first campus reports describing compliance with the Cyber-Safety security standards were submitted by campus units in fall 2005. Overall, these initial reports indicated a high level of compliance among administrative units and highlighted several challenges that academic units face in their efforts to comply with the security standards.

In spring 2006, a workgroup (see Appendix A for workgroup membership) was convened to review and clarify the security standards, and to propose improvements to the reporting tool. Additionally, the workgroup was asked to identify new central security program initiatives that would encourage and support campus units in their efforts to comply with the highest priority security standards. This report summarizes the workgroup discussions.

Security Standards

The security standard changes suggested by the workgroup consisted of language clarification, a repositioning of one security standard from the high priority list to the secondary priority list and the addition of two new security standards. The language clarifications are reflected in Appendix A and the revised priority list is shown below in Figure 1.

Figure 1
Cyber-Safety Security Standards

High Risk Areas

- Software Vulnerabilities
- Virus Infections
- Weak Authentication
- Insecure Personal Information
- Firewall Services
- Unnecessary Computer Programs/Services

Moderate Risk Areas

- Physical/Environment Controls (Previously listed within the High-Risk Area)
- Spam Generation
- Open Proxy
- Audit Logs
- Backup/Recovery
- Security Training
- Spyware Removal
- Data Removal Prior to Hardware Retirement
- Campus Unit Incident Response Plans – New
- Web Application Security - New

The two new security standards were added in response to new system-wide security recommendations. The provisions for documenting a campus unit incident reporting process and defining Web application secure coding requirements were discussed in the UC Information Security Workgroup Report, released in August 2005 (http://www.ucop.edu/irc/docs/info_sec_workgrp_final_report_2005.pdf).

Annual Reporting Tool

The workgroup suggested streamlining of the 2006 reporting survey to focus on the highest priority security standards rather than all 16 security standards. The focus on the six high priority standards should not be construed as a de-emphasis on campus unit compliance with all 16 security standards. However, the workgroup believed that the maximum campus security gains would be achieved by learning how well campus units comply with the first six highest priority security standards and by supporting compliance efforts in these six areas. The suggested questions for the 2006 Cyber-safety survey can be viewed at <http://www.zoomerang.com/recipient/survey-intro.zgi?p=WEB225CR3WVYF5>. The final survey instrument may be delivered by another method; however, the above Web site provides a representation of the content and format of questions for the 2006 survey.

Central Security Program Enhancements

According to the 2005 Cyber-safety annual reports, several UC Davis units reported that resource limitations prevented compliance with the Cyber-Safety security standards. Budget constraints have limited resource redirection to technology maintenance and support, while use of technology in campus units has increased over time. The Cyber-Safety workgroup prepared a list of new central security initiatives which could supplement individual campus unit security initiatives (see Figure 2). Developing and maintaining centralized security programs that could be used by campus units is, in many cases, more effective and cost efficient than an individual campus unit approach that is duplicated repeatedly throughout the university, and not maintained consistently across units. Moreover, central security program offerings, where practical, permit campus units to focus on the development and support of their unique technology needs. It should be noted that while central security technology initiatives can be developed, the university computing environment will become more secure only if those campus units in need of such security services actively support the initiatives through policy and active use.

Figure 2
Proposed New Centrally-Managed Security Programs
To Support Cyber Safety Compliance

<p>1. End-Point Security Solution</p> <p>Mandatory security compliance upon network connection for selected campus unit VLANs, ResNet and Wireless. Costs include hardware, software and labor.</p>
<p>2. NW Firewall Subsidy - Three Years</p> <p>a) Campus subsidization of VLAN firewall device activation and specific network costs related to network firewall use. Supported firewall costs include activation, NOC support and first year maintenance support costs for at least 30 VLAN firewalls for each of the next three years. Campus units will be responsible for subsequent year firewall maintenance/support costs (about \$2K per year).VLAN firewall subsidy to support DES labor and either for lowest cost Juniper firewalls or OpenBSD firewall.</p> <p>b) Campus subsidization of activation and annual 1GB network connection costs for a justified 1GB network firewall.</p>
<p>3. Campus-wide Internet Tools AV License</p> <p>Additional costs for AV license covering students, staff and faculty</p>
<p>4. Central Patch Management Server (Windows/Linux)*</p> <p>Provide central patch management server for campus unit use.</p>
<p>5. Central AV Update Server*</p> <p>Provide central AV update server for campus unit use.</p>
<p>6. Acquire Campus Software License(s) for Identification of Personal Information in Storage</p> <p>Site license for search utilities, e.g., Powergrep</p>
<p>7. Increase Number of Annual Audits for Cyber-safety Compliance</p> <p>3 years of contract funding for 1.0 FTE IT technical auditor</p>

Summary

The UC Davis Cyber-Safety Program policy represents a significant step towards improving the computing security environment at UC Davis. The Cyber-Safety workgroup has proposed a number of measures to improve the implementation of this policy within UC Davis. As campus units prepare their respective 2006 annual security compliance report, it is important that the security standards be clear and in order to reduce opportunities for misinterpretation and reporting errors. Furthermore, focusing 2006 compliance reporting on the highest priority security standards will permit campus units to address on security standards that represent the highest risk areas and will yield the greatest campus security improvements.

Finally, the Cyber-Safety program will be further strengthened by the development and maintenance of new centrally managed security programs that will promote efficient and effective information technology deployment by UC Davis campus units.

APPENDIX A: WORKGROUP MEMBERS

Matt Bishop, Computer Science
Randy Buechner, Veterinary Medicine
Michelle Fulton, College of Engineering
Adam Getchell, College of Agricultural and Environmental Sciences
Tim Hediger, Internal Audit Services
Tom Kaiser, College of Agricultural and Environmental Sciences
Bob Kehr, Land, Air and Water Resources
Greg Loge, College of Biological Sciences
Minh Nguyen, College of Letters and Science
Robert Ono, Information and Educational Technology
Steven Roth, College of Letters and Science
Paul Waterstraat, Geology

APPENDIX B

UC DAVIS SECURITY STANDARDS

(Refer to PPM 310-022 for a discussion on exceptions)

I. Level 1 Practices (Highest Priority)

A. Software Patch Updates

Computers connected to the campus network must use an operating system and application software for which the publisher maintains a program to release critical security updates. Campus units must apply all currently available *critical security updates* within seven calendar days of update release or be able to mitigate the related security vulnerability.

Exceptions may be appropriate for specialized and/or research operating systems, patches that compromise the usability of an operating system or application or for patches for which the installation is prohibited by regulation.

B. Anti-virus Software

Anti-virus software must be running and updates must be applied within no more than 24 hours of update release for *computing hosts* connected to the campus network.

This standard applies to computers and PDAs connected to the campus network using Windows, Mac OS X and Linux, Palm or Windows Mobile PC operating systems.

C. Non-secure Network Services

Computers connected to the network must use only network services/processes that are needed for their intended purpose or operation. All unnecessary services must be disabled. Where such services are operationally required, the available encrypted equivalent service must be used (e.g., SSH rather than Telnet) if data of a restricted nature such as passwords or other confidential information will be transmitted by the service. This standard applies to computers using the Windows, Mac OS X or Linux operating system.

D. Authentication

Campus electronic communications service providers must have a suitable process for authenticating users of shared electronic communications resources under their control.

1. No campus electronic communications service user account shall exist without passwords or some other secure authentication system, e.g. biometrics, Smart Cards.
2. Where passwords are used to authenticate users, the password selection method must be configured to prohibit the use of passwords found in common dictionaries or match the account name.
3. All default account passwords for network-accessible devices must be modified upon initial use.
4. Passwords used for privileged accounts must not be the same as those used for non-privileged accounts.
5. All campus devices must use encrypted authentication mechanisms unless an exception has been approved by a senior administrator. Unencrypted authentication mechanisms are only as secure as the network upon which they are used. Any network traffic may be surreptitiously monitored, rendering unencrypted authentication mechanisms vulnerable to compromise.

E. Personal Information

Campus units must identify departmental computing systems and applications that store personal information (personal name along with Social Security number, California driver identification number, or financial account information). Personal information must be removed from all computers for which it is not required. If the personal information cannot be removed from the computing system, the campus unit must develop a plan specifically outlining how the information and systems will be kept secure. Measures to protect the information could include removing several digits from the personal identifiers, moving the files to removable media and storing this media in a secure location apart from the computer, or encrypting the personal information.

Campus units providing electronic personal information, as defined above, to another party must do so by a formal agreement. The agreement must

include a provision that replicates this data standard for the party receiving the electronic personal information.

Campus units that develop network-based applications that host personal information must use secure application coding practices (see Web Application Security Standard within Level 2 Security Practices).

F. Firewall Services

Campus units must deploy and maintain both a network (VLAN) firewall and host-based firewall service for network connected computers. The firewalls must be restrictively configured to deny all traffic unless expressly permitted.

II. Level 2 Practices (Secondary Priority)

A. Physical Security

Unauthorized physical access to an unattended computing device can result in harmful or fraudulent modification of data, fraudulent email use, or any number of other potentially dangerous situations. In light of these risks, where possible, devices must be configured to "lock" and require a user to re-authenticate if left unattended for more than 20 minutes. Portable storage devices must also not be left unattended and be protected from data theft or unauthorized data modification or deletion. Physical security measures protecting computers hosting critical or sensitive university electronic communication records from theft must also be implemented. The use of data encryption may mitigate the security risks related to a physical security breach.

B. No Open Email Relays

Devices connected to the campus network must not provide an active SMTP service that allows unauthorized third parties to relay email messages, i.e., to process an e-mail message where neither the sender nor the recipient is a local user.

C. Proxy Services

An unrestricted proxy server for use from non-university locations is not allowed on the campus network. Use of an unauthenticated proxy server is not permitted on the campus network unless approved as an exception to the campus security standards by a senior administrative official. Although properly configured unauthenticated proxy servers may be used for valid

purposes (e.g. a caching proxy for local LAN users), such services commonly exist as the result of inappropriate device configuration.

Any proxy server for use from non-university locations must ensure that

1. all users are authenticated, and that
2. all users meet the criteria used to qualify for access to campus licensed intellectual property such as online journals restricted to UC Davis IP addresses.

D. Audit Logs

Campus units must develop and implement a policy defining the use, inspection and retention of audit logs. Audit log inspection may permit the identification of unauthorized access to sensitive electronic communication records. The use of audit logs should be extended to document activities such as account use and the network source of the login, incoming and outgoing network connections, file transfers and transactions.

E. Backup and Recovery

Campus units must develop, implement and maintain a backup plan for restricted information residing on electronic storage. The backup media must be protected from unauthorized access and stored in a location that is separate from the originating source. The backups must be tested to ensure recoverability from the backup media.

F. Training for Users, Administrators and Managers

A technical training program must be documented and established for all systems staff responsible for security administration. In addition, campus unit administrators and users handling restricted university electronic communication records must receive annual information security awareness program training regarding university policy and proper information handling and controls.

G. Anti-Spyware Software

The use of programs to identify and remove spyware programs is strongly advised to help to maintain the privacy of personal information and Internet use. The use of an anti-spyware program must be accompanied by installing program updates on regular basis to ensure the ability to detect and remove new spyware or adware programs. This standard applies to computers connected to the campus network using Windows operating systems.

H. Release of Equipment with Electronic Storage

All data must be removed from electronic storage prior to being released or transferred to another party. Data removal must be consistent with physical destruction of the electronic storage device, degaussing of the electronic storage or overwriting of the data at least three times. A “quick” format or file erasure is insufficient.

I. Incident Response Plan

Campus units must develop, publish and maintain an incident response plan. An incident response plan will identify immediate action to be taken upon incident discovery, investigation, restoration and reporting.

J. Web Application Security

Web applications developed or acquired by campus units must support secure coding practices. Web applications must mitigate the vulnerabilities described within the OWASP Top Ten Critical Web Application Security Vulnerabilities.

III. DEFINITIONS

Anti-virus software--A program that searches a computing device for evidence of a resident virus and removes the virus program from the device. An antivirus program is expected to include an auto-update feature that enables the program to download profiles of new viruses so that it can check for the new viruses either on the computer device or targeted towards the computing device as soon after a virus is discovered.

Campus electronic communications service providers--A unit, organization, or staff person with responsibility for allowing access to any part of UC Davis’ electronic communications resources.

Computer service or process--A general term for a program that is being executed in the background of the computing device. Windows services and Unix processes load and start running as a fundamental part of operating system initiation whether or not anyone logs into the computer.

Computing hosts-- This term is defined as computers and personal digital assistants (including smartphones).

Critical and sensitive university electronic communication records--See UC Business and Finance Bulletin IS-3 and Section 310-016.

Critical security updates--An operating system or application update that corrects a vulnerability whose exploitation could allow remote control of the computing device, the propagation of an Internet worm without user authorization, a denial of service condition, or an escalation or reduction of account privilege. Typically, the availability of a critical security update indicates the broad availability of exploit code that can take advantage of a computing device with the uncorrected vulnerability.

Incident Response Plan – A plan that describes action to be taken in response to an incident that originates from, is directed towards, or transits University controlled computer or network resources. Incident types include, but are not limited to, unauthorized access and use in violation of the acceptable use policy.

Information security awareness program training--A formal program to assist employees in understanding University policy for protecting information availability, integrity and, if appropriate, confidentiality and the role of employees in the implementation of such policies.

Native host-based firewall software--Software provided with the operating system that controls network traffic between a computer operating system and the campus network traffic. The firewall capability of the operating system may not be enabled by default.

Network Address Translation (NAT)--Internet standard that enables a local area network (LAN) to use one set of IP addresses for internal traffic and a second set for external traffic. The internal IP addresses are hidden from the external IP addresses. NAT services may be provided by a network firewall or a router.

Proxy--Acts on behalf of another whose identity may be undisclosed, creating an exploitable vulnerability for those who extend trust to the proxy.

Restricted Data – Restricted data is data that is considered sensitive to some degree. It is defined in Business and Finance Bulletin IS-3.

Senior Administrator – A dean, vice provost or vice chancellor or their delegate.

Simple Mail Transfer Protocol (SMTP)--An Internet protocol for sending email between servers or to send email from an email client program to a mail server.

Spyware--Also referred to as adware, these computer programs typically track your Internet use and report this information to a remote location. The more malicious spyware programs may capture and report actual key strokes or personal

information. The spyware programs may be installed without the computer owner's knowledge or identified in a lengthy end-user license agreement.

Technical training program--A program outlining the technical skills and knowledge required for job responsibilities. Where the position incumbent does not possess the requisite skills and knowledge, the program must outline the needed courses and course schedule. Where the system administrator possesses the requisite skills and knowledge, the technical training plan must document a plan for periodic skill and knowledge refresher courses.

Unattended computing device--A computer with an active login account that permits an unauthorized person to interact with the computing host.

Unauthenticated proxy servers--Also referred to as an open proxy, a computer that permits an unauthorized Internet user to connect through it to other network hosts.

Unencrypted authentication--The transmission of user account and password information in clear-text over the campus network.

Virtual local area network (VLAN)--A logical network of computers that appear as if they are connected to the same subnet even though they may actually be physically located on different segments of a network.

VLAN Firewall--A tool that implements security policy to control traffic between a VLAN and networks external to the VLAN.