Nomination of the

Berkeley Campus Information Technology Security Policy and the Minimum Standards for Security of Berkeley Campus Networked Devices for the

LARRY SAUTTER AWARD

June 4, 2004

PROJECT LEADERS:

Jack McCredie, Campus Chief Information Officer (CIO)
Craig Lant, Campus Information Systems Security Officer (CISSO)

TEAM MEMBERS:

Gordon Adams, Data Communication and Network Services
Kevin Burney, Business and Finance Information Technology
Jacqueline Craig, CIO's Office (now UC Office of the President)
Karen Eft, CIO's Office
Tom Holub, College of Letters and Science
John Ives, College of Chemistry / System and Network Security Office
Jeremy Lapidus, Audit and Advisory Services
George Lavender, CIO's Office / Computer-assisted Survey Methods
Jill Martin, Business and Finance Information Technology
Ryan Means, Boalt School of Law (Chair of Minimum Standards drafting group)
Sherry Rogers, System and Network Security Office
Barbara VanCleave-Smith, Office of the Controller

We also wish to acknowledge the helpful support provided by other individuals on the Campus Information Security Committee (CISC):
http://security.berkeley.edu/CISC/members.html

SUBMITTED BY:

Karen Eft, IT Policy Analyst
"kareneft@berkeley.edu, ph: (510) 642-4095

SIGNIFICANCE OF THE PROJECT:

Securing their information technology environments is one of the most important problems facing leaders of colleges and universities. Security ranks near the top in the 2004 EDUCAUSE critical IT issues survey; it is one of the critical issues identified by the University of California IT Infrastructure Task Force; and it is one of the most often cited challenges in the current IT strategic planning process at the UC Berkeley campus.

UC Berkeley's suite of new security policies, standards, and support activities represent a best practice framework that can be readily modified and implemented to benefit many other campuses throughout the University of California and the nation.

> *UC San Diego reports: "Your work has been a tremendous help to us. Making use of your pages saved us literally weeks of time." (June 1, 2004)*

> *UC Irvine has created a minimum security requirements policy using Berkeley's as a model. It is currently pending approval by our IS3 Coordinators. (June 1, 2004)*

PROJECT DESCRIPTION:

Introduction:

The University of California, Berkeley submits its new Campus Information Technology Security Policy[1] framework, the process that developed it, and the specific Minimum Standards for Security of Berkeley Campus Networked Devices[2] to the Larry Sautter Award Committee as an illustration of a new business process and set of services that defines crucial minimum security standards and that has gained wide acceptance by a diverse community of campus users.

A New Approach:

The Internet as it has existed for the past 30 years is no longer viable; the open, unauthenticated, unconstrained environment of the past is not meeting the mission critical demands everyone is placing on it today. The CERT Coordination Center at Carnegie Mellon University reported 1,334 computer security incidents in 1993 and 137,529 in 2003.[3] The continuing escalation of malicious computer attacks requires us to change the ways we approach security.

---

[1] http://socrates.berkeley.edu:2002/IT.sec.policy.html
[2] http://security.berkeley.edu:2002/MinStds/
[3] Carnegie Mellon University – Software Engineering Institute, http://www.cert.org/

Managers of our IT infrastructures must develop protection for the invaluable resources stored within our networks. The challenge is to develop a system that balances security while maintaining the access required of open research universities. Balancing security and access poses one of the greatest threats to our ability to achieve the strategic information technology visions we have for our individual campuses and for the entire system.[4] Like the rest of higher education, computing managers in the University of California have a long way to go to make our environment more secure and reliable while maintaining the kind of access required of an open research university.

Multiple layers of security are required to attack the current problems; central network controls and monitors can only do part of the job. One of the most important, and most difficult to implement, layers is the local security environment on the thousands of individual machines that taken together, make up the campus IT environment. The individual user plays an important role in IT security, but it is not easy to reach thousands of students, faculty, and staff. At UC Berkeley, we have learned that educational programs focused at users are not enough. We believe that an effective campus-wide security policy, agreed to and supported by a broad constituency, is an essential element in achieving a proper balance between security and access. Easy to use and inexpensive site-licensed security tools such as host-based firewall, anti-virus systems, and spam filters are also an important part of the solution.

The Berkeley Campus Environment:

Many factors combine to make our campus environment a "worst case" scenario for IT security policy creation, including: the use of the "Berkeley.EDU" domain as a favorite target for hackers, the budgetary constraints on a state public university, and the procedural autonomy granted to Berkeley's world-famous academic community. We faced a formidable challenge to the imposition of even basic IT security controls.

Building Support for Controls:

We first had to identify how choices about technology and support procedures are made and determine how those choices could be influenced. The issuance of the Controller's Office: "Guide to Administrative Responsibilities"[5] was a very helpful base upon which to build. Under the rubric of assisting high level campus officials identify their responsibilities, this Guide publicized specific resource management responsibilities, including in the area of "IT security". Very important, also, was that the Guide included academic individuals as "Administrative Officials".

---

[4] See, for example, Terry Gray's excellent paper "Security in the Post-Internet Era: The needs of the many vs the needs of the few" http://www.washington.edu/gray/papers/netsec2003.html

[5] http://controller-fs.vcbf.berkeley.edu/ResponsibilitiesGuide/index.htm

Ongoing security events served as an unfortunate but effective means to motivate individuals in locations where computers were victimized, but the "horror stories" did not reach everyone. In order to start *preventing* breaches we had to gain recognition by the whole campus community that changes were needed, that resources should be diverted to the problem, and that policy authority was required to enforce this.

It was important to use the power of peer groups. Individuals with very similar responsibilities could otherwise be isolated in scattered locations throughout the campus. Through venues such as technical staff mailing list discussions and "town meetings", it was agreed that campus administrative officials must be held responsible for devoting resources to IT security.

To this end, CIO McCredie participated in campus-wide planning groups and deliberated with campus executives. A major selling point was the advisability of spending preventative money up front, to avoid much higher expenditures if and when resources become breached. Another was that time and effort consolidated through centralized policy reduces the potential overall expense for separate, decentralized, efforts.

Composition of an Effective Policy Committee:

A collaborative policy-drafting process that includes diverse interests helps accommodate the needs of all constituencies to the highest extent possible, while maintaining overall momentum in the desired direction. Each Berkeley Campus "control unit" head was asked to appoint a member to the Campus Information Security Committee (CISC). Thus, the Committee consists of representatives from a wide range of academic departments and administrative areas.

CISC members have responsibilities at various levels of organizational authority, they come from units ranging in size from small installations to vast facilities, and they provide support for diverse types of environments such as esoteric research clusters versus administrative systems. Along with the majority of members who are technically conversant regarding IT security issues, CISC also has members who are experts in regulatory requirements and effective business practices.

Provisions of the Policies:

The Campus IT Security Policy built upon the responsibilities of "administrative officials" codified in the Controller's Office Guide, but then also added responsibilities for IT service providers and service users. The main point of the Policy is clearly stated: "each member of the campus community is responsible for the security and protection of electronic information resources over which he or she has control". The Policy also publicizes the broad scope of resources to be protected as including networks, computers, software, and data.

An important factor was the ability to assert a threat of denying network connectivity as a "stick" to force compliance with security requirements. To ensure that sufficient warning

of such actions could be given, a Departmental Security Contact Policy[6] had been issued earlier, requiring each department to appoint a security contact who must respond to security incident reports from central campus security staff and pass them on to responsible support personnel. This Contact Policy was accompanied by Guidelines and Procedures for Blocking Network Access[7], stating that when computers pose a serious risk to campus information system resources or the Internet, their network connection may be blocked, and specifying how this decision is made and the procedures followed.

Despite these initial policies clarifying responsibilities and consequences, our campus environment still seemed almost hopelessly mired in accelerating threats of security breaches, seemingly without any prospect of imposing a standardized environment. A contention was made in CISC meeting discussions that despite the many compelling reasons for supporting non-standardized campus configurations, some set of basic security standards could be identified for all networked devices and imposed upon the campus.

Development of Minimum Security Standards:

A CISC "minimum standards" working group pursued this quest. The members of the group held diverse opinions. After a collaborative process, in which all opinions were heard and considered, a good consensus was arrived at and the Minimum Security Standards Policy was issued. (A copy of the Minimum Standards is attached at the end of this Nomination document.)

Key features that make the Standards successful are:

- The language in the Policy and Standards is kept as simple and readable as possible. Security policies have to be simple or they'll be ignored.
- The Policy itself is basically a statement that minimum Standards must be complied with. The actual Standards are specified in a separate "Attachment" to the Policy. Thus, the Standards can be more easily adjusted. Rapid changes in technology need to be matched by rapid changes in our Standards.
- The Policy's "drill-down" format makes it easier to understand and follow. It has to work in a very complex technical environment, with users who have widely-varied levels of expertise. Successive layers allow a reader to choose the amount of detail:
    - Policy
        - Standards
            - Implementing Guidelines with technical descriptions
                - Detailed "how-to" instructions for different platforms

[6] http://socrates.berkeley.edu:2002/contacts.html
[7] http://socrates.berkeley.edu:2002/blocking.html

- The Policy, although already "issued", allows a one year grace period before compliance will be enforced. This helps overcome arguments that departments cannot afford to change non-compliant technology currently in-place. It provides a non-threatening period of time during which the campus community can consider the implications and decide what they need to do in their local environments, giving them time to budget any required enhancements.
- The Policy allows for exceptions to the Standards, but oversight by the CISC serves to ensure that exceptions are made only for bona fide reasons. This helps to overcome arguments of inability to finance required changes within the one-year grace period, or requirements for non-compliant technology for specialized applications such as research labs, for example.
- The Policy is readily expandable. Many of its simple statements can be enhanced later by adding other Appendices, or by linking to new outside documents as those become available. For example, the statement in the Policy that "devices that host restricted data … are required to conform to more rigorous security standards" will include a link to specific standards for restricted data, as soon as those standards are completed.
- The Standards accommodate open systems, not just proprietary operating systems.
- The Standards pertain to "networked devices", instead of computers. This was done in recognition of the fact that it is not only "computers" that are vulnerable to attack. We have seen compromised photocopiers, FAX machines, and network routers, to name a few examples of other devices. It is important for the campus to realize that vulnerabilities extend to these types of resources.
- The Policy includes, as a means of enforcement, a provision that we may block network connectivity for noncompliance. We currently enforce this through scanning activities (see the Technology section below).

TECHNOLOGY UTILIZED:

The policy framework we worked so hard to develop cannot stand on its own, but must be deployed in concert with education and technology. Conversely, the Policy provides an excellent framework and focus for coordinating those efforts.

Technologies used in support of the Minimum Security Standards have to be tailored and frequently adjusted to fit the changing threats. And, as our Standards change, for programmatic or other reasons, our supporting technologies have to be able to adapt as well. It's for these reasons that our framework is designed with continuous collaboration between the CISC (who oversees the Policies) and those groups, such as SNS, who deploy security technology campus wide.

Support technology includes not only the user's end of the connection ("endpoint" technology), but also centrally-deployed network traffic management systems.

Endpoint Security:

As these Policies were being developed, the context of "available technology" was always an important factor. We knew that we could not require our users to meet security standards if the technology to do so was unavailable, too expensive, or too complex to implement. In order to make the use of antivirus and host based firewall software a requirement, for example, we had to make sure that such software was readily available to our users.

Since we already had an agreement that provided Symantec AntiVirus to our entire community, it turned out to be a very minimal additional cost to provide the entire Symantec Client Security suite as well. We now require the use of the Symantec Client Security suite on all systems that are supported by it.

Our Standards require that any software (including operating systems) be kept patched with respect to critical security issues. The time between the availability of a security patch and the release of code that takes advantage of un-patched systems continues to decrease. Fortunately, many software vendors are now providing automated patching and update capabilities.

In our implementing documentation, we describe several simple ways for users to configure the most common automatic update facilities. We also distribute the "Security@Berkeley" CD that provides antivirus and personal firewall software, and is free to current UC Berkeley faculty, staff, and students.[8] While its configuration may need to be modified by some users, it is intended to satisfy the needs of most.

Centrally-deployed Technology:

It was clear we needed some level of central monitoring to ensure that even unmanaged systems would be brought into compliance. System and Network Security (SNS) had been performing scanning and intrusion detection on the campus network for some time, looking for vulnerable and/or compromised systems. But now SNS staff are able to look for compliance to the Standards. Rather than waiting for a new vulnerability to be discovered or a new worm to compromise thousands of systems, SNS can identify systems that don't meet the minimum standards and take appropriate action before they become vulnerable or compromised.

In addition to traditional scanning with open source tools such as Nessus, we're using several innovative technologies. By tracking automatic update activity on the network, we can now identify systems that are being kept up to date and we can more carefully watch for trouble on those that are not.

---

[8] See "Free protection from Internet threats: the C@B Secure CD": http://istpub.berkeley.edu:4201/bcc/Spring2004/cabsecure.html

To prevent vulnerable or compromised systems from posing a threat to our network, we are also planning to deploy network access control. Specifically, we will scan and verify systems before they are allowed to connect to our network.

IMPLEMENTATION TIMEFRAME

- The IT Security Policy was approved by the E-Berkeley Steering Committee on January 23, 2003.
- The Minimum Standards Policy was approved by the E-Berkeley Steering Committee on January 29, 2004 and issued via Campus Directive from Executive Vice Chancellor Paul Gray on April 30, 2004. The one-year grace period for compliance will end on May 1, 2005.

CUSTOMER SATISFACTION

June 3, 2004

Larry L. Sautter Award Committee:

The Larry L. Sautter Award recognizes excellent information technology practices in business processes and services. The UC Berkeley "Minimum Standards for Security of Campus Networked Devices" is an excellent example of a new business process that was developed with the outstanding collaboration of dozens of campus groups. The result is both a general policy that describes the principles and the framework for making our IT environment more secure, and a specific set of minimum standards that all systems attached to our network must meet in the coming year.

The need for a more secure networking environment is obvious, but the practical steps to accomplish this goal are not obvious at all. These minimum standards represent a campus consensus of what is technically, politically, and financially feasible and practical. The fact that many diverse groups reached a consensus enabled the acceptance and official adoption of this innovative new process that will help us protect the invaluable information resources stored in our IT environment.

These minimum security standards and the policy framework can easily be utilized and customized by other colleges and universities

Robert M. Berdahl
Chancellor, University of California, Berkeley

June 3, 2004

In the UC Berkeley residence halls we support over 6,000 users as they attach to our high-speed network with their personal computers. Because our open and high-speed network represents a desirable environment in which hackers can operate, our users are often the target of viruses, worms and other malicious attacks from both within and outside of our network. Most of our users have a version of Windows on their personal computer, and the recent string of Windows vulnerabilities and the worms that exploit them have made personal computer security our most pressing support priority.

In our user outreach and consulting services, we have stressed the importance of regular operating system updates, current anti-virus software, personal firewalls, and strong passwords as vital to the secure operations of personal computers. When we visit our users on a support call, we stress this with them and work to harden their computers as much as possible. The minimum campus security standards help us by providing a framework around which we can structure our security work. They are a set of simple but powerful guidelines that help make the online environment safer and less troublesome for our users, and the campus guidelines mirror the guidelines that we have developed in-house. As a policy document, the standards also help us to ensure compliance with our computer security recommendations. Having a campus-wide policy lends legitimacy to our own security policy and allows us to require that users meet our standards or face removal from the network. This strong but sensible policy combined with active implementation of its provisions allows us to effectively address the most pressing computer security issues among our users, making life easier for both our users and us as administrators.

Brad Andrews
Manager, Residential Computing

June 3, 2004

When Jack sent out the announcement about the Sautter Award, the minimum standards came to mind right away. They are groundbreaking, and I hope this achievement is recognized, as well as the committee members who worked so hard formulating them. Kudos to all of you!

At the UC Berkeley School of Law (Boalt Hall), we have about 1,250 students, faculty, and staff with a wide variety of hardware configurations, operating systems, and other software packages.

As one of the first implementers of the Minimum Standards, we have recognized their enormous value in furthering the mission of the School. Before implementing the Minimum Standards, we spent the majority of our time dealing with security issues. Since

bringing the Law School into compliance with their established baseline, we have reinvested the effort once consumed by day-to-day incident response into other goals that directly further our Mission. And now, the amount of time we spend dealing with computer security issues is trivial.

Patricia Donnelly
CIO & Director, Information Systems
& Technology (Law)

ATTACHMENT

Minimum Standards for Security of Berkeley Campus Networked Devices

The following minimum standards are required for devices connected to the campus network.

1. Software patch updates

Campus networked devices must run software for which security patches are made available in a timely fashion. They also must have all currently available security patches installed. Exceptions may be made for patches that compromise the usability of critical applications.

2. Anti-virus software

Anti-virus software for any particular type of device currently listed on the Campus software distribution website (http://software.berkeley.edu) must be running and up-to-date on every level of device, including clients, file servers, mail servers, and other types of campus networked devices.

3. Host-based firewall software

Host-based firewall software for any particular type of device currently listed on the Campus software distribution website (http://software.berkeley.edu) must be running and configured according to the "Implementing Guidelines for the Minimum Standards for Security of Berkeley Campus Networked Devices", on every level of device, including clients, file servers, mail servers, and other types of campus networked devices. While the use of departmental firewalls is encouraged, they do not necessarily obviate the need for host-based firewalls.

4. Passwords

Campus electronic communications service providers must have a suitable process for authorizing any use of shared electronic communications services under their control. See the Guidelines for Administering Appropriate Use of Campus Computing and Network Services (http://itpolicy.berkeley.edu/approp.use.html). The mechanism for providing access to service users will be referred to here as an "account".

a. No campus electronic communications service user accounts shall exist without passwords or other secure authentication system, e.g. biometrics, Smart Cards. These measures must meet minimum complexity requirements specified in the Passwords section of the Implementing Guidelines for the Minimum Standards for Security of Berkeley Campus Networked Devices.

b. Where possible, devices must be configured to enforce the aforementioned minimum password complexity requirements.

c. All default passwords for network-accessible device accounts must be modified.

d. Passwords used for privileged access must not be the same as those used for non-privileged access.

5. No unencrypted authentication

Unencrypted device authentication mechanisms are only as secure as the network upon which they are used. Traffic across the campus network may be surreptitiously monitored, rendering these authentication mechanisms vulnerable to compromise. Therefore, all campus devices must use only encrypted authentication mechanisms unless otherwise authorized by the CISC. (See "Requests for Exception" in the Berkeley Campus Policy on Minimum Standards for Networked Device Security Configurations.)

In particular, historically insecure services such as Telnet, FTP, SNMP, POP, and IMAP must be replaced by their encrypted equivalents.

6. No unauthenticated email relays

Campus devices 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. Before transmitting email to a non-local address, the sender must authenticate with the SMTP service. Authenticating the machine (e.g. IP address/domain name) rather than the sender is not sufficient to meet this standard. Unless an unauthenticated relay service has been reviewed by SNS and approved by the CISC as to configuration and appropriate use, it may not operate on the campus network.

7. No unauthenticated proxy services

Although properly configured unauthenticated proxy servers may be used for valid purposes, such services commonly exist only as a result of inappropriate device configuration. Unauthenticated proxy servers may enable an attacker to execute malicious programs on the server in the context of an anonymous user account. Therefore, unless an unauthenticated proxy server has been reviewed by SNS and approved by the CISC as to configuration and appropriate use, it is not allowed on the campus network.

In particular, software program default settings in which proxy servers are automatically enabled must be identified by the system administrator and re-configured to prevent unauthenticated proxy services. For more information on the types of software typically used for proxy services, see the "Implementing Guidelines for the Minimum Standards for Security of Berkeley Campus Networked Devices".

8. Physical security

Unauthorized physical access to an unattended device can result in harmful or fraudulent modification of data, fraudulent email use, or any number of other potentially dangerous situations. In light of this, 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.

9. Unnecessary services

If a service is not necessary for the intended purpose or operation of the device, that service shall not be running.

The Policy mandating compliance with these Minimum Standards is the

- Berkeley Campus Policy on Minimum Standards for Networked Device Security Configurations

For additional details to assist system administrators and end-users to configure their networked devices to comply with these Minimum Standards see:

- Appendix B Implementing Guidelines

For assistance interpreting these Guidelines, or to request an exception from compliance with the Minimum Standards, contact: security-policy@berkeley.edu.
