

Security and Privacy: Workstation Authentication & Records Retention

Lori Driscoll

Peter E. Murray

Gordon Wishon

*Coalition for Networked
Information*

Spring 2004 Task Force Meeting

ARL SPEC Surveys

- v SPEC Kits are the result of a systematic survey of Association of Research Library member institutions on a particular topic related to current practice in research libraries to help institutions implement new practices and technologies, manage change, and improve performance

- v SPEC Kits comprise four key elements:
 - Executive Summary of survey results
 - Survey Questions with tallies and selected comments
 - Representative Documents from responding institutions
 - Selected Resources on the topic for further study

Library Public Access Workstation Authentication

Lori Driscoll

Associate University Librarian &
Chair of Access Services
George A. Smathers Libraries
University of Florida
PO Box 117001
Gainesville, FL 32611-7001
ldriscoll@mail.uflib.ufl.edu

Library Public Access Workstation Authentication (October 2003)

- ✓ Current events (9/11 and misuses of campus computer networks) have led campus IT administrators to re-examine network access policies
- ✓ While systems administrators have moved to restrict access to information assets, librarians have worked to support barrier-free access that protects users' privacy
- ✓ Libraries must carefully balance convenient access to information with tighter controls on access to mission-critical information technology assets

The Survey

Distributed to the 124 ARL member libraries in May 2003

- √ How are users at public access workstations authenticated?
- √ What is driving IT policy changes in libraries?
- √ Who is involved in policy decision-making?
- √ How have access controls affected services?
- √ How, with tight campus IT security, are Federal Depository libraries meeting the information needs of the public?

Sample Questions

- √ How does the access management system handle user privacy?
- √ Is authentication activity at public access workstations logged? Is log data analyzed? How long are logs maintained?
- √ Who is responsible for investigating suspected misuse of library public access workstations?

Results

- √ Sixty-seven libraries (54%) responded to the survey
- √ Authentication
- √ Authentication Logs
- √ Public Workstation Access Policy
- √ Representative Documents
 - Library Public Access Workstation Authentication Policies
 - Library Computer Use Policies
 - Parent Institution Computer Use Policies
 - Security Incident Procedures

Authentication

- 67% do not require user authentication at public access workstations in the library
- 11% require authentication at all terminals
- 22% require it only at selected terminals
- 91% were Federal Depository Libraries; this did not seem to affect authentication policy

Authentication

- Use various methods: campus LDAP servers/some form of university-wide identifier
- Non-affiliated users were either limited to workstations with minimal access or were assigned guest login accounts
- Different services available to authenticated and non-authenticated users
- User privacy was handled either through anonymous access or identified access

Authentication Logs

- Activity not logged at 65% because they do not authenticate
- Of the institutions that required workstation authentication, most kept logs of the user ID and workstation ID that corresponded to the date/time of logon/logoff
- Review was prompted by a security incident for the few respondents that ever looked at the data

Authentication Logs

- Primary data analyzed
 - search patterns
 - system usage
 - workstation usage
 - unauthorized login attempts
- Most respondents did not maintain logs or were uncertain of the period of time that logs are maintained
- Retention periods ranged from one week to indefinitely

Public Workstation Access Policy

- Several different policy approaches taken toward network security and patron privacy
- Representative group of administrators, information technology managers, librarians, students
- Factors driving policy included mandates from parent institution (35%), library administration (20%), state government, and license contracts, as well as the desire to provide access to primary clientele and prevent misuse
- Reported that security incidents are requiring more time

Public Workstation Access Policy

- 95% stated that library IT staff were responsible for investigating suspected misuse of library public access workstations
- Institutional IT staff, library administration, and campus police are often involved
- Most respondents report that additional staff and resources have been assigned to IT security tasks during the past year
- USA PATRIOT Act, other post-9/11 developments, and growth of Internet use contribute to increased emphasis

Conclusion

ARL libraries are handling public workstation access to computer networks in a variety of ways. Although the majority of libraries do not currently authenticate users at all of their public workstations, most are reviewing security policies and procedures. IT policy changes in libraries are being driven by institutional initiatives, and more resources are being dedicated to controlling network access to prevent cyberattacks, identify theft, illegal file sharing, and other unauthorized uses. Policy decisions are a result of informal groups consisting of institutional IT units, library administrators, and library IT units.

Implications

Issues of privacy and security must be carefully balanced in the management of library networks. The best security procedures preserve the privacy of users and do not interfere with user access to library resources. The results of this study indicate that ARL libraries remain committed to providing information access to users with minimum disruption in services, but there is no consensus about best practices for public workstation authentication.

Selected Policy Resources

- ✓ American Library Association. *Principles for the Networked World*. Chicago: ALA, February 2003, <http://www.ala.org/ala/washoff/washpubs/principles.pdf>.
- ✓ American Library Association Intellectual Freedom Committee. *Library Privacy Policy*. Washington, DC: ALA, 13 April 2004, <http://www.ala.org/ala/oif/iftoolkits/toolkitsprivacy/libraryprivacy.htm>.
- ✓ Kaufman, Paula T., and Gerald R. Lowell. *Checklist for Drafting Electronic Information Policies*. Washington, DC: Association of Research Libraries, 4 August 2002, <http://www.arl.org/newsltr/196/checklist.html>.

-
- v Rezmierski, Virginia E., and Nathaniel St.Clair, II. *Final Report NSF – LAMP Project: Identifying Where Technology Logging and Monitoring for Increased Security End and Violations of Personal Privacy and Student Records Begin*. Washington, DC: American Association of Collegiate Registrars and Admissions Officers, 2001, <http://www.aacrao.org/publications/catalog/NSF-LAMP.pdf>.
 - v Rezmierski, Virginia, and Aline Soules. "Security vs. Anonymity: The Debate over User Authentication and Information Access." *Educause Review* 35(2) March/April 2000: 22-30, <http://www.educause.edu/ir/library/pdf/ERM0022.pdf>.

Driscoll, Lori. *Library Public Access Workstation Authentication. SPEC Kit 277*. Washington, D.C. : Association of Research Libraries, Office of Leadership and Management Services, 2003.

<http://www.arl.org/spec/SPEC277WebBook.pdf>

Security and Privacy

Workstation Authentication & Records Retention

Peter Murray

University of Connecticut Libraries

369 Fairfield Rd, Unit 2005-A

Storrs, CT 06095-2005

Phone: 860-486-0395

Peter.Murray@uconn.edu

<http://www.lib.uconn.edu/>

April 10, 2004

Version 1.1

Security and Privacy

Background

Why Do We (Librarians) Care About Privacy?.....	1
Can We Go Overboard?	2

SPEC Kit Findings

Overview of SPEC Kit 278: Library Patron Privacy	2
Some Specifics of "Library Patron Privacy" SPEC Kit	3
Survey Results.....	4

What to do?

Web Proxy to Change Cookie Lifetime	5
Remove Internet Activity Traces from the Harddrive.....	6
More than the Internet: Office Automation Tools, Too	7

Background

slide 1

Why Do We (Librarians) Care About Privacy?

- ♣ “It is the responsibility of publishers and librarians, as guardians of the people's freedom to read, to contest encroachments upon that freedom by individuals or groups seeking to impose their own standards or tastes upon the community at large.” **The Freedom to Read Statement**

<http://www.ala.org/alaorg/oif/freeread.html>

- ♣ “We protect each library user's right to privacy and confidentiality with respect to information sought or received and resources consulted, borrowed, acquired or transmitted.” **American Library Association Code of Ethics**

<http://www.ala.org/alaorg/oif/ethics.html>

Can We Go Overboard?

I'm concerned about terrorists. Does this policy mean that the Libraries will not share important information with the FBI?

Not at all. The University of Minnesota and the University Libraries will cooperate with all legal requests for information. However, the Libraries must make sure that we inform and receive advice from the University's Office of General Counsel concerning any request, to ensure that we are complying with the law. The laws governing privacy and law enforcement investigations can be complex, and we don't expect them to be invoked often. To ensure consistent, thorough, and lawful responses, we must take care of such requests centrally.

Requests for Patron or Other Private Information

<http://staff.lib.umn.edu/computers/policies/ul-rfpi.html>

SPEC Kit Findings

Overview of SPEC Kit 278: Library Patron Privacy

- ♣ Review record retention and privacy guidelines for all areas of library operations
- ♣ Focused on established public policies for users and procedures for staff
- ♣ 47% of ARL member libraries responded

Some Specifics of "Library Patron Privacy" SPEC Kit

- ♣ Caches on Public Microcomputers
 - | Does the library have a specific policy and/or public statement regarding patron transaction activity?
 - | For how long is this data stored after the transaction is completed?
 - | What demographic information is stored?
 - | For what purpose(s) is this data stored?
 - | Which library staff has access to this data?
 - | Is this data shared with another unit in the institution? What is that unit's data retention policy?
 - | When the stored data is purged, are back up files also purged?
- ♣ Disposal of Hardware
 - | Does the library have a specific policy and/or public statement regarding this patron transaction activity?

Survey Results

- ♣ Awareness of personal data on public microcomputers appears to be low:
 - | 10% of libraries have a staff policy
 - | 9% of libraries have a public statement
 - | 5 of the 45 can associate personally identifiable information with cache data
- ♣ Lack of formal policy may not be a reflection of actual practice
 - | All reported cache data not shared outside library
 - | Some clear cache upon reboot and/or established time
 - | Access is limited to systems staff

Survey Results (con't)

- ♣ 16% of libraries have a staff policy regarding the disposition of hardware
- ♣ 12% of sites have a public statement regarding this activity
- ♣ Some local policies come from institutional policies

What to do?

slide 7

Web Proxy to Change Cookie Lifetime

Privoxy (<http://www.privoxy.org>) has a setting do this: session-cookies-only

- ♣ Typical use:
 - | Allow only temporary "session" cookies (for the current browser session only).
- ♣ Effect:
 - | Deletes the "expires" field from "Set-Cookie:" server headers. Most browsers will not store such cookies permanently and forget them in between sessions.
- ♣ Notes:
 - | Most browsers will not permanently store cookies that have been processed by session-cookies-only and will forget about them between sessions. This makes profiling cookies useless, but won't break sites which require cookies so that you can log in for transactions.

From **Privoxy 3.0.3 User Manual**

<http://www.privoxy.org/user-manual/actions-file.html#SESSION-COOKIES-ONLY>.

Remove Internet Activity Traces from the Harddrive

Public Access Computing Security Tool

(<http://www.webjunction.org/do/DisplayContent?id=1608>) from the The Bill & Melinda Gates Foundation

♣ Effect:

- | In addition to its usefulness as a tool to lock down desktop configurations, the tools will also delete temporary Internet files, saved and downloaded files, and additions to the History and Favorites folders when the session is logged off.

More information at

<http://www.pacomputing.org/pactool/>.

More than the Internet: Office Automation Tools, Too

Help Provide Security in a Public Access Environment

<http://www.microsoft.com/office/ork/2000/journ/KioskMode.htm>

“Most Microsoft Office 2000 applications maintain and display a history of most recently used files. Although this feature is convenient to users, it can post a security risk in some environments.”

“ Under Microsoft Windows 2000 only, you can install Office 2000 in a public access environment - an Internet cafe or airport kiosk - where anyone can use the applications. A business traveler might stop at the computer in an airport kiosk, connect to the company network or Web site, and open Office documents. The traveler can view, edit, and save personal files or confidential documents at the kiosk and then move on. ”

Principles to Guide Efforts to Improve Computer and Network Security in Higher Education

Gordon Wishon

University of Notre Dame
Co-Chair, EDUCAUSE/Internet 2 Security Task Force

EDUCAUSE/Internet 2 Computer and Network Security Task Force

- ▼ Established in 2000 In Response to High Profile Incidents in Which Universities Were Implicated
- ▼ Participated in development of National Strategy to Secure Cyberspace
 - ▼ Chapter Devoted to Higher Education
 - ▼ Four Principal Focus Areas
 - Education and Awareness
 - Standards, Policies, and Procedures
 - Security Architectures and Tools
 - Organization, Information Sharing, and Incident Response

National Strategy Action Statement

Make IT security a higher and more visible priority in higher education

Do a better job with existing security tools, including revision of institutional policies

Design, develop, and deploy improved security for future research and education networks

Raise the level of security collaboration among higher education, industry, and government

Integrate higher education work on security into the broader national effort to strengthen critical infrastructure

Early Efforts to Understand the Problem

- v NSF Grant to identify and implement a coordinated strategy for computer and network security for higher education
 - v Commissioning of Papers, Reports, Case Studies
 - v Meetings of Security Experts, Policy Experts, and User Community
 - v Summit on Computer and Network Security in Higher Education

Common IT Security Beliefs in Higher Education – Myth or Fact?

- ✓ IT security inhibits academic freedom
- ✓ IT security compromises personal privacy
- ✓ IT security limits access to information
- ✓ Openness and community outreach are at odds with security
- ✓ A transient student body is difficult to manage
- ✓ Faculty autonomy hinders uniform IT security standards

Source: EDUCAUSE Center for Applied Research, 2003

Higher Education Values and Principles to Guide Security Policy

- ✓ Workshop conducted Aug.2002 at Columbia University
- ✓ Based on principles articulated by various higher ed groups (AAUP, ALA, etc.)
- ✓ Invited experts
 - ✓ Librarians
 - ✓ Faculty
 - ✓ Researchers
 - ✓ Administrators

Six Principles to Guide Security Policy Development

- ✓ Civility and Community
- ✓ Academic and Intellectual Freedom
- ✓ Privacy and Confidentiality
- ✓ Equity, Diversity, and Access
- ✓ Fairness and Process
- ✓ Ethics, Integrity, and Responsibility

Civility and Community

Respect for human dignity, regard for the rights of individuals and the furtherance of rational discourse must be at the foundation of policies and procedures related to computer and network security

Academic and Intellectual Freedom

Academic freedom is the keystone of American higher education. It ensures freedom of inquiry, debate, and communication, which are essential for learning and the pursuit of knowledge. Intellectual freedom ensures information access and use, which are essential to a free, democratic society.

Privacy and Confidentiality

To the extent possible in the electronic environment, users' privacy will be preserved. Privacy must be protected in information systems whether the personally identifiable information is provided or derived. Fair information practices should govern the collection and disclosure of personal information

Equity, Diversity, and Access

Approaches to security and privacy should respect the equity and diversity goals of higher education. Access to appropriate information and the Internet should be provided equitably to all members of the community.

Fairness and Process

Access to computer systems, network and scholarly resources is a fundamental benefit of joining an academic community. Revoking or limiting that access must only be done as a result of a serious offense after which a defined process is followed.

Ethics, Integrity, and Responsibility

Computer and network security is dependent on and should be designed to further the highest standards of ethics and integrity in campus communities. Good security practices are important to the entire community and are the shared responsibility of each member.

Security Task Force Projects and Initiatives

- ✓ Education and Awareness Initiative
- ✓ Annual Security Professionals Workshop
- ✓ Legal Issues and Institutional Policies
- ✓ Risk Assessment Method and Tools
- ✓ Research and Development Initiatives
- ✓ Vendor Engagement and Partnerships
- ✓ Research and Educational Networking Information Sharing & Analysis Center (REN-ISAC)
- ✓ Effective Security Practices Guide

A Word about Best (Effective) Practices

www.educause.edu/security/guide