Workstation & Voyager Authentication Changes

Introduction

We, the faculty and staff of the UIUC Library, consider the protections of patrons' rights to privacy and confidentiality as one of our fundamental responsibilities. Not only are portions of this responsibility required by state and federal law (particularly as an academic institution), but such privacy is upheld as ethically and politically necessary in a free society. Within our profession this view is prevalent and long-standing, as evidenced by the ALA's many statements on this and related subjects[1]. Our Library's official written circulation policy[2] reflects this, and the Library administration consistently confirms this stance.

However, actual practices in our Library, coupled with the present configuration of Voyager (and DRA before that) have continuously and seriously compromised this confidentiality. We and our colleagues actively denounce many of the changes to federal law that have weakened the Constitutional Bill of Rights, such as the PATRIOT Act's provisions for FBI searches without warrant and with imposition of the "gag rule." While noble and admirable, it is pointless when Library personnel balk at even minor impacts to workflow that are necessary to prevent even more egregious violations of patron privacy.

The purposes of this document are principally:

- To describe the technical and procedural modifications we've devised to minimize the potential drawbacks to implementation.
- To define the types of information that are subject to confidentiality concerns;
- To describe the technical and procedural reasons that our current practice is unacceptable and negligent;
- To remind us of the historical technical and procedural compromises that led to this situation;
- To describe the minimum changes that must occur:
    - to maintain the level of stewardship that we already nominally claim,
    - to pass future University or state security audits, and
    - to protect the Library from potential litigation;

Examples of Confidential Information Used in the Library

The privacy-sensitive information includes but is not limited to:

- Individual demographic and identification records of UIUC students, employees, and all other library patrons;
- Patron-linked circulation and interlibrary loan records, item requests, reference inquiries, printing or billing data;
- User-specific data from web access logs, error logs, search queries, authentication logs, and the like.

---

[1] ALA Statements and Policies. http://www.ala.org/ala/oif/statementspols/statementspolicies.htm
[2] Circulation Policies — Policy on Confidentiality of Library Records. http://www.library.uiuc.edu/circ/policies.htm

Current Vulnerabilities and Other Concerns

Factors that result in the current risks of compromise include:

- Many units still use shared Voyager Operator IDs and passwords for circulation functions.
- In some units, this means that dozens of employees (including high-turnover students) know the Operator ID name and password.
- These widely-known passwords are typically NOT changed when employees transfer or terminate their jobs.
- The Voyager system does not provide any mechanism to restrict the workstations or Internet addresses from which specific logins can be used.
- From an audit standpoint, though many staff operations in Voyager are logged, only the date, time, and login name are recorded with each modification event.
- All Voyager circulation logins have complete access to all patron data that is present in the system.
- Shared circ desk workstations are configured to log into Windows automatically.
- Shared circ desk workstations are almost all in publicly-accessible locations easily viewable and reachable by anyone.
- There are occasions where circ desks and workstation(s) are unattended for a short while.

Other Concerns:

- The circ desk workstations are full-featured Windows PCs with access to the Internet at large.
- While we encourage the use of Windows' "Lock Workstation" feature when a machine in use needs to be left unattended, it is not feasible in a situation where automatic Windows logins are used.
- Some of them have Microsoft Office and other applications installed and are used for more than strictly circulation functions like charging and discharging items. As such, many units want those machines to have access to Library network file servers (G: drive in particular). This is clearly unwise in any situation where the workstation automatically logs in.
- Staff workstations frequently have software security compromises, performance problems, data loss, improperly configured desktops, icons, etc. These issues can leave a workstation unusable or significantly degraded until Systems can re-image all of the software on the machine. Too often we find these are the result of the installation of unapproved and/or inappropriate software downloaded from the Internet or brought from home. While this can occur anywhere, it is most common at circ desks where student employees work with minimal supervision. With user-specific workstation logins, we will more often be able to help the unit determine who has been misusing the computer. It will also reduce the likelihood of someone accidentally or purposely making changes that disturb other people's Windows desktop and settings.

History of the Situation

Circulation terminals used to be dumb terminals hard-wired straight to the ILCSO mainframe running LCS. As such, they could not be used to access any systems except through the mainframe, and the terminals were themselves completely isolated from all other networks including the Internet at large. In LCS, privileges were tied directly to the terminals, not people

or accounts. This remained true even after hardwired terminals were replaced with PCs, through the use of IBM terminal emulation hardware & software. With FBR, the only people with individual accounts were those who did cataloging.

Before the implementation of Voyager, the staff accounts for the DRA system were created by ILCSO staff as requested by the security contacts at the UIUC Library and other member institutions. In DRA, all accounts for the entire consortium were in one table, so ILCSO staff were the only ones who could provision or privilege accounts. For most circulation locations, there was a shared circulation account, but for acquisitions & cataloging, even student employees typically had an individual login. There was of course a communications & logistical delay in the process to get new accounts authorized and created. Due to the sheer number of student workers employed for circulation functions and their rapid turnover, ILCSO could not provide individual logins for every student employee.

As time progressed, most circulation desk procedures began logging their primary circulation terminals in when the unit opened and (sometimes) logging them off when the unit closed. Even though these shared passwords were rarely required to be changed, many units still wrote them down and posted them in plain sight. From the perspective of a circ worker, this practice approximates the situation from LCS days. The longer these practices have gone on, the more entrenched their apparent necessity has become in the minds of many employees.

Minimum Changes for Compliance

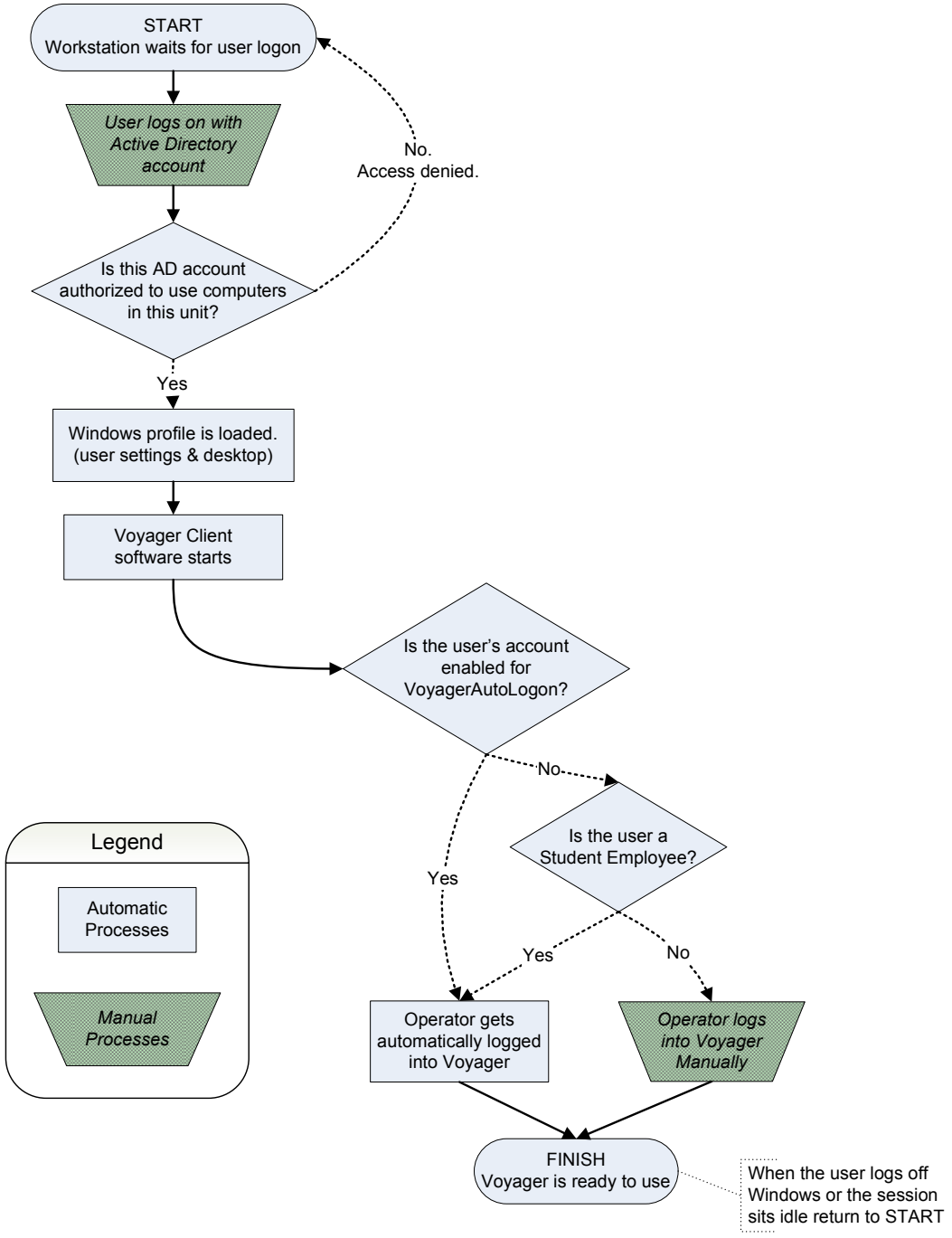
All computer accounts or other methods of access to sensitive information must be auditable – associated with a specific individual employee who has legitimate work needs for such access, and logged when possible. Additionally, such access must be disabled upon termination of employment or transfer to another position without such need. Network-access passwords can not be shared.

New Configuration and Procedures

With the integration of our Windows workstations and the campus Active Directory service, we have gained some flexibility and additional tools for managing access. CITES automatically provides Active Directory accounts for every current student and employee. In combination with software the Library Systems Office has written, it is now feasible to simultaneously provide the necessary access to the Voyager Circulation module and the Library's file and web servers without compromising our collective responsibilities as stewards of sensitive information.

Any overall solution to this problem by definition must incorporate changes to both software and employee behaviors as they relate to computers and accounts with access to sensitive information. In devising this solution we have gone through multiple revisions to avoid or minimize all impacts on workflow to the extent possible. Some change to workflow is however necessary and intended. It is not an unfortunate side-effect to be circumvented. The change can be summarized thus: **at every computer you use, log on using your Active Directory account, and log off when you are no longer personally using or monitoring that computer**.

The new configuration and procedures are represented here with a simplified state diagram:



Efficiency notes:

- It typically takes about 7 seconds to get from FINISH/logoff all the way to START.
- It typically takes about 12 seconds to get from START to FINISH.

Additional Benefits Gained

Simplifications for Employees:

- No longer will people need to memorize their unit's generic Voyager circulation usernames or passwords. Only staff who have an individual Voyager Operator ID will need to remember a Voyager password.
- Everyone's Active Directory username is the same as their NetID, making its memorization unnecessary. Additionally, you may choose to set your AD password[3] the same as your NetID password[4], reducing the need for memorizing another password.
- The Active Directory account is what all Library employees use to gain access to any Library workstation or file services.
- Large units especially will no longer have the chore of spreading the word when a shared Operator ID's password gets changed. Only the Voyager system administrators and the *VoyagerAutoLogon* program need to know it.
- Staff or students who temporarily substitute at another unit's circ desk (such as the CAMELS team) will not need to learn another Operator ID & password.

Security:

- A worker from Unit X substituting in Unit Y will also not be able to access Unit Y's happening location unless
    - They are physically present in Unit Y logged in there, or
    - They have an individual Voyager Operator ID that has specific authorization for Unit Y's location.
- The passwords for shared/generic Circulation Operator IDs will not have to be changed coincident with each departure of a student or staff employee, because they won't know the passwords at all.
- Conversely, Library Systems will be able to change the passwords for those shared Operator IDs at any time without impacting anyone.

[3] To change your Active Directory password, go to http://www.ad.uiuc.edu/accounts.aspx
[4] To change your NetID password, go to https://www-apps.cites.uiuc.edu/password/