



Innovative Practice

Accommodating Community Users in an Authenticated Library Technology Environment

Jonathan T. Younker
Brock University
St. Catharines, Ontario, Canada

Abstract

This article documents the creation of an automated kiosk that allows users not affiliated with Brock University in St. Catharines, Ontario, Canada to obtain temporary usernames and passwords for computer workstations in the library. Non-affiliated users provide certain forms of identification to automatically generate temporary accounts that comply with campus-wide security and privacy policies, as well as licensing agreements for electronic resources.

In the spring of 2006, a Brock University Campus Security officer came to the James A. Gibson Library to gather information about an incident that had recently been reported. A user of the library's computers had used a common web-based email provider to send an anonymous defamatory email to a Brock University professor, and the officer wanted Library Systems and Technologies staff to provide him with the username of the perpetrator, along with applicable log files. This was not the first time a message of this type had been sent from computers in the library, but because we provided open and unfettered access to computers to all users, students, faculty, staff, and community members alike, we simply had no way of providing the officer with any useable data.

Brock University, with a student population of roughly 17,000, is a publicly funded university located in St. Catharines, Ontario, Canada. Prior to 2006, the library had already begun planning to authenticate students, faculty, and staff, which would allow us to restrict and track inappropriate activity, while at the same time providing better technical support and customization of service. However, we still wanted to accommodate members of the public at large conducting research at the library. How could we allow community access to our resources while conforming to campus-wide authentication policies, Campus Security requests, privacy legislation, and still keeping it as a low-maintenance, self-serve solution? Like many in the world of library technology, we were faced with tight budgets, custom specifications, and aggressive timelines, so we decided to do it ourselves rather than purchase a software solution.

Planning and Rationale

The Library's Systems and Technologies department consists of two systems administrators, an Innovative Systems Coordinator, a Web and Graphics Specialist, two Copying and Printing staff members, a Digital Services Librarian, and me, the department head. I hold an M.L.S. from the University of Western Ontario and serve as manager for the library's technology-related projects and services. It fell to me to identify the goals of this project, assign work to staff, and monitor progress.

The first step was to query colleagues at other academic libraries in Ontario via telephone, email, and listservs to learn how similar-sized institutions handle computer access for members of their communities (see Appendix A). Solutions varied, and many libraries simply restricted access to their own students, faculty, and staff. At the outset of our investigation, we asked ourselves if community access was absolutely necessary, and was it something that was worth spending time and effort to accommodate. Ultimately, we decided that as we are a publicly funded institution that provides much needed services to the local community, public access to our computers and resources was a must. The next step was determining how to provide this service in a way that would be user friendly, maintenance free, and economical.

We investigated various hardware and software solutions and found that they were either too expensive, relied on service desk staff to handle requests, or were overly-complicated. We knew that we could create something ourselves that would do exactly what we wanted.

We learned that many peer institutions used a rotation of pre-created user accounts, and most required community members to present a form of identification at the service desk. We knew that service-desk staff would be busier than usual in September, as they would be helping students and faculty with the new authentication procedures on all of the library's computers. A staff-intensive approach would significantly increase load on the service desks and add to user and staff frustration.

Some other libraries channeled non-affiliated users through campus information tech-

nology departments. However, because our campus Information Technology Services department had no such on-demand authentication system in place at the time and was physically far removed from the library, this solution was not feasible.

Our first priority was to make this solution as automated as possible. The vision was to have a stand-alone workstation with a card reader, through which community members would swipe appropriate identification and be presented with automatically generated usernames and passwords. This temporary account would last until the end of the business day, permit general Internet usage, and allow for access to databases with license agreements allowing unrestricted walk-up use. We had the good fortune of having two library systems administrators with programming skills and experience working with Brock's Information Technology Services department. Nevertheless, we still had a number of hurdles to clear before we began collaboration on the technical aspects, not least of which were privacy concerns.

Privacy Concerns

The system that we sketched out involved collecting and processing data encoded onto drivers' licenses to generate the temporary accounts. There were obviously some privacy issues involved in that process, and we worked with our University Secretariat and the Freedom of Information and Privacy Coordinator to review the ramifications of storing such data. They provided some excellent feedback about what we could ask, what information we could keep, how long we could keep it, etc. Based on their input, we created privacy and usage policies to explain to users exactly what we were collecting, how the process works, what we do with user data, and how long we store it. This consultation was invaluable in this process (and subsequent revision of the software) in that none of us were required to become experts on provincial and federal privacy laws. Instead we could rely on experts to provide us with the guidance we needed to proceed. Armed with a general plan and with a set of newly crafted policies, the heavy lifting could begin: the actual construction of our user kiosk.

Technical Implementation

Like most technology departments, we had plenty of older, underpowered computers lying around, and one was quickly pressed into service as our kiosk machine. It was a Pentium III Dell Optiplex GX 150, more than powerful enough to run a small application in kiosk mode. We purchased three magnetic card readers (Panasonic ZU-M1242L4DK) for \$75 each. One was for production, one was for testing, and one was a spare. To print the usernames and passwords for users, we purchased an Epson M188D thermal receipt printer (\$250). We added a keyboard, monitor, and mouse, thus completing the hardware for the kiosk.

Creating the software was the biggest challenge and the most time consuming element of the entire project. The system consisted of three components: the client-side application, the server-side scripts, and the database. The client-side application was written in Microsoft Visual Basic 6 and read the data on the user's license, requested an account

from the server-side scripts, and sent the user's temporary account username/password to an attached receipt printer. The server-side scripts used a service account in Active Directory to create a temporary user account that expired at the end of the day. The data is also inserted into a database, and kept for 30 days--a retention policy developed in conjunction with our Campus Security officers and our Freedom of Information and Privacy Coordinator--after which all personally identifiable data was purged. Thirty days allowed for enough time for an incident to be reported to Campus Security and for an investigation to be initiated. The challenge in this model was our ability to create Active Directory accounts on the fly, and here is where having systems administrators with the knowledge, experience, and the contacts necessary to accomplish this was crucial.

We implemented the solution at the same time as our implementation of library-wide Active Directory authentication on all public machines. Timing was critical as we wanted to accommodate community members immediately. The system proved reliable, and community users were able to generate their own temporary accounts easily and efficiently right away. We did encounter some technical glitches (described below) and although we accepted drivers' licenses that conformed to North American standards, there were some non-standard and international licenses that the system could not handle.

We encountered some usability issues from the outset that could not be easily solved. Brock University's Active Directory authentication implementation has password complexity rules that require special characters, numbers, and a minimum length. Even though the system was designed to be as automated as possible, staff members working at the library service desks were often called upon to help interpret the cryptic passwords. Adding to the confusion, many special characters were difficult to read when printed via a thermal receipt printer.

We found that many first year undergraduate students were confused about how to log on to our computers, and would often attempt to swipe their student cards at the temporary account station. Many students used the temporary account stations with their drivers' licenses, unaware that every student had a Brock University account with which they could access public workstations. We also had many international visiting scholars and faculty members who were unable to use their identification to create accounts.

Improving the Process

In order to allow service desk staff to create accounts for users with international or non-standard identification, we immediately set to work creating a secure web interface for the system. We also adjusted our policies to specify that users could present government-issued photo identification and be issued a temporary account. Whereas most of our accounts are generated through the self-serve kiosk, service desk staff members create accounts for international users on a regular basis.

After two years of use and staff turnover in the Library Systems and Technologies department, we embarked on a major rewrite of the original code. We found that the origi-

nal system could take up to a minute between a user swiping a license and when the printer would finally print the account information, during which time the user would often assume the system had hung, and simply leave. Instead of using Visual Basic 6 for the front and back end code, our new Systems Administrator, Mike Tisi, determined that we would achieve major speed and stability improvements if we split the code into VB.net for the user interface, and PHP for the back end.

We discovered that our card readers were not robust enough to handle day to day usage, as the wiring quickly frayed and disconnected. Our original readers did not have the ability to be surface mounted, and using double-sided tape to attach the unit to the computer proved ineffective. Ultimately, we decided to migrate to a USB card reader (MagTek SureSwipe USB Reader), and Kyle Knox, another newly hired Systems Administrator, used his metal-working skills to create a VESA-compatible metal mounting plate for the reader to be mounted to the side of the LCD monitor (see Figure 1).

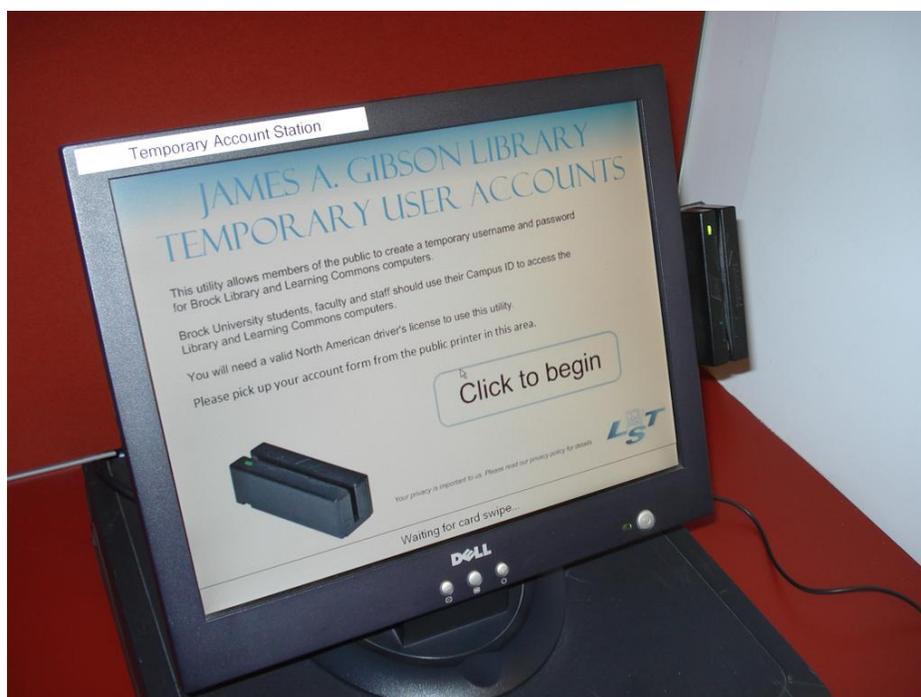


Figure 1

Finally, the thermal receipt printer was removed from the system, as the printed usernames and passwords caused confusion due to poor print quality. Instead, the system printed to the networked laser printers located next to the temporary user account station. In terms of hardware and software, the upgraded system is much more streamlined and robust than the original system.

The original system purged all data in the database every 30 days in order to comply with our policies and privacy regulations. This, coupled with the fact that the system was not designed to track usage statistics, meant that retrieval of usable data about the number of accounts created was impossible. After additional consultations with the University's Freedom of Information and Privacy Coordinator, we revised the system to

purge all information about identities after 30 days, but still retain general usage statistics. We are also able to track basic demographic information, which helps us understand the needs of our guest users. From the implementation of the new version of the software in June 2008 until July 15, 2010, the system generated 1,751 accounts, serving 666 unique users. Since our move to authentication and the implementation of our temporary user account station in the fall of 2006, we have only had one occasion where an inappropriate message was sent from computers in the library, and we were able to provide our Campus Security officers with the information they needed for their investigation. In that case, it was not a member of the community using our temporary account system that sent the message, but a member of the Brock University community using their Active Directory credentials.

Conclusion

Although the process to plan, code, build, and implement our temporary account workstation was a lengthy one, we are extremely pleased with the way the system provides access to our resources to members of the community, while still respecting University policies and procedures. The automated process reduces the strain on our service staff, and allows quick and easy computer access to international students, visiting scholars, and community members. We were fortunate to be able to work closely with our colleagues in the University's Information Technology Services department, to have the guidance of our University's Freedom of Information and Privacy Coordinator, and to have the staff members with the talents and skills necessary to conceive, program, and implement such an efficient and secure system.

Appendix A: Questions asked of Ontario Academic Libraries in 2006

- Does your library offer access to electronic resources (computer access, database access, etc.) to community users, and other users not affiliated with your institution? If not, why not?
 If yes, please explain the process used to give these users access to resources.
- What restrictions do you have in place for these users?
- Do you have any written policies that govern this access? Are these policies publicly available?
- Do you have any procedures to store information about these users for statistical or security purposes? Please explain.
- What issues have you encountered with your system?

Appendix B: Technical Description of the Process of Authenticating Non-Affiliated Users

User swipes North American driver's license at kiosk. If the patron does not have a North American driver's license, a valid passport can be used at the Circulation desk. Library staff can manually enter ID data into a web accessible form. This form is only accessible to Circulation desk machines.

If user swipes their card at the automated kiosk (TUKiosk), it determines if card is valid AAMVA license, and whether there were any errors during read.

User is presented with Brock University Library Public Workstation Use Privacy Policy which also points the user to the Campus Computer Acceptable Use Policy. If the user agrees to the Terms, the following procedure takes place:

- TUKiosk sends card data over a secure channel (HTTPS) to Temporary User Web Service (TUServer)
- Temporary account is created in Active Directory by the TUServer. Account is created over secure LDAP (LDAPS) using the adLDAP PHP class (<http://adldap.sourceforge.net/>)
- The accounts are created with the following specifications:
 - Username format is capital letter "L" + timestamp of request (e.g. L1265651833)
 - Password is automatically generated conforming to University password policy (e.g. ZpOMTs0V8)
 - Temporary account is added to the appropriate AD security group
 - Temporary account is limited to log-on to specific library computers
 - AD security group is denied access to certain licensed resources and enforced by a proxy server running Microsoft ISA Server
 - AD security group is denied access to the campus-wide wireless network
 - Temporary account expires at the end of the day that it was generated
- Temporary account details are returned from TUServer using HTTPS.
- Temporary account details (date created, username, location, first name, last name, identification number, id type) are logged and retained for 30 days according to FIPPA regulations.
- Every day, an automated process is run to remove all identifiable information from all records older than 30 days.
- Temporary account details are sent to printer for retrieval by user.

Jonathan T. Younker is Head, Library Systems and Technologies, Brock University, St. Catharines, Ontario, Canada.

©2010, J. Younker. *Journal of Library Innovation* is an open access journal. Authors retain the copyright to their work under the terms of the following Creative Commons license: Attribution-Noncommercial-No Derivative Works 3.0 (United States)

<http://creativecommons.org/licenses/by-nc-nd/3.0/us/>