CIC Library Automation Directors
Security/Authentication Issues in the CIC Virtual Electronic Library
March 29, 1996

This document outlines the major network security and authentication issues related to the CIC Virtual Electronic Library. The content reflects informal discussions of the CIC Library Automation Directors over the past several years. It is based on a working document developed in 1994 and updated recently into this version. The document has three parts: a continuum of security needs from those library systems/services requiring the least security over the network to those requiring the most security, a discussion of some important related issues, and finally a brief overview of security in the current CIC networked environment and some general observations.

A. Continuum of needs for security from lowest to highest level of security.

1. *Systems open to anyone: for example, online catalogs.* Some systems are designed inherently to be secure and present no licensing issues so that open, unrestricted access is the goal. Our Z39.50 online catalog servers and their interfaces are a prime example. That said, library resources are limited and it could be possible that contention for access might force a CIC site to restrict access to local clients first, the CIC or other partners sites second, and to others on a space-available basis.

2. *Useful to know who is using a resource (usually does not require identification of user by name/id) for statistics or other information gathering uses: for example, ERIC or local files created by the library.* Some systems/services can be made widely available with no content restrictions, but the library will want to know in general terms who the users are to justify the expenses associated with offering the systems/service. In these cases, log files of IP addresses for analysis will be sufficient and may even be kept/analyzed on only a sampling basis.

3. *Best effort to limit access to authorized users for licensed information (broad categories): for example, H. W. Wilson files, Encyclopaedia Britannica* These systems need to be restricted to local campus and/or authorized campuses within CIC, but the suppliers of the data and/or search engines are comfortable with moderate "best efforts" at restricting access, such as domain name restrictions. The CIC institutions need to have a way to discriminate between "true" members of the campus community and "guest" members of the campus community. For these systems, typically, access is allowed by the non-CIC community only when they are in a CIC library using a public workstation.

4. *Meet password requirements of remote systems: for example, OCLC First Search, block search option; RLIN Eureka; Grateful Med over the Internet.* These

systems require each user to sign on to the remote system. Each system has its own password requirements although anyone on the campus may have access if s/he has a valid password. These systems can require restricted manual distribution of individual passwords, sharing of single passwords across campus, programming of special password servers to distribute passwords, distribution of clients with, or capable of getting, the required passwords, or programming of a gateway machine that logs user in using a script.

5. *Best effort to limit access to authorized users for licensed information (restricted categories): for example, LEXIS.* Some services that the libraries use require restriction based upon rather fine distinctions but still access is allowed to broad categories of users. For example, a legal database or a subscription is available to faculty and students who are not in the law school and not available for research and business functions, including campus attorneys, of the institution.

6. *Limit simultaneous access: for example, OCLC First Search or RLIN Eureka gateway service*. Gateway services or server software can be priced according to the number of simultaneous users. In these instances the provider may well limit the number of simultaneous connections for the CIC or a campus, but CIC may need to further manage this traffic, e.g. to guarantee one or more connections to each participating library. In this model, timing-out users can be important to assure that ports are not being held needlessly by users.

7. *Identify user as eligible to perform some general activity in order to be able to take responsibility for user's actions: for example, limit telnet or e-mail from Web-browsers from library public workstations.* The CIC libraries expect to provide access to most of their services via the Internet. Many CIC libraries expect that robust full-featured kiosk versions of Web-browsers will be used as graphical interfaces for public workstations. The needs to restrict functionality to provide a secure and responsible environment and to allow users the freedom to use all the library's services from any place are in conflict. The CIC security environment must address this problem in the context of the public outreach and/or land-grant tradition of the CIC members.

8. *Identify user and log activity of account in order to be able to assign responsibility for problems or for billing/charge back: for example, to charge back electronic document requesting, printing, or downloading.* The CIC libraries have recognized that the cost of some services can not be carried by the libraries on behalf of their users. Services such as printing and downloading may be passed on to the user. Copyright or delivery costs may be passed on to the user. As we contract for systems where each transaction carries an individual cost, the libraries may want to track these costs for other reasons, for example to identify users who abuse the privilege of access to a system/service.

9. *Limit access user-by-user because of restrictions related to access to data: for example, Dept. of Defense files, some STN files.* Some information sources and systems have externally imposed security restrictions. Users of the system must have government security clearances (DOD) or must be recipients of grant money from a particular agency to have access to a system.

10. *Limit type of access and assign update/write capabilities to restrict access to remote systems: for example connecting to production systems for purpose of daily work.* The library staff will use the network to connect to local and remote library management systems to perform work. Sharing cataloging expertise across the CIC means that catalogers from one site must be able to connect securely to the database at another site. Cooperative acquisitions programs may require access to other (sensitive) internal library records. Further, our users will need to connect securely to the local system and to remote systems to renew books themselves or to find out the status or items on loan, overdue etc.

11. *Limit port access to a particular user or group of users: e.g. interlibrary loan staff connections to the ILL/DR server.* Library systems sometimes have special characteristics or functionality built into particular ports. An example of this is the diacritic character set capability used by catalogers. Circulation staff must always have a port ready and waiting to do their work. In these instances a specialized port must be maintained and made available only to a limited set of users.

12. *Maintain and provide secure proprietary (i.e. non-TCP/IP) networks for EDI: for example, for library purchasing and transferring financial data (fines, payments etc.)* Most CIC libraries are looking to speed up local routines by using X.12 and other such schemes to transmit payment and billing information within the university, to other universities, and to vendors.

B. Other related needs/issues.

1. *Encryption of passwords or files, authentication of passwords across the network, sending passwords over the network, authentication of files and documents sent over the network or stored on the network*. Both users and objects must be authenticated over the network. In some cases, encryption must be supported. Not only must we authenticate that an object is an authentic copy but also that it came from the place it was supposed to come from.

2. *One time and multiple use authentication tokens.* Network security must support both kinds of user authentication, one-time tokens for high risk systems and multiple use tokens for low-risk system.

3. *Software distribution and dynamic/automatic updating of clients to current version.* The CIC libraries will be distributing multiple specialized software clients, like Crossfire for Beilstein or Grateful Med for MEDLINE. These clients are upgraded from time to time. The libraries need not only efficient and secure ways

to distribute these clients to legitimate users but also to upgrade or replace all or part of a client on the users workstation. For example, the list of Z39.50 accessible databases stored in a Z39.50 client may need to be replaced because of new sites or changes made to existing sites.

4. *Number of passwords a user must have.* Clearly, the fewer the passwords and userids a user must have, the more likely s/he is to remember them and to keep them in a safe place. The more passwords s/he must have, the more likely are these to be written on post-its in offices or the more likely is the user to choose insecure passwords, like the names of pets. Since the average library user will probably need a dozen or more passwords, each with its own scheme, for access to the library systems and services, other alternatives than managing all these passwords must be found.

5. *Limiting access by IP address or domain name.* Increasingly we have put this method into use because it is the one method we have. At the same time, the CIC community is buying their home Internet connectivity from other sources (with our encouragement) because of stressed-out modem pools. As more and more of the CIC community get non-CIC domains for their home access, the CIC must figure out how to use other methods to authenticate these users so that they can use library systems and services. Even in the library, library staff are relocated due to power outages, staff vacancies, and other needs, and require access to specialized ports from different machines.

6. *Library public workstations.* The anonymous Web-browsers or similar interfaces on library public workstations can present a major security loophole. The major one, of course, is the possibility to send anonymous electronic mail for nefarious purposes; at the same time, there are legitimate compelling reasons (the CIC interlibrary lending/document delivery project, for one) to provide this feature. How will CIC confront this?

C. CIC Environment.

Currently CICNet is primarily a trusted peer network environment. IP domain checking/firewall software is the major way we limit access. Therefore the expectation is that home domains authenticate users before they are allowed to connect to remote systems. This expectation is generally respected by the libraries, but has not been codified as a guiding principle of inter-CIC security.

There are many sources for authenticating the members of the CIC community: email, X.500, or campus directories; computer accounting files; library patron files; and campus registration or payroll files. All of these are possible sources of authentication. There is a great need to decide what databases will be used for authentication. This is a very complicated issue that must be resolved soon. All the parties with strong interests, including of course the libraries, need to be involved in the process of deciding.

Not so long ago, we expected CIC to move to a Kerberos-type environment. We understand that there is less agreement among the campus-level technology experts now and wonder whether CIC will have a homogeneous or heterogeneous authentication environment. How will the libraries cooperate if multiple authentication routines, for example, Kerberos and DCE, are used? Kerberos needs a number of additional features in order to be useful for CIC: expansion of the number of users is an issue, ability to use multiple servers is an issue, the ability to carry tokens across the network and cash them in at designated remote systems is another one if we are to have full functionality in a distributed computer environment. The relationship of any chosen security method to other methods must be understood. For example, library vendors may provide systems which use proprietary packages such as Novell's RSA. We must be able to integrate these into the CIC Virtual Electronic Library.

For the immediate future, it seems that linking Internet node (i.e. to a range of nodes within a given domain or set of domains) to authentication is the best first phase option. At least that way, we can look at sharing databases before most of us have authentication systems on the campus networks that can travel across the CIC and to the library's vendors of systems and services. Increasingly this is not enough as more and more of our legitimate users come in from domains outside the campus. Unfortunately, the other issues outlined in this paper are also becoming more pressing on our campuses and we can't put off dealing with them much longer.

Committee on Institutional Cooperation
302 E. John St. / Suite 1705
Champaign, IL 61820
(21) 333-8475
cic@uiuc.edu
http://www.cic.net/cic/