

**CIT/I&D IDENTITY MANAGEMENT
POSITION ON SUPPORT FOR AUTHENTICATION PRODUCTS FOR
UNIX/LINUX ENVIRONMENTS**

by Ron DiNapoli, November 20, 2003

STATEMENT OF POSITION

Due to limited resources it is not feasible for CIT to support—at a binary level—authentication products for all variants of UNIX/Linux in use on campus. We have also been reluctant to release source code to these components because doing so would allow more people to alter those components—something we feel would compromise our ability to guarantee the behavior of those components to auditors, application developers, functional users and the security office. In an effort to ascertain if our concerns in this matter are justified we are releasing UNIX/Linux source code to two minor components of our authentication infrastructure. The release of this source code will provide the UNIX/Linux community with the ability to authenticate to new releases of Java based administrative applications as well as authenticate to the web without using SideCar or CUWebLogin (for servers/services which support this method). This will allow us to “test the waters” with an open source approach to UNIX/Linux authentication support.

HISTORY

One of the highlights of a career in higher education is the diversity inherent in such an environment. We experience this diversity every day in a way not possible in the corporate world. It is what attracts many of us to Ithaca, and it is what keeps many of us here year after year.

In the realm of Information Technology, the diversity I speak of manifests itself in the form of many people making choices about what technology works best for them. At an institution which strives to achieve an “Open Doors, Open Hearts, Open Minds” policy of diversity and inclusiveness, individuals—in a perfect world—would be able to make those choices without being hindered by support barriers of a central organization.

However there are barriers. Officially “supporting” an operating system takes staff resources that are in scarce supply. It is difficult to justify expending those resources to support products (development/testing/packaging/deployment/support) on an operating system with a relatively small user base—especially when that user base is itself splintered across multiple distributions/versions of the base system. This has been the challenge we face when we evaluate the prospect of supporting authentication products for UNIX/Linux (on the desktop) officially here at Cornell.

THE OTHER SOLUTION

Most people don't argue the support argument above, especially since the UNIX/Linux community has been traditionally more "self-supporting" than their Windows/MacOS counterparts. Instead, they argue that we should engage in an "open source" environment for authentication products here at Cornell. With source code, UNIX/Linux users could build and support their own versions of the authentication software without the need for taxing the CIT support infrastructure.

While this solution solves the support problem, it creates other problems. The Identity Management group has an obligation to provide a secure means of central authentication guaranteed to function in a certain way. We must guarantee this behavior to our application developers, to our security office and to our auditors. So while we agree that an open source program could very well improve our ability to support more operating systems and even improve our source code itself, it's the other staple of open source development that causes a problem with our ability to guarantee behavior: *You can change it if you don't like it!*

In addition to concerns over losing the ability to guarantee behavior, the open source approach also raises concerns that we would still need to allocate a non-trivial amount of staff time to coordinate the open source effort.

TRAVERSING THE IMPASSE

We could sit on opposite sides of the virtual fence on this issue--firmly stating our respective positions repeatedly as if we were starring in an old beer commercial: "Open Source" ... "Guaranteed Behavior for auditors" ... "OPEN SOURCE!" ... "Guaranteed Behavior for AUDITORS!"

Our other choice is to find a common ground to meet on where we feel our respective concerns are being taken into consideration as we move forward. The Identity Management group at CIT is willing to take a first step towards this with some of our desktop authentication products.

COMMON GROUND

A little over a year ago the Identity Management group began work on a small shared library called CASAPI (Cornell Authentication Services Application Programmer's Interface). The idea behind CASAPI was that it would be a library that could (theoretically) be supported on all platforms and provide a common API for client side security. The Java applications (Colts II, JTF, PEDL, others?) could then depend on CASAPI for authentication instead of Project SALSA's VCSAPI library. The smaller size of CASAPI would make it easier to support in more places. CASAPI has been built under MacOS X, Windows and Linux. It is our hope that the Java applications will

migrate to a CASAPI base in the future (there are some crude prototypes internally today), and that any future client side authentication products would be based on it (such as the SideCar replacement).

We are proposing that full source code to CASAPI is released for Linux with the hope that it will be embraced by the Linux community and built/installed/tested under multiple environments. We would hope—as the open source ideology claims—multiple eyes on this product will help improve it both from a “platforms supported” standpoint and a “code robustness” standpoint.

But what good is an authentication library with no apps to take advantage of it?

We are also proposing that full source code to our reference implementation of a Mozilla component which performs SideCar-like authentication for Mozilla be released. This component allows “inline” kerberos authentication to any web server running CUWebAuth v1.0.10 or later (provided the web administrator has enabled the capability) and works well behind a NAT.

MOTIVATION AND RATIONALE

Clearly, the willingness to release source code is a departure from the position we’ve held over the past 4 to 5 years. Why the change of heart?

First of all, the back end technology (CUWebAuth) has improved dramatically over the years. It has finally matured to a point where it is being used by a large number of servers. This provides a homogeneous “enough” back end against which new clients can be developed.

Clearly, there is no support model we can come up with which allows us to support all flavors of UNIX/Linux ourselves with binary-only releases. This is impractical. It is also clear that we are not diving “head first” into this venture with all of our source code. In fact, CASAPI and the Mozilla component make up a very small percentage of our code base. It allows us to “test the waters” with a more open approach to development. If it works well, we could consider releasing more source code in the future.

Finally, we’d like to find a way to work together to benefit as many people as possible. It is a common misconception that we are trying to “horde the technology” or “hide vulnerabilities” when we don’t release source code. I don’t believe this is the case. I do believe we are attempting to live up to the expectations and responsibilities we all feel are a part of our jobs. Perhaps it is our misconception that the release of source code would automatically compromise our ability to do that. To help allay our concerns, we ask that you would adhere to the following guidelines.

GUIDELINES FOR WORKING WITH SOURCE CODE FOR CENTRAL AUTHENTICATION PRODUCTS

1. If you are planning to do anything other than simply compile the code on your system to use without modification, please let us know what you are doing.
2. If you are planning to build the software to distribute to others with similar systems, please allow us to look over any modifications you felt were necessary.
3. Any modifications made should not alter the basic functionality (with respect to authentication) of the software. Any published protocols and policies must be adhered to such as (but not limited to):
 - a. length of time a credential is valid
 - b. conditions in which credentials must be invalidated so that the user is re-prompted
 - c. never asking a user for their password directly
4. Any problems found with the authentication protocols should be brought to the attention of Identity Management staff instead of publicly broadcast.
5. Submitting code back to CIT is encouraged, but there should be no expectation of any time frame associated with incorporating such code back into the distribution.
6. Individuals who would engage in irresponsible behavior with this code should be discouraged from doing so.