

# Turning the Titanic: Changing a PIN to a Password

Dianne Brotherson  
Iowa State University  
Administrative Technology Services  
2<sup>nd</sup> Floor ASB  
Ames, IA 50011-3601  
(515) 294-0293  
dkbroth@iastate.edu

## ABSTRACT

AccessPlus was unveiled on the Iowa State University (ISU) campus in 1996 as a web-based resource for accessing important and confidential university information for students, faculty, and staff. Currently, many services are available to students on AccessPlus such as class registration, grade reports, and financial aid. Faculty and staff are able to view payroll, vacation/sick leave benefits, and university business and administrative applications.

At its inception, an ID and a 4-digit Personal Identification Number (PIN) were needed to login to AccessPlus. This was the login model until recently when an initiative was begun to change the AccessPlus four-digit PIN to a six to eight character password. The need for a stronger password was to improve AccessPlus security and safe-guard critical data as well as to respond to new and increased legislation concerning privacy and security requirements. The transition period began February 18, 2004 and affects over 45,000 students, faculty, and staff.

How do you inform over 45,000 people that their AccessPlus PIN needs to be changed to a password and not compromise security or productivity? This paper will discuss the process and tools used at Iowa State University to make this transition as smooth and seamless as possible.

## Categories and Subject Descriptors

D.4.6 [Operating Systems]: Security and Protection – *access controls, authentication*

**General Terms:** Security.

**Keywords:** PIN numbers, passwords, password security, strong passwords, login, conversion.

## 1. INTRODUCTION

Iowa State University is a comprehensive, land-grant university located in Ames, a progressive community with a population over 50,000. ISU has an enrollment of 27,000 students and 6,000

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

*SIGUCCS'04*, October 10–13, 2004, Baltimore, Maryland, USA.  
Copyright 2004 ACM 1-58113-869-5/04/0010...\$5.00.

faculty and staff members and an annual budget exceeding \$780 million.

ISU has two computing centers: Academic Information Technologies (AIT), which focuses on the academic and research needs of the campus, provides e-mail and computer support for the students, and manages many of the computer labs that are located on campus and Administrative Technology Services (ATS), which focuses on the administrative needs of the campus.

ATS concentrates on the development, implementation, and support of enterprise-wide information systems used to conduct the business of the university. These systems include accounting, human resources, payroll, purchasing, and student systems. With these systems, ATS and the appropriate departments become the provider of the information displayed in AccessPlus.

With a professional staff that numbers around 100, ATS works to develop, integrate, maintain, and support information systems that enable university entities to manage data. Services also include office information and desktop computing systems, data access and use, administrative network support, training and education, a help center, and a broad range of technical services. ATS is a cost recovery center, which for the most part means that users of the services pay for the services. ATS's goal is to provide quality and responsive services for its supported clients.

## 2. HISTORY

ATS first offered students a chance to view their personal university information from five kiosks installed on campus in August of 1995. During the summer of 1996, ATS added seven additional kiosks on campus and also added web access. Since then, ATS has continued to expand and enhance web access to include a broad range of services available to students, faculty, and staff. The AccessPlus system benefits ISU by allowing students, faculty, and staff access to information and services at a time that is convenient for them. To use AccessPlus, a person logged on using their Social Security Number or University ID and their 4-digit PIN.

Prior to AccessPlus, all university information systems were only available using ISUAS. ISUAS is an online menuing system which serves as a 3270 terminal access point to many of the administrative information systems that ATS develops and supports. Hours of access for ISUAS are from 7:00 a.m. to 9:00 p.m., Monday through Saturday. ISUAS has been the traditional way that faculty and staff access accounting, human resources, payroll, purchasing, and student systems data. Figure 1 shows the signon screen for ISUAS.

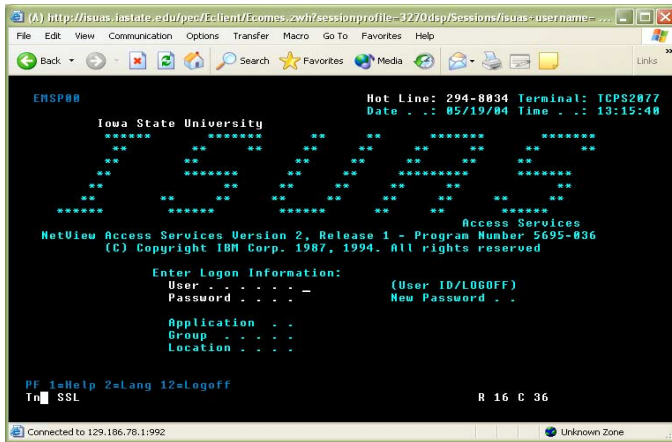


Figure 1. Signon screen for ISUAS.

### 3. CURRENT USE OF ACCESSPLUS

Today, many services are available to students on AccessPlus such as class registration, grade reports, and financial aid. Faculty and staff are able to view payroll, vacation/sick leave benefits, and university business and administrative applications.

#### 3.1 Student Systems

Figure 2 displays the web page displayed for the student systems available on AccessPlus. Prospective students use this page to accept their offer of admission to ISU, and current students use the page to register for classes, pay their bill, deposit money to their CyCash account, check grades, and other business-related activities. Students who have graduated use the system to order official transcripts.

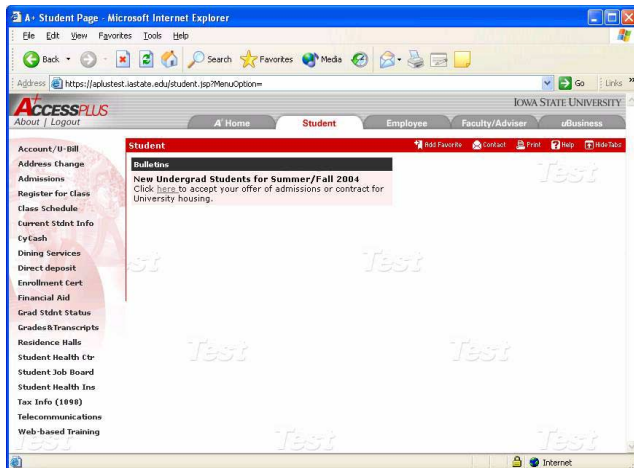


Figure 2. Student systems available on AccessPlus.

#### 3.2 Employee Systems

The employee systems available on AccessPlus include billing, CyCash, direct deposit, payroll information, vacation/sick leave, and travel reimbursement. It is also used for benefits and training sign-up.

### 3.3 uBusiness Systems

Systems under the uBusiness tab include travel vouchers, purchasing requisitions, eReports, and others. More systems are being added as this venue is seen as the model for new program development.

### 3.4 Faculty/Advisor Systems

Clients with this tab have the ability to display a student's class schedule, grades, general student information, and unofficial transcript information. They can also display class lists for departments, instructors, and advisee lists.

## 4. GOAL

The goal was to change from a four-digit PIN to a six-to-eight character password to login to AccessPlus for all students, faculty, and staff. The transition period began February 18, 2004 and is still in progress.

#### 4.1 Reasons for the goal

A longer password that consists of a combination of letters and numbers is a stronger password improving AccessPlus security and safe-guarding ISU data. Also, the change was needed in response to new and increased legislation concerning privacy and security requirements for ebusiness best practices. In addition, the student systems fall under Family Educational Rights and Privacy Act (FERPA) guidelines that must be followed.

#### 4.2 Communicating the goal

The goal appeared easy and straight-forward and it seemed that changing from a PIN to a password would be a simple task...until various clients and processes were considered and then what seemed simple turned daunting. The task was considered a year earlier but was tabled because of the outstanding issues. To help with the implementation, a communication plan was written to identify change management issues and recommend communication support for the implementation of PIN to password.

Part of the plan involved interviewing key departments and identifying the stakeholders/clients and the expected impact to them and/or their areas of responsibility. The plan also identified the target audiences, the key messages that needed to be delivered, opportunities to deliver the message, and who should be responsible for the delivery.

Many stakeholders/clients were identified from the interviews. Some of the stakeholders/clients are new students, current students, past students, and students who are on-campus and those who are off-campus. There are the employees who have AccessPlus and ISUAS and those that only use AccessPlus. Another situation was student employees with ISUAS access. There were also ISU contacts that do not come to campus and affiliate groups. The impact of the change was documented for each group of stakeholders/clients and then shared with the stakeholder departments.

It is important to note that the systems in ISUAS and the systems in AccessPlus utilize the same databases in the ATS Central Systems and therefore, the password is the same password for both ISUAS and AccessPlus (see figure 3). This is an important concept for clients to grasp to avoid confusion with their

password. To simplify the process for those that had ISUAS, a convert button was available to change their PIN to their already existing ISUAS password.



**Figure 3. Passwords are the same for both.**

The Pin-to-Password change was communicated by presentations to administrative groups and to academic groups. It was posted on the ISU news web page, the ATS web page, and on the login screen of AccessPlus and ISUAS.

Beginning in May, e-mails were sent to groups of clients informing them that they had to convert from a PIN to a password. To break down the task into manageable pieces, the e-mail messages were sent to groups of 150 people at a time. These messages came from one of our staff members and included her phone number so our clients would have a human contact for any questions or concerns. In a typical group of 150 clients who received the e-mail, 100 voluntarily changed their PIN to a password and 50 waited to change to a password at their next login. There were typically one to two irate phone calls per mailing.

## 5. DAY-TO-DAY OPERATIONS

Under the old PIN management process, the PIN was created by default to be the client's birth day/birth month and was communicated to the clients verbally or from information posted on the ISU web site. The PIN was a one-time PIN and had to be changed after signing in but the PIN never expired. Most PIN resets were handled by student services offices and required an in-person visit. As more programs were added to AccessPlus, such as payroll information, more staff were given the rights to reset PINs. Over time, more than ninety ISU staff spread across campus had the ability to reset PINs.

With the change to a password, processes had to be developed to create the password, inform the client of the password, and provide password resets. This was an opportunity to change the current methods and tighten up security. After much discussion, it was determined to use a random password generator to generate the password and e-mail the client their new password via their official university e-mail account. The password is a one-time use password and has to be changed after the first login. Those clients that have systems under the uBusiness tab and/or Faculty/Advisor tab are now required to change their password every six months. Also, all password resets are logged and can be reviewed. The number of staff who can change passwords has been reduced by half.

### 5.1 Forgetting the Password

Which department should reset the password if the client forgot? Should it be AIT since they provide the student computing support or should it be ATS since they provide the systems?

Should in-person requests be required? Is it possible to verify a person's credentials over the phone? After discussion with the stakeholder departments, it was decided that the ATS Help Center would handle password resets over the phone. To verify the credentials of the caller, an ISUAS screen was created specifically for that task. The screen includes fields from the following systems; admissions, student information, human resources, affiliate, and foreign national. Depending on the information available, the Help Center staff person generally asks for the client's university ID or social security number and other questions based on their status as a new student, current or former student, current employee, or former employee. If the Help Center staff feels uncomfortable with the verification of a person's identity, they can refer the client to a student services office or the Human Resource office and let them verify the person's identity based on additional information they have.

Because the ATS Help Center is dedicated to support those administrative clients who pay a monthly support fee, a separate phone number was established for password resets. This phone number is published on the AccessPlus web page as well as in informational materials from the Admissions and Registrar office.

To help with the multitude of password resets and questions being directed to the ATS Help Center, a secret question/password reset was instituted. If a client forgets their password, they can answer their secret question and if answered correctly, a new one-time password will be e-mailed to their e-mail address on record. It was decided that a client correctly answering their personalized secret question is both practical and secure. It allows a client to prove their identity and receive a new password at off-hours when the ATS Help Center is not staffed.

As of June 1, about 20 AccessPlus resets are being handled on a daily basis by the ATS Help Center. This year's freshman class will all be issued passwords so one-fourth of the student body will be using passwords. The rest of the student body will be converted in groups after the start of fall semester, taking into account the timing of class registration and the posting of grades.

Another change that was made on July 1 was the billing model for ISUAS access. In the past, a fee was charged to set up an account and then a monthly fee was assessed based on the amount of usage. Because of this, clients sometimes shared their NetID and ISUAS password so that others could login using their credentials. Under the new model, the department is assessed the yearly ISUAS charge based on total department usage and the set-up fee was waived for ATS-supported clients. The goal of this change was to remove any hindrances to adoption of the password related to billing issues.

## 6. ISSUES

As can be expected with any change, adoption of the new password was slow and painful. Many clients were not aware of the PIN to password change until they received an e-mail telling them they had to convert. Others were very upset about the password expiring in six months. They felt this hindered security because they would need to write the password down since it changes so often. One of the reasons given for not wanting to convert was because they shared their ISUAS password with others in their office so they could login in their absence. Another reason given was that their current PIN matches their bank PIN

and they wanted to keep them the same. Also, with all of the computing systems on campus, there is confusion over which password is being changed and who to call for a password reset. Most of these issues were dealt with on an individual basis by explaining the reasons and benefits for changing to a password and by having administrative support for the change.

Another issue was the desire not to disrupt the business of ISU. The need to change from a PIN to password was tempered by the need to keep staff productive and have access to the computer systems that they need. This was done by carefully timing the e-mails so that there was no interference with month-end or year-end business cycles. For students, this meant avoiding the start and end of a semester and during class registration.

## **7. CONCLUSIONS**

The planning and system changes are complete for the PIN to password conversion and the implementation has started and is in full swing. Questions and concerns remain about the start of fall semester and the impact the conversion will have on new and returning students and staff. But, by that time, the ATS Help Center will have a wealth of experience dealing with password resets, the new freshmen will be using a password, and the majority of the staff will be using a password. The goal of protecting data is progressing towards completion.