



A Search for New Horizons



Robert Carrigan,
Chairman of the Chairmen's Committee

Ron Milton,
Vice-Chairman of the Chairmen's
Committee

Dan Morrow,
Chief Historian

EDUCATION SECURITY

2005 COMPUTERWORLD HONORS CASE STUDY

EDUCATION & ACADEMIA

DELAWARE STATE UNIVERSITY CONVERGED ITS PHYSICAL AND INFORMATION SECURITY SYSTEMS BEHIND SMART CARDS FOR STUDENTS, FACULTY AND STAFF TO USE FOR ACCESSING BUILDINGS AND IT SYSTEMS, RESULTING IN GREATER PROVISIONING AND ADMINISTRATIVE EFFICIENCIES, SATISFIED USERS, LESS THEFT AND GREATER OVERALL CAMPUS SECURITY. [20055207]

SUMMARY

Using metadirectory technology to centralize security administration, Delaware State University (DSU) converged its physical and information security systems behind smart cards for students, faculty and staff to use for accessing buildings and IT systems. Results? Greater provisioning and administrative efficiencies, satisfied users, less theft and greater overall campus security.

APPLICATION

Like business and government, DSU has made physical and information security a high priority and a key component of its overall information technology strategy.

In addition, DSU is part of a statewide security consortium because Dover Air Force Base is its neighbor and that may require DSU to provide emergency housing and to know who is on campus at any particular moment. And like many universities, DSU conducts classified research for the federal government, which demands a high degree of network security.

DSU's security enhancement project goals were similar to those of other universities: (1) safeguarding its 2,200 resident students, 650 faculty members and staff, plus campus visitors; and (2) protecting its networks and information resources from breaches by hackers and malicious code.

What differs from other universities, however, is the extent to which DSU has converged its physical and information security infrastructure using smart card and metadirectory technologies. As of this writing, no other university is known to have deployed these technologies as pervasively as DSU.

Before it overhauled and converged its security systems, DSU relied on traditional physical security solutions and policies such as photo-identification badges for students, faculty and staff; automobile ID stickers; restricting dormitory access to students and academic building access to students and faculty; motion sensors; and ordinary keys for access to dorms, academic buildings, and other facilities.

Campus access was controlled through gates manned by police officers. To visit buildings open to the public, such as the library, visitors needed passes from campus police

Although some of these tools and processes still help control who is on campus and the buildings and equipment they have access to, DSU knew it needed to do more to boost security. In just one example, keys to buildings and computer rooms were too often being lost or stolen and even if not they could provide no information about who was in a building at any given time.

DSU also had no way to ensure that former employees of the university could not access the network or certain electronic files. If people retired, quit or were fired, they could still log onto email remotely or have access to applications through a modem even without being on campus.

University officials wanted a security upgrade that would take advantage of both the latest available technology as well as the existing technology infrastructure on campus that includes a fiber optic network linking every building and a Siemens HiPath 5000 Real-Time IP System used for voice-over-IP (VoIP) communications.

To achieve this upgrade, DSU chose a Siemens HiPath Scurity solution comprising the HiPath Scurity Card smart card and HiPath MetaDirectory suite. The credit-card sized smart cards control access to both physical facilities and information systems. The MetaDirectory suite keeps identity information up-to-date and provides centralized administration so that any changes in a single data repository take effect in other directories and IT applications throughout campus. What's more, DSU is using the smart card and MetaDirectory suite for e-commerce and other electronic transactions.

The project started in 2002. Now fully deployed in a third of DSU's 22 campus buildings with additional buildings being phased in during 2005, the smart card technology has been a logical extension of the ID cards that were already being used on campus.

Each \$22 smart card provides a photo ID of its holder and contains a five technologies: (a) an identification chip with PKI encryption to manage user identities; (b) an antenna for activating electronic

locking mechanisms by contact; (c) an antenna for activating electronic locking mechanisms without contact but just by waving the card near a lock's reader; (d) a magnetic stripe that provides an "electronic purse" with transactional capability; and (e) a barcode for the DSU library scanners, allowing checkout of library materials.

Altogether, the smart cards provide tamper-resistant storage for passwords, account numbers, and other information. With the card's single sign-on capability, anyone with an authorized ID and password can use the card to log on to Windows PCs as well as email and other applications on DSU computers. There's no need for multiple passwords. The cards also ensure that former employees—and others who are not authorized—are denied access to the university's network, applications, and files. Another smart card application enables the ID cards to provide physical access to buildings. In turn, the existing campus-wide fiber optics network will enable DSU security managers to obtain information about which individual accessed a particular building at a particular time.

A third application for the smart cards provides an electronic purse that enables electronic purchases, such as purchases in the campus bookstore and cafeteria as well as entrance to sporting events. DSU also has an agreement with the Delaware Department of Transportation to allow students and staff to use the card for bus transportation.

Cards already have been distributed to all university students, faculty, and staff. Keys now used for access to buildings and rooms will be gradually replaced with smart cards, although some places on campus will always require keys for access. All new computers purchased by the university will include readers for the smart cards.

The smart cards are providing vastly improved control of access to campus buildings and computers. DSU have experienced reduced operations cost of seven to 10 percent through automation and more simplified applications deployment as well. It found an immediate decrease in the number of calls to the help desk to restore passwords, with lower costs of managing computer IDs and an opportunity for the university to better track who's getting in and out of buildings. What's more, the strengthened security will help deter theft on campus, given that people know DSU's security system can identify who is going in and out of buildings at different times.

The total project cost was about \$700,000, including the metadirectory suite, servers, smart cards, a card printer and its required laptop, and the various development work needed to make it all work. Interestingly, DSU has more than offset the system costs by selling advertising on the smart cards for between \$50,000 and \$100,000 a year, given that a single smart card has room for four to five commercial logos. Without the offsetting advertising revenues, the security project's return on investment in the first year was 17 percent, based on the initial return rate from the two card system the Siemens system replaced and included minimum staff hours reductions in the student services area. With the advertising, the ROI has grown to 60 percent.

BENEFITS

The DSU security enhancement project has succeeded in helping four key campus constituents:

1. **Students:** Until smart cards were issued as multipurpose ID badges with a single campuswide credential capable of providing building access, network access, library checkout, and electronic purse for campus purchases, students were forced to carry a pocketful of ID and access cards or traditional keys. ID badges once carried a student's Social Security number, which in itself opened all kinds of possibilities for identity theft. In addition, students had to use multiple passwords for the various campus IT systems and applications. For all that, intruders could still get into dorms but now that smart cards make that much more difficult – and the cards have been tied into video surveillance systems. In all, the smart cards have provided tremendous convenience for their users, which can translate to greater individual productivity, plus the technology combined with video surveillance has increased their protection against crime.
2. **Faculty and Staff:** Having but one multipurpose ID badge and single sign-on convenience benefits faculty and staff in similar ways to students. And although dorm safety does not apply, the safety of working in a building with smart card-secured access can be increased, extra assurance for anyone working in off-hours.
3. **Campus Security:** The campus police were having a difficult time with thefts that were clearly associated with thieves gaining building access using "lost" or stolen keys. In fact, in a single year more than \$70,000 worth of computer gear had disappeared. In those buildings where smart cards were issued, the number of lost keys dropped to zero and overall campus thefts was cut 20 percent. In addition, the issuance of smart cards effectively put thieves on notice that they should start looking for easier targets because campus security would know who entered a building when and for how long and correlate that information with crime incidents. The unified system makes it easy to cut off access immediately to buildings or networks should security rules be breached. Integrated with video surveillance, it also effectively gives DSU's security staff extra "reach" across campus.
4. **Information Technology Staff:** The IT staff has gained considerable productivity enhancements

and overhead savings by consolidating into a single smart card ID badge all the various access cards, key entry systems and network passwords once required of a student or faculty and staff member. It also gained additional productivity and control by administering them centrally via the Siemens metadirectory technology so that any changes in a single data repository take effect in other directories and IT applications throughout campus.

Overall, DSU's security enhancements have changed not only how each of these three constituencies go about their daily work but also their respective expectations of technologies role in physical and information security. That is, they expect a higher level of security with greater convenience and less intrusiveness. One can imagine the reaction of a DSU student transferring to another university that lacks the same physical and information security and requires going back to the mish-mash of passwords and access technologies, even old-fashioned keys.

For all its benefits, converging physical and network security does raise the specter of violating personal privacy. To counter that, DSU has strong, publicly posted privacy policies. Also, the IT group does not have access to data about smart card badgeholders' movements around campus. Even further, it is the campus police chief, not anyone in IT, who holds the password to the system that can provide an audit trail of an individual's presence and activities.

IMPORTANCE

The DSU security enhancement project combined the following base technologies in a new, unique way to deliver the benefits already described:

- a. A campuswide IP-capable, fiber optic network connecting the 22 buildings and dormitories on campus;
- b. A Siemens HiPath 5000 Real-Time IP server for delivering voice and data IP applications over campus wide area network and in-building local area networks;
- c. Siemens HiPath Scurity Identity and Access Management solution for providing metadirectory services and centralized identity management;
- d. Siemens HiPath Scurity Card for smart card applications that offer both physical and logical access control, including a single sign-on for all network and systems access;
- e. A webserver that provides students, faculty and staff a portal where they can conveniently order new ID badges.

While each of these technologies has its own set of features and benefits, DSU tied them together with legacy campus systems such as electronic purchasing, building alarms, and video surveillance to provide a complete solution to its security requirements that not only enhanced security but also made it more convenient and useful for all users. The solution also made the work of the IT and campus security teams much easier and more effective. Finally, the solution's component technologies all are standards-based and therefore open to future technological advancements as they become available.

ORIGINALITY

As of this writing, no other university is known to have combined and deployed the various technologies described above as pervasively as DSU to realize a converged, comprehensive solution to physical and information security and control across an entire campus.

What's also unique is the extent to which DSU has tied in legacy systems such as the electronic purchasing system and then continued on to seek additional capabilities and value for the solution's users such as its success negotiations with the Delaware Department of Transportation to allow the smart card badges to be used for public transportation. It also has obtained a state grant to explore the use of Global Positioning System (GPS) technologies to help track the real-time presence of badgeholders.

Last, another unique aspect of the DSU solution is its holistic design – the result of a close collaboration with the campus security and its chief and the IT group (with this collaboration being a critical success factor of the project).

And while both groups sought to improve DSU's physical and information security for the sake of their own respective missions at the university, they focused on the end-user as their design point. That is, they aimed to simplify security compliance through the use of the smart card ID badges while adding as much value through features like electronic purchasing and library checkout. In fact, studies have shown that the more complex security schemes are, the less likely users will comply with those security measures.

SUCCESS

The DSU security enhancement project is fully operational across a third of its 22 buildings, including dorms and the administration building. The entire campus population of nearly 3,000 people has

benefited from it.

Given that security is best addressed as a set of preventive measures, specific goal-setting for the project was not appropriate. In other words, it's impossible to measure criminal or malicious events that will not or cannot occur because new security measures have been implemented.

Clearly, however, the expectations for enabling greater security have been met, if not exceeded. And some security symptoms such as major thefts have shown improvement, as rates dropped 20 percent in the year following deployment.

On the productivity side, the project benefits all key constituencies – students, faculty and staff, security and IT. For nearly 3,000 students, faculty and staff, just saving five minutes a day via single sign-on, paying for cafeteria meals electronically, and accessing buildings without having to fumble for keys can translate to 35 person-years. In a corporate environment, that can be worth millions of dollars a year in productivity gains.

For campus security, the greater security deterrence means less criminal activity and alarms to respond to and investigate. For buildings with smart card badge access, key replacements for lost or stolen keys has been cut to zero. In effect and especially with video surveillance integration, security staff gain a much stronger presence, albeit virtual, as criminals are less likely to breach security systems that they know can provide the intelligence and data needed to convict them if caught.

For IT, the helpdesk calls for password resets have diminished considerably. Centralized identity management and administration through metadirectory technology has markedly boosted network security by enabling immediate network or application access denial as soon as someone leaves DSU or changes jobs within DSU. At the same time, centralized identity management has enabled the synchronization of user identities and passwords across a wide range of campus systems that would never have been manually possible before.

DSU's new ID badges, independent of their smart card technologies, have given the university a new revenue source that more than offsets the system's \$700,000 capital costs. By selling advertising on the smart cards for between \$50,000 and \$100,000 a year and with room for four to five commercial logos, the university can realize between \$200,000 and \$500,000 in incremental revenues.

Without the offsetting advertising revenues, the security project's return on investment in the first year was 17 percent, based on the initial return rate from the two card system the Siemens system replaced and included minimum staff hours reductions in the student services area. With the advertising, the ROI has grown to 60 percent.

Future plans include getting every door in every building equipped with smart card badge readers; incorporating two-factor authentication in every laptop and desktop computer; adding GPS location capabilities; extending electronic purchasing to the state's mass transit; and looking for additional ways to add utility and value to the badges to benefit their holders.

DIFFICULTY

Among the challenges of the project, two were key: (1) financing, which was dependent upon the state's budget cycles; and (2) metadirectory training, which required a lot of coordination with those people responsible for the various IT systems that the metadirectory cut across.

The most surprising challenge occurred after deployment when an outcry from badgeholders arose over the \$100 replacement charge for a lost badge. The premium over the actual \$22 replacement cost wasn't designed to be a profit to DSU but instead be an incentive for users to not lose their badges. In considering the matter, the administration decided that the replacement charge was too steep and lowered it to \$50.