Application Note:

Student Records—Increased Security and Authentication with Time Synchronization

Colleges and universities are among the leading adopters of Information Technology (IT) systems. With many institutions continuing to automate processes and provide wireless access to these networks, there is a growing need for improved IT security. There are multiple federal and state laws that relate to privacy and IT security, but only in recent years has IT security started to take center stage.

A growing concern is the fact that college and university networks collect and store detailed and confidential information, including student transcripts, course syllabi, and financial information. Maintained in a digital format and no longer locked in physical file cabinets away from prying eyes, these electronic records are exposed to new risks. Without proper protection, they could be accessed inappropriately from within the institution and by intruders outside the network.

Colleges and universities must make sure that student records are secure and confidential. This isn't just an institutional policy; it's the law. Under the Family Educational Rights and Privacy Act (FERPA), higher education institutions are required to protect the confidential information of their current and prospective students. FERPA also prohibits institutions from disclosing student information without a student's written permission.

The data associated with a student record can include grades, Social Security numbers, financial aid information, payment information, and information dealing with disabilities. As more student records are stored in electronic formats, digital signatures are used increasingly as substitutes for handwritten signatures. A student's digital signature is a legal form of authorization. The institution must therefore be able to prove that a given digital signature is authentic. Tracking when and where the signature was created is part of this authentication. Legislation such as the Electronic Signatures in Global and National Commerce Act (E-SIGN) and the Uniform Electronic Transactions Act (UETA) eliminate barriers to the use of electronic technology for signatures and document storage. They call for legal recognition of electronic records and signatures.

There are many ways to protect student information while verifying the authenticity of that information. One crucial step in increasing IT security is to synchronize an institution's network using one secure, accurate, reliable time source. What does time have to do with network security? Time synchronization is at the root of all operating systems.

Synchronizing a network to one time source immediately improves the institution's ability to authenticate and verify the creation and alteration of documents. Synchronizing time across a network produces verified time stamps, on which the authenticity of digital signatures depends. The time stamp must be secure, accurate, and reliable—both for purposes of synchronization and to protect the confidentiality of student records. If the time source is not secure, hackers and other unauthorized personnel can gain access to the records. If the time source is not accurate, it cannot be used to prove the exact time at which records were created, accessed, or altered. If the time source is not reliable, the same problem occurs.

One method of time synchronization is to use a time source accessible through the Internet. This creates the potential for problems. If the Internet source is unattainable (as any site can be from time to time), the network's ability to provide accurate time-stamping is compromised. An Internet time source may also be inaccurate, providing what is essentially false information. Using the Internet for a network's time source also requires opening port 123 in the edge firewall at the network boundary, creating an entry point for hackers.

A better solution for time synchronization is a dedicated network time server. Such a device provides a common time source used by all devices on a network. It is a dedicated piece of hardware, not an external source outside the control of the network owner. Installing a dedicated time server enables a college or university to comply with regulations, policies, and mandates concerning time-stamping, audit trails, and authentication verification.

Spectracom Corporation offers its highly reliable, cost-effective NetClock® time server for such applications. NetClock is a low-cost investment that solves high-risk problems. The NetClock server synchronizes time across a network, receiving the official Coordinated Universal Time (UTC) through a Global Positioning System (GPS) signal. The time accuracy can range from ±50 microseconds to 1 millisecond relative to UTC time without compromising security. NetClock operates behind the edge firewall, which means it requires no additional open network ports through which hackers can gain access to the system. NetClock uses industry standard Network Time Protocol (NTP) to distribute secure, accurate, reliable, Legally Traceable Time®. Time synchronization supports security and authentication of student records as well protecting the confidential financial and employee information in college and university settings.

May 3, 2012 - AN01-101(D)

USA | 1565 Jefferson Road, Suite 460 | Rochester, NY 14623 | +1.585.321.5800 | sales@spectracomcorp.com
FRANCE | 3 Avenue du Canada | 91974 Les Ulis, Cedex | +33 (0)1 64 53 39 80 | sales@spectracom.fr
UK | 6A Beechwood | Chineham Park | Basingstoke, Hants, RG24 8WA | +44 (0)1256 303630 | info@spectracom.co.uk