Sinclair Community College Secure LAN Strategy Project

Scott McCollum from Sinclair Community College accepted the Award for Institutional Excellence in Communications Technology at the Annual Conference in San Diego. Left to right: ACUTA President 2005–06 Patricia Todus, McCollum, Awards Committee Chair and Immediate Past President Tamara Closs, and Rick Cunningham, PAETEC Communications, sponsor of the Award.

The Sinclair Community College Information Technology Services (ITS) team is responsible for maintaining a secure, manageable, and scalable IT system that facilitates a balance between secure and collaborative network computing for the college's students, faculty, and staff. Information Technology Services had completed a great deal of work researching, testing, and implementing technologies that address specific issues for the college network; however, the college faced some complex challenges in achieving a truly secure LAN solution.

Most network infrastructures allow unrestricted access once a connection is made by a client with the assumption that the only necessary security is to protect the resources on the network servers where there are very sophisticated authentication and access control mechanisms. The main goal is to route communication on the network as fast and efficiently as possible. This leaves the entire network exposed to any software that can take advantage of this openness to find and exploit vulnerabilities in the connected systems.

The growth in wireless networking on the Sinclair campus, the need to provide protection from the introduction of wired and wireless "guest" computing devices, and the need to protect the network from the proliferation of network-borne viruses and worms caused the ITS team to develop a strategy for a Secure LAN Solution. This strategy was completed in October 2004, and it has provided a road map for the implementation of network switch port-based authentication; the authentication, verification, and provisioning of guest and unknown devices; and the identification, isolation, and remediation of problems with unpatched or virus-infected PCs and other devices.

This project was initiated to build intelligence into network devices so they can limit the type of communication that they will forward. These limitations vary based on the type of user and the type of device that is attempting to connect to the network. This puts the control over the network's security into the hands of the college rather than at the mercy of the various devices that can be connected.

A unique approach used in this system was the creation of a partnership between the college and a provider of free wireless services. Because the partner uses the same wireless equipment as the college, the partner's wireless network has been designed with the ability to access the college's secure wireless access over the same equipment. This has been beneficial to both the college and the wireless partner as the college obtained additional wireless services and coverage areas at no cost using its secure wireless access system, and the wireless partner gained additional installation areas and customers.

The Secure LAN Strategy defines a clear path toward a network where access to network resources on the entire Sinclair Community College campus is based on the role of the user, the configuration of the computing device he or she is using, and the verifiability that the device is problem-free. When the plan has been fully implemented, no computer will be able to communicate on the Sinclair network, via wired or wireless connectivity, without the user of the device passing an authentication process. The plan also provides for different levels of access based on whether the device is a Sinclair-imaged computer or a device with an unknown configuration.

Planning, Leadership, and Management Support

ITS was already working toward a secure LAN solution, but to address the significant challenges involved, the team defined the Secure Network project for inclusion in the IT division's master plan, a major component of the division's planning and budgeting process. The college's administration provided the funds to proceed, and the project began with exploration of the IT marketplace to get a broader view of available products and to acquire additional expertise. Blue Spruce Technologies, Inc., was selected to help develop the Secure LAN Strategy because much of the infrastructure and tools that were in place were from Enterasys Networks and many of the Blue Spruce staff were former Enterasys employees.

The development of the strategy began with a vision of the desired end state which included these components:

- Role based access
- Separation of users/systems by risk level
- Differentiation between known and unknown
- Definition of what is unallowable
- Quarantine of policy violators
- Registration of unknown devices

The definition of the Secure LAN Strategy allowed us to evaluate existing resources for their ability to fit within the framework and identify gaps where other products or new procedures were needed. The college's administration has been very supportive of security initiatives and maintaining up-to-date technologies, so there was already a significant investment in products and technologies that could meet the goals of the strategy, including the following:

• *Enterasys Matrix E7/N7 Switches.* A total of 29 seven-slot modular switch chassis connected at the edge via gigabit fiber uplinks to Enterasys 8600 core routers. Each edge switch is connected to two separate core routers using VRRP to provide redundancy in case of link failure. Each building contains at least one edge switch supporting one to three separate networks.

• *Enterasys X-Pedition 8600 Router.* The network core consists of one 8600 router in buildings 2, 5, 12, and 13 connected in a meshed topology via single-mode fiber to provide full redundancy. The X-Pedition 8600 delivers full-function, wire-speed IP routing using OSPF and IGMP and DVMRP.

• *Enterasys Dragon IDS.* The Dragon provides high-speed sensors to detect security events such as network misuse, network intrusions, system exploits, and virus propagations. In addition, it facilitates the analysis of forensic data to determine the impact of network attacks. It combines events on the network with those on the hosts, switches, and routers to help provide automated threat detection, isolation, and containment.

• *NetSight Atlas Management Suite.* This suite of software products enhances the security, management, troubleshooting, and control of all infrastructure devices. The products used are:

1. NetSight Atlas Console. The command and control console from which all NetSight management products are launched. It also provides a centralized console for enterprise wide monitoring of all infrastructure equipment.

2. NetSight Inventory Manager. This component enables the centralized management of all infrastructure components cohesively as a system, keeps a centralized database of all infrastructure components and provides for data collection and reporting.

3. NetSight Policy Manger. This component allows policy rule sets to be defined and allocated at the port level of each switch, across the entire enterprise. These policies define the types of communication allowed on each port.

• *McAfee VirusScan and ePolicy Orchestrator (ePO).* Virus detection and removal is a critical capability within any network to ensure uninterrupted availability of services. However, the ability to ensure that every computer has the software loaded and that the software continues to function as it should is a nearly impossible task. ePolicy Orchestrator is a software solution that enables ITS to centrally manage and enforce antivirus policies transparent to the users. According to policies that are enforced VirusScan is

▶

installed and constantly running, and virus definitions are updated within one hour of their release by McAfee. Memory scans take place every hour, and every file is scanned when it is opened. If any of these policies are not detected, they are enforced within 5 minutes.

In addition to detecting viruses, McAfee VirusScan 8.0i includes firewall capabilities, spyware detection and removal, and buffer-overflow prevention. ePolicy Orchestrator distributes updates to VirusScan settings to all campus users without any user or technician intervention.

• *Altiris.* Desktop workstation images are deployed using software from Altiris that uses IP multicasting to install an entire lab of computers concurrently via a single stream of data that is sent across the network infrastructure. Processes are also in development to use Altiris to install individual applications or updates to applications over the network.

• *Microsoft's Windows Server Update Service.* Keeping desktop operating system software updated is critical in order to prevent the exploitation of vulnerabilities that are regularly discovered and patched within the Windows operating system. With the increase in network-based attacks, the removal of viruses and spyware from a computer is not sufficient. Other computers can take advantage of vulnerabilities in the operating system through its network connection. ITS uses Microsoft Windows Server Update Service (WSUS) to distribute patches to the operating system that are made available as vulnerabilities are discovered.

ITS maintains a standard "core" workstation image for employee computers and builds lab-specific images that contain the software required in various departmental academic labs. The software tools listed above are all part of this core, so the ability to identify imaged workstations from other devices allows the network to treat imaged PCs as trustworthy.

The Five-Step Plan

Once we had created the Secure LAN Strategy and identified existing technologies that could be used within that strategy, we needed to develop a plan for implementing the strategy, identify gaps in our existing technology, and determine how to plug these gaps. The resulting plan consists of five phases:

Phase 1: Acceptable Use Policy. During this phase the various roles were defined that would be used to categorize network users and the type of access that they would be given. Initially the roles would be manually assigned to ports based on the type of user connected to that port. However, once the authentication phases were implemented, the role would be dynamically assigned using groups within Active Directory.

Phase 2: Network Management System (NMS) Application Configuration. The NMS applications assist in the administrative tasks necessary to quickly perform tasks such as device management, switch configuration backup and restore, firmware upgrades, device inventory management and change control, and policy configuration and deployment.

Phase 3: Dynamic Intrusion Response (DIR). In this phase, response processes to network security events were implemented. This phase brought together work that was done in the two earlier phases by dynamically changing the user role assigned to a switch port to a quarantine role when a security event is identified as being sourced from that port.

Phase 4: Authentication of imaged devices. This phase addresses the authentication steps for imaged PCs (a Sinclair PC with standard set of software including antivirus and security patches). After the imaged PC is recognized by the system, the user's role is defined upon login to a network switch-port and the policy that enforces that user role is applied.

Phase 5: Authentication of non-imaged devices. In this phase, non-imaged PCs are scanned by the system, and if the PC has problems, the system places the PC in a predefined quarantine role. If the PC has no problems or its problems have been remediated, it is provided "Web only" access.

Some challenges that needed to be addressed in these phases included the following:

- Creating policies that allow secure communication between network users and systems while simultaneously preventing threats from spreading.
- Mapping the Sinclair business functions which are modeled in the Windows Active Directory OUs with effective and manageable network usage policies.
- Identifying imaged versus non-imaged PCs and assigning "gold" network access to imaged PCs.
- Redirecting non-imaged PCs to a registration/remediation server for the purpose of validating PC configuration.
- Ensuring that the machine meets an acceptable level of security or complies with Sinclair's Acceptable-Use Policy.

- Identifying a viable 802.1X client for non-Windows-XP systems that will be compliant with the security goals of the Sinclair network.
- Determining the best EAP type for desktop 802.1X authentication.

Additional technologies that would need to be implemented to meet the requirements of the plan included:

- NetSight Automated Security Manager (ASM). This additional component of the NetSight suite integrates the Enterasys switching and routing infrastructure with the Dragon IDS to automatically take action on the network, down to the port level, when an attack is identified using NetSight Policy Manager to dynamically modify the role assigned to a switch port, thereby changing the allowable communication for the connected device.
- Microsoft Windows Server 2003 Internet Authentication Service (IAS). The Microsoft IAS Server is a Remote Authentication Dial In User Service (RADIUS) server. A RADIUS server accepts authentication requests from network devices and forwards them to an authentication server, which, in a Windows Server 2003 domain, is the domain controller. The authentication server confirms or denies the authentication request and forwards the result to the RADIUS server, which in turn forwards it to the device requesting authentication.
- Cisco Clean Access. This is a system that authenticates, authorizes, evaluates, and remediates wired, wireless, and remote users and their machines prior to allowing users onto the network. It identifies whether networked devices such as laptops, personal digital assistants, or even game consoles are compliant with the network's security policies and repairs any vulnerabilities before permitting access to the production network.

Figure 1. Sinclair Network Access Levels

Access Level	User	Device
Level One: This is the highest level of access. The user must login with their Sinclair network username and password.	College Employees: This includes all faculty, staff, and student employees. It also includes student use of login IDs that are assigned to campus lab computers.	College-Owned Laptops and tablet PCs with the Sinclair Administrative Software Image
Level Two: "Web Only" access similar to the type of access when connected to the Internet off-campus. The user must login with their Sinclair network username and password.	College Employees: This includes all faculty, staff, and student employees. It also includes student use of login IDs that are assigned to campus lab computers .	Devices without the Sinclair Administrative Image or not owned by the college: PDAs, non-imaged laptops, personal laptops, smart phones, etc.
Level Three: This is a "Guest" access granting "Web Only" access similar to when a user is connected to the Internet off-campus. A login is NOT required.	Anyone: This includes all students and the public.	Any Type of Device

Once the plan was defined, it became clear that a different wireless technology would be required to implement the same controls placed on the wired infrastructure for wireless access. In order to meet the requirements of this strategy, a new wireless technology from Airespace, which has since been acquired by Cisco, was selected through an RFP process. This system uses a "thin" access point with a central controlling switch. The roles of the Acceptable Use Policy, which are implemented on the wired ports using VLANs, are made possible on the wireless network using multiple WLANs, each with a different SSID and authentication method.

The Acceptable Use Policy that was developed in Phase I of the project defined an access framework based on three levels of service. Each level provides a different level of service based on the type of user and the type of device that is being connected. Level One would provide authenticated users on college-owned, imaged devices to connect with the highest user access. The second level access allows authenticated users to use non-college owned or non-imaged devices to connect, but at a lower level of "Web only" access to the network. The third level of service is what can be thought of as "guest" network access. (See Figure 1.)

Even though we defined the Level 3 access within the plan, we had no immediate interest in providing the guest access due to the costs of the infrastructure as well as the cost of supporting this type of access. This led us to investigate vendors that would be willing to bear these costs and provide the service that our customers would require. In August 2005, the College signed a contract with Harborlink to provide the guest wireless access in various public spaces in all of Sinclair's Dayton campus buildings. ▶

Because Harborlink uses the same wireless equipment as the College, Harborlink's wireless network has been designed with the ability to access the college's secure wireless network over the same equipment.

The contract with Harborlink not only provides the guest wireless access at no cost to the college, it also allows ITS to extend wireless access into 30 more areas on the Dayton campus at no additional cost. Harborlink is also working with the City of Dayton to provide free wireless access throughout downtown Dayton. This would eventually expand the guest access available inside Sinclair campus buildings to the outside areas around the campus buildings.

Promotion of Technology and Maturity of Effort

The Secure LAN Strategy, completed in October 2004, has provided (1) a road map for the implementation of network authentication for all computers that connect to the Sinclair network; (2) controlled access for unknown devices; and (3) the isolation and remediation of problems with unpatched or virus-infected PCs. The plan defines a clear path toward a network where access to network resources is based on the role of the user, the configuration of the computing device they are using, and the verifiability that the device is problem free.

Implementation of the plan began in December 2004 with the definition of the various authentication roles for users and devices. The next 2 phases, NMS and Dynamic Intrusion Response, were completed in February 2005. These 3 initial phases were all fairly easy to implement in short time-frames due to their minimal impact on existing services. The authentication phases have both been implemented but will take several months to make fully functional due to the changes that must be made to the computers and other network attached devices. These changes are currently underway using documented processes, and the network grows more secure with every step toward the project's completion.

The first three phases of the project are complete, and all 20 of the campus's buildings are protected by the Acceptable Use Policy. We currently have the full plan implemented on the network switches that support two of the college's buildings. One of the buildings is on the downtown Dayton campus and the other is a newly opened Learning Center in Englewood, a suburb of Dayton. All network switch ports in these two buildings are not only protected by the Acceptable Use Policy, they also require authentication of devices and users trying to connect to the network.

As soon as a connected device is powered on, it is required to authenticate using 802.1x. The network switch passes the authentication request to IAS and if it is successful, the user is required to authenticate. If the user authentication succeeds, he or she is provided with the access defined by the Acceptable Use Policy. If the device authentication fails, the device is isolated into a quarantine VLAN. This separate network authenticates the user and then requires the machine to be scanned and remediated if it is found to have vulnerabilities. The user who is able to be authenticated on a device that was not authenticated is provided with Web-only access but only after the scanning and remediation steps are performed.

Initial wireless access for college-owned laptops and tablet PCs began in August 2005. The contract with Harborlink for the guest wireless access was completed in late August 2005. The guest wireless access and the expanded wireless access areas were implemented in early November 2005. The wireless access control process is functionally the same as the wired process that was described above, even though the technologies and methods used are different.

ITS extensively promoted the expanded wireless services to the campus community. A Web page and other documentation were created to provide information about wireless services to Sinclair faculty, staff ,and students. Sinclair's publications department created posters, flyers, and table tents to advertise the expanded wireless services around campus.

ITS also worked with Sinclair's Web systems team to create a virtual tour of wireless services on the Dayton campus. The tour is found at http://tour.sinclair.edu/. The wireless tour was integrated into the existing campus virtual tour, and it includes maps of wireless access areas and user support information. The campus wireless project was featured in the Dayton Daily News as an economic development innovation for downtown Dayton.

Though another institution may use different tools, the problems that all networks are faced with are similar, and the concepts employed by Sinclair to develop a secure LAN could be adapted and used by any institution.

Quality, Performance, and Productivity Measurements

The greatest quality, performance and productivity measurements are those experienced by users who are not impacted by the secure LAN system itself but by the system's results. The positive impact of a secure, dependable, and available LAN on the productivity of campus faculty, staff and students can't be measured in dollars. However, a system that is not secure and dependable can have a huge impact on productivity, which is directly related to costs.

Every person who uses, or attempts to use, the Sinclair Community College network including current and future students, alumni, and conference/seminar attendees, develops an opinion about the network. This experience contributes to user opinion of Sinclair as an educational institution and ultimately affects enrollment and funding.

In today's IT climate, users expect the network to be everywhere and available at all times, but they expect it to be secure as well. This is the balance that must be maintained through the implementation of this plan. In addition, Sinclair Community College will be able to protect and enhance its reputation of the institution as one who leads the way in IT innovation.

Cost, Benefit, and Risk Analysis

Enterasys acknowledges Sinclair as an important partner in the use of its technologies and agreed to combine the ASM software with a large purchase of equipment as a donation to a fundraising campaign run by the Sinclair Foundation.

ASM is a key component in creating a secure network due to its ability to recognize inappropriate network communication and dynamically change a computer's ability to communicate over the network. After the acquisition of ASM, ITS had all of the tools necessary to complete its vision, but there was much planning that needed to be completed to ensure that the new and previously installed technologies would be integrated into a single, interactive system.

BlueSpruce Technologies, a company founded by some of the creators of the ASM product, was selected to help develop the plan. Once the plan was complete, ITS and BlueSpruce began discussing its implementation. This developed into a second commitment with BlueSpruce in which the company would assist ITS in all of the plan's project phases.

The contract with Harborlink not only provides guest wireless access at no cost to the college, it also allows ITS to extend wireless access areas into additional areas on the Dayton campus at no additional cost.

Security incidents can create intangible costs to the college such as lost productivity or lack of customer satisfaction. In addition, they can create breaches of confidential information that could cause financial penalties for the College. Minimizing the possibility of these types of incidents is absolutely critical.

Customer Satisfaction and Results to Date

Changes within the network infrastructure are being phased in to ensure that each set of changes are thoroughly tested before the next changes are applied. The result is an increasingly secure network that protects user productivity from the malicious or accidental spread of network-borne threats.

All wireless access and wireless devices are now 100 percent secured by this system. This project increased the number of wireless access locations, allowed faculty and staff to be more productive by accessing the campus network wirelessly, increased student satisfaction with the college, and benefited guests and visitors.

ACUTA congratulates Sinclair Community College, winner of the 2006 Institutional Excellence Award. The information presented here was taken from the documentation they submitted for this award. If you have questions about Sinclair's Secure LAN Strategy, contact Scott McCollum, Director, Information Technology Services, at scott.mccollum@sinclair.edu.

▼