Get Connected: An Approach to ResNet Services

Indiana University explains what to do when 13,000 unknown computers connect to your network in three days

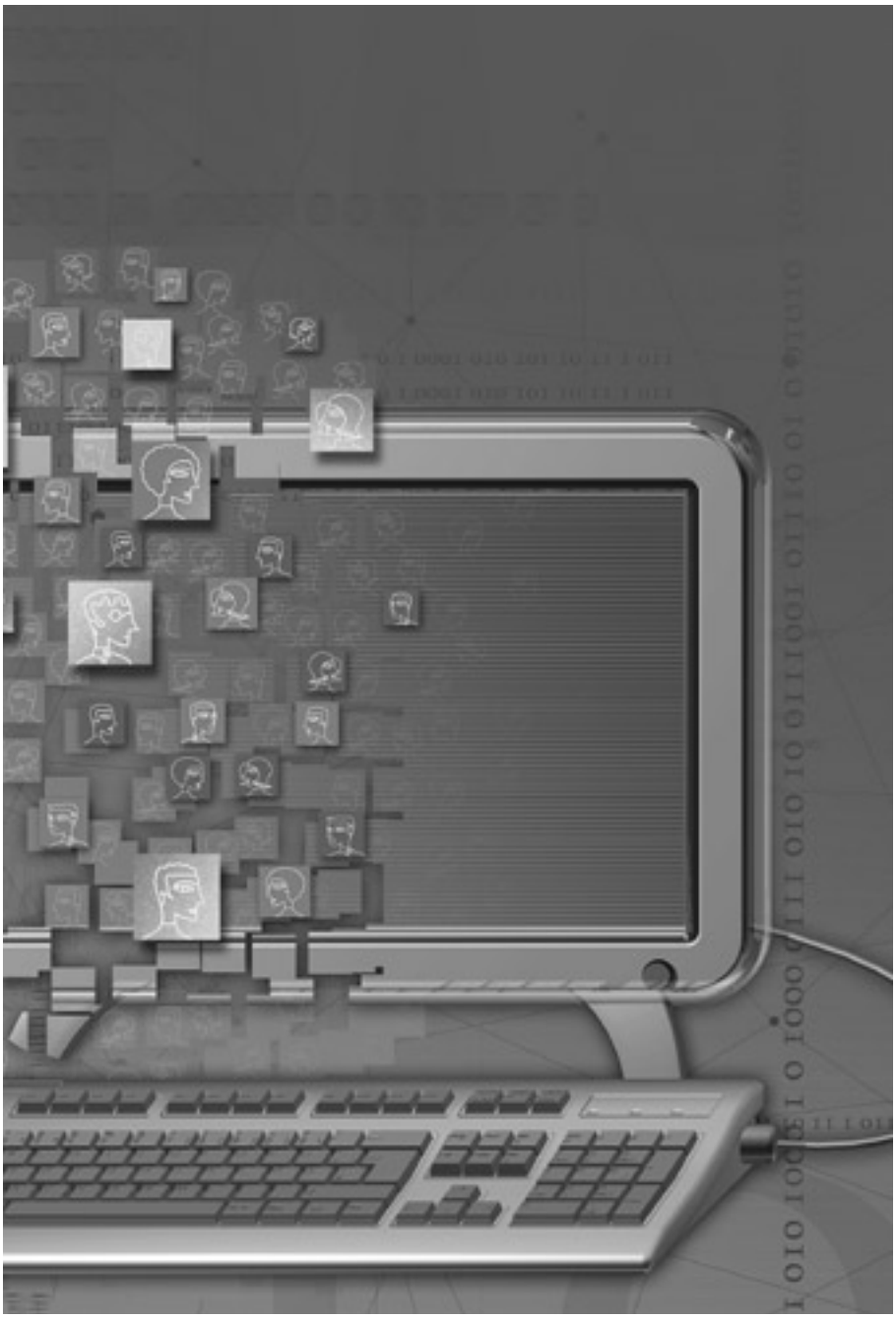
By **Sue Workman, Melody Childs, Jim Causey, Brent Moberly,** and **Christine Fitzpatrick**

As happens on many college campuses at the beginning of an academic year, thousands of students move into campus housing on Indiana University's Bloomington and Indianapolis campuses within a three-day period. More than 96 percent arrive with at least one personal computer (and possibly also a PDA, cell phone, and gaming system), and most expect to connect to the campus network within a few hours, if not minutes, of arrival. Indiana University Information Technology Services (UITS) is charged with ensuring these connections within a reasonable amount of time and without compromising network security.[1]

Many ResNet professionals concur that the task of connecting more than 13,000 computers to the network seems especially daunting in an environment where one compromised machine can cripple an entire network, as happened with the Blaster computer worm in 2003. In a nationwide 2005 ResNet survey conducted by the ResNet Applied Research Group and published by the EDUCAUSE Center for Applied Research (ECAR), IT security "including spyware, adware, and viruses" was reported as the biggest challenge facing ResNet professionals.[2]

Approaches to network access policy and control, quarantine, and mitigation vary greatly across institutions of higher education, ranging from no network policy and no access control to a variety of both home-grown and commercial solutions. According to the 2005 ResNet survey conducted by the ResNet Applied Research Group, about 22 percent of responding universities lack a network registration and access control process for their ResNets.[3] Of those that do offer network registration and access control, nearly half develop in-house solutions. Regardless of whether the solutions are commercial or custom built, few universities actively scan their ResNets for security threats after initial registration, and few solutions employed (less than 30 percent) can quarantine noncompliant computers for self-remediation.

Commercial solutions for network access control and network mitigation typically offer several advantages to smaller institutions, in particular a reduced need to employ software developers and network engineers to maintain, monitor, and manage the university/ResNet network. For the 35 percent of universities that employ fewer than two full-time people to support their residential networks, staffing can be a critical issue.[4] The trade-off when purchasing a commercial solution comes in the lack of ability to customize the solution, plus both large initial capital investment and ongoing maintenance required for network appliances and software. Universities with large amounts of bandwidth may also find that some commercial network mitiga-



Bryan Leister

tion and access control solutions actually create unacceptable bottlenecks in their networks.

Indiana University's home-grown solution, Get Connected, offers unlimited flexibility and at least a degree of stability over the three-to-four-year life span of each version of the Windows operating system. Following implementation of the Get Connected project, the data suggest that efficiency of our ResNet services has improved, support costs have been contained, and student satisfaction with ResNet services has dramatically increased.

Perhaps one of the greatest benefits of Get Connected has been the avoidance of massive disruption resulting from security attacks (such as worms, viruses, and rootkits) on the Windows platform in recent years. This article discusses the history and context of Get Connected, describes the impact the project has had on student connectivity and computer security at IU, and discusses the support model and engine, which IU has licensed for use at Louisiana State University.

The Context

Founded in 1820, Indiana University has grown to eight campuses, 100,000 students, and 16,000 faculty and staff. Bloomington (IUB), a doctoral/research-extensive university, is the flagship campus. With more than 38,000 students, including out-of-state and international students, IUB is home to many nationally ranked programs. Approximately 11,000 students live in IUB campus housing. Indiana University-Purdue University Indianapolis (IUPUI) is IU's urban campus, a doctoral/research-intensive university that is home to the School of Medicine, School of Dentistry, and other professional programs. IUPUI enrolls almost 29,000 students, 98 percent of whom are Indiana residents; about 2,000 students reside in campus housing.

In recent years we have observed trends in computer use and ownership that make our support tasks particularly onerous. Responses to our annual user surveys suggest that personal computer ownership at IU has increased 53.8 percent over the past 15 years, to 96 percent.[5] Wireless coverage for academic areas has grown exponentially (from 1 percent to nearly 100 percent in three years), as have classroom and residential network connections (approximately 100 percent in four years). Use of IU's course management system, Oncourse, has rocketed past 80 percent since its introduction in 1998. Not surprisingly, reports of the time spent using computers by students, faculty, and staff during 2001–2005 increased by 10.6 hours per week to an average of 29 hours per week per user. We have also seen an increase in the number of campus residents who connect more than one IP device to the network (currently about 13 percent). The confluence of these trends creates quite a challenge for the university's front-line IT support staff, particularly

during the early days of a new academic year.

An Evolving Strategy for a Growing Problem

In 1998, IU's IT strategic plan established a vision for a seamless computing environment "across the boundaries of campus, home, residence hall, and community."[6] As implementation of the strategic plan commenced in 1999, IU began a program to revitalize the technology in campus housing on the Bloomington campus. Before this, students residing in campus housing at IUB used a different computing environment from **the one** supported centrally by the IT organization. While the number of machines connected to the network had increased eight-fold, campus housing still had many inactive data jacks, low bandwidth (much of campus housing was not on campus fiber), and an array of outdated and nonstandard equipment in a few residential IT centers. In fall 1999, a number of students were still not connected to the network by the sixth week of classes. While some of these residents were affected by serious issues, others had easily resolvable problems, but the overwhelmed ResNet support staff took weeks to contact even these users. Irate parents telephoned IU's president with their complaints. The situation was clearly unacceptable.

In March 2000, responsibility for IT services in the IUB residence centers moved from Residential Programs and Services to UITS.[7] A manager was hired for the new UITS Residential IT Services group, the network infrastructure was updated, processes were reengineered, and the process of creating a high-quality support model began. Developers from the UITS Support Software and Engineering team were called in to introduce new software tools for Residential IT Services. These network configuration tools were designed to ease the difficulty of network software installation and configuration on the Windows 9x series of operating systems. The tools eased the task of configuration networking for many installations, but were complex and sometimes caused reliability problems. When move-in activity during fall 2000 generated 30,000 calls to the Support Center, it became clear that more needed to be done to improve this experience for students.[8]

A New Approach: Get Connected

The following fall (2001), processes were further improved, and the first Get Connected kit and support model were introduced. Get Connected evolved from earlier network configuration tools but supported a wider range of operating systems and automatically logged process results with a centralized UITS database. These logs allowed support staff to diagnose issues on end-user machines, developers to refine the Get Connected engine's code, and administrators to better evaluate the status of move-in activity.

By 2002, additional improvements were made in IU ResNet services and in the network configuration CD. Get Connected kits distributed during move-in week in fall 2002 included bi-directional Ethernet cables, UITS network configuration CDs, printed user information, and red hang tags for residence doorknobs (to serve as flags for roving support consultants). As many as 60 consultants scoured campus residences looking for users who needed help establishing connectivity. By the end of the five-day move-in period, more than 7,400 students had successfully connected to the IU network. As reported in the UITS annual accomplishments summary, "Fall 2002 marked the most successful Residence Hall move-in week since UITS accepted responsibility for IT in the Halls of Residence."[9]

The environment kept changing, however, and as Internet use grew and the incidence of malicious online activity increased, IU's developers and network stewards recognized Get Connected's potential to protect network resources from hackers, viruses, and worms. The appearance of the Blaster worm in July 2003 further galvanized partnerships with IU's IT Security Office and the UITS Messaging Team, both of which share in the definition of the features of today's version of Get Connected. During the month before the beginning of the 2003–04 academic year, Residential IT Services staff worked with Support Software Engineering and Distribution, the Support Center, Networks, Messaging, and the IT Security Office to assure that student machines in campus housing were secured before being allowed to connect to the IU network. Beyond advancing a more efficient model of support for connectivity, Get Connected became an important agent in IU's IT security program.

Watching the Metrics

Consistent with IU's economic model, UITS has a long-established process of monitoring the cost and quality of its services.[10] This practice has proved invaluable in charting the effects of changes, including the implementation of new services. For example, current data for user support reveals that the UITS support organization logs about 2.5 million personal contacts with users at IU each year, averaging about one contact every 12 seconds 365 days per year. Among the types of personal contact with the Support Center, user walk-in visits are by far the most expensive, averaging $14.19 per visit in 2004–05 (the last year for which data is available at this writing).[11] In addition, the UITS Support Center receives about 16 million online contacts for support each year, including e-mail consultations ($6.36 per contact in 2004–05) and contacts via our online support services (from $.04 to $.11 per contact). The Get Connected CD and process do not eliminate the need for in-person support, but our automated service makes contacts less necessary.

Get Connected costs the university about $100,000 annually to produce—a small price given its many benefits. With the recent reengineering of the Get Connected master setup engine, we expect annual development and maintenance costs to shrink. At the same time, Get Connected helps contain costs for residential IT support at IU. Prior to Get Connected, the Support Center received more than 12,000 calls about network connections during a

single day of move-in week. We did not have enough staff to meet the demand, students could not get their computers connected, and students and parents became very anxious. With Get Connected, the process is automated, and much more secure and helpful. Support areas can handle the demand during move-in week, and virtually all students are connected securely to the network before the first day of classes.

UITS provides in-room support for $25.23 per resident per year. We can also monitor user satisfaction with our services through the annual UITS user survey. A review of data for 2002–03 shows that the introduction of the Get Connected processes and services coincided with a marked improvement in student satisfaction with IT support in residence halls. User satisfaction increased from 85.0 percent in 2001 to 96.8 percent in 2002. The overall opinion rating in 2002 was also very high: 4.08 on a 5-point scale. In 2004, user satisfaction in residence hall IT centers reached 99.4 percent. These satisfaction rates persisted over time. In 2006, Residential IT Support rated 96.2 percent user satisfaction.

The Get Connected Kit

The current Get Connected kit is distributed in a plastic zipper bag to all new residents at the time each receives the key to his or her room. The kit consists of a network cable (compatible with IU's proprietary wiring), a network configuration CD containing the automated Get Connected engine, an IT information booklet, and a red hang tag.[12]

The hang tag appears to be a key to our success with this package. The tag lists a schedule of times support consultants will be circulating through the residences. Students are instructed to put the hang tag on their doors for help during the scheduled hours. A result of this effective mechanism for managing expectations is that students refrain from calling the Support Center while they await their appointed support visits. The hang tag also averts the need for appointment scheduling and reduces instances of missed appointments.

The Get Connected Support Model

More than a software solution that automatically secures, patches, and configures student computers, the Get Connected process at IU is part of a larger online support initiative, IU's Online Support Environment (OSE), which uses online and self-service services and support to leverage support resources.[13] The success of IU's move-in week hinges on intelligent leveraging of technology and people. A contingent of 60 consultants is critical to making the move-in process work. Even with the assistance of the sophisticated Get Connected engine, we estimate that one of every 10 students attempting to connect to the network will need assistance. Students may have arrived on campus with poorly functioning equipment, they may have problems with trojans or viruses, or they may be unable to install the software. Our experience suggests that each of the 60 consultants assigned during move-in week will engage in approximately 20 in-room consultations. The schedule for moving this small army of consultants through 15 campus locations is quite intense. It is coordinated around other Welcome Week activities on campus to maximize use of the time students are likely to be in their rooms. Consultants circulate until about 11:00 each evening.

In the week prior to move-in, the consultants participate in intensive training. They learn to troubleshoot common and not so common problems that prevent computers from connecting to the network. As the consultants sweep through campus housing, they communicate with each other via radio and share knowledge. Seasoned consultants advise rookies, who soon become adept at solving problems quickly and courteously. Communicating effectively is critical in an environment when conditions can change in the blink of an eye. For example, the sooner the network operations people can track the source of a rogue DHCP server, the sooner the affected users can get online.

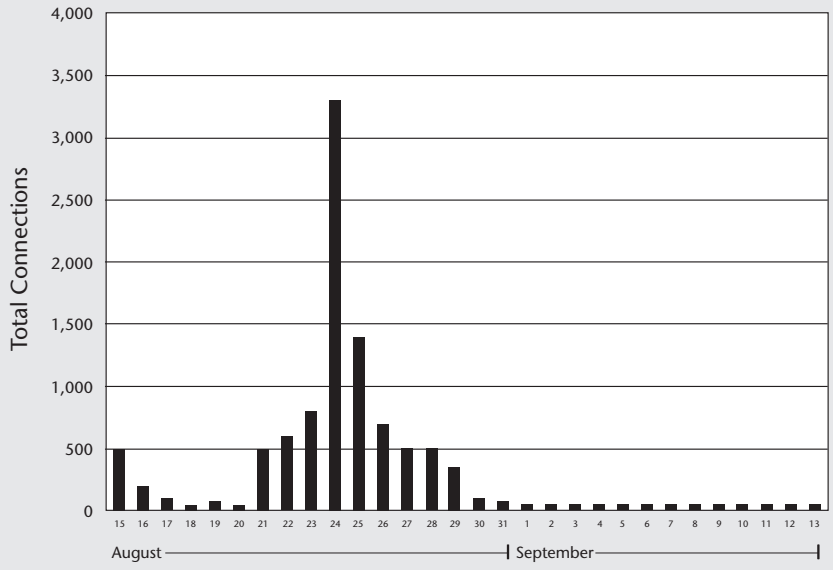
The intensity of move-in week at IUB is apparent in the connection reports we receive from Get Connected (see Figure 1).[14] The spike at midweek occurred on a day when about 8,000 students arrived on campus. Not all arriving students attempted to connect to the network that day, but many obviously did.

Today's Get Connected Engine

Get Connected serves two audiences: student residents and technology

Figure 1

IUB Move-in Week Get Connected Activity, 2005



support staff. For residents, Get Connected provides an interface that allows them to track their progress through the installation, lets them overcome errors that arise in this complicated process, and provides them enough information to report persistent errors accurately to support staff. Local workstation changes are mitigated as much as possible to avoid burdening the user with irreversible changes.

Get Connected also provides important tools for support staff. Diagnostics allow support providers to determine exactly why particular machines cannot connect. Short-term response data enables us to identify new problems, such as a new worm on the network. Finally, the diagnostic and reporting features provide useful information for improving the engine. We can also determine immediately whether or not there is a bug in the engine, and we can apply changes that will affect anyone who connects with the same version of the engine during the semester.

Security Features

Modern operating systems can often connect to the Internet without support intervention (barring serious workstation problems). However, the constantly escalating pace of attacks, particularly on Microsoft products, requires a layered approach to minimize threats posed both to student workstations and to the university's network infrastructure.

Get Connected takes a number of steps to deal with security threats. First, it prevents users with insecure versions of the Windows operating system from connecting to our network by requiring Windows XP and installing Service Pack 2 if needed. Get Connected also blocks critical network ports used for threat propagation and deploys Microsoft's Malicious Software Removal Tool in scan-only mode to detect if the user's computer is infected by known viruses and worms.[15] It also configures the Windows Automatic Update Service to perform automatic updates daily. If the user is not running third-party firewall software, Get Connected activates the built-in Windows firewall and verifies that the user has up-to-date antivirus software installed that is actively protecting the operating system. It also configures the user's computer to use more secure network authentication protocols and applies comprehensive security policies developed by IU's IT Security Office. Finally, Get Connected adds computers running Windows XP Professional to our Active Directory in a campus housing-specific group to allow for remote management. Once these steps have been completed, Get Connected notifies the DHCP server that the system is ready to receive a valid IP lease, and the user may continue the process of registering the system.

The constantly escalating pace of attacks requires a layered approach to minimize threats posed both to student workstations and to the university's network infrastructure

Windows users who opt out of, or encounter insurmountable technical issues with, the automated Get Connected process can request manual network registration. Support consultants must first confirm that users' computers meet the security standards implemented by the automated Get Connected process before granting a manual registration. Residents who need to register gaming consoles or other Internet-enabled appliances can also request manual registration.

Get Connected for Macintosh is dramatically simpler, due to the reduced attack surface and lower number of threats posed against that platform. Get Connected for Macintosh installs Norton Antivirus to help prevent the spread of viruses.

How Get Connected Works

Get Connected relies on components that run on individual student workstations and on central Web servers. It is specifically designed to work with the Indiana University network infrastructure.

Student computers that have not been verified by the Get Connected process are placed in restricted subnets by the university network address servers. These subnets allow users to access network support resources, but other network requests are redirected to Web servers that require the users to register their computers for network access. If the user attempts to connect to any site with a Web browser manually, or before Get Connected has finished, the Web server will tell the user to complete the Get Connected process.

Get Connected for Windows consists of the following key elements:

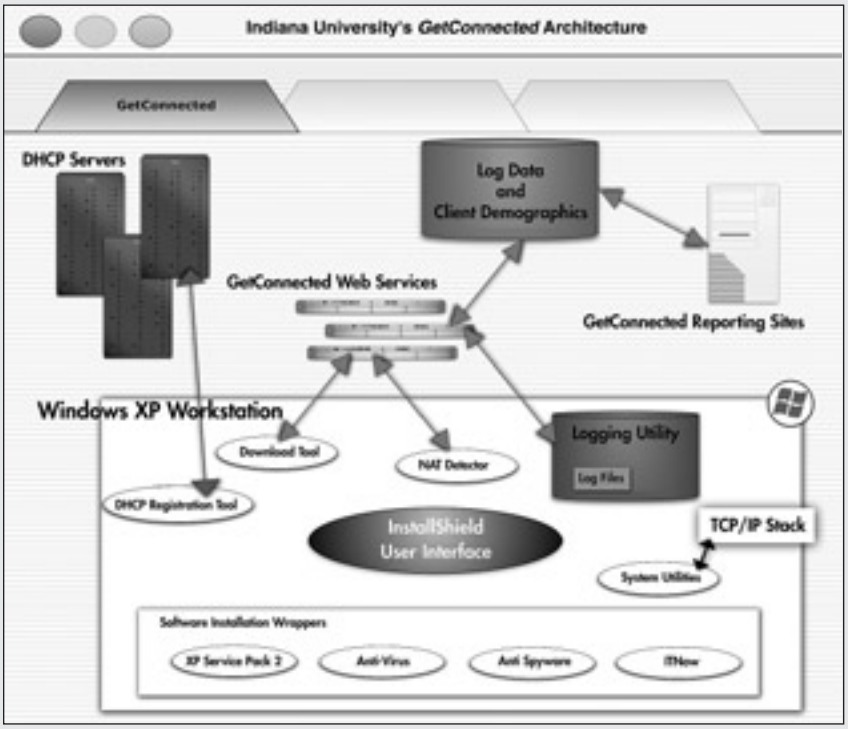
- A master setup engine that drives the entire configuration process, providing the primary user interface and a state machine that tracks tool progress across system reboots.
- Software installers for critical updates, components essential to Get Connected, and licensed commercial software. Depending on the licensing requirements for these installers, some are included with the engine itself, while others are automatically downloaded from UITS Web servers for installation.
- Helper libraries that handle such tasks as creating system restore points, sending logs to UITS servers, downloading and updating various utilities and installers, and generating and communicating the credential used by DHCP servers to verify that the process is complete.

Each library or installer is executed by the master setup engine, which then evaluates the success or failure of that component, logs the results locally and centrally, and notifies the user appropriately. (See Figure 2.)

We wrote the majority of our code in the .NET Framework because of the tremendous productivity and code-quality benefits received from developing in a managed code environment. This choice was initially controversial, both due to the time needed to install the .NET Framework on user workstations and the newness of the languages at the time we switched to them. This invest-

Figure 2

Get Connected Architecture



ment easily paid off in terms of tool reliability and industry support.

The server end of Get Connected consists of an SQL Server 2000 database accessed by ASP.NET Web services running on Microsoft's Internet Information Server. All communications between Get Connected clients and the Web services use SSL-encrypted HTTP for additional security. The Web pages used for real-time and aggregate reporting are ASP.NET pages as well (see "The Logging System" below).

The Get Connected Engine

The Get Connected engine follows a progressive or "checklist" model, stepping through a series of tasks, evaluating the success or failure of each task and acting accordingly before moving on to the next task. Each time the engine is run, it starts at the top of its task list and works its way through the list until it either completes the list or encounters an error condition. If need be, the engine can restart the user's computer and continue after the restart. In this case, the engine bypasses redundant interface tasks, but it always performs a key set of verification tasks before continuing.

The User Interface

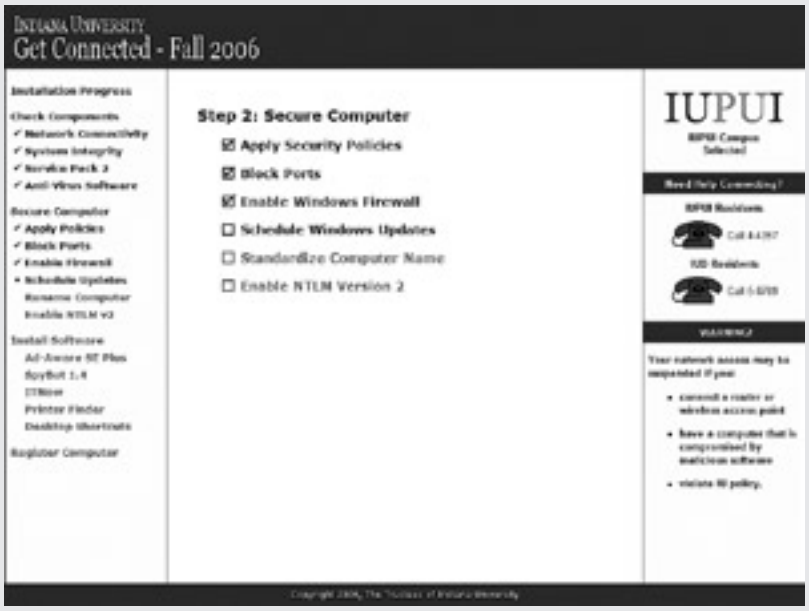
The Get Connected user interface primarily allows residents to monitor their progress through the connection process. The user interface also contains campus support contact numbers and a summarized version of the resident's responsibilities as a citizen of the campus network community. (See Figure 3.)

The Logging System

The engine's logging system provides support consultants and developers with a detailed account of residents' progress through the Get Connected process. The user interface's master and stage-specific checklists provide efficient summaries of the engine's progress, but the logging system provides a detailed task-by-task accounting of the Get Connected process. As the engine iterates through its various tasks, it appends entries to the log file, allowing support staff and developers to evaluate the success or failure of each task. The log file itself is in HTML format, and the engine leverages HTML's markup potential to distinguish significant events within the log. This allows support personnel to scan the log file more efficiently for potential issues.

Figure 3

Get Connected User Interface



The Get Connected engine uploads log files at regular intervals to a logging server, where they can then be viewed remotely by developers and support personal. Log files uploaded to the server contain event codes that describe individual events in the process, as well as the state of the process as a whole. The engine also classifies each log file according to the username and campus provided by the resident. Even if this information is not yet available, the engine transmits each log file with a unique, user-specific identifier.

Consultants can use any or all of these details to access residents' log files remotely from the logging site. A consultant can also retrieve every log file associated with a resident and use this information to understand that resident's installation history. For example, if Windows XP Service Pack 2 fails to install because a resident lacks the hard-drive space required for the installation, then that resident's Get Connected log file will indicate as much, and the consultant can then recommend an appropriate course of action. Likewise, if a resident has run the engine multiple times and encountered the same issue each time, then the logging site will allow a support consultant to understand this trend and act accordingly.

The logging server also provides information in real time about the engine's performance. We can average the number of restarts needed to complete the Get Connected process and determine how long it takes a resident to complete the process. We can aggregate data for all users and thus have an accurate picture across the board. These data also tell us when residents choose to start the process. This information helps us allocate support resources.

Because each error condition is a specific event, we can also track error trends in real time and use these data to allocate support resources. For example, early log results showed that many residents running the fall 2005 version of Get Connected were encountering error 1103: No Administrator Password Set. We were then able to inform the support consultants about this trend before the fall rush and distribute additional instructions to residents about how to resolve the issue. We also used this data to improve future versions of the Get Connected engine.

Because we can now use data gleaned from the logging server to get a fairly accurate picture of move-in events, we are far less likely to fall into the "Chicken Little" mode of crisis management

Because we can now use data gleaned from the logging server to get a fairly accurate picture of move-in events, we are far less likely to fall into the "Chicken Little" mode of crisis management, where issues affecting perhaps 1 percent of residents get 99 percent of our attention because those residents (or their parents) are unusually vociferous. The logging system allows us to contextualize each error report and assign support resources accordingly.

Current Issues and Plans for Improvement

As soon as move-in week ends, planning for the following year's version of Get Connected and support cycle begins. A week or two later, we debrief with our partners. We assess whether the DHCP servers were up to the task, whether support staffing was adequate throughout the week, and what bugs or connection failures were identified. All this information is crucial to our ability to make further refinements to our process and Get Connected.

The following refinements are earmarked for future versions. First, Get Connected currently installs Windows XP SP2, turns on Automatic Updates, and runs Microsoft's Malicious Software removal tool in scan-only mode to guarantee that user workstations are free of viruses or other malware recognized by that utility. It does not guarantee that the user's computer has received all extant critical security patches before allowing DHCP registration. Results from internal tests show that the Windows Automatic update service begins downloading and installing missing updates on users' computer often within 10 minutes of the user's obtaining an active network lease. Right now, we feel that this provides an acceptable level of protection, but we are investigating ways of applying critical post-SP2 updates.

Second, Get Connected currently relies on users' being logged in with administrative privileges. This is not compatible with the new user access control model designed for Windows Vista. Get Connected is currently being redesigned to allow limited users to run the tool, elevating them to administrative privilege only when such access is necessary.

Third, Get Connected would ideally also encourage users to run their own Windows XP workstations in least-privilege (or user) mode and to log in with administrative privileges only when such an elevated privilege level is absolutely necessary (say, to install new software). Such a step would greatly reduce a system's attack surface to various types of malware and rootkits delivered via social engineering attacks. However, it is difficult to implement, both technically and due to issues with user education.

Fourth, we primarily distribute the Get Connected engine on CD, which has two primary benefits: (1) it reduces network traffic associated with downloading Get Connected installers as well as the engine itself, and (2) it allows us to implement security precautions before users physically connect their computers to the network. For summer 2006, however, we produced a lightweight, downloadable version of Get Connected for IU visitors, and this fall, we plan to deploy a similar version of Get Connected for Greek housing residents. Of concern, however, is that these users could potentially be vulnerable to attacks while downloading Get Connected, and we are monitoring them closely as we consider whether or not to make Get Connected downloadable to the more general campus housing population.

The Get Connected Engine in the Commercial Context

During the years in which the Get Connected process was initiated and refined, the commercial network security space has blossomed, and a large number of products from vendors both major and minor have come on the market. Some of these products provide functionality not currently available in the Get Connected engine, such as guarantees of network quarantine based on system health criteria. Others come from industry consortia made up of major players, such as Cisco and Microsoft. IU continues development of the Get Connected engine in the face of these significant players for several reasons:

- *Vendor lock-in.* Many commercial solutions are designed to work only with one client operating system (such as Windows) or with specific network hardware or server infrastructures. IU, like many higher-education institutions, has a heterogeneous environment designed to provide maximum functionality for all users. The university cannot easily replace significant long-term investments in server hardware and software and networking equipment, nor can it dictate to users that they not use certain platforms or products.
- *Scalability.* Get Connected relies on client-based software to carry the heavy load of securing client workstations, relying on our servers only for logging, downloads, and final certification. This makes the product extremely scalable. Get Connected's server resources provide downloads, data logging, and reporting for two campuses and thousands of users on production hardware shared for a number of other mission-critical services, with virtually no issues of load or downtime.
- *Customization.* The Get Connected engine allows customization for the features we and our customers require. Commercial solutions typically provide features that we will not (or cannot) use while lacking critical features we would still have to develop ourselves.
- *Cost/performance benefits.* Lastly, IU continues to focus on development and refinement of Get Connected because of its excellent cost-to-performance ratio. The expenses incurred in developing the product are dramatically less than those of equivalent commercial products, particularly when factoring in the costs of integration and customization of off-the-shelf products.

Get Connected provides a broad range of functionality found nowhere else. At the same time it provides the majority of security features provided by heavyweight solutions but at a fraction of the cost. *e*

Acknowledgments

In any undertaking of this sort, organizational partnerships are essential to delivering effective service. The process of improving ResNet services at IU and developing the Get Connected process could not have been accomplished by an isolated residential IT services group. The cooperation and partnership of many within and outside the IT organization were crucial, including UITS network operations, network engineering, and messaging staff; the UITS Support Center; the IT Security Office; the UITS Support Software and Engineering team; our colleagues in the IU residential housing unit; all the resident advisors; and especially the students themselves.

Endnotes

1. Much of the information in this article was previously presented by Workman, Childs, and Causey at the EDUCAUSE 2005 Annual Conference in Orlando, Florida.
2. K. Bullard et al., "2005 ResNet Survey Results: A Baseline Analysis" (Boulder, Colo.: EDUCAUSE Center for Applied Research, Research Bulletin, Issue 20, 2005).
3. See <http://www.resnetsymposium.org> (accessed August 7, 2006).
4. Ibid.
5. The annual UITS user survey is available at <http://uits.iu.edu/scripts/ose.cgi?anwq.ose.help> (accessed August 7, 2006).
6. "Indiana University Information Technology Strategic Plan: Architecture for the 21st Century," May 1998, <http://www.indiana.edu/~ovpit/strategic/> (accessed August 7, 2006).
7. Subsequently UITS was also charged with support for IT in IUPUI student residence facilities.
8. Because 2000 was the first year UITS supported IT in the residence halls, we do not have telephone data from previous years for comparison. Indeed, this level of difficulty may have been typical for semester start-up prior to implementation of the improvements described here.
9. *UITS Accomplishments Report 2002–2003*, Indiana University, 2003, <http://www.indiana.edu/~uits/cpo/accomp/accomp03.pdf> (accessed August 7, 2006).
10. C. S. Peebles et al., "Measuring Quality, Cost, and Value of IT Services," *Proceedings of the Annual Quality Congress*, American Society for Quality, Charlotte, N.C., Vol. 55, No. 0, May 2001, pp. 468–493.
11. "UITS Report on Costs and Quality of Services," UITS, Indiana University, <http://uits.iu.edu/scripts/ose.cgi?apjw.ose.help#cost> (accessed August 7, 2006).
12. Our current hang tag was inspired by those presented at the 2001 ResNet conference at Stanford University.
13. G. Elmore, J. Holloway, and S. Workman, "Customer-Centered IT Support: Foundations, Principles, and Systems" (Boulder, Colo.: EDUCAUSE Center for Applied Research, Research Bulletin, Issue 23, 2004).
14. Graphical assistance for this figure was provided by John Herrin, UITS Communications and Planning Office.
15. Microsoft's Malicious Software Removal Tool also has the capability of removing many of the viruses and worms that it detects, but we require users to run the tool manually to clean their systems or contact our support center for assistance in doing so. Here, our goal is to alert the user to potential problems—we do not want to automate a process that could result in the user's losing data.

At Indiana University, Sue Workman (sbworkma@indiana.edu) is Director of User Support, Jim Causey was an architect and software engineer with the SSED team who designed the first version of Get Connected and is now a programmer-writer with Microsoft, Brent Moberly is a software developer for Information Technology Services, and Christine Fitzpatrick (cfitzpat@iu.edu) is Communications Officer, Office of the Vice President for Information Technology and CIO. Melody Childs is Deputy CIO and Executive Director of User Support and Student IT Enablement at Louisiana State University and Chair of ResNet.