

Case Study:

**Planning and Operating a
Wireless Authentication
and Policy Management System at
Harvard Medical School**

Wireless at 'The Med School': Past, Present and Future



www.bluesocket.com

The Organization:

**Harvard Medical School
Boston, Massachusetts (USA)**



The Harvard medical community is a complex group of independent yet interdependent hospitals, teaching & learning organizations, and research institutions in which the Harvard University Faculty of Medicine conduct research, educate future physicians and scientists, and provide state-of-the-art patient care.¹

All together, Harvard Medical School (HMS) includes 50 academic departments that employ approximately 13,000 full and part-time instructors, professors, researchers, residents, interns and post-doctoral fellows as well as 700 medical students.

While the community extends to facilities around the world, the nexus of HMS is based in the Longwood Medical Area of Boston, Massachusetts in a beautiful marble quadrangle that houses the School's administration and basic science departments. Less than one mile from "The Quad" is a collection of affiliated, world-class hospitals including Brigham & Women's, Children's, and Beth Israel/ Deaconess Hospitals that also serve as the clinical training grounds for Harvard medical students. This massive community is associated with three health care systems Partners Health Care, CareGroup and Harvard-Pilgrim Health Care, each which share HMS's academic missions of teaching and research.

Harvard Medical School has a large WLAN infrastructure with a wide variety of networking equipment is in use: Nortel and Cisco switches, Cisco Access Points for 802.11b networks, Bluesocket Wireless LAN Gateways (for user authentication), and a multitude of wireless access cards and mobile devices. HMS employs 53 people in its central Information Technology Department to keep its computing systems and networks up and running.

Past: State of Wireless at Harvard Medical School in 2001

Students have often become the catalyst for change and this is certainly true of their push on the Harvard Medical campus to wirelessly connect with campus IT resources.

It started with students deploying low cost wireless access points across campus. By 2001, an increasing number of wireless access points were operating in public areas on the Harvard Medical School campus. These access points include those installed and supported by HMS's Information Technology Department as well as APs installed by students and faculty themselves independently. From the library to classrooms to study centers, WLANs proliferated.

Not surprisingly, supporting and securing this expanding wireless infrastructure emerged as a concern to the HMS IT department. Given the wide variety of wireless technologies being used or planned—different protocols (802.11b, 802.11a); offerings from different vendors (Cisco, D-Link); and a widening assortment of wireless devices (laptops, PDAs)—managing these networks and ensuring interoperability became a daily challenge.

In early 2001, there still was no standard method in place to provide wireless end-users' with access to HMS's wireless networks. "Some of the wireless networks were operating with no security provisions at all," says Joe Bruno, Associate Dean for Information Technology and Chief Information Officer, Harvard Medical School. "Others used WEP encryption (which can be easily broken); and yet another group used a security scheme based on MAC IDs on wireless devices, which we found as imperfect because Harvard wants to authenticate users, not devices. Additionally, operating networks used different names and naming conventions which created a bigger management headache," says Bruno.

"Interoperability between networks was impossible," says Steve Martino Director, IT Computing and Network Infrastructure, Harvard Medical School. "We wanted to ensure continued access when a wireless user leaves their local network and comes within access range of another network."

In the summer of 2001, a wireless initiative was launched at HMS to evaluate and explore the implementation of a campus-wide authentication and policy management solution. This wireless initiative derived its guidelines and objectives from a meeting held by Harvard's University Technology Architecture Group (UTAG) in May 2002. The guidelines of this group were summarized in a document entitled "**Core Principles for Wireless Networks.**"

Harvard's Core Principles for Wireless Networks (May 2001)

1	Harvard wireless users should be able to use wireless facilities seamlessly anywhere in the University
2	Individual schools manage their own portions of the network & set own rules for access
3	Network should be constructed with standards-based technology & support all popular user platforms
4	The wireless security strategy for non-Harvard users should not hinder the service of existing Harvard users

The UTAG agreed to work towards a technical solution that:

- Is browser-based
- Supports SSL for encryption/security
- Supports multiple authentication mechanisms: Harvard University ID/PIN
- Standard end-user menu driven interface

Harvard Medical School's Checklist for Wireless Deployment/Management

"Beyond what the UTAG recommended as its guidelines, at HMS we had our own wish list for a solution for wireless authentication, authorization and policy management," says Joe Bruno. Here's what Bruno says HMS-IT was looking for:

	1	<p>A solution that is simple to implement and easy to manage "It was important that the wireless systems we deployed would be easy to install and operate. Decreasing the number of support calls, would give our team more time to provide help and services in other areas."</p>
	2	<p>Support for the trend of converging technology "Given the assortment of different wireless options (devices, access points, platforms, etc.) available and coming soon, we were cautious to avoid a single vendor solution. It was important that our management platform be open to support whichever ways our wireless users choose to work."</p>
	3	<p>Imperative support for current and emerging standards "There's an alphabet soup of Wireless LAN standards today. While 802.11b is the predominant standard today, HMS needs to be flexible to support other emerging standards in order to accommodate future wireless activity. 802.11a looks especially inviting to researchers who work with bandwidth-intensive medical imaging---large files that could clog throughput on an 802.11b WLAN."</p>
	4	<p>Scalability "Speaking to a number of my counterparts at other medical schools, I learned from the prior experience of peer institutions that wireless starts in small workgroups, and then can rollout in a targeted way vs. needing to do a complete enterprise-wide deployment. At the same time, wireless spreads like wildfire and any solution we would adopt would need to be able to scale throughout our enterprise, quickly, efficiently and as painlessly as possible."</p>
	5	<p>No more clients "Any solutions requiring device client software would be a violation of our key principle for browser-based access. We expressly wanted to avoid the pains of having to install and constantly update current versions of client software on every wireless device on campus! Client software is a throwback to the days of tethered computing."</p>

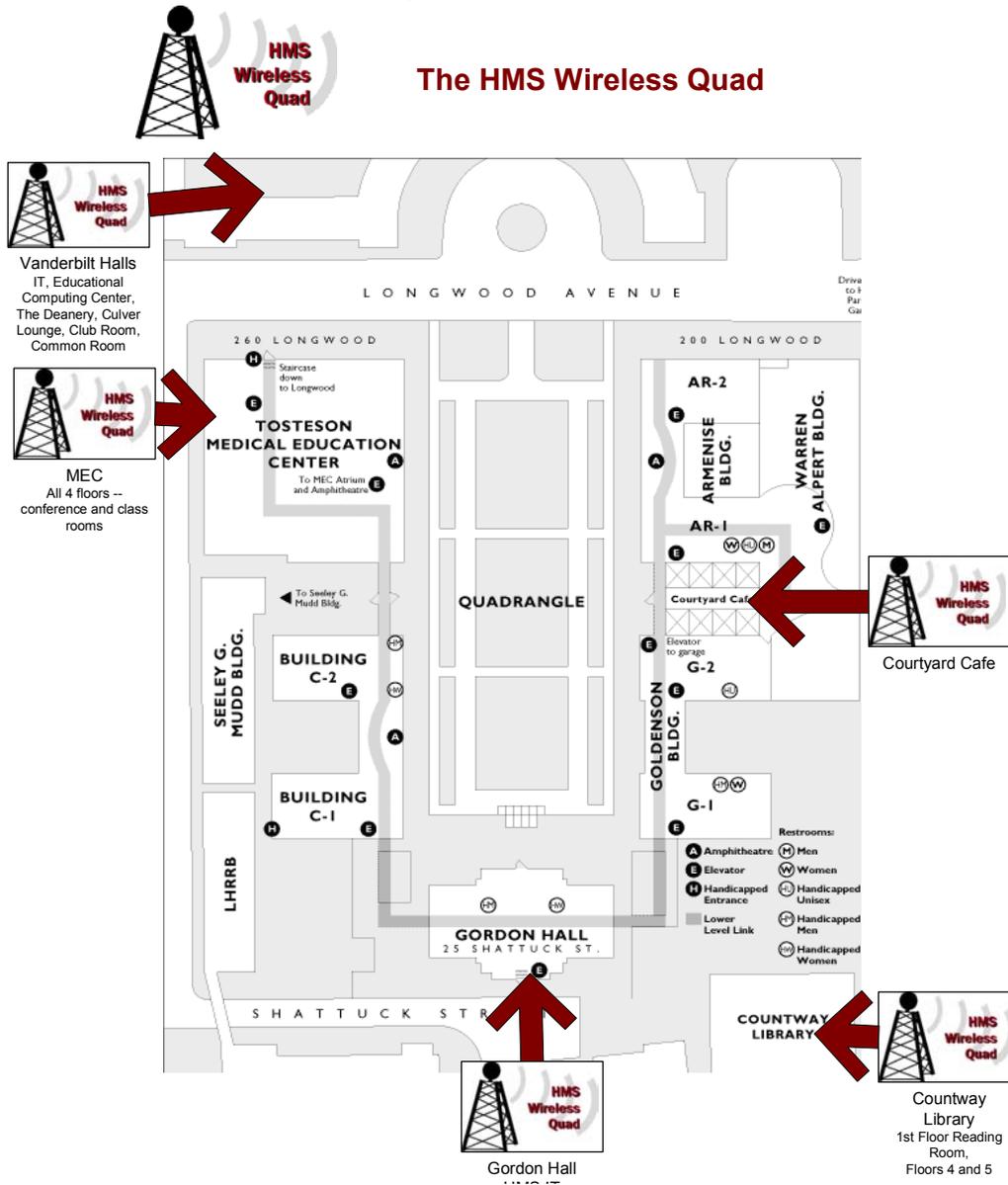
Based on the UTAG "Core Principles," HMS IT's Wish List, and an intensive evaluation process including trials in a non-production network, Harvard Medical School selected a solution based on Bluesocket Wireless LAN Gateways to support wireless networks throughout the campus.

Present: Harvard Medical School's "Managed" Wireless Campus

Today, using Bluesocket's Wireless LAN Gateway products, wireless networks on the HMS campus are inter-connected in a way that simplifies wireless network management and improves the end-user experience while ensuring appropriate security, support for standards, and interoperability.

Wireless Access across Campus

Widespread wireless access is now possible from various locations around the HMS campus centered on the "HMS Wireless Quad."



Universal authentication of wireless users via Harvard's Directories

“There shall be no access without authentication,” says Joe Bruno. “The HMS Wireless Quad is dependent on authentication of approved users through existing databases as a way of allowing or disallowing connectivity to networks or the Internet. In order to allow maximum usability we determined that the solution needs to be an open system and would not require software clients. This means that a user who has associated with an access point but has not authenticated to the network can access other hosts associated to the same access point.”

Today, when members of the HMS community attempt to log-on wirelessly they are directed to a browser-based user interface that prompts them to select an authentication server, and then enter a user name/password combination. Bluesocket Wireless LAN Gateways then authenticate each user to HMS’s LDAP directory maintained by HMS IT. Once authenticated, network users are then able to access network resources for which they have been authorized.

“Because Bluesocket Wireless Gateways integrated easily with our LDAP directory, providing widespread authenticated access for the entire Harvard Medical community happened within one week of installing our Bluesocket devices,” says Joe Bruno.

Authenticating users, not devices, has proved to be a prudent policy/approach as students and faculty may seek access to servers from a variety of devices and from a variety of locations. In summer 2002, Harvard University rolled out universal authentication across most of its campuses in the Greater Boston area. Now, when a Harvard Medical student wants to travel to Harvard Yard in Cambridge and conduct research at either the Widener or Cabot Science Libraries, they can just turn on their laptop and get connected.

Welcome to Harvard Wireless

Wireless Communication

Harvard Users

Authentication Server
Any

User Name
[Input Field]

Password
[Input Field]

Login

Change Password
Install CA Certificate
Help

July 23, 2002
Powered by bluesocket™

HMS Wireless Quad

Use of this network acknowledges that you are accepting responsibility for your actions and security of the computer you are using.

[Security](#)
[Speed](#)
[Airspace Policy](#)
[Wireless Enabled Areas](#)

Logging In: For members of the HMS Community:
Select the HMS eCommons and enter your eCommons login name and password.
For visitors from other Harvard Schools:
Select the appropriate authentication server and enter your user name and password.

Getting Help: wireless.med.harvard.edu
For Faculty or Staff: Contact the IT Help Desk at 432-2000 or Help_Desk@hms.harvard.edu
For Students: Support@student.hms.harvard.edu

Security of the Airwaves

Beyond authentication and authorization security, the well publicized lack of privacy and confidentiality inherent in most wireless networks caused Harvard's IT managers to seek WLAN security solutions that could encrypt data as well.

A June 2002 article in **The New Architect** entitled "Prescription for Wireless" quotes John Halamka, associate dean of Harvard Medical School and CIO of CareGroup on the importance of security for wireless on the HMS campus:

*"We had security concerns with this project," recalls Halamka. "But we took the appropriate steps to address them." The school uses standards like IPSec for protected tunneling and authentication across the wireless network. HMS also deployed security hardware from Bluesocket, a wireless LAN specialist in Burlington, MA. Bluesocket's hardware is similar to a firewall that sits between a company's wireless access points and its core, wired network. If a hacker breaks into the system, Bluesocket's hardware prevents the hacker from probing wired networks and connected back-end systems."*³

The HMS IT department recommends that wireless users of the HMS Wireless Quad use encryption techniques such as Secure Socket Layer (SSL), Virtual Private Networking (VPN), and Secure Shell (SSH) to protect themselves from attacks and ensure the integrity and security of data transmissions. By channeling all wireless data traffic from wireless devices and access points through Bluesocket Wireless WLAN Gateways before it reaches the wired network, HMS-IT is able to run each user session in a separate IPsec tunnel and set appropriate levels of security to protect network resources and data transmissions from unwanted security breaches.

Ensuring Interoperability with Other Wireless Systems

The definition of an HMS "faculty member" is anything from a physician or researcher who reports to the HMS campus every day to a visiting lecturer who comes for an hour a month to deliver a specialized tutorial to students. In addition, HMS attracts academics from other Harvard schools as well as MIT, so having a system that would require common equipment on the end-user part was imperative. "Bluesocket's open and non-proprietary approach addresses the fact that students and faculty alike may go between several different wireless networks within the same day," says Andy Abrams, a former network analyst who worked on the project.

Wireless Networking at Harvard Medical School Today

▪ MyCourses E-Curriculum

Beyond the convenience that wireless provides members of its community to browse the Web or send e-mails without having to plug in an Ethernet cable, HMS has made its entire curriculum available online. MyCourses (an eCurriculum platform), was rolled out in August 2001 following a pilot program. Making extensive use of PDAs and wireless access, MyCourses lets students track their calendars, lecture locations, breaking school news and announcements virtually while reducing the need to print out reams of daily agendas and course notes. Not only has this made students more efficient but in its first year of use, the MyCourses system saved the university \$150,000 in paper costs.

- **Connect, Communicate, And Collaborate**

Working and studying wirelessly enhances collaboration among students and fosters improved interaction between students and faculty. "During tutorial, having wireless web access on my notebook computer facilitates accessing resources immediately as they are relevant to discussion," says Ben White, a second year HMS student. "It also creates a much more efficient work environment and allows me to save a significant quantity of time during the day." Communication between members of the school is easier, even relaxing as faculty, staff and students can sip a cappuccino in the Wireless Quad's Courtyard Café while responding to e-mail or surfing the web.²

HMS's wireless networks integrate into the School's innovative eCommons project—a pioneering effort launched in 1998 to foster better collaboration and communication between members of the HMS community and its affiliates. eCommons lets community members create their own personalized desktop, and access electronic resources including websites and libraries, databases and e-mail directories. The eCommons portals let users manage information based on their role in the community (e.g. faculty or student) or interest in particular topics (e.g. bone tumors or eating disorders).

"I believe our efforts to provide seamless access to all sorts of digital resources and a real commitment to a collaborative work environment sets Harvard Medical School apart from its peers," says Joe Bruno.

- **Flexibility**

At HMS, wireless goes hand-in-hand with in-dorm high-speed wired access. For students living in student housing, each room is equipped with a 100MB connection, implemented with a certified CAT5e Ortronics cabling system and Nortel Baystack 450 fast Ethernet switches. As most students own their own laptops, they now have the option to plug in, or unplug, whenever and wherever they want to.

- **Mobility in Medicine**

Healthcare pros never stay put—from the beginning of their medical education throughout their entire careers as physicians, medical students/doctors are increasingly mobile. Moving from classroom to operating room; lab to library; offices to patients' rooms in teaching hospitals—members of the HMS medical community increasingly expect "anywhere, anytime" access to information and the ability to share that information with whomever they wish. While wireless is not yet found all over the HMS campus, students, administrators and faculty all find the concept of ubiquitous access very attractive. "Bluesocket's support for Secure Mobility—the ability to stay seamlessly and securely connected as wireless users move across subnets is a capability that our mobile students (in particular) have been asking for," says Steve Martino.

- **Wireless Improves Research**

With wireless access availability at HMS's Countway Library of Medicine, students can use their laptop while conducting research at one of the great medical libraries to look up a resource, go to the resource online while in the stacks, find it, evaluate it and then place it into a bibliography or literature search database much more efficiently than in the days BW ("before wireless"). According to Joe Bruno, "Students now use their laptops to compile their own datastores while doing research. In the past, the use of lab-based computers allowed students to transport some, but not all, information.

With the increased use of web-based resources, students are now able to use their wireless devices to manage large quantities of data in the manner that best suits them.”

- **Location, Location, Location**

The Longwood Medical Area in which HMS is located is very crowded. Classrooms, libraries and public venues compete for scarce available space with crucially important research laboratory facilities. Deployment of wireless networks maximizes limited physical space. Limiting the need to run networking cable through the walls and ceilings of facilities also reduces disruption, complications, support costs and repair visits.

In addition to lowering the total cost of ownership of networks and IT in general for HMS, Steve Martino comments: “wireless LANs are a particularly good fit to provide wireless access in large public areas and temporary workplaces which are awkward to wire. Furthermore WLANs help with building aesthetics and fill safety and legal requirements with which we must comply when deploying networks.”

Future: Taking Learning beyond the Walls of Medicine

Joe Bruno and Steve Martino believe the effects of wireless networks at HMS have just begun to be felt. As more users opt for wireless, more applications become available and wireless bandwidth increases—new possibilities and challenges will emerge.

Standards and Policy

“A key issue for us currently is defining standards and policies around wireless,” says Joe Bruno. HMS-IT publishes a “Network Policies and Procedures” document for its users to manage user requests and set expectations for issues like requesting a network connection, notifying outages, scheduling maintenance, and supporting standard and non-standard network protocols. However, wireless networking changes many aspects of networking—use, classes of users, location, etc. and brings with it some issues.

“Wireless networking goes beyond the walls, and as that happens we want to retain some control,” says Martino. “Authenticating users when they worked on fixed desktop computers was one thing – wireless mobility has impelled us to seek simple standards for authentication wherever the user chooses to operate.” Ultimately the authentication mechanism built into HMS’s Bluesocket systems give wireless users what they expect from wireless networking – a seamless handoff between network coverage areas without loss of service or the need to re-authenticate as they traverse the campus – much like the kind of transparent and reliable service they get using cell phones.

Role-Based Access Control

Over time, HMS-IT plans to extend the capabilities of Role-Based Access Control (RBAC) built into Bluesocket’s authentication mechanism. By consciously managing ‘classes’ of wireless users within the school community, HMS-IT can allow authentication and access control to enable different levels of access, and support. Martino explains: “For example, in the future, by connecting to profiles we run on an Oracle database, the wireless management system could make a SQL Call to see that students get delivered one document or presentation; faculty – another. RBAC can also help with bandwidth management—so that students downloading MP3 files don’t bring down network performance. ” Extending wireless RBAC to additional systems on campus in the future will enable “guest” privileges and access to POP e-mail access for a wide range of visitors: from prospective students and their parents, temporary workers, even vendors and suppliers... the FedEx man who wants to update his inventory from a loading dock.

Going beyond b: Leveraging bigger bandwidth of 802.11a technologies

All lectures at HMS are videotaped and can be viewed usually within an hour of the end of the session. With the future availability and rollout of high bandwidth 802.11a networks, WLAN access to Video/Image Transfer/VoIP Optical networks on campus will let students watch their favorite professors in the theater of their choosing – right on their laptops.

“The vision of ubiquitous campus-wide wireless access delivering ‘anywhere, anytime’ connectivity is more reality than fantasy,” says Harvard Medical School’s John Halamka. “The next several years are certain to bring increased wireless integration with our MyCourses eCurriculum and PDAs accessing our eCommons information portals. Within the decade, wireless communications will become increasingly a part of a medical education and of medicine in general. Instead of paging doctors over an intercom, doctors in hospitals will carry a wireless

GPS device that will tell whoever seeks them where they are at any given time. In the bedside manner of tomorrow, to avoid transcription errors and improve accuracy, nurses and physicians will take notes on patients' conditions and order medications right from the bedside via wireless tablets or Palm-based handhelds."

After they leave Harvard Medical School, having been exposed to the wireless workplace in school, tomorrow's doctors will expect the same powerful wireless tools, processes, possibilities in the hospitals, clinics and private practices in which they will spend their careers.

Conclusion

Wireless networking is changing the very essence of medical education. As the training ground for many of the 'best and brightest' physicians and scientists in the world, Harvard Medical School employs wireless technology to improve the quality of student life, curricular delivery, and research methods. In the words of Susan DeLellis of Harvard University Information Systems, Bluesocket's wireless gateway solutions "give Harvard the infrastructure required to provide a standards-based, secure and 'seamless' user wireless experience across campus while still allowing 'local' management of wireless networks."

###

References:

- 1) Material abstracted from www.hms.harvard.edu website
- 2) Adapted from HMS.edu site: <http://wireless.med.harvard.edu>
- 3) **The New Architect: "A Prescription for Wireless"** by Joseph C. Panettieri, June 2002

Disclaimer: This case study in no way represents an endorsement by Harvard Medical School or any other Harvard University affiliated school/department of Bluesocket, Inc. or its products. The purpose of this document is to provide an overview of how wireless technology has evolved in its deployment (to date) at HMS for educational purposes. Full disclosure: This document was initiated and sponsored by Bluesocket, Inc. with input and the approval of Harvard Medical School and Harvard University.

© 2002 Bluesocket, Inc. All Rights Reserved

About Bluesocket

Bluesocket, Inc. (www.bluesocket.com) manufactures solutions to manage and secure wireless local area networks (WLANs) in enterprises, educational institutions and public hotspots worldwide. Bluesocket's product family of Wireless Gateways reduce the total cost of ownership (TCO) of wireless LANs while maximizing their benefits—from small businesses and departments; to warehouses, hospitals, universities and large enterprises. Bluesocket provides organizations including KPMG Consulting, Best Western Hotels, Microsoft, and the Universities of Texas and California with simple yet comprehensive systems to secure, manage, and profit from their WLANs (802.11 family, HiperLAN2, Bluetooth).

Bluesocket's Wireless Gateways give users of laptops and PDAs wireless access to corporate networks and the Internet while moving within their campus buildings, other corporate premises and public coverage areas with Secure Mobility™.

With offices in Burlington, Mass., Silicon Valley (USA), London (UK) and Asia, Bluesocket, Inc. is a privately held, global corporation managed by executives from 3Com, British Telecom, Ericsson, Intel; other industry leaders.

HMS CS V-090402

Appendix:

Chronology of Wireless Deployment at Harvard Medical School *Eight Phases of Wireless Rollout*

Dates	Activity	Phase
May 2001	UTAG issues guiding principles for a Harvard-wide wireless implementation, which addressed user experience, security, access, and support.	Phase I
Summer 2001	A technical working team was formed with membership from many of the Harvard schools, including Harvard Medical School.	Phase II
Fall 2001	The technical working team conducted pilots of several wireless access points, including proprietary access/security mechanisms.	Phase III
Late Fall 2001	The technical working team identified two (2) leading vendors for LDAP-based authentication, Bluesocket being one of those vendors.	Phase IV
Winter 2001-2002	The technical working team came up with design and vendor recommendations for a Harvard-wide wireless implementation.	Phase V
Spring 2002	Funding proposal, acceptance.	Phase VI
Summer 2002	Implementation and rollout	Phase VII
Fall 2002 and Beyond	Expansion of wireless networks to additional locations on campus and within the Longwood medical community.	Phase VIII