Systematic Disadvantage at UMass Boston

Joseph Paul Cohen
joecohen@ieee.org
140 Milton Street
Dedham, MA USA

March 24, 2013

Open Letter: Students Facing a Systematic Disadvantage at UMass Boston

The students of UMass Boston face a systematic disadvantage in their education and later careers as a direct result of the decisions made by the directorate and management of the UMass Boston's information technology personnel.

The campus network policy and implementation diverge far from the standard nationwide university practices, resulting in an education that cannot be equal to that of our peers around the country. I have no confidence that the current directorate and management, without a significant change in objectives, can or will make decisions in the interests of the students.

Problems: I am a computer science Ph.D student here at UMass Boston. I am also a certified and experienced systems administrator who has worked in industry; at one point, I managed over 700 computers in a medical university environment and therefore feel I understand the IT challenges faced by this campus. In my opinion, most UMass Boston IT infrastructure restrictions/limitations that are imposed on students are NOT due to technical limitations. Many other members of the UMass Boston community with significant industry experience agree with me on this point. These restrictions/limitations are the result of decisions made NOT in the interests of the students. In some situations I believe they are designed to deter usage of these services in an attempt to lower the demand on the network. This deterrent may be to deal with limited resources but in 2010 I made them aware of these issues and they have not planned accordingly.

The three main problems that I want to discuss are listed below because IT has been aware of them for over 2 years:

1. Difficult wireless network login, and frequent disconnections
2. Blocking of outbound ports on the wireless network
3. Blocking use of VPN and other methods to connect to remote workplaces

History: To make the UMass Boston IT department aware of these issues I started a petition in 2010. I believed that the UMass Boston IT department had gone too far by forcing the students to install software in order to connect to the wireless. This software had the ability to scan student's files which I felt was unacceptable and didn't solve any security problem. I had never and still have never seen anything like this at another university.

Every student and faculty member I spoke to about this was also strongly against the intrusive software, so I met with then-Assistant Vice Provost for Communications and Infrastructure, Daryl Ford as well as then-UMass Boston Information Security Officer, Robert Sarao to seek a repeal of this rule, and before the next academic year, the software was no longer required to be installed.

While this change was a step forward for the university, the other issues outlined in the 2010 petition

were not acted on, and have gone unresolved. I want to explain the most important issues and how they impact students. The next three sections will detail the major issues.

Difficult wireless network login: UMass Boston uses a captive portal login system for the Student wireless connection. This system is designed to authenticate students before they can access the web over WiFi. When a user connects to the wireless, they don't have access to the internet, even though their device thinks they do. Every webpage request is redirected to a login page which alerts the user that the security certificate is not trusted, and only after a student logs in to this system do they have access to the internet. This happens every day, to every device, when students enter every building, forcing a username and password to be entered multiple times per day. If the student saves the password in a browser, it is only saved for one building, because the login page URL is specific to each building.

Because of this, applications such as email are unable to work continuously throughout the day. Many students opt to disable their cell phone WiFi when on campus so they don't have to log in. While some students are able to buy mobile data plans others see this as a financial hardship. I would rather spend money on rent instead of a mobile data plan. Some carriers such as T-Mobile do not have signal on campus and a mobile data plan cannot even solve the problem. WiFi on campus becomes a necessary burden to stay connected. Other universities aim to reduce the number of logins to one such as MIT, Harvard, Northeastern, Princeton, Stanford, Ohio State University, and Boston University. Some do this by linking the hardware id of the device to the user and never requiring a login again or they use a standard system called 802.1x which allows a device to save the password and send it each time. Both of these methods remove the burden from the student.

The unsigned certificate use for the login page which prompts the user to trust the possibly fake certificate is a huge security flaw. Anyone could set up a fake wireless network called "UMB-Student" and redirect users to a login page which would look identical to the official login page. This is called a "man in the middle" attack. Login pages should use real certificates so that when the browser alerts them that the certificate is not trusted they know to not continue to log in.

Blocking of outbound ports on the wireless network: This problem affects the majority of students because mail clients that connect to mail servers using industry standard protocols are blocked such as POP, IMAP, and SMTP. These are even blocked for UMass Boston email servers. Students are forced to use the web based UMass Boston email. If a student is not using gmail or another web based mail then they are not able to check that email on campus.

I want to single out the hardest hit group, which are the computer science students. These students access a UNIX/Linux server to turn in all their work for classes called the "users" system. Students connect over a protocol called SSH which runs over port 22. The WiFi at the university only allows HTTP and HTTPS (ports 80 and 443) and does not allow the SSH protocol to this server. Instead of demanding the port be opened, the SSH server was configured to use port 80 so it appears as HTTP, allowing students to connect by reconfiguring their computers in a special way. The burden was shifted to the students who must now specify port 80 when connecting to the server, every single time they log in. Students are forced to reconfigure their SSH clients to talk over a different port. Some applications do not allow non-default settings and the student is forced to not use the WiFi.

Why would the university implement a policy like this? There are no clear security advantages to having the campus network configured in this way, and this only impedes the progress of the students and faculty in trying to do their work. The reader is reminded here that there is no

technical limitation to allowing SSH connections over WiFi, making this configuration ignorant at best and malicious at worst. Why would UMass Boston put a policy like this in place if it was only going to be circumvented by a college inside it? Wouldn't the university realize that they are only making it harder for students to get coursework done? What makes this worse is that it is NOT a technical limitation to allow SSH traffic over the WiFi. A decision was made not to allow the Computer Science department's coursework system to be accessed using it.

Blocking use of VPN and other methods to connect to remote workplaces: This is the ability for a student to sit on campus and connect to their business network through the schools network. When a student works for a company and takes classes they might have the opportunity to do some work between classes while on campus. Commonly a VPN tool is used so that the students laptop can access documents on a server located at the business securely. This is blocked at UMass Boston. Students are not able to connect to their businesses. For a commuter school to block this I do not understand. There is no technical limitation for this. This punishes students who work. This applies to computer science students greater than most. There are so many computer science students that work day jobs the courses are offered mostly after 4pm.

E-Mail is another technology that is blocked on the wireless. It's often confused with web based email which will work because it's just a website. Often, email uses POP, IMAP, and SMTP services. These services use ports that are blocked on the wireless. Students that use anything but services like gmail and live.com are blocked. Because of this even using the UMass Boston provided email service is blocked if the student tries to use a desktop application such as Thunderbird, Evolution, or Outlook. If a student finds it more productive to use a desktop application instead of a web browser then why are they denied this ability?

For computer science students this causes more of an issue. Writing serious software requires collaboration services that work on ports that are blocked by the wireless. Services such as GIT, SSH, and Perforce are used to collaborate and develop systems. Having these services blocked on the wireless forces students to work from coffee shops or their homes. While on campus their inability to react quickly to an issue at work makes hiring students less desirable. Limiting their exposure to these technologies while on campus also puts them at a disadvantage when entering the job market

Systematic Disadvantage: What makes me draw the conclusion that these problems cause a systematic disadvantage in the future careers of students? These problems impede student progress by forcing them to deal with the imposed barriers on the network and not the barriers of their knowledge. Students are not able to embrace the technology that is shaping our world because they are only allowed to witness a small portion of it on campus. The time spent working around unnecessary restrictions doesn't allow students to grow as they otherwise would. This would not be the case if the university didn't deviate so drastically from standard academic practices. These students are paying customers and are here to educate themselves. This process is only made harder when these restrictions are imposed on them.

For these issues to not be addressed for so long there must be the assumption that complaints by students are shallow or not technically significant. UMass Boston students ARE truly encountering problems and their complaints ARE well warranted. There is a need to have security restrictions on a network and sometimes there are technical limitations that must be tolerated. However, the configuration of UMB's network is unwarranted for an academic institution and is not like anywhere else. The blocking of ports and protocols specifically targets computer scientists who are unable to

collaborate with universities using technology outside the scope of the web.

Student experience is significantly different at other UMass campuses. For instance Amherst has 802.1x authentication on their wireless and SSH traffic is allowed to their computer science servers. They either addressed student concerns or never introduced problems.

Instead of staying on the UMass Boston campus, and using resources that students pay for, these policies encourage students to return home or visit coffee shops to connect to the internet. However, at these locations they are unable to connect with their peers as they would in the library or the campus center. These students must choose between the quiet environment of the library and the busy environment of a home or public area. Students should not have to make this choice.

I released a smartphone application to solve the WiFi login problem for Android phones in 2012 (and was swiftly stripped of my university research website without a reason for 2.5 months) one of the responses from a fellow student echos exactly what solving these problems can do and how much these issues impact students:

"Now I can walk anywhere on campus and use the internet without having to fiddle around for five minutes trying to log into the UMass system each time. Brilliant! According to my calculations this app should save me about 25 minutes a day which I can spend doing homework instead." - Comment left January 24, 2013 on the Google Play Store for "Umass Boston Wifi Autologin" https://play.google.com/store/apps/details?id=the.umbautologin

A university, in my mind, is designed to act as a foundation to propel students into the economy with as much momentum as they can build during their tenure. A university has the goal of providing the student with the best education that they can. How can students prepare to impact society from UMass Boston's network when networks outside the university are less restrictive and better functioning? Where is the nurturing environment provided by the university?

Solutions:

After almost 3 years of petitioning and complaining I believe significant change in the direction of the directorate and management of UMass Boston's information technology is required.

I request that the university fix whatever is preventing the directorate and management from making decisions in the interests of students. I feel more money is not the problem. I feel it is the mindset and mission of directorate and management of UMass Boston's information technology that must be changed in order to save students from future systematic disadvantage.

At other universities the name of the department is "Academic Computing Support" which broadly aligns the decisions with the interests of the students and academic ideologies.

I have spoken to many experts from industry and they believe that working at a university such as UMass Boston is prestigious and rewarding. However, none of them are interested in working under the leadership that is making the current decisions at UMass Boston.

Joseph Paul Cohen