The Massachusetts Daily Collegian
October 10, 2008

Pacemakers Secured

By Sara Cody
Collegian Correspondent

Future recipients of the newest line of implanted medical devices may share a common enemy with the computer sitting right in front of you: internet hackers.

In the U.S. alone, there are more then 2.5 million IMDs, including pacemakers, defibrillators, and insulin pumps, are currently residing in patients.

In the future, doctors will be able to receive patient data through the Internet and other wireless sources, and also to manipulate these devices via the same pathway according to the information they receive. While this would provide a whole new world of convenience to the recipients of IMDs, this would also be making an immense number of people vulnerable to the ill-will of hackers and cyber terrorists.

Thankfully, Kevin E. Fu, an assistant computer science professor at the University of Massachusetts at Amherst, is working on a solution to this frightening potential problem. He was recently awarded a three-year grant of $449,000 by the National Science Foundation to improve upon the security measures of these life-saving devices.

“The main goal of the study is to understand the patients’ expectations of security and privacy,” explained Fu.

Fu will be conducting a two-part research project. He will not only work on developing a working prototype of a secure IMD, but also he will be conducting interviews with patients who are receiving new cardiac IMDs at Beth Israel Deaconess Medical Center in Boston. The patients will be questioned about their expectations for security and privacy with their medical information, and the amount of trust they place on their IMDs.

Fu said if his team is successful, “then all sorts of new therapies can be employed much more easily.”

Fu reassured that patients who receive an IMD today are at very minimal risk for being attacked by ill-meaning hackers. “What we mainly care about is that in the future, we know that these devices are going to become more connected to the Internet and to wireless and we want to catch these problems before they result in something bad,” he said.

Dr. Craig Smith, MD, an interventional cardiologist and the Director of Cardiac Care at UMass Memorial Hospital in Worcester, agreed that this is a very concerning problem for the future.

“Absolutely, there would be ramifications because you could easily, easily send someone into [cardiac] arrest if you were Machiavellian enough to control these devices,” he said. The idea may seem far-fetched to us now, but, according to Smith, it’s not “beam-me-up-Scotty far-fetched.”

Smith recalled that during the development of automated external defibrillators, or AEDs, there were similar concerns of people using these machines for malicious intent.

"One of the concerns was that would not only be causing unnecessary harm to a patient, but you could use it as a security breach weapon by just slapping the pads on someone and shocking them, knocking them out or killing them," Smith said.

During the nineties, scientists worked to develop a computer algorithm that would make the machine smarter. They found a way to program the machine so that it would deliver a shock only after the computer within the machine has analyzed the patient and all of the appropriate bodily conditions have been met.

Today, AEDs are found in many places such airports and train stations, and have remained tamper-proof since their introduction to the general public.