Conrad Buerger

Article Review II

Security Think

Dr. Schilling

January 9th, 2011

This review is about the article 'Security Think', published in the IEEE Security and Privacy Magazine. In this article Steven M. Bellovin talks about how there is a problem with educating people about security. His reasons behind this argument are that we are teaching the wrong people about security. Another reason that backs his argument is that we are teaching the wrong subjects to the wrong people. Steven finishes the article with a personal story about how easy it is to breach security in a large chain store.

When Steven talks about how people who teach security to people are teaching the wrong people what he means is that all the people being taught are the security specialists. From what I can gather from the article, a security specialist, judging from its name, already knows security well enough. Steve claims the people who really need to be taught security are the application and system builders. He claims this because they are the ones who are "creating the security holes that plague us." (Bellovin) He further explains his reasoning by stating that students also need to be taught. The students should be taught the basics, from firewalls, to access control lists, to passwords.

In addition to the students not being taught the basics, the wrong subjects of security are being taught to the professionals. Cryptography, Steven claims, is an important subject that people need to know and that people should never try and "invent his or her own crypto." (Bellovin) The subject that is not being taught enough is the subject about how to think about security. An example supporting this that is used in the article is that:

"A security specialist is rarely ever told to figure out how to secure [a] TCP connection; usually, the proper response is something like use TLS (or, in some cases, enable the TLS option in the application), at which point most of the solution can be left to any programmer who can read the documentation." (Bellovin).

This shows that people are simply being told what to do instead of actually thinking about what needs to be done to make something secure.

Finally, Steven finishes the article about a personal experience he had while purchasing a router bit. There are physical security failures all the time in the physical world, especially in stores when purchasing an item. Essentially what happened without quoting a giant block of text is that he went to buy a router bit from a large chain store, but when he found what he was looking for, the plastic cabinet that the router bit was in was locked. When he went to find someone with a key, no one could be found, so another personnel decided just to take a knife to the plastic case and let Steven walk off with the router bit. Steve then went to a self-service check-out lane in which he did not bag his item and since he went to a self-service check-out lane the item never went by the gadget that deactivated the antitheft transponder. So, when Steve walked out of the store with the router bit in hand, the alarm sounded, but no one responded to the security alert. One can imply from this that false alarms happen all the time or that the cost of catching the person is more than the actual product that was gotten. Either way, there were many security failures in this example that support Steven's point of view.

In this article review, the topics that were brought up were about how the people who teach security are not teaching application and system builders how to properly implement security into their applications. After that, Steven talks about how we are spending too much time teaching topics like cryptography and too little time teaching about how to think about security. Steven tops off his argument by giving a personal example of a security flaw in a large chain store. Overall, it was an informative article that used simple language to get some very important points across to the reader.