Zero-interaction authentication:
Review by Frank Fetters

This paper introduced a way to help combat the threat of secret data being stolen when a laptop is stolen or left-alone long enough for a malicious person to try and obtain the sensitive data. The old way of protecting this data was to encrypt the file system and then do aggressive authentication where the user would have to re-login every few minutes to decrypt whatever new data he wants to see. For those users who only need a few minutes of access at a time and are very patient with lots of time to spare, this is a good solution. Unfortunately, no user has time to spare and patience is virtually non-existent in today’s fast-paced world.

The first thing that came to my mind while reading this was that if someone grabbed the laptop and the token, they would have a day’s worth of access which is all it would really take. The paper did talk about the threat of a stolen laptop/token pair, but seemed to dismiss it too quickly. The way this threat is handled is to make the token something wearable so that the intended user wouldn’t take it off or set it down while they did something else. While it less likely that your watch will get stolen, I believe it is still a large threat, especially when talking about the medical field. If a doctor is called to a surgery, during prep he has to scrub his hands and arms up to just above his elbows, which means his watch has to be removed. If a doctor or nurse has to give an MRI or some other medical scan, no metal is allowed in the room and therefore would have to be taken off and put somewhere. I would add the ability to disable or log/out of the token during certain periods of time (possible with just a button push) to allow temporary removal of the token.

One addition to the token was the requirement that the user must perform some simple acceptance task to allow the laptop to continue using the keys. For example, the user must push a small button on the watch to allow the opening of a file. This is to combat the tailgating attacks of malicious users who steal the laptops and try to access the data while the user is in the restroom or in the next cubicle over. I believe this will be very effective in stopping the tailgating attacks. However, in my mind this might be pushing to the limits of the intended “zero-interaction.” If the user has to access multiple files and has to keep pushing this button on his watch, it becomes less-intense interaction, but interaction none-the-less. In addition, this increased interaction with the token will place a requirement that the token must be easily accessible to allow the button pushes which could increase its vulnerabilities to theft.

Overall, I found this to be a neat solution to the hospital’s problem. The solution works well because of the rigid nature of hospital administration and staff security which already exists. I find it more difficult to extend its use into more relaxed working arenas because of my belief that the keys can be easily stolen and with a one day window and a quick program to access/copy the files the security is greatly reduced, but with refinement it may become a wonderful solution.