Zero Interaction Authentication (ZIA) is a way for users to authenticate themselves with a computing device while not requiring repetitive verification of their identity. ZIA solves this problem by having users wear a token that transmits unique keys to the computing device requiring authentication. These keys are transmitted using an 802.11 wireless network. This was a little confusing to me since my understanding of 802.11 ranges can reach 500 feet. While the paper mentions that the wireless connection was in 1Mb/sec mode, my understanding of the different wireless physical (PHY) layers is that PHY mode is determined by signal attenuation. I was not aware that setting the mode PHY mode to 1Mb/sec would reduce the power of the transmitted signal from the token. I feel like Bluetooth would be a better physical transport medium to use instead of 802.11.

ZIA uses a key-encrypting-key, stored on the token, and encrypts keys stored on the laptop. These encrypted keys on the laptop are used to encrypt files stored locally. Each encrypted key on the laptop is used to encrypt a directory of files. The encryption used is AES, cipher feedback mode, and the initialization vector is determined by the directory’s inode number and page offsets. By using a single key to encrypted/decrypt directories, it was easier to cache encryption keys and to reencrypt data. The reason keys were assigned to directories and not to individual files are that files with in a single directory are accessed with some degree of temporal locality. This made the caching of keys and the encrypting/decrypting of data faster. I found it interesting that group and user keys were also implemented in the project. Since such a strong majority of laptops are given to a single user, I saw no real need for group keys. However, I was able to see that it was relatively easy to implement given that the ZIA system could be ported to a stationary computing systems.

The paper also describes the algorithms used when a token leaves or enters the virtual boundary created by the wireless network. The ZIA system caches plaintext pages in main memory while the token is in range. When the token can no longer be reached, the pages are encrypted in place instead of encrypting them and storing them to disk. This makes the next transition, of the token becoming in range, much quicker. By encrypting the pages in place, the laptop is closer to the same state as when the user left the device. The paper notes the delay to encrypt/decrypt files in place in main memory should be less than 5 seconds.

The paper also talks about the performance hit caused by ZIA and the ways this performance hit can be reduced. The heuristics mentioned in the paper make ZIA only slight worse and cryptfs when performance is being analyzed. The paper notes that there is a 9.3% computational above normal file systems procedures. The paper concludes that this performance hit “is indistinguishable from the costs of simple encryption”.

The paper was of great interest to me since I am working on a replacement to the card readers around campus. While those card readers are currently only used for access to computers labs and dormitories. A “one token/card” system is desired by university housing directors for all student activities. This type of systems in combination with a low cost, low power token device could be realized University wide.