

The Security of a College Residence Hall's Wireless Lock System: Proposal

Mike Benza
benza@
Rice University (rice.edu)

Christopher Warrington
chrisw@
Rice University (rice.edu)

Thursday, October 16, 2008

We propose to study the security of Rice University's Martel College's swipecard based locks. Previously, all of the outer doors to rooms at Martel required a key to enter. Now, a swipecard is all that is needed. The new swipecard system adds many features over a traditional lock and key system, but is the result of integrating many technologies, each of which has its own set of vulnerabilities. For example, the locks can be reprogrammed without physical access, they can be used to audit who enters a given room, and temporary access can be easily granted to guests. We've even been told that the doors can be opened remotely in the event that a resident is locked out. In our research, we would like to investigate the security of the physical devices, the security of the underlying network, the data stored on the swipecards themselves, the effectiveness of the policies regarding the use of these readers, the devices' effectiveness in a power loss, and their ease of use for emergency personnel.

Our original research was based on an article in *The Rice Thresher*, "Cards replace keys at Martel"¹. The article states that the new system is the Basis G system by Stanley Bess. Research has shown us that this system is in fact manufactured by Stanley Best and is not even a wireless access system. However, we know for sure that the locks are at least maintained by Stanley, since Stanley has been observed servicing them. We have been told that they are wireless. Based on information from the Best website², we know that there are two wireless systems: Stanley Online and Wi-Q. Little information could be found on Stanley Online: it appears to have reached its end-of-life and is being replaced by the Wi-Q system. Wi-Q implements IEEE 802.15.4 using AES with a 128 bit key.

1 <http://media.www.ricethresher.org/media/storage/paper1290/news/2008/08/22/News/Cards.Replace.Keys.At.Martel-3401390.shtml>

2 <http://www.bestaccess.com/index.asp?Mode=WIQ>

ZigBee is generally viewed as equivalent to IEEE 802.15.4. The latest version of ZigBee, ZigBee 2007, has Symmetric-Key Key Exchange built into the standard³. We do not know if the locks in fact use ZigBee or a proprietary implementation of IEEE 802.15.4, or if they use ZigBee 2007. Nor do we know if they use AES appropriately.

To conserve battery power, the Stanley locks download access information periodically. Using this information, the local lock can make the decision to grant or deny access. No server involvement is required for basic operation. The server is engaged to download new access lists, to upload access logs, and to report notable events. Additionally, the server can push out new settings to the locks.

Anecdotal evidence indicates that the locks are fairly new technology, since Stanley has been at Martel frequently to work on repairs, often working for days at a time. This indicates to us that the technology may still be in development. Based on our experience, Martel could be a beta tester for Stanley Best's product using the new Zigbee 2007 protocol.

We intend to first look at the locks to see if we can find any part numbers leading to information about the locks. If they do in fact use ZigBee, we will try to capture the data. There is an existing ZigBee capture product that works directly with the popular network capture and analysis program, Wireshark. We will also use existing card reader technology to figure out what data the lock uses to make its access decisions. If we are able to obtain a device to examine in depth, we will observe its operations in low- and no-power modes. Finally, we will interview the Rice University Office of Housing and Dining about their policies regarding the new locks. By correlating their policies with our other findings, we can analyze the security of the system in depth.

³ <http://en.wikipedia.org/wiki/Zigbee#Overview>