

The Security of a College Residence Hall's Wireless Lock System: Update 2

Mike Benza
benza@
Rice University (rice.edu)

Christopher Warrington
chrisw@
Rice University (rice.edu)

Tuesday, November 4, 2008

Our [proposal](#) to study the security of Rice University's Martel College's swipecard-based locks has been approved. In the past two weeks, we have conducted some preliminary hands-on research with the system. We have not intruded into the system in anyway—we have only passively monitored ZigBee traffic.

We started our research by contacting Dr. Lin Zhong, a professor in the Electrical and Computer Engineering Department at Rice University. He researches low-powered networks, including the ZigBee protocol. Dr. Zhong gave us a sample ZigBee toolkit intended to be used for product development. We found it limited and unable to detect any ZigBee traffic. Christopher Warrington is currently learning more about the ZigBee protocol in an attempt to observe the network's traffic.

Our next step was merely taken by chance. Mike Benza met David Brown from Rice University's Housing and Dining. He asked Mr. Brown about the wireless locks and was referred to William Diegaard in Rice's IT. Mr. Diegaard was unable to provide us with any information and referred us to Jeff Murray in Rice's Administrative Systems department. Mr. Murray has only recently been contacted.

As mentioned in our [proposal](#), we have frequently seen Stanley Best at Martel, apparently working on the system. On November 4, 2008, Mike Benza saw someone from Stanley Best in the Martel Game Room. They spoke for about an hour about the system.

The following is a list of facts learned during the discussion.

- The locks do in fact operate using the ZigBee protocol: they use AES 128-bit encryption, and the vendor's representative is very confident in their security.
- The wireless portion of the system was designed by OSI in 2004 and 2005, which was bought by Stanley Best in 2007.
- The locks “wake up” every minute and contact a Portal Gateway to download an updated list of people allowed to use that door.
- The Portal Gateway is a ZigBee receiver with a standard network connection. The

network connection is used to communicate with a central authorization server.

- There are multiple Portal Gateways around Martel. One is in the game room; another is in room 126. Mike believes the vendor's representative mentioned that there are 12 Portal Gateways around Martel.
- The connection between the Portal Gateway and the central authorization server is by default not secured. It is the responsibility of the customer (Rice in this case) to secure that connection as fits best into its network.
- The locks in Martel at the beginning of the semester were prototype locks. They will be replaced with full production locks this week (November 3–7).
- There were two major changes (unspecified by the vendor's representative) to the locks between the prototype revision and the production revision.
- Martel is in fact a beta tester for a new lock system. The locks are part of the Wi-Q system, but they will have a BASIS interface, which is common to other Stanley Best electronic locks.
- The BASIS interface is a cobranded version of [Lenel OnGuard](#).
- The lock communicates with a Portal Gateway, which in turn communicates with a SQL server using the Wi-Q interface. The SQL server ideally also communicates with another SQL server using the BASIS interface.
- The Wi-Q SQL server currently does not communicate with the OnGuard server.
- The system monitors signal strength from the Portal Gateway to the lock and from the lock to the Portal Gateway. It also monitors the packet-to-error ratio. The lock can signal its battery is low.
- The locks in Martel use only two of the 16 available ZigBee channels.

The vendor's representative was understandable hesitant to reveal the details of the system. Mike provided Stanley Best with his contact information as well as the contact information of Dr. Wallach. Mike made sure to stress that we very strongly wish to do no harm and we understand the ethical dilemmas inherent in an investigation of the security of door locks.

Finally, the main contact at Rice for the system is now known to us. We have asked to meet to discuss our research and how he can help.

For the upcoming week, we plan on meeting with our new contact and discussing the

technology and the policies in place. Additionally, we plan to use our newfound knowledge about ZigBee networks to try to passively observe the locks and their communication with the Portal Gateways. Hopefully, Stanley Best will feel comfortable discussing more of the system's details with us.