Study shows hotels' Internet connections unsafe

October 1 2008, By George Lowery

(PhysOrg.com) -- Travelers who use a hotel's Internet network risk the possibility of data theft, concludes a new study from Cornell's School of Hotel Administration.

The analysis of the networks in 46 hotels and a survey of 147 U.S. hotels found that a majority of the hotels do not use all available tools to maintain network security.

For example, about 20 percent of the hotels surveyed still use simple hub-type systems, which are most vulnerable to hacking. The findings of the firsthand analysis of 46 hotels were no more encouraging.

"Even with hotels that required authentication, I found helpful employees who got me past that barrier," said Josh Ogle '08, a Cornell Hotel School graduate, president of TriVesta LLC. and a co-author of the study. "So, authentication is not as effective as we think, and then I found that of the 39 hotels that offered WiFi connections, only six used encryption to help protect the system."

Added co-author Erica L. Wagner, assistant professor of information systems at the Hotel School: "On balance, we were forced to conclude that guests' data transmissions are often at risk when they use a hotel's network. However, we did find hotels that were paying attention to the security of their guests' data. I should point out that improving security does not have to be costly."

The report concludes with a case study of the W Dallas - Victory Hotel, which has taken a security step not used by most hotels. "What the W Dallas has done is to set up each node on its network as a virtual local area network, or VLAN," explained co-author Mark P. Talbert, a Hotel School senior lecturer in information systems. "By using these VLANs, the hotel has separated each guest's computer in a way that should protect against stolen data. It also gives the hotel greater control over the guest side of the network."

Provided by Cornell University