Safe and Cozy in your Hotel Room

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Many readers are familiar with the writings of Prof. Stephen Cobb, CISSP, a prolific writer who has also written guest articles for this newsletter. Stephen recently became the Chief Security Executive at STSN, a major supplier of broadband services to hotels and conferences worldwide. We were chatting on the phone a few days ago and I asked Stephen about his new job and he very kindly responded by interviewing himself (!) and sending me this excellent report.

I have lightly edited his words, but otherwise the rest of this article is entirely Stephen’s own work.

* * *

Q: Hotel broadband service sounds like a niche market and not something that immediately comes to mind when we think about network security. Can you give readers some idea of the size of this field and why, as a security professional you decided to get involved?

A: Well, initially STSN got my attention with four facts.

* First, the average number of broadband connections that they serve up every month, including both wired and wireless averages is over 700,000.

* Second, the rate at which the number of wireless connections is growing month-on-month is about 50 percent.

* Third, the primary use of these connections, both wired and wireless, is to access corporate virtual private networks (VPNs).

* Fourth, and this rang alarm bells for me, is that some broadband connections are a lot less secure than others.

Q: In what ways are some hotels less secure?

A: Well, for example, some let guests browse the laptop hard drives of other guests. That presents a golden opportunity for people like criminal hackers, identity thieves and unethical competitors looking for an edge. For example, sometimes you just have to click on Network Neighborhood to see your fellow guests. And at hotels with poorly configured Wi-Fi, you could be sitting in a car a block away and do the same thing.

Q: So STSN considers its network secure. How do you back up that claim?

A: Well, for starters, you won't be able to see computers belonging to other guests when you are staying at an STSN hotel. In turn, they won't be able to see yours. And if any of your readers
Q: How can you achieve this when other providers apparently can't?

A: The short answer is that we use a virtual local area network (VLAN) for each connection through several layers of network address translation performed by our own on-site network controller which feeds traffic over a dedicated back haul to a regional point-of-presence (POP) that has enterprise-class physical and logical security and redundancy, all backed up by 7x24x365 monitoring.

But the real answer is that our patented iBahn network was designed from the ground up to serve the hotel and public access environment, which is radically different from your typical 'open' office network. On an office network you want people to be able to see each other, so to speak, because you want sharing and collaboration. A hotel is almost the opposite. You don't want to share your data with fellow guests (or the war driver in the parking lot). You want a 'closed' network that takes you out to the Internet on your own private connection, one that supports your company's VPN.

Q: You mentioned VPNs before. If I am using a VPN and have a personal firewall on my laptop, why do I need to worry about who is providing my hotel broadband connection?

A: First all, the VPN has to work. STSN actually certifies and supports, via our 7x24 toll free number, specific corporate VPN configurations from many of the Fortune 500 companies. Second, a client firewall is only as good as its operator. For example, a few days ago I was invited to a Webcast that was very relevant to my work and the access page actually told me to turn off my personal firewall. Is your typical laptop using business traveler going to remember to turn it back on? The bottom line is that you want to use as many different security layers as you can get and STSN can provide several of those layers.

* * *

For further reading:

For more information about STSN see <http://www.stsn.com>.


* * *

A Master's degree in the management of information assurance in 18 months of online study from Norwich University – see <http://www3.norwich.edu/msia> for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at