Security and Privacy in Broadband Internet Services

Robert Ellis

Tomorrow's consumer Internet connection is likely to be broadband provided by either Digital Subscriber Line (DSL) or cable modem. Several characteristics of theses services ("always on", static IP addresses and the use of LAN technology for the computer interfaces) present increased security and privacy issues. In addition, the likely deployment of home networks means that there is both more at stake and an added complexity in providing appropriate security and privacy.

The "always on" and static IP address nature on these connections present a much greater level of vulnerability to "crackers" than the more familiar dial-up connections with their relatively short connection times and pool assigned IP addresses. With a dial up connection, if a cracking program has found something interesting on your computer, it will find a different computer after a new IP address is assigned. A partially mitigating situation is the fact that most DSL providers assign a floating IP address each time you do reconnect. It is unclear to what extent cable TV Internet providers may adopt similar practices.

The use of LAN technology for the computer interface to these services presents another challenge to the typically network naive consumer. This means, for example, that the people with whom you are sharing your cable Internet access channel may have access to your files and even your printers unless network parameter settings are set appropriately. This problem is particularly acute for users of MS Windows which typically has the default network parameters set to "share everything". Of course, the customer who has a home network may find that the needs of the home network and security and privacy of the Internet connection require contradictory settings of network parameters. Recent reports in the popular press ("Internet Sharing Can Undermine Security", Kim Komando, Arizona Republic, December 13, 1999) have highlighted this situation with descriptions of neighbors having access to each other's files and printers!

Unlike industrial and academic Internet users who's organizations have implemented substantial security measures, such as firewalls, the typical consumer has no knowledge or convenient means to implement such security measures. However, there are some technically sophisticated home computer users who implement a firewall computer separate from the computer they use for processing. Such users report break-in attempts several times per hour. Given the low level of network security of the typical home computer, this means sooner or later such a break in attempt will probably succeed

and possibly compromise the operation of and files stored on the computer. Several firewall products have recently become available.

A number of issues are associated with this topic. First and foremost, we need to decide if there is indeed a problem. Conflicting reports and positions are presented by service providers, consumers and researchers.

Assuming that there is a problem, what technical solutions are available? Should a high level of security and privacy protection be built into cable and DSL modems? Should separate boxes be used?

There are a number of policy issues as well, such as the appropriate roles of industry, consumers and government. Privacy and security may become an issue best left to the marketplace with providers competing on the basis of their solutions to these problems. Is there a role for government? Many consider Internet connections to be the same as telephone service with its common carrier status. Different rules apply to common carrier services than proprietary, primarily entertainment systems, such as cable.

Finally, we need to acknowledge that the consumer has a role to play by being an intelligent consumer. But it is appropriate that the knowledgeable consumer be provided with information on what to do to enhance the security and privacy of their broadband Internet service. Where should that information come from?