Panel on Information Technology and Broadcasting

Special Meeting on July 18, 2007 at 2:30pm

Release of spectrum for broadband wireless access services

The providing of public broadband access service to the Hong Kong general public is long overdue. While the citizens in nearby countries have enjoyed the service in years, Hong Kong is still in its consultation stage. There obviously are much to think about before such service can be made available, and by all means they should be thought about carefully and solutions should be available to resolve any potential issues that may affect the public safety and enjoyment of the service.

With a background from an Internet Service Provider and Information Security, I have the following comments and concerns with the recent development relating to the broadband wireless access service:

Information Security:

- The wireless access should provide reasonable security measures to protect its own infrastructure from being abused and used as a jumping board to further attacks or criminal activities over the internet.
- The wireless access should also provide reasonable security measures to protect users' sensitive data traveling over the network such as personal information and online transaction data.
- However, users of the wireless access server should be made aware that security risk is inevitable in using public wireless access service. They should be recommended NOT to use the network for sensitive transactions such as online banking, accessing sensitive business data, etc.
- The network should have the mechanism and capability to identify the users to the machine level. Since it is not convenience to have everyone of the users to apply for an user's ID before accessing the network, it is only possible to use technology to identify the machine. In case malicious use of the network is detected, the event would be traceable.
- The service provider should provide adequate logging capability to record enough user information of the network connection to facilitate cyber crime investigation. If adequate logging is not available, the public wireless access service will become heaven for hackers and malicious users worldwide. Such information can include, but not limited to the following:
  - User computer's MAC address (the user computer's ID, unique to each machine);
  - Logon and logout time to the network;
  - Websites or network visited but no content is recorded;

- The network should provide adequate access control and content filtering to obscene and malicious website. However, name and location of such websites are usually changed very frequently, so it would be impossible for the network service to control such access with 100% success rate. Users should be alerted of the consequences of accessing such websites using the public wireless network and be discouraged.

Serviceability:

- Since it is after all a service provided to the public, it must be easily to be used. In other words, all of the security measures (except the ones that are intentionally made known to users) should be transparent.
- Bandwidth and access time per user should be limited for fair use purposes

IT Voice
17 July 2007