New Bluetooth Devices set up replay of WiFi Security Crisis, @Stake warns

Submitted by: Pleon
Tuesday, 16 December 2003

~ With a 100m range, Class A devices must be secured “out of the box” ~

London, December 16th, 2003 - @stake, Inc., (www.atstake.com), the leading digital security consulting firm, today warned that the mass arrival of Class 1 Bluetooth devices, with a transmission range of up to 100 metres, might usher in a security crisis equivalent to that associated with the introduction of Wireless LANs based on the 802.11b (Wi-Fi) standard. Class 1 devices will appear on everything from laptops to mobile phones, meaning that rogue third parties may gain access to sensitive information and/or interfaces without the obstacles of hunting through corporate networks.

Ollie Whitehouse, Director of Security Architecture, @stake, said, “With this class of devices, wireless transmission of information leaves the office environment and travels anywhere an employee does. This means that third parties can access information without penetrating the physical security of an office or dealing with the problems of circumventing existing network security. The onus really is on vendors to ensure that all devices are optimised for security before they are put in the hands of customers.”

In a recent White Paper, @stake drew attention to the fact that devices released as non-discoverable still respond to direct name and services enquiry and were therefore open to detection and attack. Other common problems identified included: Windows 2000 hosts that were configured to connect to all Bluetooth devices; Windows registries that retained details of all devices to which it had connected; and mobile phones set by their manufacturers to retain pairing information details when SIM cards are swapped, meaning that a third party that has access to a phone for even a few minutes can place a bond upon it and use it as a platform for future attacks.

Whitehouse continued, “The very real risks of Bluetooth will only multiply as adoption increases and the drivers vary from their default configurations. Many vendors release Bluetooth products with a best effort approach to security that can only compromise the integrity of the information held on those devices. Vendors should understand these issues and risks and develop mechanisms for delivering security out of the box. While it’s not a time to panic, it’s certainly a time to act.”

Two key vulnerabilities potentially exposed by the Bluetooth are associated with the OBEX standard that deals with vCards and other Personal Information Manager synchronisation details and the file transfer Protocol which relates to the transfer of data and applications from the device. This means that literally any stored personal information or document to which the user has access can potentially accessed by third parties – both significant compromises of enterprise security.

~ends~

About @stake, Inc.
@stake, Inc., the premier digital security consulting firm, helps corporations secure critical infrastructure and electronic relationships. Delivering world-class consulting and education through its

SmartRiskSM methodology and proprietary tools, @stake clients include six of the world's tops ten financial institutions, four of the world's top ten independent software companies and seven of the world's top ten telecommunications carriers. Using the @stake Security BlueprintTM, clients keep security investments in line with business requirements. Headquartered in Cambridge, MA, @stake has offices in Chicago, London, New York, Raleigh, San Francisco, and Seattle. For more information, go to www.atstake.com.

For further information please contact:
Ghezala Beg
Brodeur Worldwide
Tel: 0207 298 7063
Email: gbeg@uk.brodeur.com

Vicki Cook
Brodeur Worldwide
Tel: 0207 298 7113
Email: vcook@uk.brodeur.com

Brodeur Worldwide Contacts

Ghezala Beg
+44 (0)20 7298 7070
+44 (0)870 242 8323
gbeg@uk.brodeur.com

Vicky Steel
+44 (0)20 7298 7070
+44 (0)870 242 8323
vsteel@uk.brodeur.com

Company Contacts

Please refer all questions regarding this news release to Brodeur Worldwide