

Bangkok Post

database



Wednesday
16 February 2005
Last updated 8:48
AM Thai local time

SEARCH

Recent Editions [Go!](#)



Bangkok
High:35 Low:24 [more](#)



Check the weather
anywhere

Sub
Ban
Post
Stud

CLASSIFIEDS

[AUTOS](#)

[BANGKOKPOST
JOBS.COM](#)

[EDUCATION](#)

[PROPERTY GUIDE](#)

[SALES SERVICE](#)

[OTHERS](#)

NEWS

[Daily](#)
[Business](#)
[Your Money](#)
[McKinsey Quarterly](#)
[Sports](#)
[IT \(Database\)](#)
[Auto Industry](#)
[Sunday Perspective](#)

ENTERTAINMENT

[Cover page](#)
[Hotel Bookings](#)
[Horizons Travel](#)
[Outlook](#)
[Real.Time](#)
[Restaurant Reviews](#)
[Restaurant Search](#)

BANGKOKPOST.COM

[Exclusive](#)
[BP e-Directory](#)
[Thai-language news](#)

SEARCH

[Recent Editions](#)
[Complete Archives](#)
[Site map](#)

SISTER PUBLICATIONS



SPECIALS

[People's Progress](#)
[Tourism Review 2003](#)
[57 Prominent](#)
[Enterprises](#)
[Tribute to the King](#)

[Front page](#)

[News](#)

[Business](#)

[Entertainment](#)

DATABASE - Wednesday 16 February 2005

News list [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [11](#) [12](#) [13](#) [14](#) [15](#) [16](#) [17](#) [18](#) [19](#) [20](#) [21](#) [22](#) [23](#) [24](#) [25](#) [26](#) [27](#) [28](#) [29](#) [30](#) [31](#) [32](#)

[Previous story](#)

[Next story](#)

SECURITY / KEEPING OUT STRANGERS

Are wireless and broadband networks secure?

RONALD VAN KLEUNEN

Do you get connected to your company's network from hotels? Are you using wireless networks around the city to get connected to the Internet with your laptop or PDA? Do you use your Internet connection at home continuously?

If the answer to any of the above is yes, then are you aware that your data and passwords can be stolen from your PC without even knowing it? Even hotel networks are not secure.

Wireless and broadband networks are now being deployed rapidly in Bangkok and other parts of Thailand.

Users can be connected via the different telecom organisations to the home. Or for business purposes, wireless and broadband networks are provided by hotels, serviced apartments, coffee chains and so on.

When using broadband "wired-connectivity", your communication habits are different compared to a dial-up connection. You will listen to radio stations, watch television, chat online, etc. In some cases you will be connected around the clock, especially when there is no extra charge for the data usage by the service provider.

However, your security risks increase when your PC is connected all the time. Hackers around the world scan the network (when you sleep, they can be active in Europe or the US). They can eavesdrop your connection and find out user IDs, passwords, web sites you visit, or use spyware tools to find out details about your chat connections, bank transactions and more.

These security risks are similar for wireless connections, which are even more vulnerable. Take the so-called Wi-Fi (802.11a/b/g) networks that are deployed here. My company has tested major hotels in Bangkok, ranging from three to five star, coffee chains and the airport. In most cases we could see the user IDs, passwords, and web sites used by other users working wirelessly at that

[In memory of Prince Mahidol](#)
[Next Generation](#)

Economic Review
[Year-End 2004](#)
[Mid-Year 2004](#)
[Year-End 2003](#)
[Mid-Year 2003](#)
[Year-End 2002](#)
[Mid-Year 2002](#)
[Year-End 2001](#)
[Mid-Year 2001](#)
[Year-End 2000](#)
[Mid-Year 2000](#)
[Year-End 1999](#)

SERVICES

[Printing](#)

SOCIAL PROJECTS

[Leper Foundation](#)
[Post Foundation](#)
[We Care](#)

EDUCATION

[Learning Post](#)
[Student Weekly](#)
[Word-a-Day](#)

ADVERTISING

[Int'l Print Ads](#)
[Web Ads](#)

SUBSCRIBE

[Bangkok Post](#)
[Post Today](#)
[Student Weekly](#)

ABOUT US

[Annual Report 2003](#)
[Annual Report 2002](#)
[Annual Report 2001](#)
[Annual Report 2000](#)
[Annual Report 1999](#)

CONTACT US

[Join our team](#)
[Get our newsletter](#)
[Register with us](#)
[Contact us](#)

location. We were able to see not only the data on the laptops of the users, but at the hotels we could see their servers and documents too.

Furthermore, we did some "war-driving" to detect wireless setups in Bangkok (installed in the home or at the office) and were able to connect to several networks. This is actually "stealing" bandwidth capacity, but sometimes it is hard to avoid since wireless clients (like those in Windows) automatically connect to these networks.

How can you minimize your security risks?

In the wired broadband environment the basic components you need on your PC, home or office network are: a personal firewall, anti-virus software and an adware/spyware removal program. This software or hardware, when configured properly with the correct security policies, will prevent your data becoming available to everyone on the network.

Furthermore the "services" you run on your computer or at the office (like an FTP server, RCP service, Windows Terminal Server, mail server, HTTP/web server) are targets for hackers and it is important to minimise these running services.

The last item which is important is the communication over the network (for example, from the hotel network here in Bangkok to your company's network in Europe). In most cases this traffic is unprotected and user IDs and passwords are seen clearly on the network.

Some of the protection mechanisms to use are encryption, like a VPN (virtual private network) _ basically a long "pipe" back to your company's network. Or to use secure protocols like HTTPS (SSL _ Secure Socket Layer), SSH (Secure Shell / Secure Telnet) or SFTP (Secure File Transfer Protocol).

In the wireless environment it is important to protect the wireless piece between the wireless access point (which is connected to the cabled network) and the wireless client. There are some basic solutions available, like WEP (wireless encryption protocol), or using so called MAC addresses (hardware addresses of the clients allowed on the network') and using encryption mechanisms like 40-bit or 128-bit encryption. WEP is still vulnerable and can be hacked, but it fulfils a basic security need.

Nowadays, more advanced security mechanisms are used to protect wireless networks, like EAP (Extensible Authentication Protocol) or RADIUS (Remote Dial In User Security) and others.

A wireless access point itself can be secured by adding a password on the device (in some cases users do not protect it and re-configurations can be done). Also, the so-called SSID (Service Set ID) shows the identification of the access point and is useful information for the hacker.

The type of antenna used and the strength of the radio frequency are aspects to consider as well.

Ronald van Kleunen is director of IT Consultancy Services at Globeron (www.globeron.com).

Email: ronald@globeron.com

[Previous story](#)

[Next story](#)

[Front page](#)

[News](#)

[Business](#)

[Entertainment](#)

© [Copyright](#) The Post Publishing Public Co., Ltd. 2005

[Privacy Policy](#)

Comments to: [Webmaster](#)

Advertising enquiries to: [Internet Marketing](#)

Printed display ad enquiries to: [Display Ads](#)

Full contact details: [Contact us](#)