

Chancen und Risiken im Bereich von WLAN's

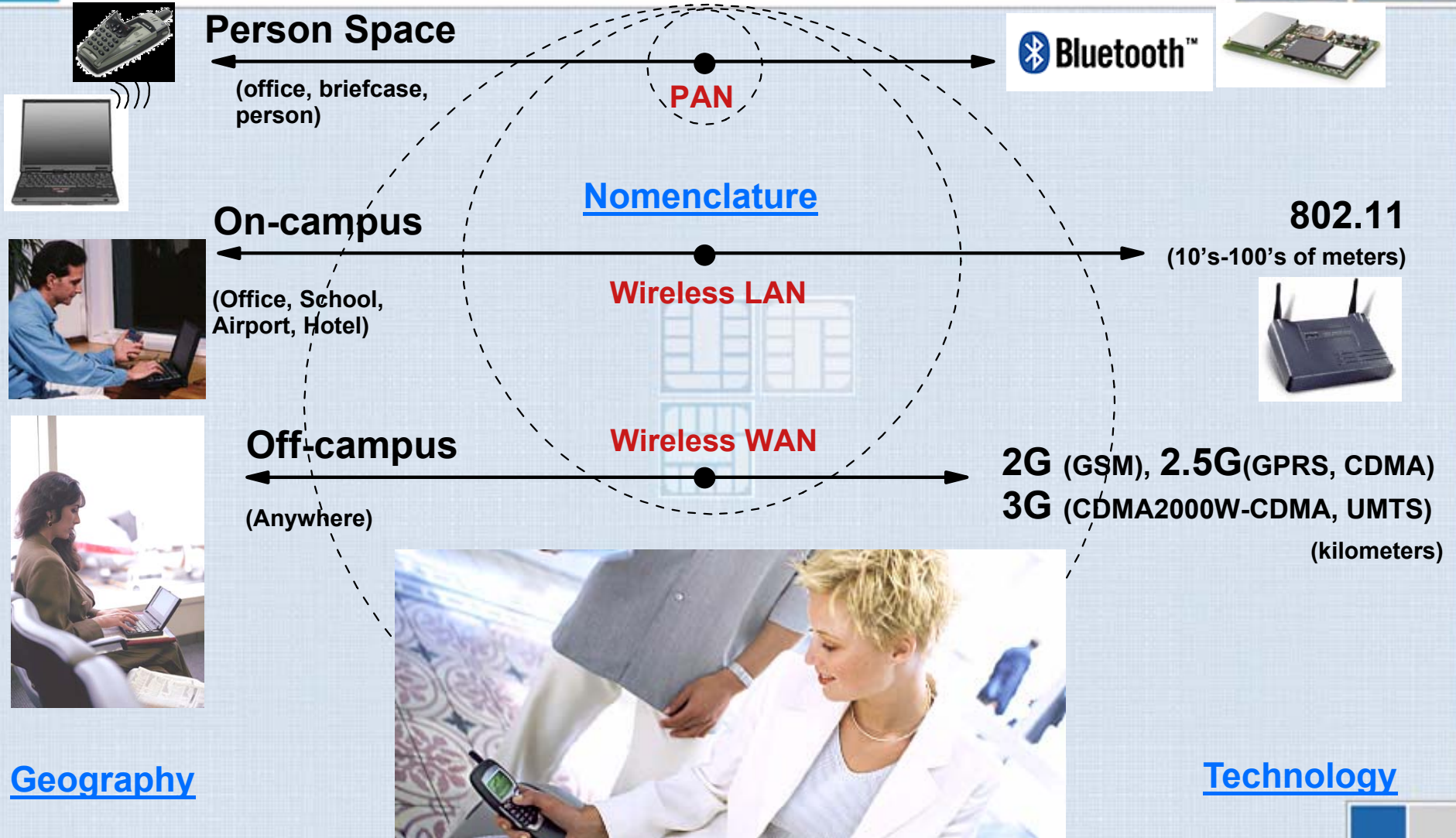
FGSec - Vorabendveranstaltung 20. Juni 2002

Uwe B. Kissmann

Leader IT- Security Services
IBM Global Services Switzerland

UKIS@CH.IBM.COM

Currently, we are working with customers to secure their wireless LANs. They look as follows:

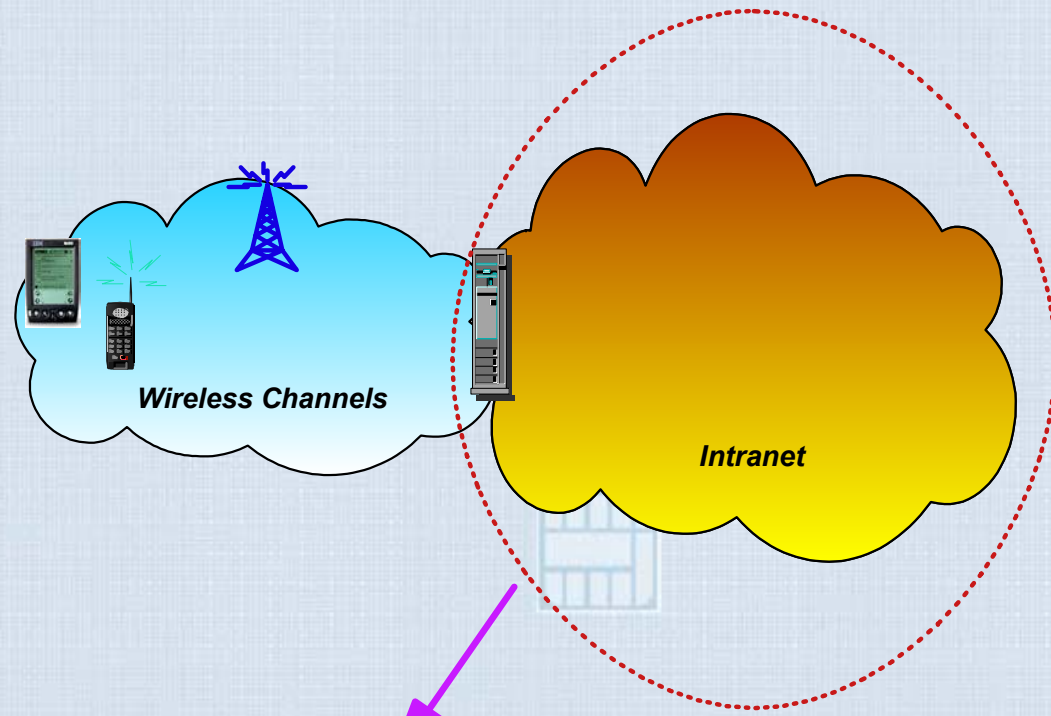


Wireless LANs (WLAN IEEE802.11b) the facts



- A Wireless Local Area Network (WLAN) is a flexible wireless data communications system implemented as an extension to, or as an alternative for, a wired LAN
 - The most widely adopted standard for wireless networking is IEEE 802.11b
 - This provides a theoretical transfer rate of 11Mbps. Actual transfer rates are 6Mbps and lower when security and encryption are enabled. Higher rates (up to 56Mbps) are planned
 - Range varies from 400-1500 feet (up to 300m). Range can be extended by using multiple access points (roaming possible)
- WLAN technologies:
 - Allow the enterprise to extend network coverage to allow for in-building or campus communication for mobile users
 - Can help solve access in hard-to-reach areas improving workforce mobility (i.e. Warehousing, Point-of-sale handheld equipment) and
 - Allows organizations to extend their wired networks without laying expensive cable

Existing "wired" security controls will be pushed to their limits and become increasingly important



- Policy management
- Intrusion detection
- Hardened platforms
- Security verification
- Secure device management
- Incident management
- Firewalls
- Content/E-mail filtering
- Anti-virus
- Identification & authentication
- Authorisation
- Security organisation

A new sport? Drive-By-Hacking, War-Driving, ...



BBC HOMEPAGE | SPORT | WEATHER | WORLD SERVICE | MY BBC

BBC NEWS

Search BBC News Online

GO

You are in: Sci/Tech

Tuesday, 6 November, 2001, 13:14 GMT

Welcome to the era of drive-by hacking

Front Page
World
UK
UK Politics
Business
Sci/Tech
Health
Education
Entertainment
Talking Point
In Depth
AudioVideo



The slow network

By BBC

Drive-By Hacking in London

Posted by [CmdrTaco](#) on Tuesday November 06, @11:20AM

from the only-a-matter-of-time dept.

delibes writes "The BBC News website carries this story about *hacking wireless networks in London's financial centre.* " There isn't really much in the way of details, just saying that many businesses don't encrypt their networks. They talk about finding 12 networks while driving 1km... 8 of which had no encryption.

([Read More...](#) | [67](#) of [100](#) comments)

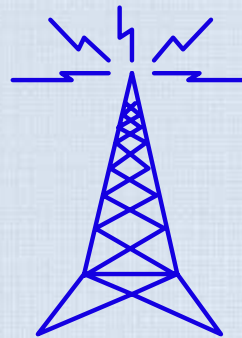
See also:

- ▶ 06 Nov 01 | Sci/Tech
Wireless networks wide open
- ▶ 17 Oct 01 | Sci/Tech
Hackers take to the air
- ▶ 06 Aug 01 | Sci/Tech
Park bench goes online
- ▶ 31 Jul 01 | Sci/Tech
Hackers to the honey
- ▶ 17 Jan 01 | Sci/Tech
Driving data to new highs
- ▶ 04 Oct 01 | Sci/Tech



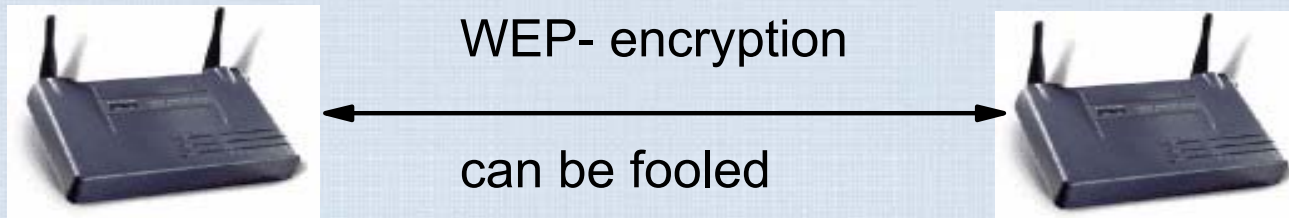
Wireless LANs: Security Issues

- *License free radio frequency technology*
 - *data easily “sniffed” by eavesdroppers*
- *RF signal leakage through buildings*
 - *no need to break into the office to gain LAN connectivity*
 - *tools available to detect vulnerable wLANs (“drive-by hacking”)*
- *Susceptible to radio interference*
 - *can be adversely affected by microwave ovens, bluetooth or malicious denial of service signal jamming attacks*
- *Lack of standards*
 - *Only agreed standard (WECA Wi-Fi for 802.11b) is 40bit WEP – Very Weak!*



Wireless LANs: Security Issues

- Security Issue 1: the Management Issue
 - most installations "out of the box" -- it's that easy...
 - protection options not in use / not enforced....it's sad but it's so true.....
- Security Issue 2: the Technology Issue
 - Choice of encryption technology WEP- break in within hours
 - in public WLAN sites, public network providers often forward weak keys



Wireless LANs: How to make them secure

- Several solution available
 - Firmware update (eliminate use of weak initialisation Vectors)
 - Draft standard IEEE 802.1x (today only proprietary implementations)
 - use of additional VPN technology (IPsec , SSH)
 - nomadic workers; use trusted public providers, who understand and adress the security management issue as well
 - most important: think about security management, not only about technology!

The challenges can be addressed using safe security methods
These solutions help enable Wireless e-business



Technology

- Session cryptography/VPNs
- File encryption
- Content and virus filtering
- Personal firewalls
- User and device authentication
- User authorisation
- Wireless PKI
- Intrusion detection
- Security management

Architecture

- Structured design method
- Functional architecture
- Operational architecture
- End-to-end security design

Secure and resilient industry solutions

Processes

- Risk management process
- Incident management process
- Change management process
- Audit process
- Security awareness program

Skills

- Risk management expertise
- IT security expertise
- Architecture and design expertise
- Industry knowledge

More wireless security information is available at ibm.com

www.ibm.com/services/security

The screenshot shows a Netscape browser window displaying the IBM Security Services website. The browser's address bar shows the URL <http://www-3.ibm.com/security/services/>. The website header features the IBM logo and navigation links for Shop IBM, Support, and Downloads. A main navigation bar includes Home, Products, Consulting, Industries, News, and About IBM. The page title is "Security Services".

The main content area features the headline: "Because when it comes to the risks and rewards of doing business in cyberspace, the sky's the limit... It's the dawn of a new frontier!". Below this, a paragraph states: "Cyberspace offers new adventure and opportunity, but at the same time it's full of dangers. (Read more)".

The central message reads: "IBM security services can help you determine what the risks are, then design a security program to cover them:". This is followed by a list of services:

- [Determine where you are now.](#)
- [Determine what assets need to be protected.](#)
- [Determine the best way to protect critical assets.](#)
- [Implement your secure environment.](#)
- [Manage your customer's privacy.](#)
- [Other security offerings.](#)

Additional security questions and information are listed:

- [How safe is that new Web server?](#)
- [We already have a firewall. Why do we need anything else?](#)
- [How can we conduct security audits in a distributed environment?](#)
- [Can secure technology open new business opportunities for us?](#)
- [IBM completes first customer secure product evaluation using the new Common Criteria \(CC\) standard.](#)
- [Special service offering for security product vendors seeking formal government certified evaluation of their products.](#)

On the right side, there are two boxes: "Related links" containing [Security and Privacy Services](#), [Business Partners](#), and [Products](#); and "Brochures" containing [Security Services](#), [Privacy Services](#), and [PKI Services](#).

The browser's taskbar at the bottom shows several open applications: Exploring - C:\User..., Sametime Connect..., Microsoft PowerPoint..., IBM Security: Se..., and Acrobat Reader. The system clock shows 11:29.

One part of IBM's answer to it

www.ibm.com/services/security

Wireless Security Auditor (WSA)

