



Microsoft Security Day 2008

Hacking and Defense Demonstration: Security Holes in Your Network

by

Professional Information Security Association (PISA)

專業資訊保安協會

Alan Ho
Sang Young

23-May-2008




Disclaimer

- The material and discussion in the demonstration is solely for promotion of security awareness and educational purposes. This material is NOT intended to be adopted in the course of attacking any computing system, nor does it encourage such act.
- PISA would warn that unauthorized access to computer system, damage of data and computer system are offences
- PISA takes no liability to any act of the user or damage caused in making use of the demonstration material



About PISA

- Professional Information Security Association (專業資訊保安協會) – www.pisa.org.hk 
- Established in 2001; not-for-profit organization
- Facilitate knowledge and information sharing among the PISA members
- Promote highest quality of technical & ethical standards and best-practices in information security
- Promote security awareness to the IT industry and general public in Hong Kong
- To be a de facto representative body of local information security professionals



Trojan Attack Demo





Basis

- What is a Trojan? A piece of software which appears to perform a certain action but in fact performs another (something malicious)
- Trojan may be installed by means of opening a malicious email attachment or installing a malicious software



Different Types of Trojans

- Remote Access Trojans
- Data-Sending Trojans
- Destructive Trojans
- DoS Attack Trojans
- Proxy Trojans
- FTP Trojans
- Security Software Disablers
- **All-in-one Trojans**



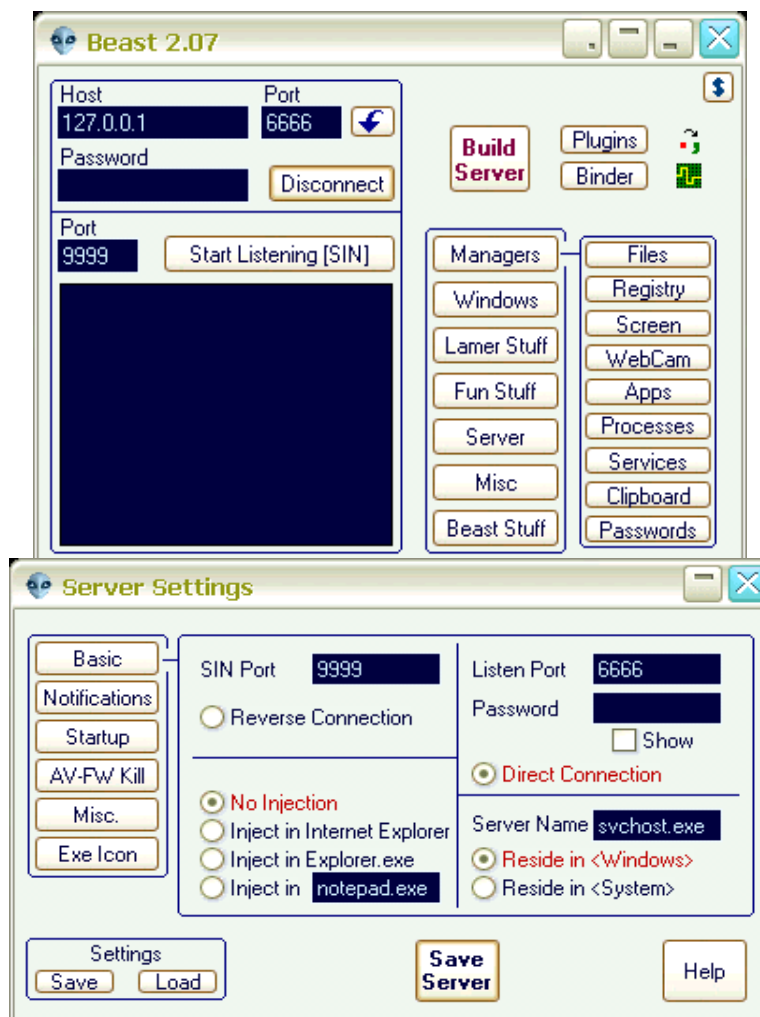
Trojan Penetration Ways

- Email Attachments
- IM
- Browser or Email Software Vulnerabilities
- P2P File Sharing
- Fake Programs
- Un-trusted Sites and Freeware
- Downloading files, games, screensavers etc.
- Legitimate “shrink-wrapped” software packaged
- Physical Access

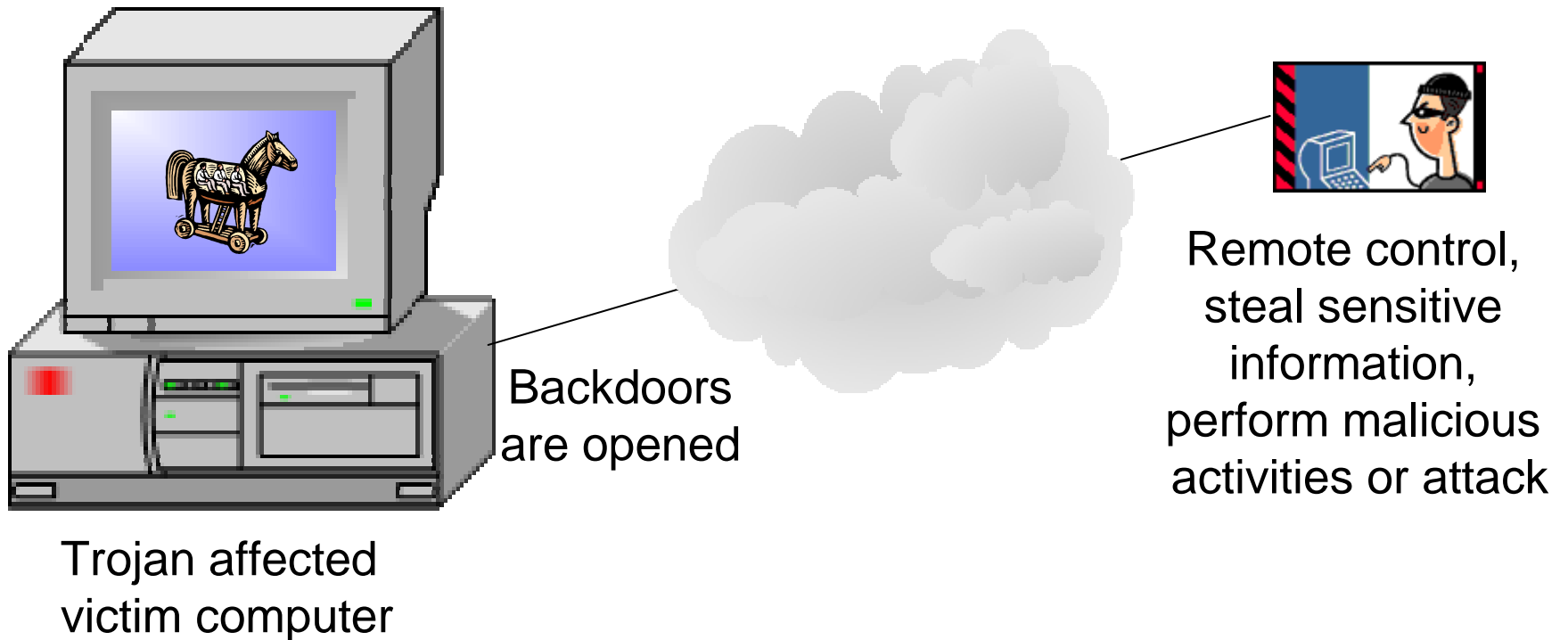


Trojan for Demo

- Demo Trojan: Beast 2.07
- Category: RAT (Remote Administration Tool – a Trojan that when run, provides an attacker with the capability of remotely controlling a machine)
- Date of origin: August 2004
- Threat assessment: high risk



Trojan Attack Demo

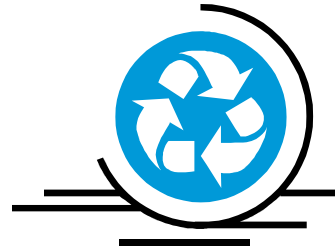


Countermeasure



It is very dangerous if antivirus/antispyware is not properly installed & maintained

- Install antivirus/antispyware software properly
- Keep virus/spyware definitions & signatures up-to-date



Demo of Unpatched Software Attack





Basis

- Vulnerabilities exist in unpatched software
- A software vulnerability may be caused by software bug, design flaw, etc. that prevents the software from behaving as intended






Software Vulnerability for Demo

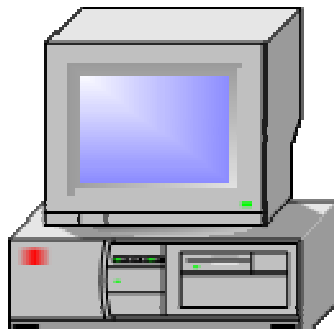
The screenshot shows the Microsoft TechNet website. At the top, there is a search bar for Microsoft.com and a navigation menu with links for TechNet Home, TechCenters, Downloads, TechNet Program, and Subscriptions. Below the navigation, there is a search box and a breadcrumb trail: TechNet Home > TechNet Security > Bulletins. The main content area displays the title "Microsoft Security Bulletin MS03-026" and the subtitle "Buffer Overrun In RPC Interface Could Allow Code Execution (823980)". It also lists the original posting date as July 16, 2003, and the revised date as September 10, 2003. A "Summary" section follows, with sub-sections for "Who should read this bulletin:" (Users running Microsoft Windows), "Impact of vulnerability:" (Run code of attacker's choice), "Maximum Severity Rating:" (Critical), and "Recommendation:" (Systems administrators should apply the patch immediately).

- Vulnerability: MS03-026 (Buffer Overrun In RPC Interface Could Allow Code Execution (823980))
- Impact of vulnerability: Run code of attacker's choice
- Posted date: July 2003
- Severity rating: Critical
- Affected software: Windows NT 4.0, 2000, XP, Server 2003



Situation of Victim Computer

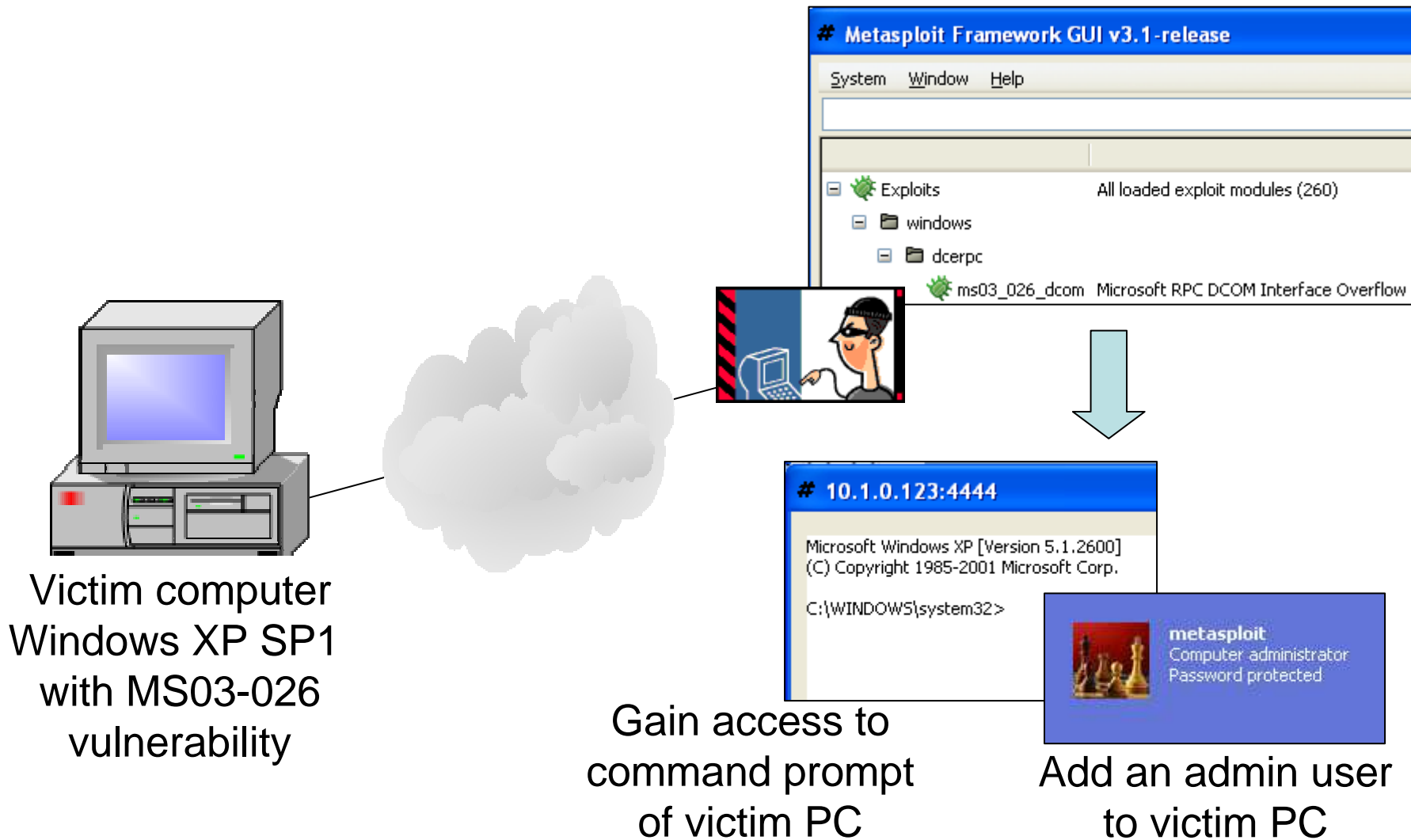
Tenable Nessus Security Report	
10.1.0.123	
 10.1.0.123	7 Open Ports, 23 Notes, 3 Warnings, 7 Holes.
microsoft-ds (445/tcp)	<p>✗ Synopsis : Arbitrary code can be executed on the remote host.</p> <p>Description : The remote host is running a version of Windows which has a flaw in its RPC interface, which may allow an attacker to execute arbitrary code and gain SYSTEM privileges. An attacker or a worm could use it to gain the control of this host. Note that this is NOT the same bug as the one described in MS03-026 which fixes the flaw exploited by the 'MSBlast' (or LoveSan) worm.</p> <p>Solution: http://www.microsoft.com/technet/security/bulletin/MS03-039.msp</p> <p>Risk Factor : Critical / CVSS Base Score : 10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) CVE : CVE-2003-0715, CVE-2003-0528, CVE-2003-0605, CVE-2003-0715, CVE-2003-0528, CVE-2003-0605 BID : 8458, 8460, 8458, 8460 Other references : IAVA:2003-A-0012, OSVDB:2535, OSVDB:11460, OSVDB:11797 Plugin ID : 11835</p>



Victim computer
Windows XP SP1
with MS03-026
Vulnerability



Demo of Unpatched Software Attack

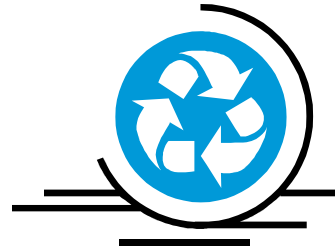


Countermeasure



Hackers can gain control of victim PC via software vulnerabilities and open backdoor for malicious activities

- Review and apply the software patches on a regular basis



Sidejacking Attack Demo





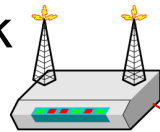
Basis

- Data in a wireless network can be “sniffed” if it is not well encrypted.
- “Cookies” are commonly used in web pages to store the state information of a browser session. “Sidejacking” – capture cookies & URL information in a wireless network and then enter to a connected browser session without the notice of the victim user
- Wireless network can be the weakest point of network security



Sidejacking Attack Demo

Open ~~lock~~ or WEP ~~lock~~
enabled wireless
network



cookies, URL



Laptop



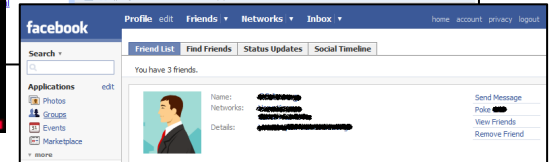
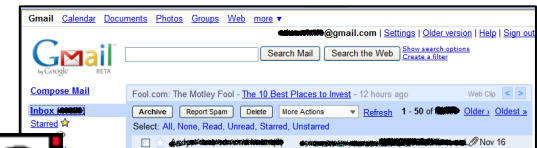
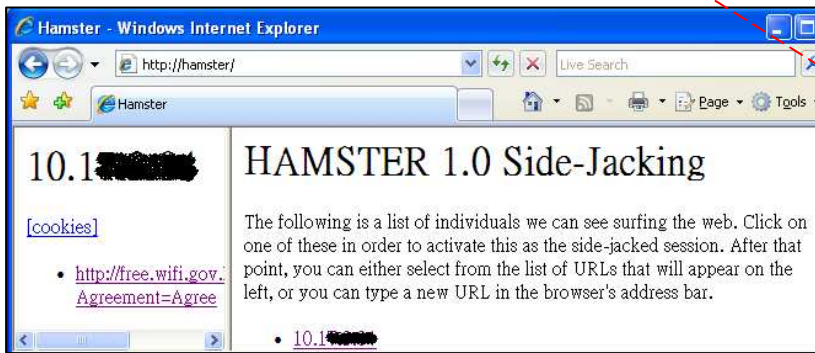
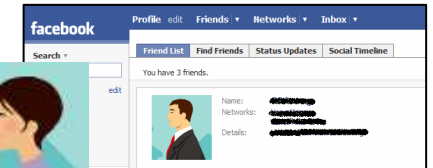
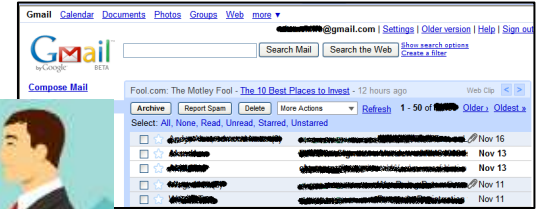
cookies, URL



Laptop



sidejack

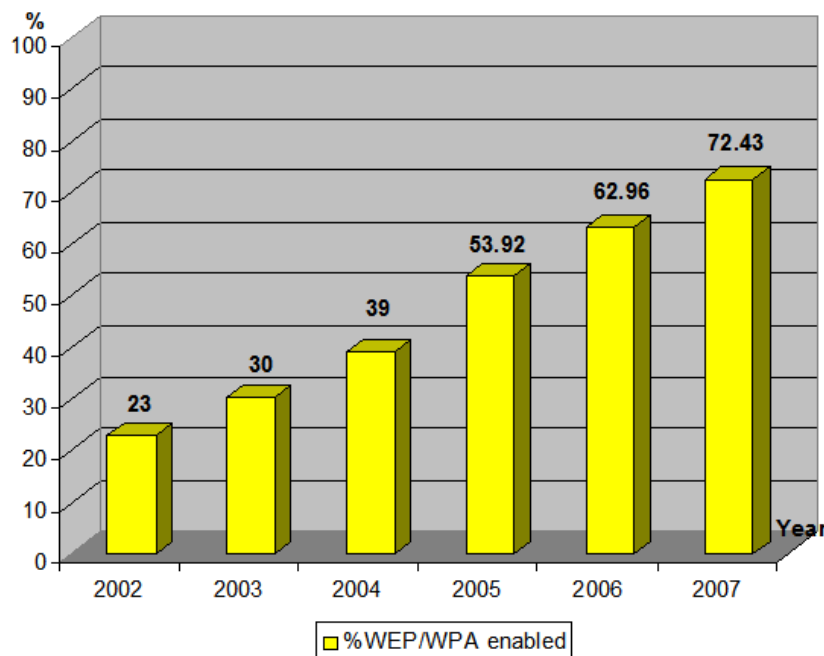


Enter to victim's browser sessions

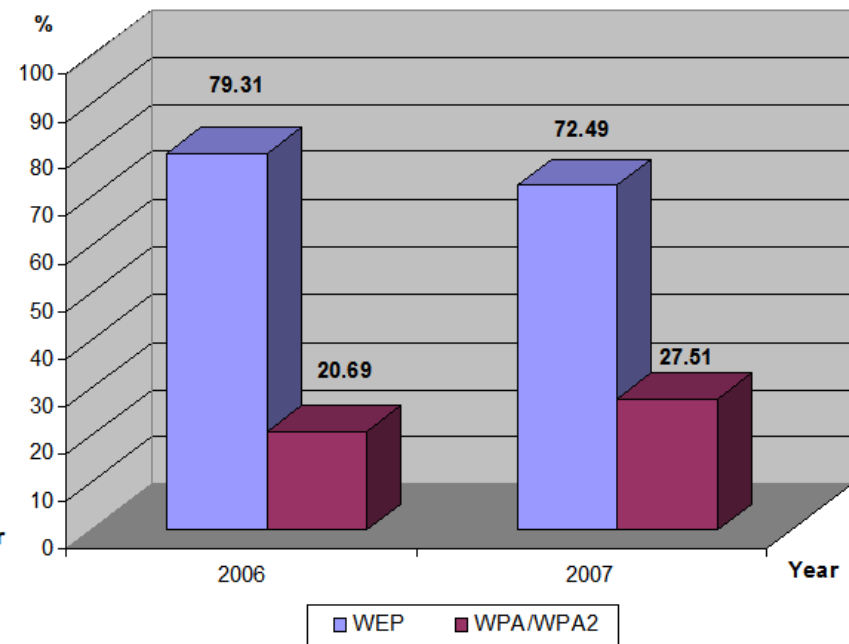


Wi-Fi Security Mode

- PISA & WTIA war-driving statistics 2007
 - Increasing adoption of encryption settings; though encrypted, % use of WEP was high (WEP is insecure nowadays)



% of AP with encryption enabled

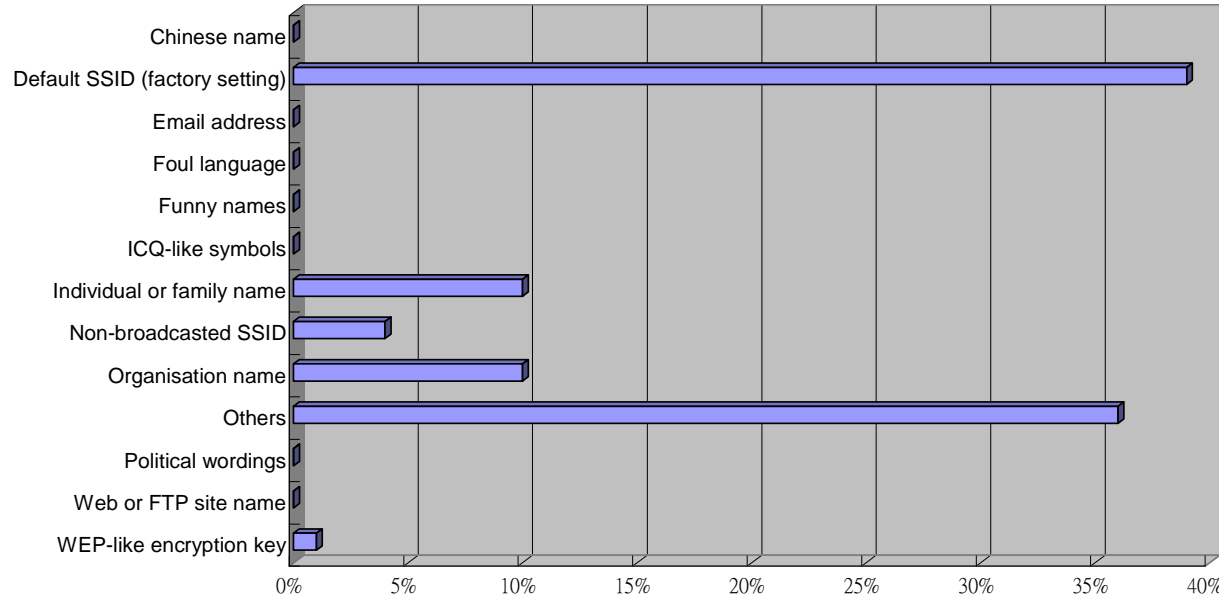


Security mode % -- WEP vs WPA/WPA2

SSID Setting

- In 2005's SSID analysis, about 20% SSID were associated with individual/family names or organization names.
- Using factory default SSID (about 40% SSID) may mean other default settings including the administration password have not yet changed
- Recommend to change to be not easily identifiable.

High-Level Analysis of SSID



Category	Percentage
Chinese name	0.01%
Default SSID (factory setting)	39%
Email address	0.01%
Foul language	0.01%
Funny names	0.01%
ICQ-like symbols	0.01%
Individual or family name	10%
Non-broadcasted SSID	4%
Organisation name	10%
Others	36%
Political wordings	0.01%
Web or FTP site name	0.01%
WEP-like encryption key	1%

Countermeasure



WEP encryption is insecure nowadays. Information can be sniffed & viewed if the wireless network is not secure enough

- Encrypt the wireless LAN using WPA/WPA2
- Use SSID that is not easily identifiable
- For additional security, place the wireless LAN router/access point outside the Intranet (e.g. in DMZ) and then connect to Intranet via VPN, etc.



Contact PISA

- Contact
 - Alan Ho : alan.ho@pisa.org.hk
 - Sang Young : ws.young@pisa.org.hk
- Website
 - <http://www.pisa.org.hk>

