

WLAN :
Har du koll på dina grannar?
Eller kollar de dig?



Håkan Lindberg på Internetdagarna 2004
hakan@twoviews.se

Konvergens vs. säkerhet

- JA!
 - IP-konvergens kan medföra säkerhetsproblem!
 - Men alternativet är inte bättre:
”security by obscurity”

Jämför med:

- webbens utveckling
- Metcalfe’s lag (nyttan av ett nät ...)
- modern militär strategi

Öronviveln:



- (*Otiorhynchus scaber*)
- Slutsats:
 - Ett allena rådande operativsystem är ett problem.
Hur bra det än är.

Användningsområden för WLAN



hemmanät

WLAN har gått ner kraftigt i pris.

Utrustningen anpassas: DHCP, webbgränssnitt



småföretag



skolor, offentliga miljöer



större nät



publika platser - ”hotspots”

Trådlösa nätverk är här för att stanna

- WLAN är EN teknik som används hemma, publikt och på större företag
- Intel Centrino: Priset för WLAN-kretsar fortsätter ner
- Vanlig bedömning (USA) 90% av alla bärbara datorer har WLAN år 2005-2006?

Arbetsgrupper inom IEEE

- Task Group= TG
- TGe
 - quality of service, för tex. röst
- TGf
 - förbättrad roaming
- TGg
 - Mer Mbit i 2,4 GHz-bandet. Fastslags 2003
- TGh
 - Anpassning av 802.11a mot bl.a. HiperLAN
- TGi
 - Förbättrad säkerhet, WPA och TKIP
- TGj
 - Förbättrad bryggning
- TGn
 - mer fart åt folket

Säkerhet

Richard Feynman

- “Safecracker meets safecracker”
ur boken “Surely you’re joking
Mr. Feynman”.
- Vad är problemet?
- Vad har vi lärt oss sedan
1940-talet?

Bärbart och trådlöst

- Bägge är faktiska säkerhetsproblem



Svårt fixa till WEP

- Allmän misstänksamhet mot enkla strömkrypton
- Det finns inte en enstaka brist utan flera
- TGi har tagit gott om tid på sig.
 - Wi-Fi Alliance tog till slut fram en (övergångs)lösning: WPA
- Wi-Fi Protected Access (WPA) består av två delar
 - WEP förbättras med nyckelbyte och "hashing"
 - Autentisering via EAP - 802.1x
- WPA 2
 - bättre krypto i grunden: AES (blockkrypto)

Vad kan man se?

Packet: 54

- Seq. Number: 2159
- Frag. Number: 0
- 802.2 Logical Link Control (LLC) Header
- IP Header - Internet Protocol Datagram
- TCP - Transport Control Protocol
 - Source Port: 3085 pcihreq
 - Destination Port: 21 ftp
 - Sequence Number: 2263120076
 - Ack Number: 3450805313
 - Offset: 5 (20 bytes)
 - Reserved: %000000
 - Code: %011000 Ack Push
 - Window: 16590
 - Checksum: 0xB83E
 - Urgent Pointer: 0
 - No TCP Options
- FTP Control - File Transfer Protocol
 - Line 1: PASS secrets@test.se..
- FCS - Frame Check Sequence
 - FCS (Calculated): 0xF2768AB6

0000: 08 01 02 01 00 02 2D 07 9E E0 00 05 5D F1 DF D8-.....}...
 0016: 00 90 27 E1 66 FD F0 86 AA AA 03 00 00 00 08 00 ..'.f.....
 0032: 45 00 00 3E 0C 21 40 00 80 06 D8 7C C3 54 85 6C E..>.!@...|.T.l
 0048: C2 47 0B 14 0C 0D 00 15 86 E4 78 CC CD AF 1C 41 .G.....x....A
 0064: 50 18 40 CE B8 3E 00 00 50 41 53 53 20 73 65 63 P.@...>..PASS sec
 0080: 72 65 74 73 40 74 65 73 74 2E 73 65 0D 0A 00 00 rets@test.se....
 0096: 00 00 ..



Får man avlyssna?

- Vad är syftet?
- Är det radio eller data vi avlyssnar?
 - Konvergens ställer till det...
 - (Är IP-telefoni telefoni eller IP?)

Lösning: Bättre design från början

- Betrakta WLAN som Internet
- Lägg säkerheten ”högre upp”
 - IPsec, VPN, ssh
 - VPN, brandväggar och inloggningsservers
- Använd en protokollanalysator och kanske Aircrack för att kontrollera att nätet blev bättre

Lösning: Relativt lätta lösningar

- Privatpersoner
 - Slå på WEP
 - tillverkarspecifika lösningar
- Företag
 - Windows Server innehåller möjligheter för att flytta säkerheten upp till autentisering av användare:
 - VPN
 - 802.1x och certifikat
 - Är tillverkarspecifika lösningar för bättre säkerhet ett stort problem?

Framtid 1

- VoIP över WLAN är intressant om priset konkurrerar med DECT. Annars en nisch-lösning
- Vid implementation: det finns ett skäl till att billig utrustning är just billig. Främst i accesspunkter:
 - dåligt stöd för externa antenner. Billiga radiodelar med dålig känslighet.
 - buggigt om man kör en tidig version
 - begränsad funktion för roaming

Framtid 2

- 100 Mbit/s över wlan (inte bara 2 kanaler á 54)
 - En arbetsgrupp har startat: 802.11n
- 802.11a anpassas för Europa
 - 5 GHz används inte så flitigt och har mer plats än 2,4 GHz-bandet
- Att få till hyfsad säkerhet tar tid (jämför med SSL/HTTPS)
- Videoströmmar

Delar av detta material kommer från boken ”Trådlösa Nätverk - WLAN, WEP och Wi-Fi” utgiven av Studentlitteratur 2002



© Studentlitteratur och Håkan Lindberg