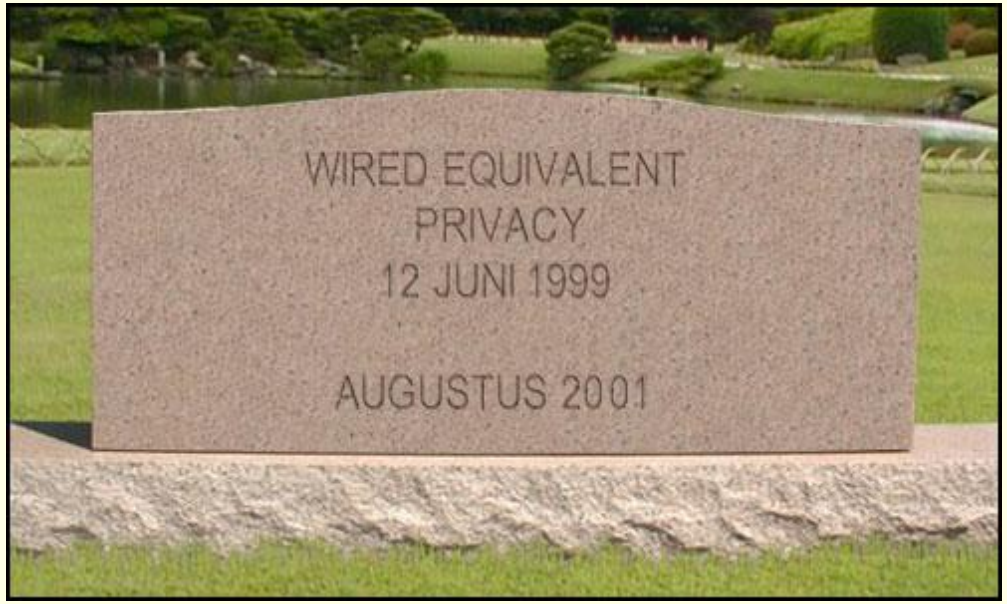
Wireless security anno 2006

Koos van den Hout

mailto:koos@kzdoos.xs4all.nl

16 September 2006



1 Deze presentatie

Inhoudsopgave

2 Waarom wil je wireless beveiligen?

- Ongeautoriseerde toegang
- Afluisteren

3 Maar wat als ik het niet wil beveiligen?

- Regels ISP
- Aansprakelijkheid

4 WEP

Wired Equivalent Privacy

40 bits WEP
104 bits WEP

WEP beschermt je wel tegen ongeautoriseerd gebruik, maar niet tegen afluisteren van verkeer door andere gebruikers.

WEP heeft slecht sleutelbeheer

RC4 zwakheden werden bekend in Augustus 2001.

Actieve aanvallen bekend in 2005.

WEP is dood.

5 Demonstratie WEP kraken?

Nee.

6 Nieuwe wireless security: WPA / WPA2

WPA = Wi-Fi Protected Access

WPA Enterprise / 802.1X

WPA Private / PSK

WPA / WPA2

WPA TKIP sleutels

Rekeying timer

7 WPA PreSharedKey

Eerste aanvallen hierop zijn al bekend. Neem een goed wachtwoord/wachtzin!

Been1riefohneuziengafahsodoyaexeegatuiyangiemeiteiyookasinejoh

Maar dan een andere.

8 Alfabet soep in WPA Enterprise: EAP

- EAP-TLS
- EAP-TTLS/MSCHAPv2
- PEAPv0/EAP-MSCHAPv2
- PEAPv1/EAP-GTC
- EAP-SIM

Eduroam als toepassing van WPA/Radius.

9 Nog vragen?

Slides: http://idefix.net/~koos/wireless2006/wireless2006.pdf

Aantekeningen:
http://idefix.net/~koos/wireless2006/wireless2006.txt