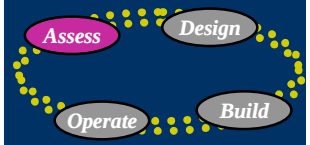
## Daniel Seid

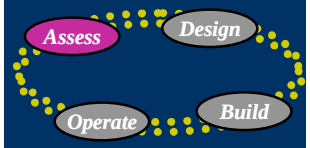
- 1989 Östra Real
  Studenten
- 1989 Polisen CKR
  Assistent
- 1990-1996 Falck Security
  Skydd och Ordningsvakt, mm
- 1996 Utrikesdepartementet
  Assistent
- 1997 Esselte
  PC-systemtekniker
- 1997-2000 PRV
  IT-samordnare
- 2001 Säkerhetskonsult
  Cap Gemini Ernst & Young

## Dennis Bergström

- 1987 Vasa
  Studenten
- 1988 Ericsson
  IT-support
- 1997 Ericsson
  IT-samordnare
- 1998 Securitas
  Ordningsvakt
- 1998 JUSEK
  IT-Support
- 1999 Magisterexamen 160p
  Data –och systemvetenskap
- 1999 Säkerhetskonsult
  Cap Gemini Ernst & Young



# WLAN




- Fördelar (sälj-pitchen) ----Exempel från Dustin----

**D-LINK WIRELESS KIT, 3 PCMCIA + ACCESSPOINT**

Tillverkare: D-LINK

**6,895.00 kr** (exkl moms), **8618.75 kr** (inkl moms)

Antal:

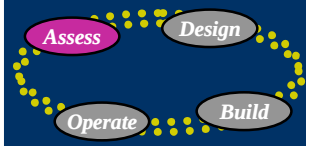
**Lagerstatus:**1-2 dagar
**Artikelnr:** 5010027258
**Tillverkares artnr:** DWL-1000-KIT

**Gruppnamn 1:** NÄTVERK
**Gruppnamn 2:** TRÅDLÖST ETHERNET

**D-Links DWL-1000AP** är en IEEE 802.11b kompatibel 11Mbps trådlös LAN accesspunkt. Enheten oppererar på 2.4 GHz DSSS (Direct Sequence Spread Spectrum) för trådlösa nätverk i hemmet eller i kontorsmilö. DWL-100( har transperent bridging och roaming egenskaper.
Administration av accesspunkten kan skötas på distans v programvara.

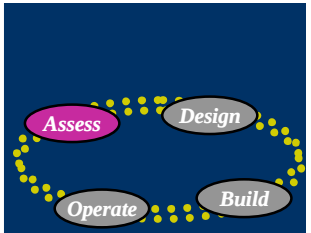
Även stöd för WEP (Wired Equivalent Privacy) kryptering, MAC adress kontroll och användar autentisering för att ge en hög säkerhet.

# 802.11b




- Inbyggd säkerhet !
  - MAC -Autentisering, Hårdvarukontroll
  - SSID –Autentisering, AP nätverksnamn
  - WEP –Autentisering & kryptering, nycklar
- Inbyggd säkerhet ?
  - MAC -Fejka MAC adress (klartext)
  - SSID –sniffa SSID (klartext-broadcast)
  - WEP –kryptoanalysera – Berkeley rapport. (kommenterat av bl.a B.Schneier & IBM)

# Verktyg




**NETSTUMBLER**

**release 2001-07-13 Internet**

**AIRSNORT**

**Release 2001-08-17**

**Internet/HAL2001**

-----Original Message-----
From: Seid, Daniel
Sent: den 28 juni 2001 14:34
To: 'Staffan Hagnell'
Subject: RE: SV: Ditt anförande internetdagarna

Hej Staffan
Här är ett snabbt utkast, medvetet icke tekniskt....
Tror att det stämmer överens med det ni har diskuterar och föreslagit ;)

**”AirSnort requires approximately 100M-1GB of data to be gathered.**
**Once enough packets have been gathered**
**‚AirSnort can guess the encryption password in under a second.”**

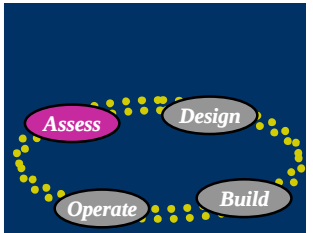
Vi har gott om tid att ändra detta dessa huvudrag, om ni så önskar (kan ta in WEP i detalj, en del kommer nog att hända på attack-verktygs-fronten tills det är dags för seminariumet).
Feedback mottages gärna och tackeamt.

**WEPCRACK**

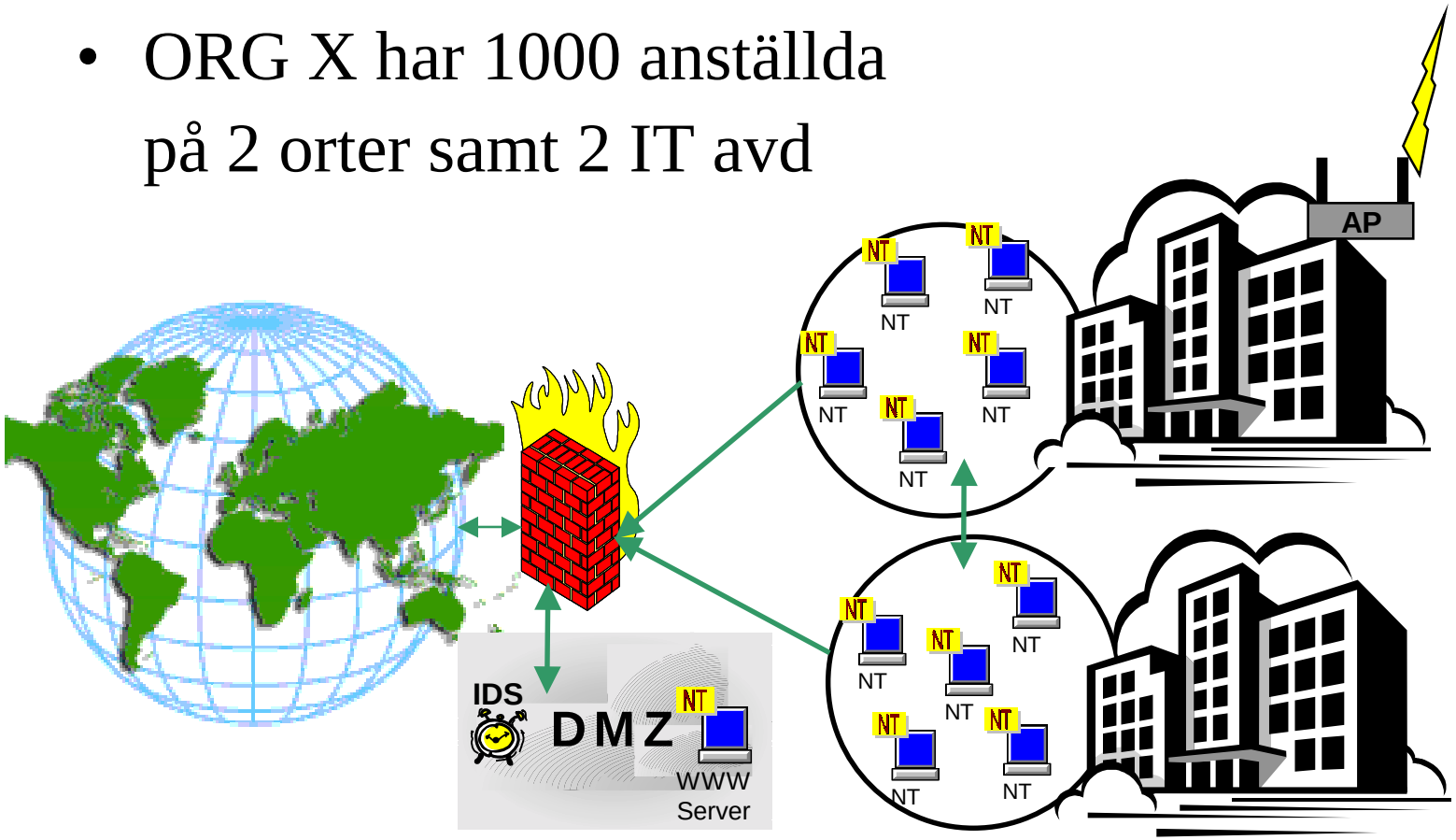
**Relase 2001-08-21 Internet**

Mvh
Daniel

# Fysisk säkerhet

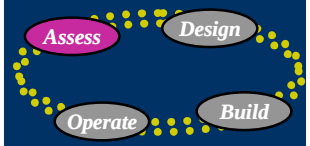



- ORG X har 1000 anställda
  på 2 orter samt 2 IT avd




- Någon ”går på” reklamen och installerar ett WLAN startkit –självklart default.

# Anonymitet

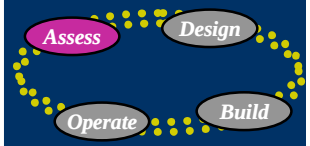



**http://www.barometern.se/artikel_standard.php?id=83462&avdelning_1=103&avdelning_2=102**
**Datorbrott**
**Polisen i Kalmar har spårat minst 50 misstänkta brott till datorer på Kalmar kommuns bibliotek, skriver Barometern-OT. Det rör sig om Inter- netbedrägerier, men även hotbrev till kommunalråd. Användarna är okända.**

- Skäl till varför anonymitet är attraktivt för angripare
- Spårbarhet = undvikande av åtal
  - ”Spåret slutade vid ORG X FW”
- Riktighet = undvikande av upptäckt (bedrägeri)
  - ”Beställt från ORG X ekonomisystem”
- Sekretess = ekonomiska vinster (stöld)
  - ”ORG X år av forskning patenteras

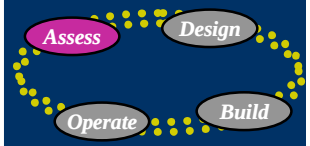
    (och licenstillverkas till en bråkdel av kostnaden) av konkurrenten Z

# ”War-Driving”




- Wardrivning = Medias Terminologi
- I praktiken ”mobilt scanna efter nätverk (strafik)”
- Förkrav (för en angripare):
- Bärbar dator
- WLAN –Kort
  - =total  kostnad ca 25000 kr
- Kommersiell / fri mjukvara = ”*gratis*” på Internet
  - IP-solarwinds
  - (wireless) network sniffer 4.6
  - Ethercap

# ”War-Drivning”

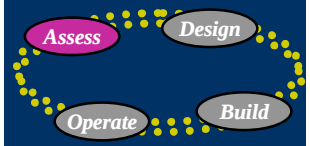



- Förkrav för ”offer”:
- Fysisk närhet dvs. samma stad
- Installerad Accesspunkt
- Helst default - jmf ”test”
- Helst i skarpt driftnät

- Har funnits ***-och finns-*** redan idag, jmf mässor ?

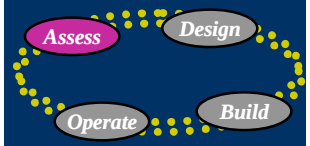
- Target Rich Areas ?
  - http://www.netstumbler.com/query.php
  - 2001-07-23 50 nätverk registrerade
  - 2001-08-20” We have almost 4,000 unique access points in our database as a result”

# Angriparen




- Bärbar dator med hård/mjukvara
  - Falsk MAC
  - Personlig FW –IDS
  - ”Bastion”-härdad
  - Computor ”Error” – Workgroup ”Anonymous”
- Bil eller cykel ”Drive-by-scan”
- Motiv  Nyfiken/uppdrag/invitationstest/
- Bil eller cykel ”Drive-by-attack”
  - enda oros-moment IDS ?

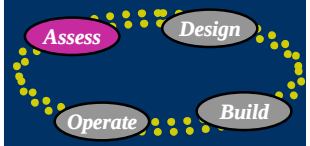
# Offer-mentalitet ?




- *Jag har ändå inget intressant i min dator...*

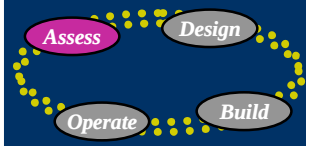
- Men snart kan *dina* system ha:
  - Barnpornografiska bilder
  - Lagrincentral crackade program
  - Språngbräda ut på Internet
  - Hotat-trakasserat via mail
  - Angripit internationella Polis, Militär eller Regeringars IT-system (ex DDOS)

# Juridik




- Problem med nationell – Internationell /teknikuppdatering
- Lagtext BrB 4:9
  - Motiv = Uppsåt= Åtalbart
- Exempel 1
  - Med en bärbar dator påslagen på stan, i ”ett” kvarter ”inbjuds” man med automatik utan aktivt handhavande till ett nätverk (DHCP) och blir med automatik av ”gäst-systemet” SNMP scannad
    = vem är det som begår dataintrång ?

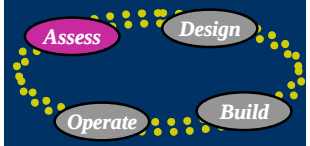
# Polisiär mardröm ?




- ORG X blir angripna från Internet
- ORG X gör Polisanmälan
- Polisen tar kontakt med ISP och får loggar ;-)
- Loggar visar att trafiken kommer från ”AP”
- AP är en anonym AccessPunkt
- För att nyttja AP köper man ett *anonymt* kontant-kort.
- *Anonymt* tidsbegränsat *internetabbonemang*.
- AP bör inte få logga annat än IP-trafik,
  dvs. ***inte*** MAC el dy, som skulle betraktas som integritetskränkande.
- Polisen har inga spår och lägger därför ner ärendet !

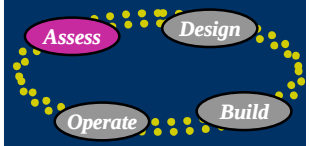
- Nästa gång kan angriparen nyttja detta nät som startpunkt till internet för nästa generation av s.k ”*super*” virus-spridning .

# Slutsatser




- Toppen av isberget
- Ett växande (ökande) problem
- *Alla* inbyggda säkerhetsmekanismer i 802.11b har bevisade brister.
- Tekniken tillgänglig för envar
- Införskaffningskostnad acceptabel
- ”Dina vänner är mina fiender” = tredjeparts info
- Befintliga skyddsmekanismer åsidosätts jmf FW
- *När* verktyg publiceras ökar dessa risker
- Organisationer med resurser ? NSA ?
- Framtid = ???

# Motmedel



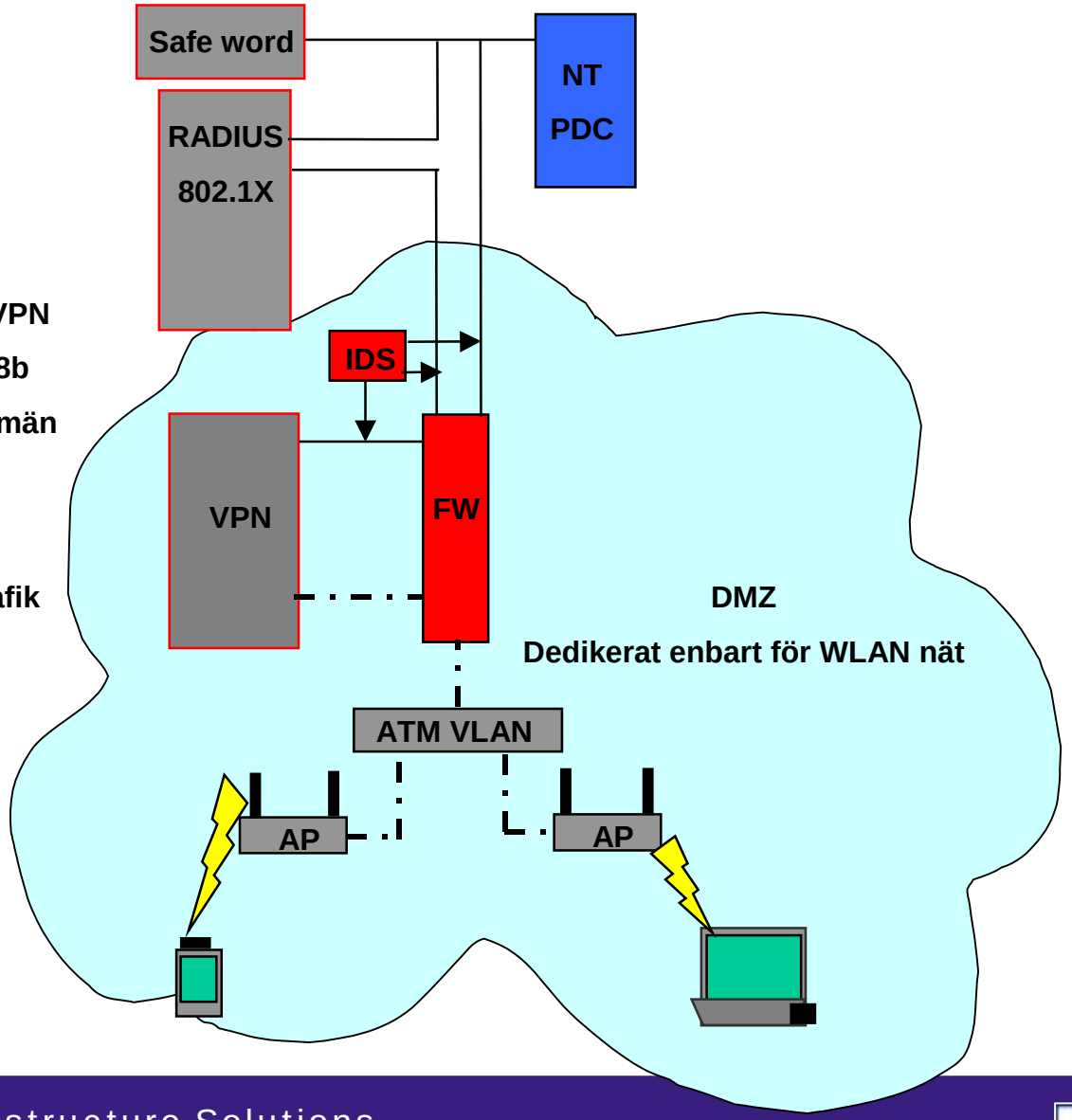

- Juridiskt ”missbruk av X kommer att åtalas”
- Organisation ”säkerhetschef”
- Personal ”informerad och utbildad samt kontrakt”
- Policy ”icke auktoriserade nätverkskomponenter”
- Tester ”NIVA”
- Tekniskt ”NGA = nät ***design*** = djupledsförsvar”
- Teknisk 802.1x
  - Cisco

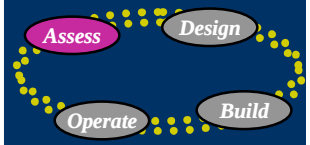
- Vid behov kontakta NIS för NIVA & NGA,
  Cap Gemini Ernst &Young tel 08-7045000

# Nät förslag

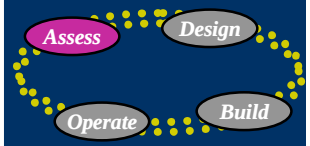
1. Klient – AP
2. Klient - VPN .
3. VPN - Radius
4. Radius - Safeword
5. Safeword- Radius- VPN
6. VPN –Klient 128+168b
7. Påloggningg på domän

– · – = krypterad trafik



# Referenser




- Säkerhet och skydd nummer 3
  - Artikel skriven av CGEY (NIS) om WLAN-risker
- http://www.cs.umd.edu/~waa/wireless.html
  - Sammanställning av wep-problem
- http://www.netstumbler.com/
  - Hittar trådlösa nätverk
- http://airsnort.sourceforge.net/
  - Airsnort + wepcrack knäcker wepkryptering
- http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/a350w_ov.htm
  - 802.1X
- http://www.elektrosmog.nu
  - Svensk länksamling & maillista