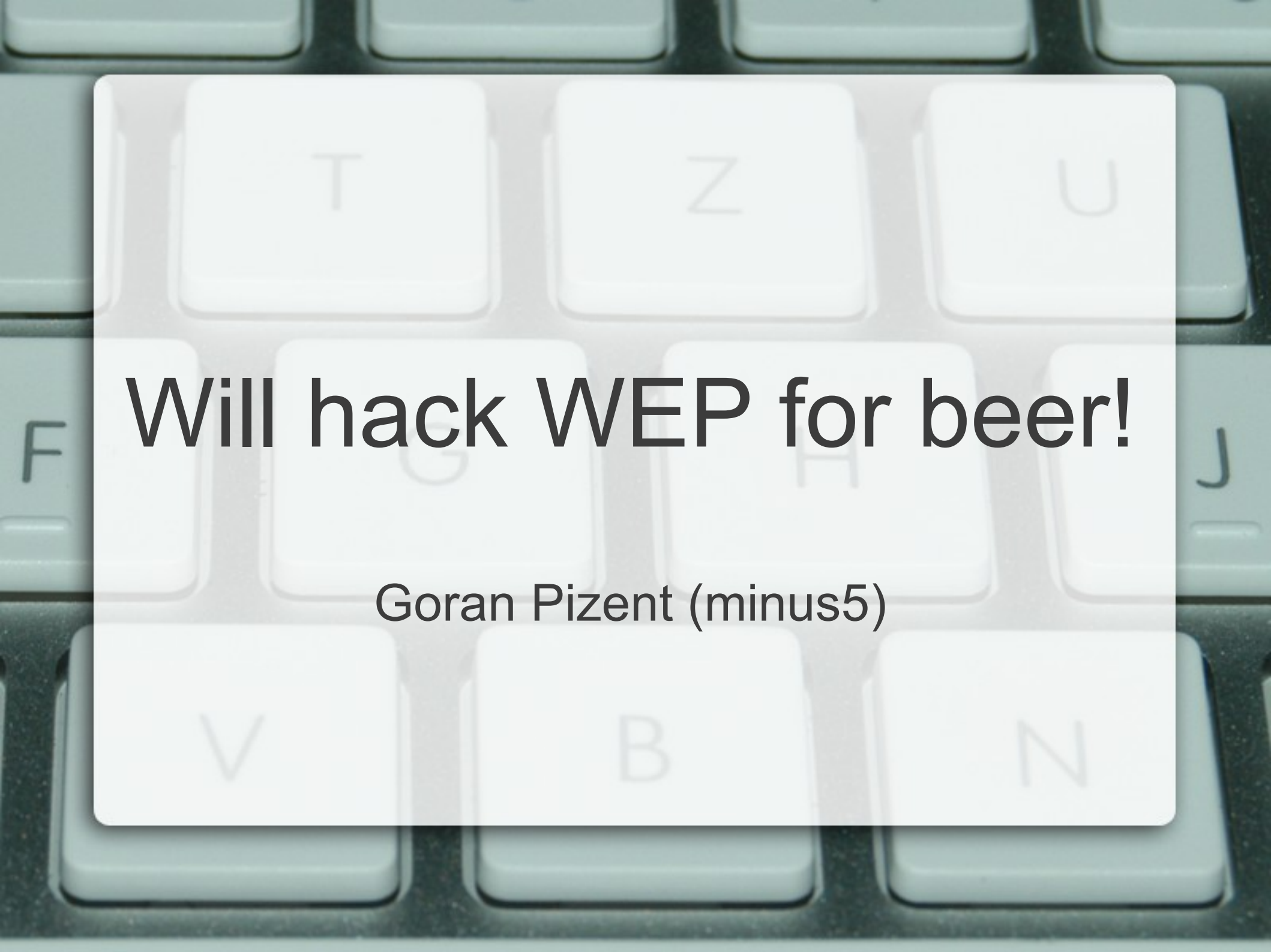


Will hack WEP for beer!

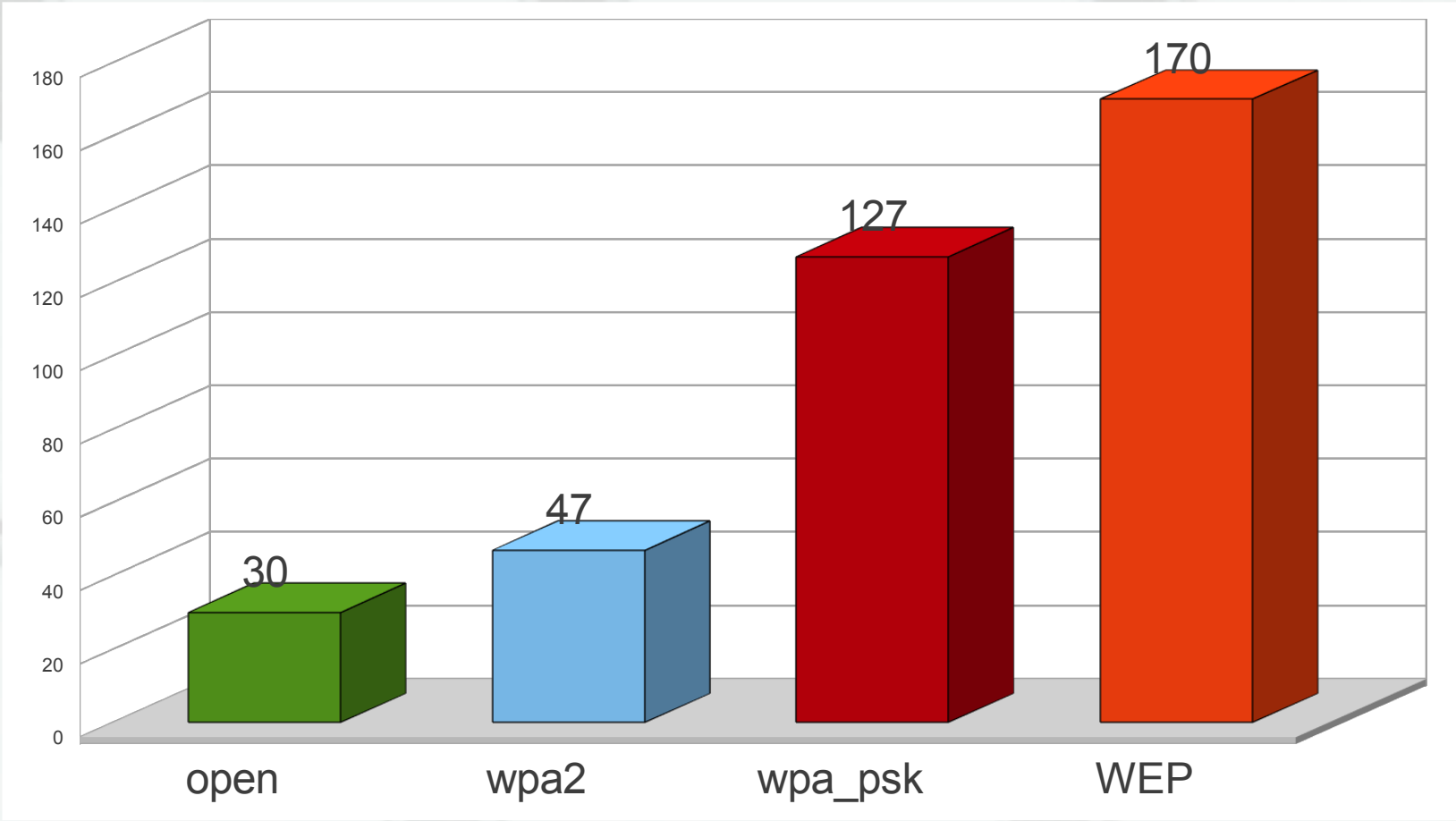
Goran Pizent (minus5)

The Wisdom

“Thus, what is of supreme importance in war is to attack the enemy's strategy.”

Sun Tzu

What a hell?? Why old WEP?



What shouldn't I do for beer? (agenda)

- WiFi is everywhere
- Inherent insecurities
- Wired Equivalent Privacy
- Wi-Fi Protected Access/2
- Attacks
- DEMO

WiFi is everywhere

- Easy to setup
- Easy to use
- No tedious cables
- Cheap
- Almost 100% coverage in cities (yeah good for hackers!)

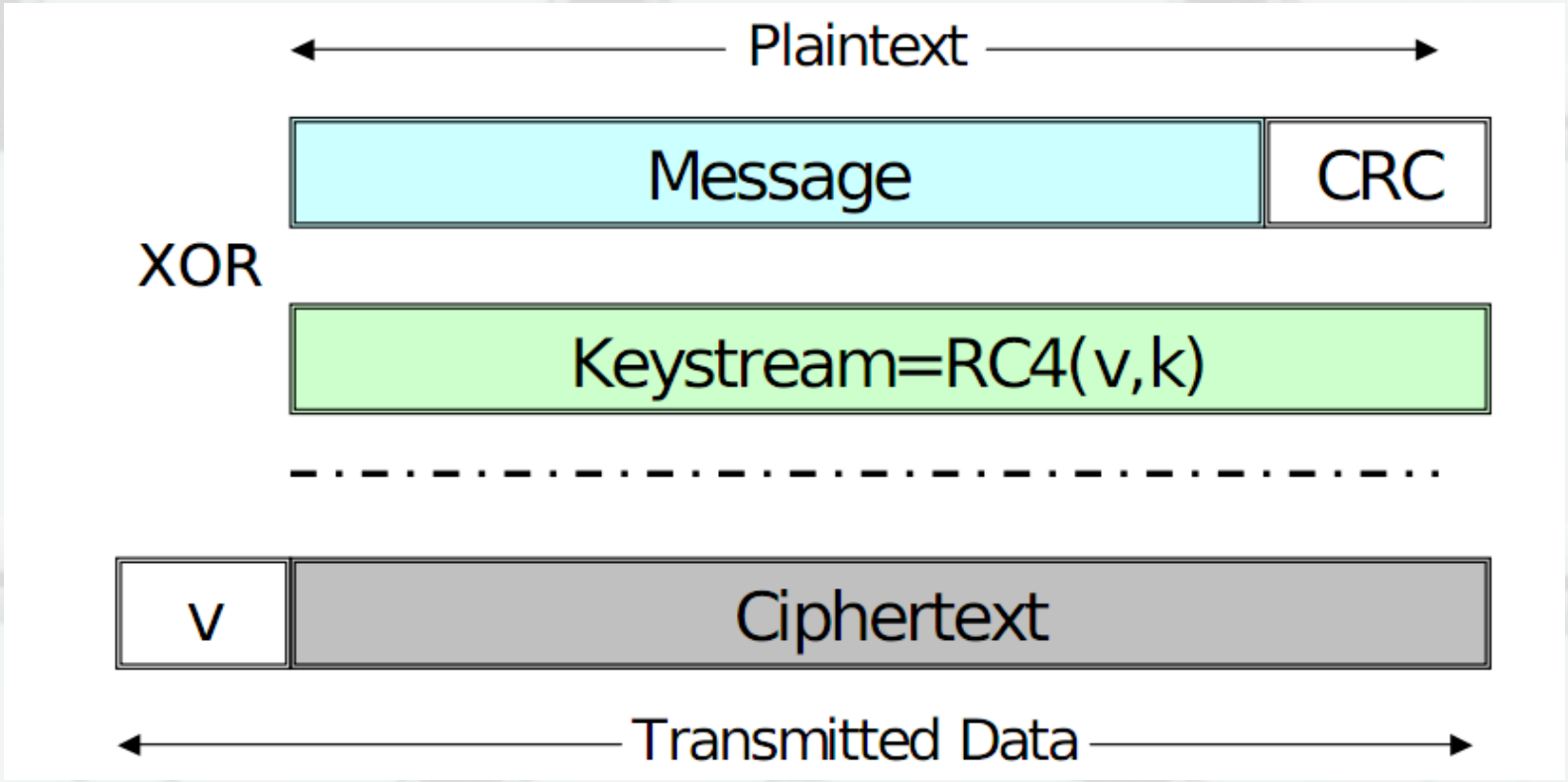
Inherent insecurities

- Management frames
- Control frames
- Data frames
- Headers of packet are not encrypted
- No integrity protection
- No packet replay protection
- Data is in the air (easy sniff)

Wired Equivalent Privacy

- Flawed as early as 2000
- Crypto weaknesses
  - RC4 weakness due to key construction
  - IV 24-bit field too small (50% chance of IV collision after 5000 packets)
  - No proper integrity check (CRC32 not cryptographically secure)
  - No method for updating keys

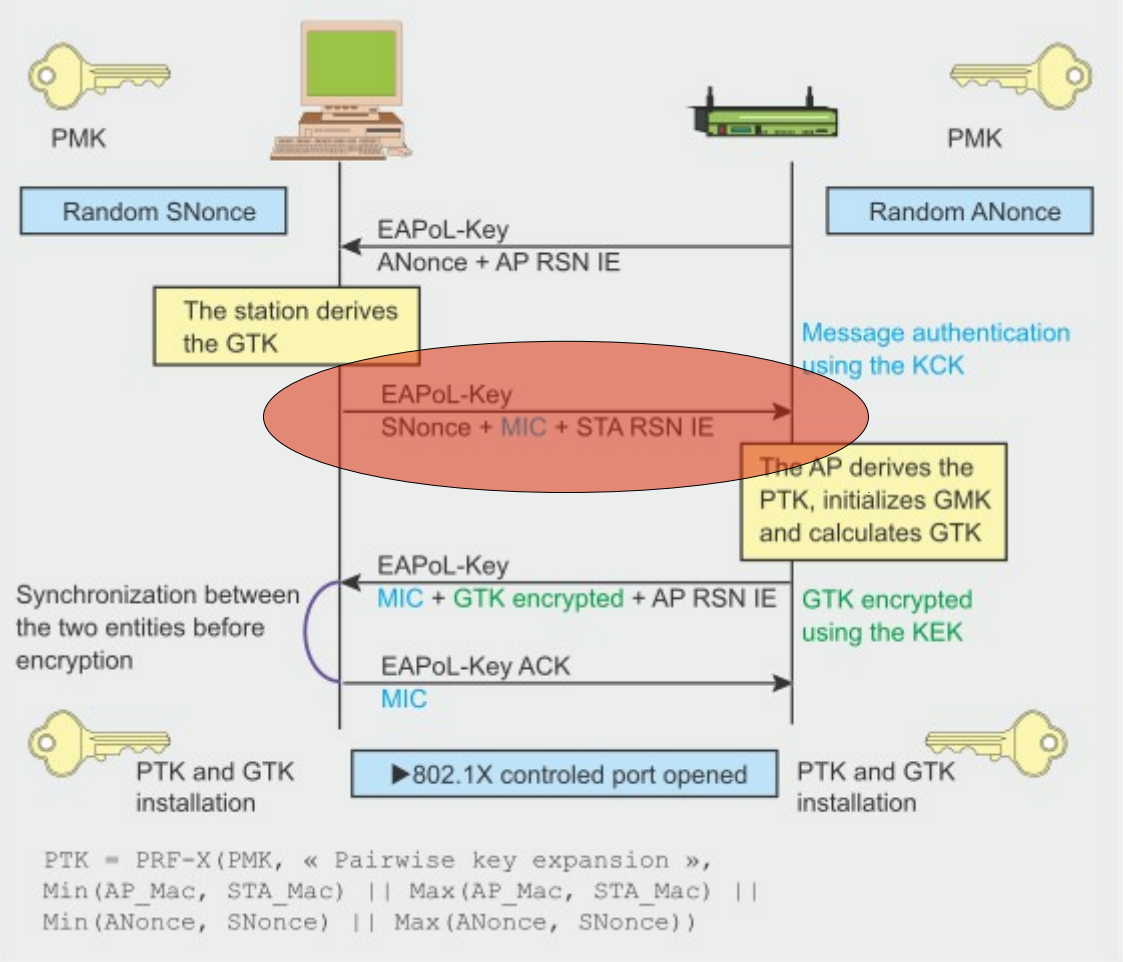
Wired Equivalent Privacy



Wi-Fi Protected Access/2

- WPA - enhanced security WEP
  - TKIP encryption protocol
  - Flaw in TKIP alghorithm → Erik Tews and Martin Beck, Toshihiro Ohigashi and Masakatu Morii, Halvorsen(2009), Martin Beck (2010) – decrypting all traffic
- WPA2 - IEEE 802.11i-2004,
  - CCMP/AES instead of TKIP
  - WPA2 certification is mandatory for all new devices

Wi-Fi Protected Access/2



Wi-Fi Protected Access/2

- EAP - Extensible Authentication Protocol, EAP-TLS, EAP-*, LEAP, PEAP
- Weaknesses
  - WPA-WPA2/PSK – dictionary && offline brute force attack
  - Message spoofing - EAPoL Logoff, EAPoL Start, EAP Failure...
  - DoS – de-authentication, de-association
  - Radio jamming!! :)

Attacks

- KoreK – Cracking the WEP
- ChopChop – byte by byte
- Caffe-Latte – attacking the client, no AP
- Arpreplay – injecting arp packets
- Deassociate
- Fakeauth

DEMO

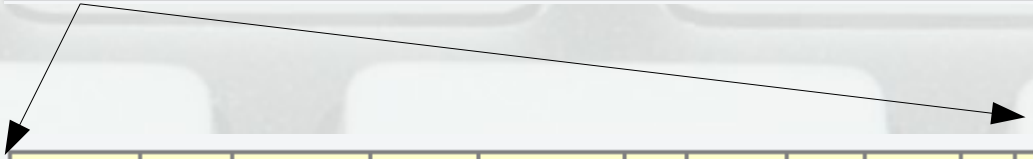
????PITANJA???

goran.pizent at minus5.hr

Inherent insecurities

- 802.11-1997 (802.11 legacy), 802.11a, 802.11b, 802.11g, 802.11-2007, 802.11n
- WLAN frame

2	2	6	6	6	2	6	0-2312	4
Frame Control	Duration	Address 1	Address 2	Address 3	Seq	Address 4	Data	Check sum



2	2	4	1	1	1	1	1	1	1	1
Version	Type	Subtype	To DS	From DS	MF	Retry	Pwr	More	W	O