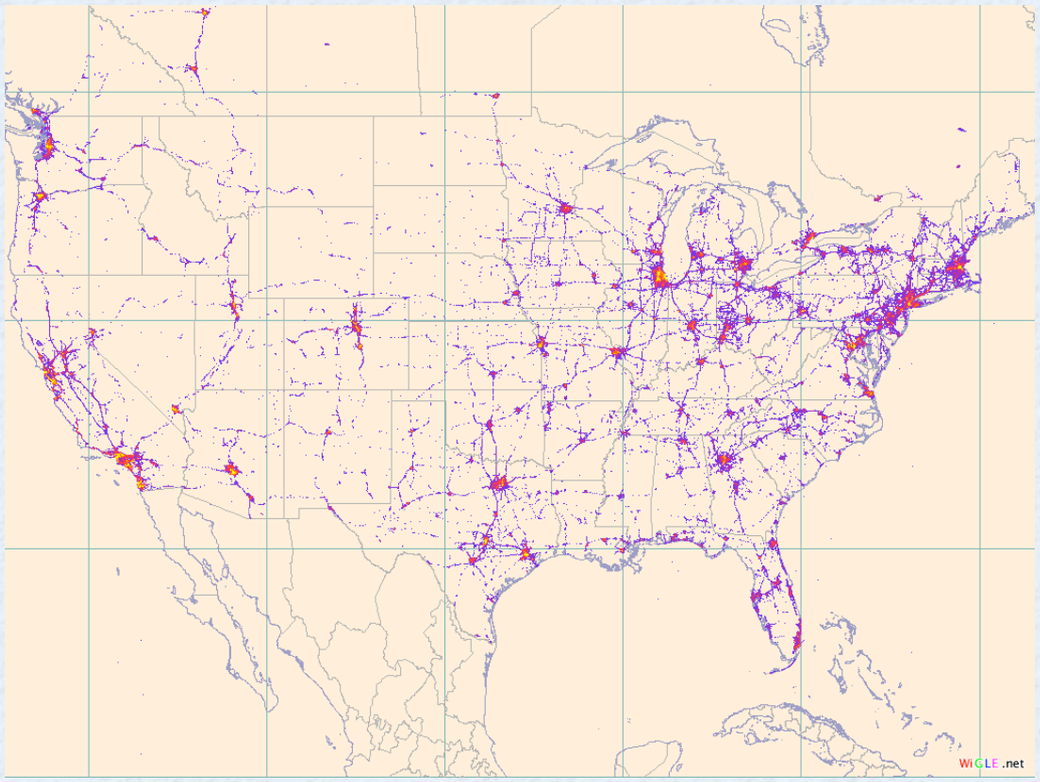
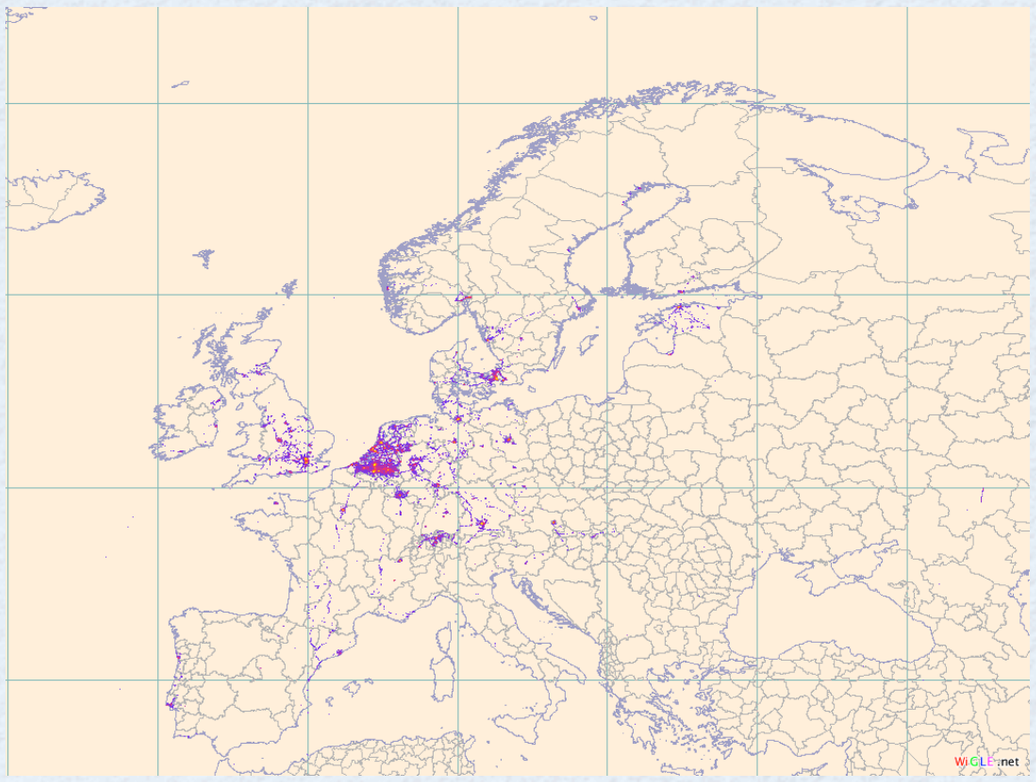
WIRELESS SECURITY

Cal Poly Linux Users Group
Jacob Farkas

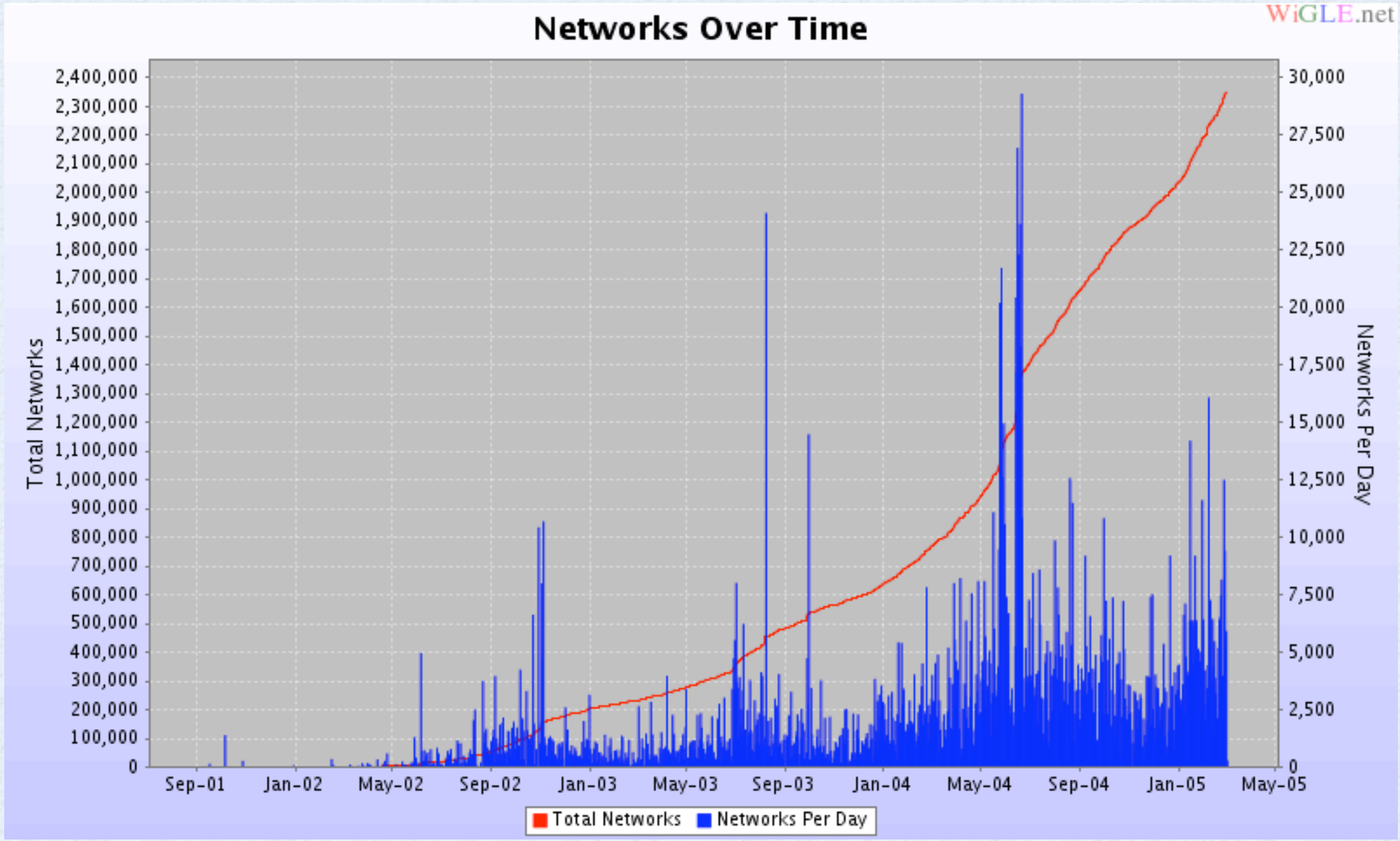
WIRELESS IS EVERYWHERE

- WiGLE.net, a wireless mapping database, has over **2.25 million** wireless networks





WIRELESS IS GROWING



San Luis Obispo

- Wardriving in SLO:
  - 755 networks in 2 hours
  - 70% without WEP
  - 47% using default SSID

SAN LUIS OBISPO MAP

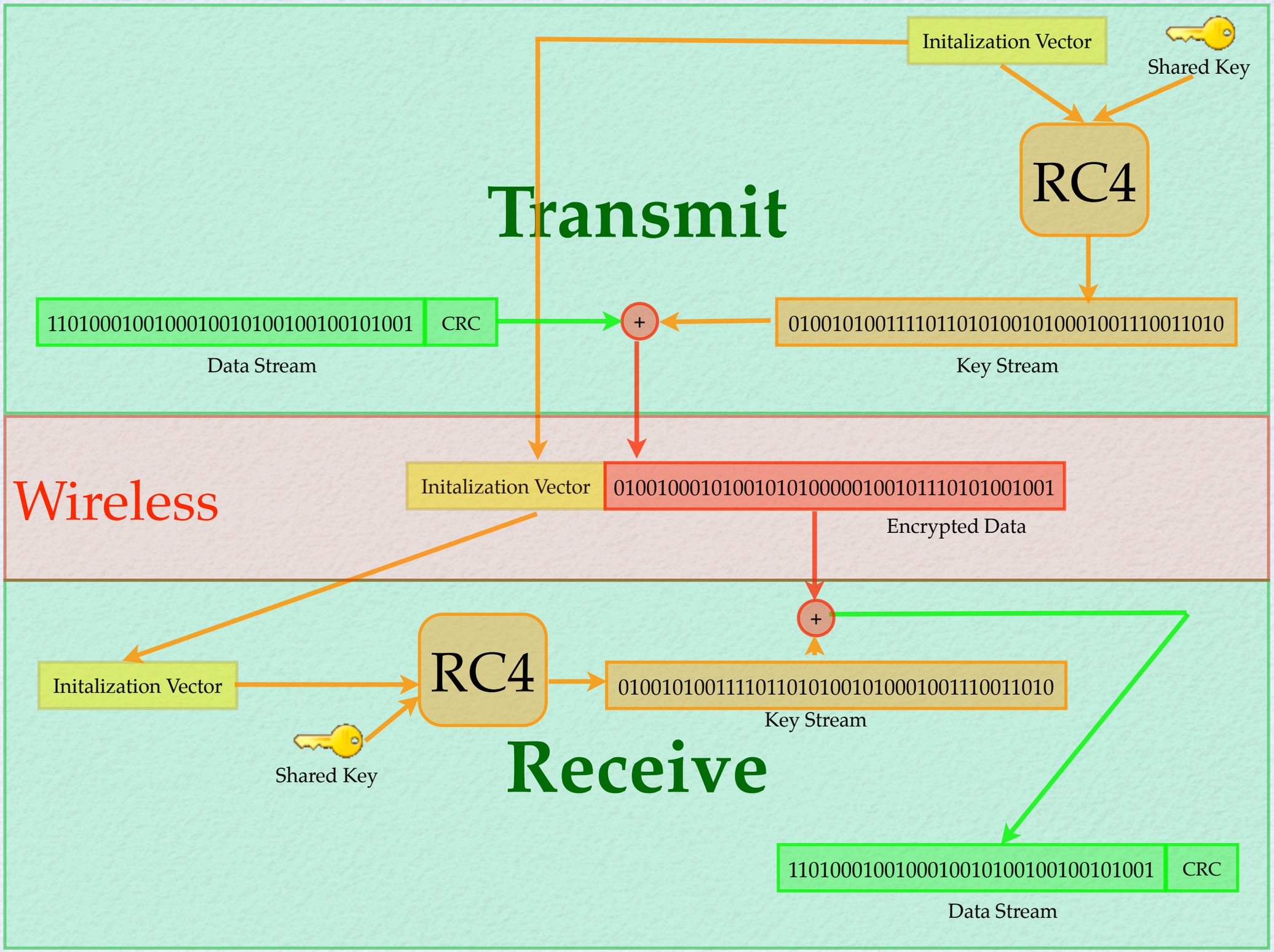
How secure is wireless?

- Without WEP (Wired Equivalency Protocol), wireless traffic is trivial to sniff.
- Most data is sent unencrypted:
  - Email passwords and email messages
  - Instant messenger conversations
  - Majority of web page traffic

WEP

- **W**ired **E**quivalency **P**rotocol
- Uses the RC4 algorithm to generate a keystream which is XORed with the data to be sent
- Shared keys and Initialization Vectors (IV) are used to generate the RC4 keystream.

WEP DIAGRAM


Initalization Vector
Shared Key
RC4
Transmit
1101000100100010010100100100101001
CRC
+
0100101001111011010100101000100111001101O
Data Stream
Key Stream
Wireless
Initalization Vector
01001000101001010100000100101110101001001
Encrypted Data
+
RC4
Initalization Vector
01001010011110110101001010001001110011010
Key Stream
Shared Key
Receive
1101000100100010010100100100101001
CRC
Data Stream

The RC4 Algorithm

- Generates a stream of bytes to be used for encryption
- Two parts:
  - Key Scheduling Algorithm (KSA)
  - Psuedo-Random Generation Algorithm (PRGA)

THE RC4 ALGORITHM

- An array of 255 bytes is initialized using the given key and the KSA algorithm
- For every byte of the keystream needed the algorithm chooses two bytes from within the 255 byte array, swaps them, and outputs the byte at the sum of the two swapped bytes.

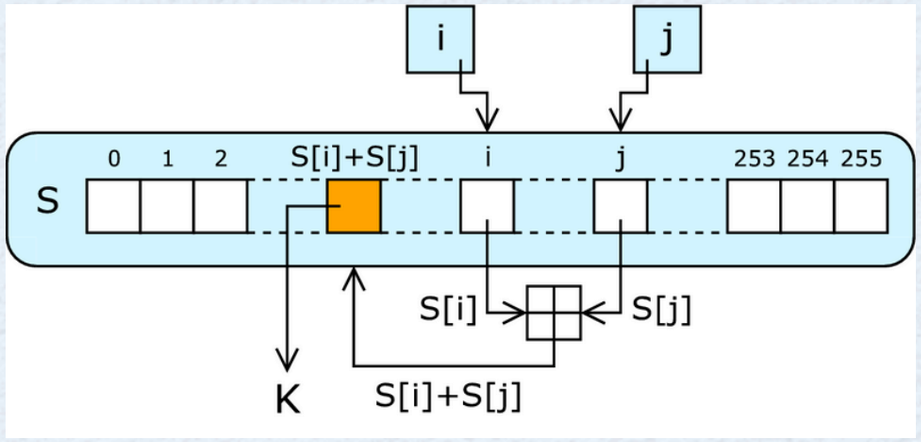
RC4: Key Scheduling Algorithm

- Uses a 8-2048 bit key to generate the array
- For WEP, this key is called the Initalization Vector.
- WEP uses 24 bit IV's and either 40 or 104 bit shared keys
- The strength of RC4 lies in a key never being reused

RC4: Pseudo-Random Generation Algorithm (PRGA)

- Uses two variables pointing within the 255 byte array and swaps their values.

```
i := 0
j := 0
while GeneratingOutput:
    i := (i + 1) mod 256
    j := (j + S[i]) mod 256
    swap(S[i],S[j])
    output S[(S[i] + S[j]) mod 256]
```



Source: wikipedia.org

- Pseudo-random: the sequence of numbers is deterministic given a specific key

What's wrong with WEP?

- The security of RC4 relies on keys never being reused.
- With only 24 bits of IV, the space is exhausted after 16,777,216 packets are sent
- The IV's are sent in plaintext.
- WEP does not specify how to pick IV's. Some routers start at 1 and go in order.

What's wrong with WEP?

- Almost all routers ship with WEP disabled.
- WEP is difficult for most users to set up.
- Shared keys mean that the user must remember and type in a 40 or 104 bit password. Most users don't bother.

WEP ALTERNATIVES

- IPsec
  - Encrypts data at OSI layer 3
  - Most hardware routers don't support IPsec
  - Included in Linux kernel 2.6
  - http://www.ipsec-howto.org

WEP ALTERNATIVES

- Access control list
  - Limits access to network to only those with authorized MAC addresses
  - Data can still be intercepted, but unauthorized users cannot access the network
  - Included in almost all hardware routers

WEP ALTERNATIVES

- VPN
  - Set up a VPN between clients and router over wireless connection
- 801.1X
  - New specification for wireless authentication
  - 3rd party authentication protocols are used

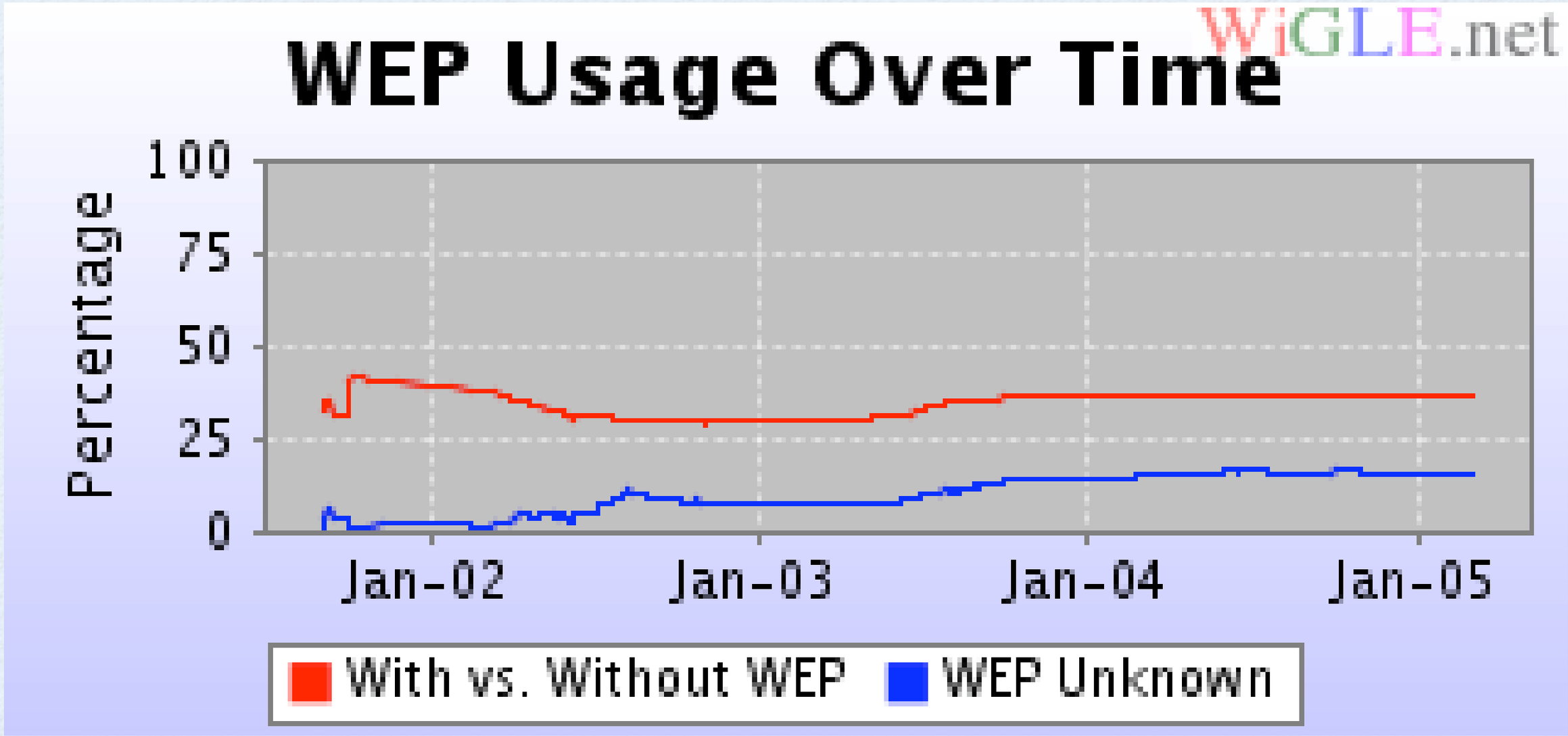
WEP ALTERNATIVES

- Disable SSID Broadcast
  - Security through obscurity
  - Network isn't instantly noticeable, but packets can still be sniffed with appropriate hardware

Wireless Security and the Average User

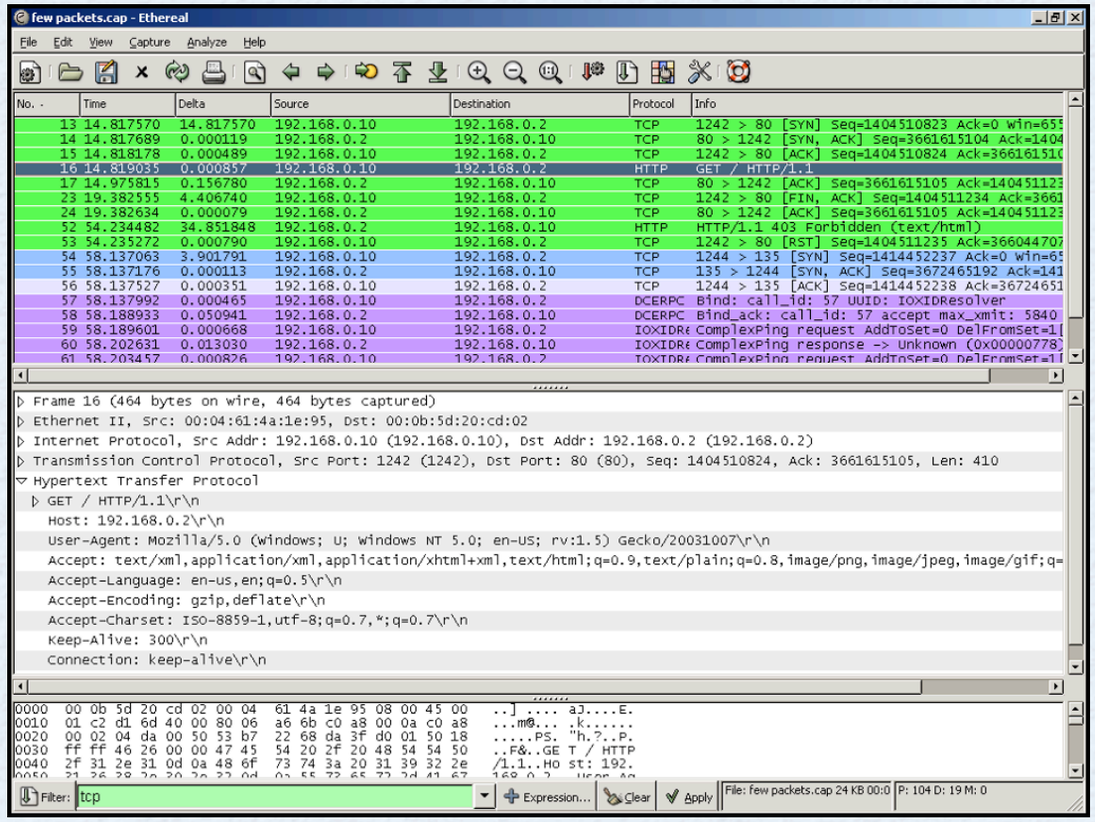
- The average user doesn't realize how easy it is to intercept wireless data
- Most users don't want to deal with setting up security or simply don't know how to
- Most hardware routers don't make an issue out of security- usually they don't even prompt the user to change the default password.

WEP USE


WiGLE.net
WEP Usage Over Time
Percentage
100
75
50
25
0
Jan-02
Jan-03
Jan-04
Jan-05
With vs. Without WEP
WEP Unknown

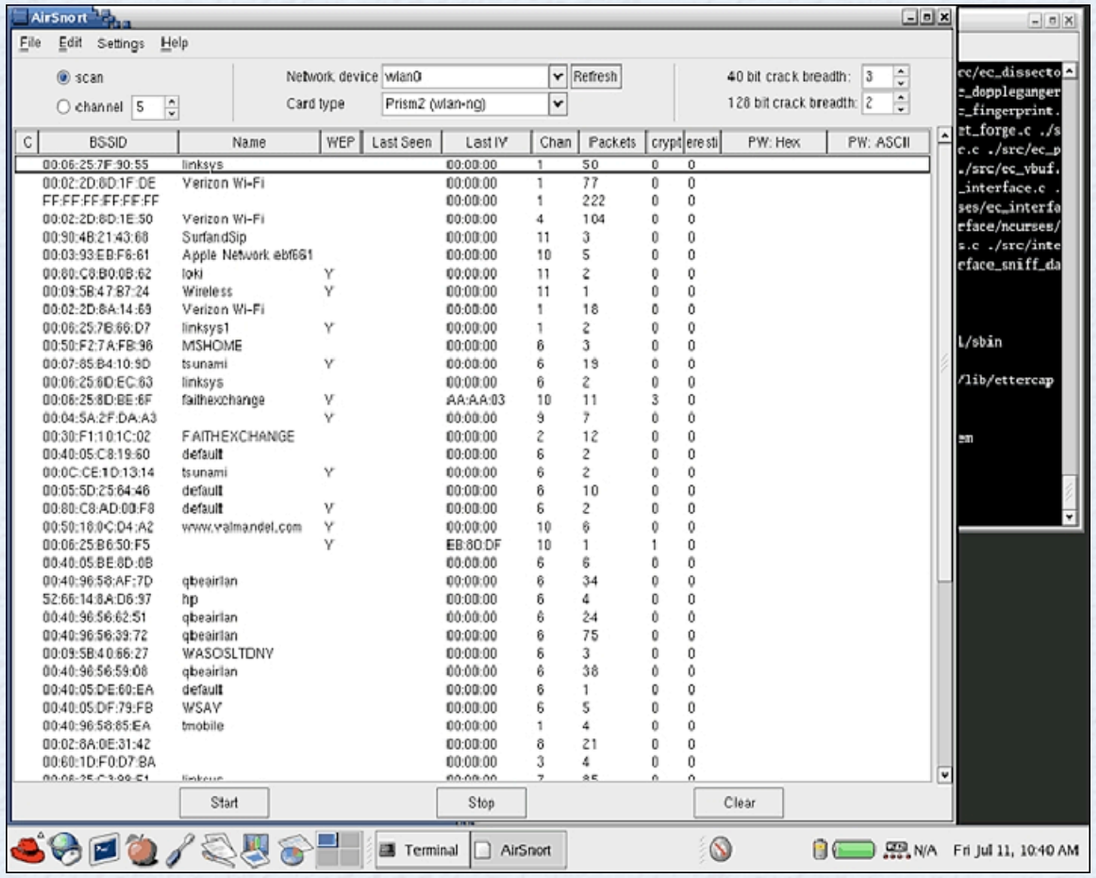
Wireless Programs

- Ethereal (Cross-platform)
  - http://www.ethereal.com
  - Capture and analyze network data from any network card



Wireless Programs

- AirSnort
  - http://airsnort.shmoo.com/
  - Cracks WEP encryption keys



Wireless Programs

- Driftnet (Linux)
  - http://www.ex-parrot.com/~chris/driftnet/
  - Captures and displays images from wireless

WIRELESS PROGRAMS

- EtherPEG (OS X)
  - http://www.etherpeg.org
  - Captures and displays images from wireless. Inspiration for driftnet.