Xi Chen

ATTACK ON WEP

Stream Cipher

- Symmetric Key Cipher
- Pseudorandom cipher bit stream (keystream)
- Encryption:
  - E_k = P XOR keystream
- Decryption:
  - D_k = C XOR keystream
- Difference between Block Cipher
  - every single bit
  - Faster execution
  - Lower hardware complexity

What is WEP

- WEP – Wired Equivalent Privacy
  - Introduced September 1999
  - Security Algorithm for IEEE 802.11
  - Uses RC4 for confidentiality
    - Generate encrypted message
  - Uses CRC-32 checksum for integrity
    - Check error during transmission
- Standard WEP
  - 64-bit: 24-bit IV followed by 40-bit key
  - 128-bit: 24-bit IV followed by 104-bit key

RC4 – River Cipher

- Designer: Ron Rivest (RSA Security)
- Designed in 1987
- Variable key-size and byte-oriented opertaions
- Initially a trade secret
- Leaked in 1994
- Widely used in popular protocols
  - WEP, SSL
- Speed and simplicity
  - 10x faster compare to DES

RC4 – cont.

- Key-Scheduling Algorithm (KSA)
  - Used to initialize the array S to the identity permutation
  - Process S for 256 iterations, similar to PRGA, and mixes in bytes of the key at the same time.

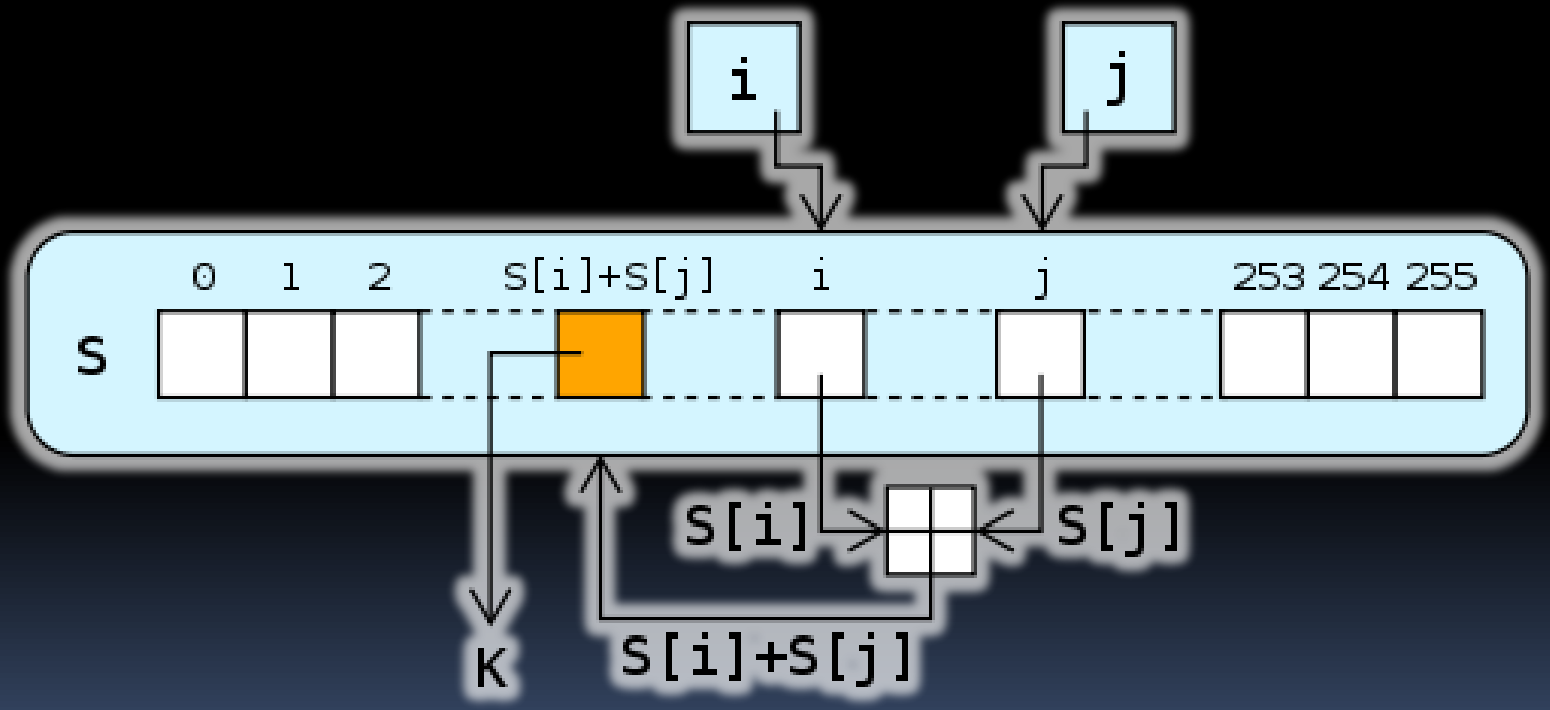
```
for I from 0 to 255
        S[i] := i
end for
j := 0
for j from 0 to 255
        j := ( j + S[i] + key[I mod keylength]) mod 256
        swap values of S[i] and S[j]
end for
```

RC4 – cont.

- Pseudo-random Generation Algorithm (PRGA)
  - Translate the patterns generated by KSA to patterns in the prefix of output stream

```
i := 0
j := 0
while GeneratingOutput:
   i := (i + 1) mod 256
   j := (j + S[i]) mod 256
   swap values of S[i] and S[j]
   K := S[(S[i] + S[j]) mod 256]
   output K
endwhile
```

RC4 – cont.



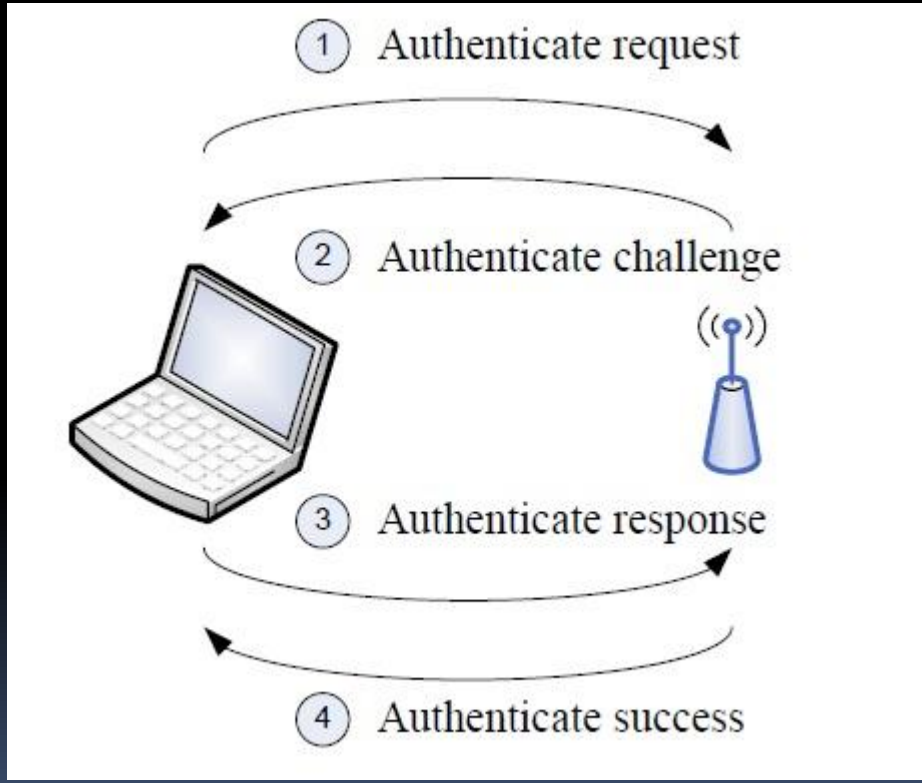
How WEP works?

- AP
- MPDU
  - Medium access control Protocol Data Unit
  - Data
- ICV
  - Integrity Check Vector
  - Cyclic Redundancy Check – CRC 32
- IV
  - Initialization Vector
  - Auto-generated

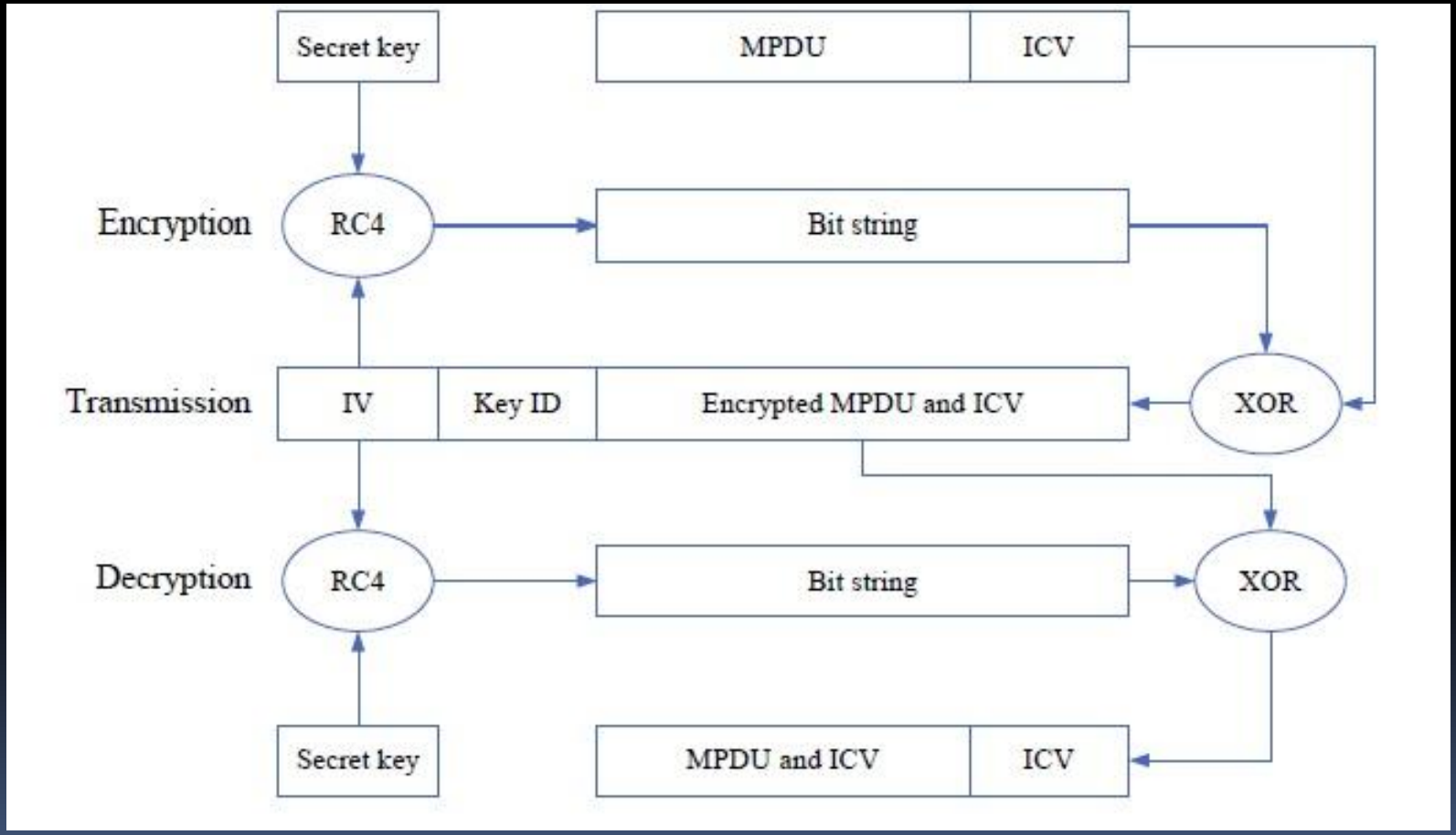
How WEP works - Authentication

1. Station sends a request
2. AP sends a challenge
   - 128-bit random value: x
3. Station sends a response
   - response = $E_k(x)$
4. AP decrypts the message and compare it with x

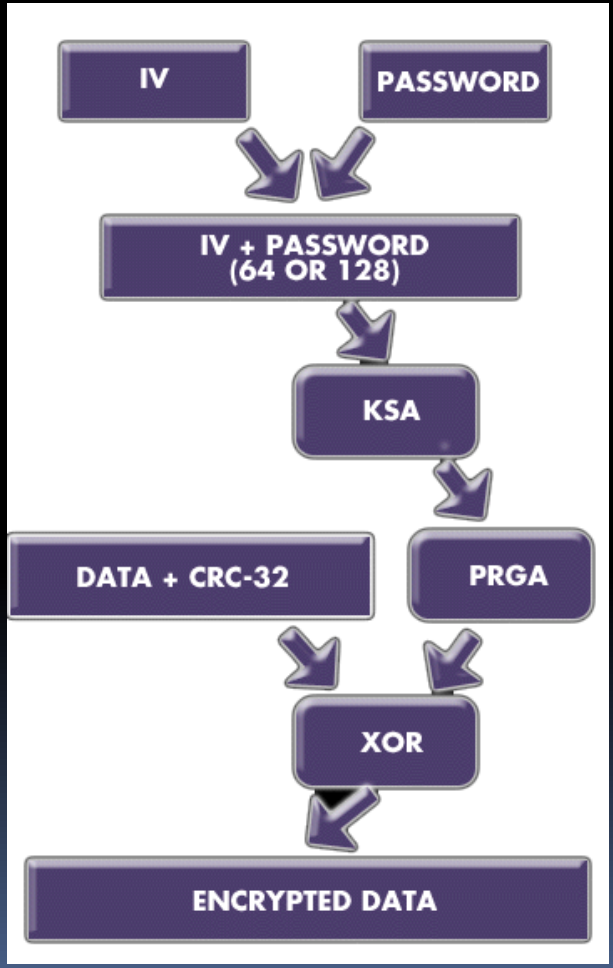
How WEP works - Authentication



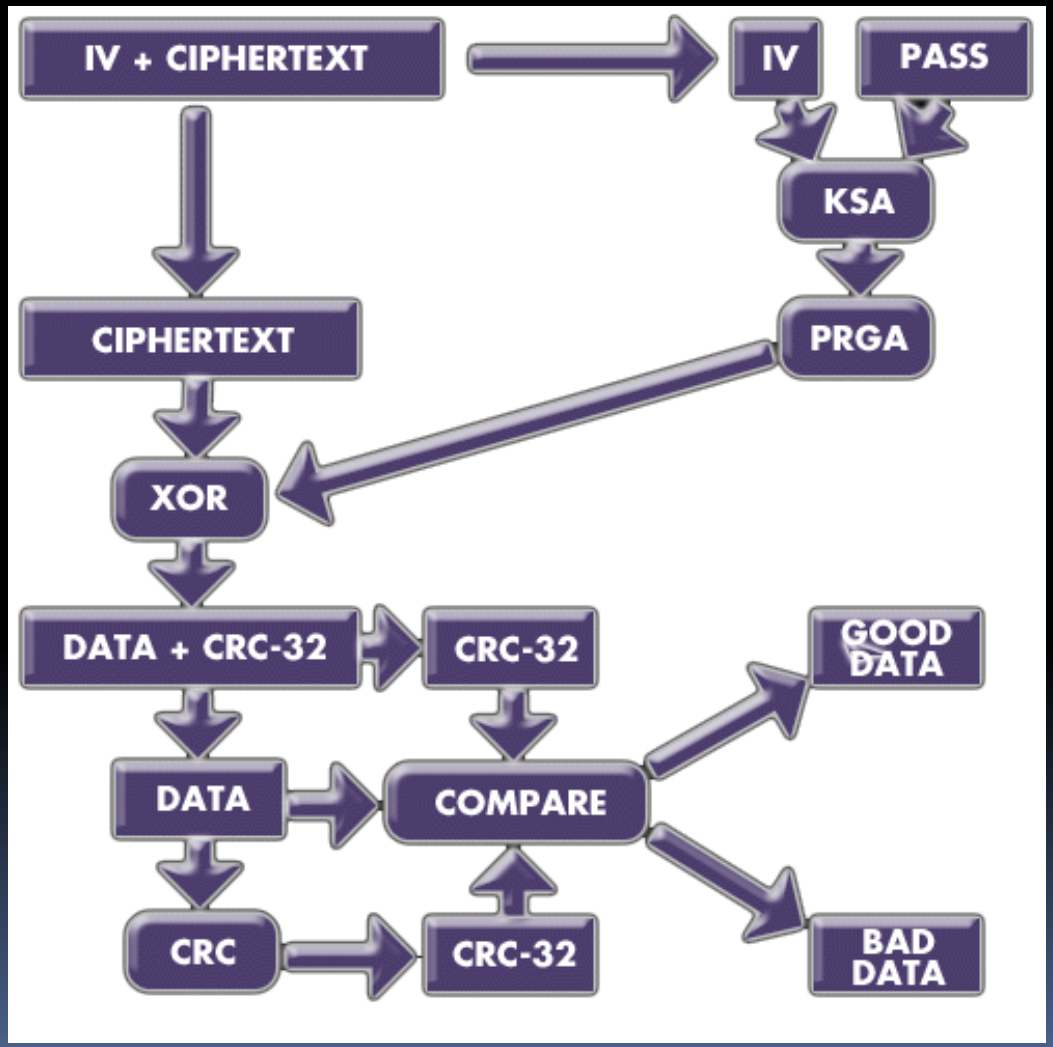
How WEP works – cont.



How WEP works - Encryption



How WEP works – Decryption



Is WEP safe?

- The answer is NO
- More than one weakness exists in WEP
  - Authentication
  - IV reuse
  - RC4 weakness
  - CRC 32
  - DoS
  - Vendor
- For these days, WEP could be cracked within few seconds

Goals for attacking WEP

1. Getting legal identity (KEY)
   - Using some others' network
   - Monitor the network traffic
2. Commercial issues
   - Getting secret data
   - Bring down a network

Attacking WEP

- Authentication is one-way
  - AP uses challenge-response to verify station
  - Station cannot verify APs
  - Rouge AP with the same Service Set ID
- Brute force
  - Key is short
  - 40-bit key could be broken in 50 hours

Attacking WEP – cont.

- IV reuse
  - WEP uses 24-bit IV, 2^{24} possible IVs
  - $$\frac{100 \text{ Mbps}}{8,192 \text{ bits/frame}} = \frac{100 \times 10^6 \text{ bps}}{8,192 \text{ bits/frame}} = 12,207 \text{ frames/second}$$
  - $$\frac{17 \times 10^6 \text{ IV values}}{12,207 \text{ frames/second}} = 1,393 \text{ seconds}$$
  - IVs are sent without encryption
- XOR problem
  - Consider how WEP works
  - $IV_1 = IV_2$
  - $C_1 \text{ XOR } C_2 = (P_1 \text{ XOR } RC4(IV_1, \text{key})) \text{ XOR } (P_2 \text{ XOR } RC4(IV_2, \text{key}))$

Attacking WEP – cont.

- KSA flaw in RC4
  - Scott Fluhrer, Itsik Mantin, and Adi Shamir in 2001
  - During the KSA iteration, S[i] might not change for i = 0~3
  - SNAP Header's property could be used to determine the plaintext
  - With those two values combination, we can find out the key
  - 5% chance for every single calculation

Existing Attacks – FMS

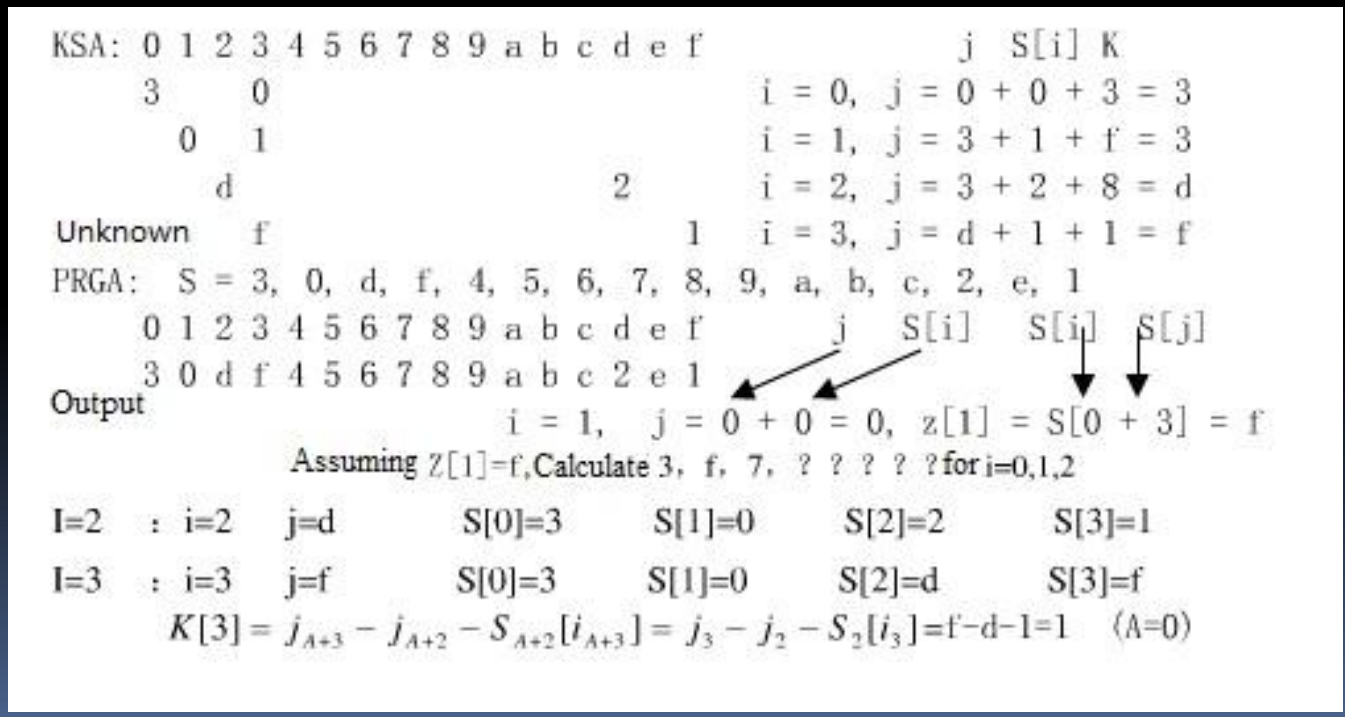
- FMS attacks
  - Assuming attack knows "K[0], K[1], K[2]…K[A+2]
  - We are looking for K[A+3]
  - Capture packet with IV of (A+3, N-1, X)
  - Record first bit Z[1] from PRGA
  - Base on type of network and type of transmission
    - Ex: SNMP Header: oxFF
  - Z[1] = C[1] XOR P[1](guessed)
  - $Z[1] = S_{A+3}[A+3]$

FMS attacks – cont.

- $S_{A+3}[A+3] = S_{A+2}[j_{A+3}]$
- Search Z[1] in S_{A+2} (from known keys)
- j_{A+3} could be found from above
- $j_{A+3} = j_{A+2} + S_{A+2}[i_{A+3}] + K[A+3]$
- From all calculations, we get an approximate value of K[A+3]
- Choose different X value might return different K[] values

FMS attacks – example

- Assuming: K[0] = 3, K[1] = f, K[2] = 7, K[3] = 1, K[4] = 2, K[5] = 3, K[6] = 4, K[7] = 5



FMS attacks – cont.

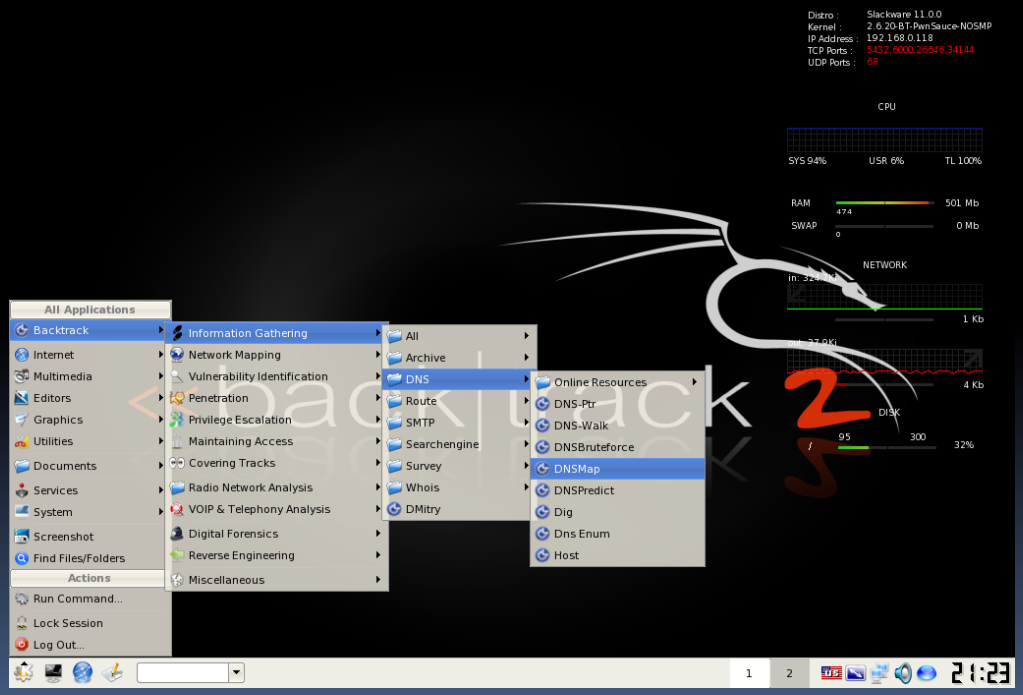
- Original attack only uses first bit of PRGA
- Improved attack uses second bit or combination of both bits
- Improved attack provides better performance

Implement – Tools

- AirSnort - 2001
  - Key recovery attack
  - Based on FMS attack
- AirCrack-ng
  - Used for cracking WEP and WPA
- KisMAC
  - Mainly used for Mac OS X

Implement – Tools – cont.

- BackTrack Linux



Reference

1. Scott Fluhrer, Itsik Mantin, and Adi Shamir "*Weaknesses in the Key Scheduling Algorithm of RC4*"
2. Michel Barbeau "*Mobile Wireless Network Security*"
3. Adam Stubblefield, John Ioannidis, Aviel D. Rubin "*A Key Recovery Attack on the 802.11b Wired Equivalent Privacy Protocol (WEP)*"
4. Xiao Yu, Luyong Zhang, Zhou Zheng "*Research of WLAN Security Encryption Algorithm*"
5. *"Wireless Mobile Network Security HW1 Analyze Weakness of WEP Protocol"*

The quieter you become,
the more you are able to hear…

Quiz

1. What does WEP stand for?
2. What are the two algorithms used in RC4?
3. How does authentication work for WEP?
4. What kind of message is sent by using WEP?
5. How long is it going to take to use all IVs

Bonus: who designed RC4, and what did RC4 design for?