WIRELESS NETWORK SECURITY

Ashwin Mani
RWTH Aachen University
9th February 2011.

WIRELESS NETWORKS

- Refer to connections not involving the use of wires.
- Important means of communication amongst computer systems and hand held devices.
- Sensitive information is sent across these networks.
- Security of such data is essential.

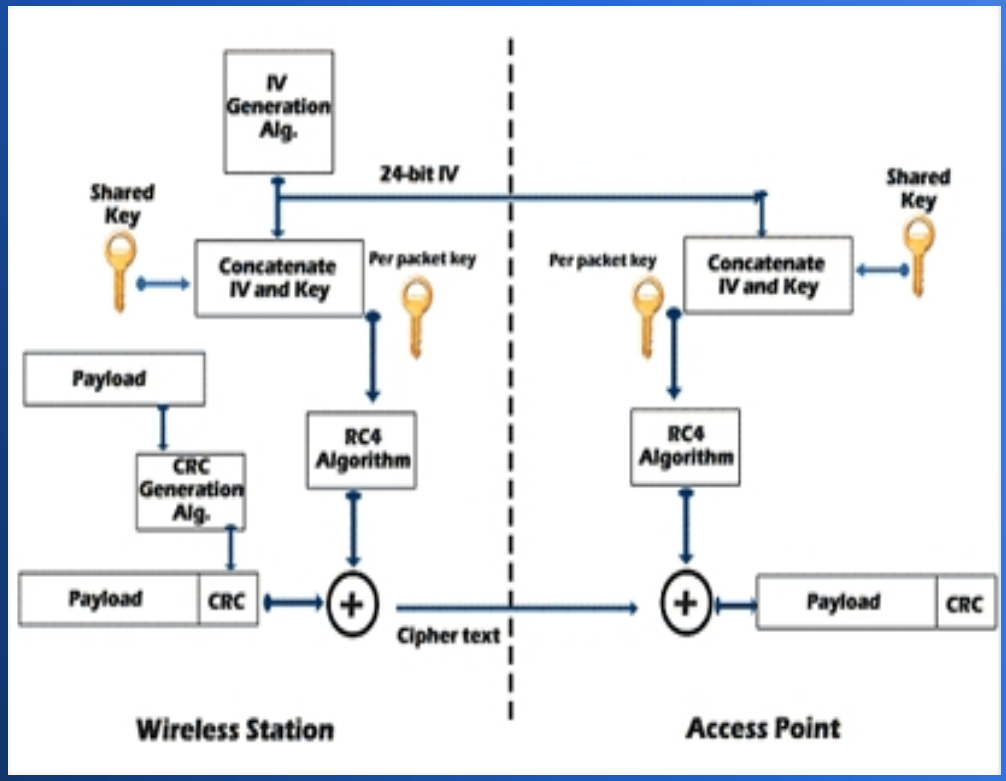
IEEE STANDARDS

- IEEE introduced the 802.11 standard for secure communication amongst wireless networks.
- The first version of this standard was the WEP (Wired Network Privacy)
- This standard was completely broken and hence is deprecated.
- New standard called the Wi-Fi Protected Access(WPA) was introduced in 2003.

WIRED NETWORK PRIVACY

- Introduced as a security algorithm for

  IEEE 802.11 wireless networks in 1997.
- Uses the “RC4 Stream Cipher” for confidentiality and the “CRC-32” for integrity.

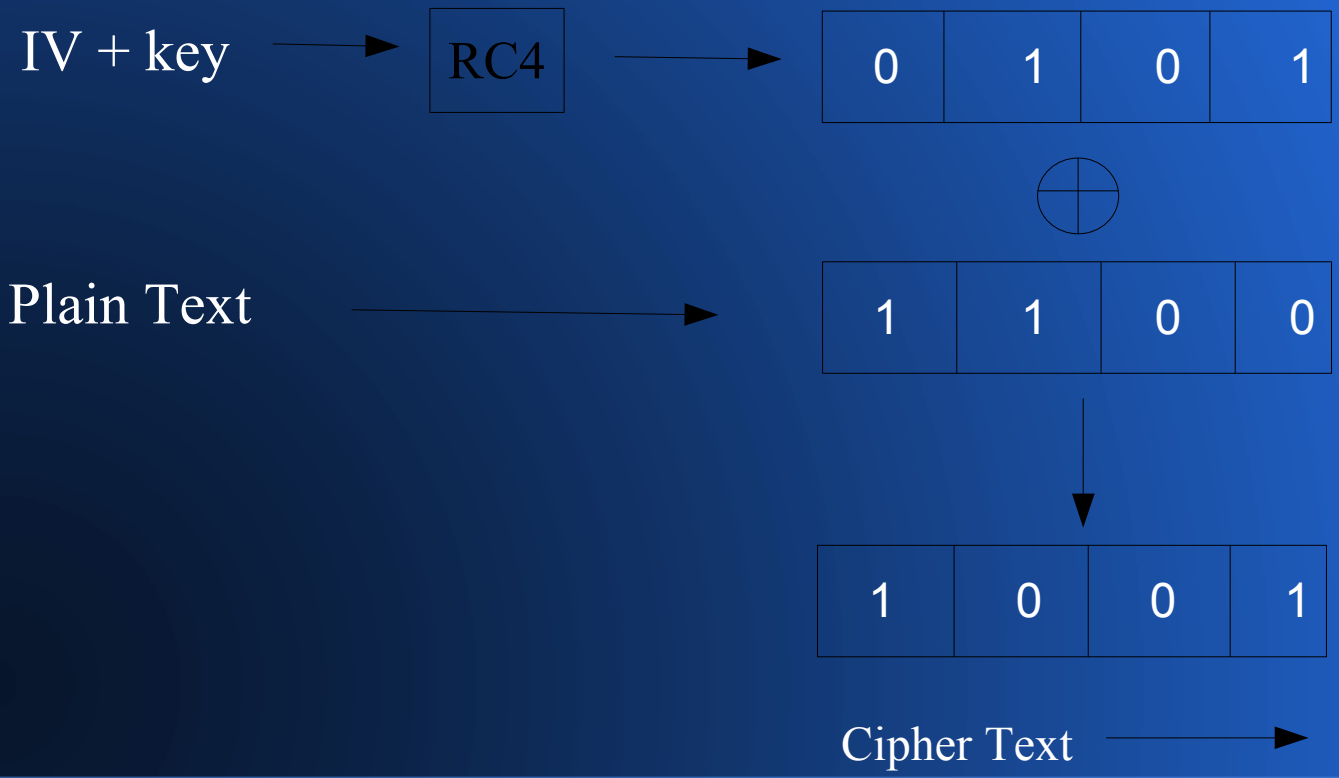


WEP OPERATION

- **Encryption**:Firstly a seed is created by adding the secret key to the Initialization Vector (IV) and using this seed to set up the Key Scheduling part of RC4.
- XORed with the keystream
- **Integrity**: In order to ensure the integrity of the keystream a CRC-32 checksum is applied before the encryption.

WEP OPERATION

- WEP Encryption Process



WEP OPERATION

- **Decryption**:Cipher text XORed with the keystream and the CRC is checked.
- Notes:

  a) The IV is different for each packet.

  b) Linear counter is used to generate the Initialization Vector.

PROBLEMS IN WEP

- Basic problem in WEP arises from the RC4 Stream Cipher.
- FLUHRER, Shamir and Martin exploited weaknesses in RC4 and completely broke it in 2001.
- Most prominent attack on a WEP system and other attacks are more or less inspired from it.

RC4 STREAM CIPHER

- RC4 basically consists of two parts

  a) **Key Scheduling Algorithm**: Converts a random key (whose typical size is 40-256 bits) into an initial permutation S of 0,...,N.

  b) **Pseudo Random Generation Part: G**enerates a pseudo random sequence by utilizing the above permutation.

FLUHRER, SHAMIR AND MARTIN ATTACK ON RC4

- Key Scheduling and the Pseudo Random Number Generation algorithms used in RC4

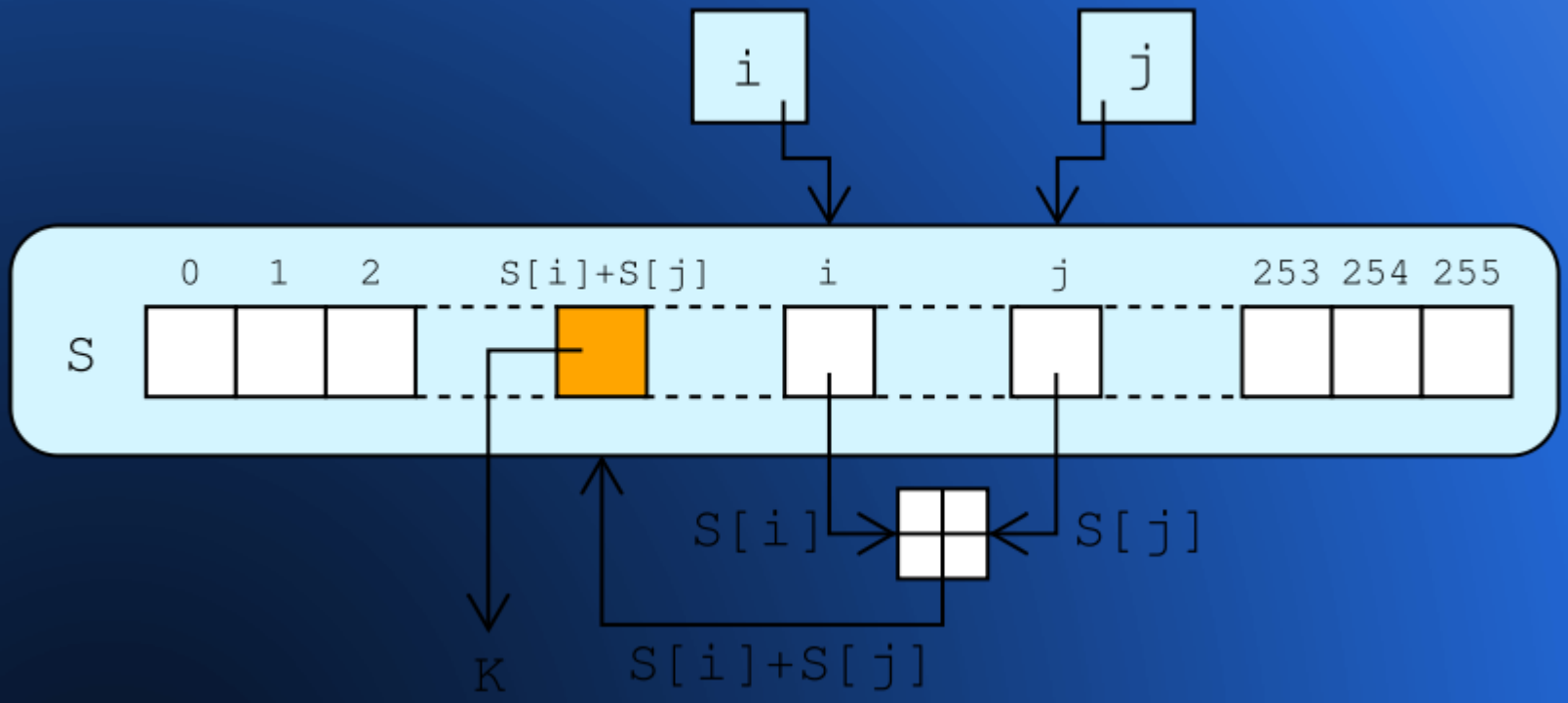
Key Scheduling

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

PRGA

```
Initialization:
i := 0
j := 0
Generation Loop:
while GeneratingOutput:
    i := (i + 1)
    j := (j + S[i])
    swap values of S[i]
and S[j]
    K := S[(S[i] + S[j])
    endwhile
```

RC4 LOOKUP STAGE

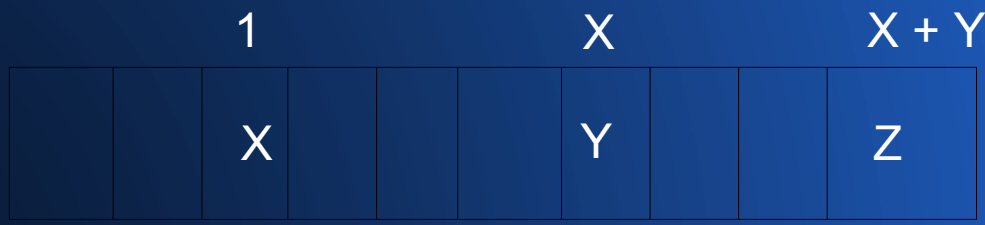


FLUHRER, SHAMIR AND MARTIN ATTACK ON RC4

- **Objective** : Estimate the secret key when the input to the KSA part consists of a secret followed by an Initialization Vector (IV).
- If the same secret key is used with different Initialization Vectors, then the attacker is able to estimate the secret key by eavesdropping on the network and observing the first word of the RC4 output.
- Effort depends on combination and the key.

FLUHRER, SHAMIR AND MARTIN ATTACK ON RC4

- The first word depends on three elements of the permutation S in the KSA step.
- For example:when the three words of the permutation have values as shown in the figure, then the first word of the output would be Z.



FLUHRER, SHAMIR AND MARTIN ATTACK ON RC4

- When the key setup approaches a stage where i is greater than or equal to 1, X =Si [1] and X + Y = Si[1] + Si [Si[1]].
- When other elements are modelled correctly, these three will not participate in a swap.
- Referred to as the "**resolved condition**". In such a case, the value S[S[1]+S[S[1]]] is the first word.
- The aim of the attack to examine particular vectors such that the KSA is resolved.

FLUHRER, SHAMIR AND MARTIN ATTACK ON RC4

- Using the first word information described earlier, one can obtain information on the secret key.
- Note:

  a) The order in which the IV and the secret key are added helps us to determine where the resolved condition.

  b) In the case of a WEP system, the secret key is prefixed by an IV.

IV IS A PREFIX TO THE SECRET KEY

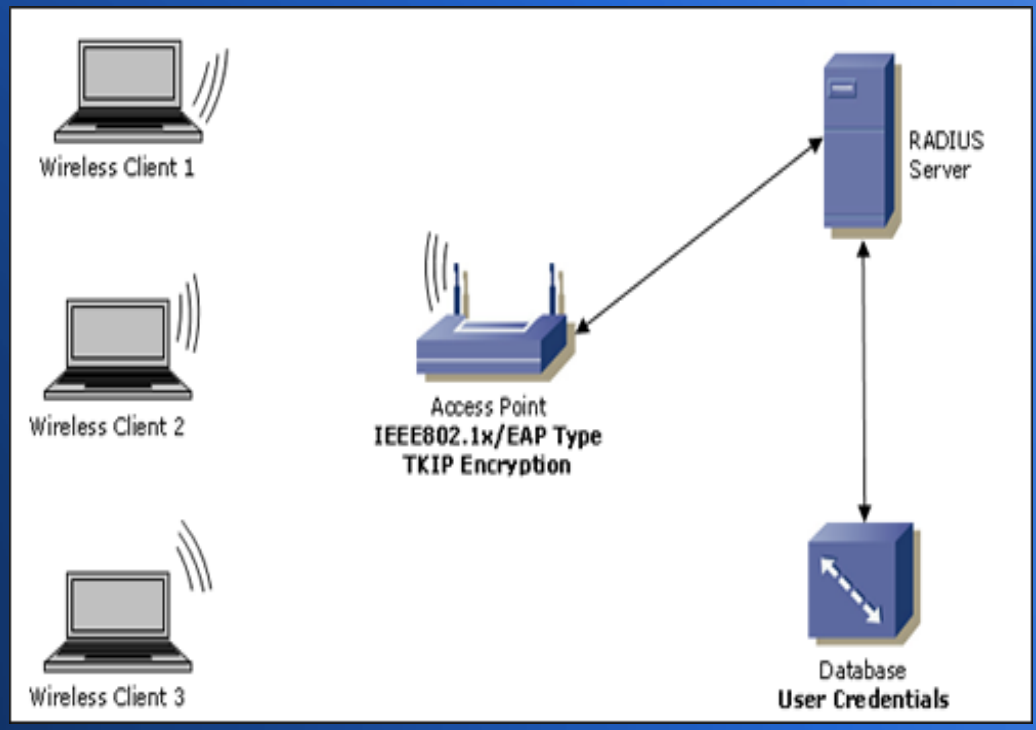
- Try to derive information on a particular word B of the secret key(K[B]) by searching for IV values so that, after the first I steps, Si [1] < I and Si [1] + Si [Si [1]] = I + B.
- High likelihood that we get a resolved condition after step I+B
- Analyze word and indices to obtain the secret key.

OBSERVATIONS

- Fluhrer, Shamir and Martin showed that by observing 60 Initializations for a basic 3 word scenario proposed by Wagner ([Wag95]), they were able to obtain the secret key in polynomial time.
- Other possible attacks include the KoReK attack and the Chop Chop attack.

Wi-Fi PROTECTED ACCESS

- Certication program developed by the Wi-Fi Alliance in 2003.
- Uses the TKIP (Temporal Key Identification Protocol) and a Message Integrity Check which replaces the CRC from WEP.



POSSIBLE ATTACKS ON WPA

- Has not been completely broken yet.
- Certain Weaknesses Observed
- **Social Engineering :**

  a) Weak passphrase makes the system prone to a brute force attack.

  b) Choice of passphrase very important.

POSSIBLE ATTACKS ON WPA

- Recently Erik Tews and Martin Beck, researchers at TU Dresden and TU Darmstadt uncovered a flaw in TKIP
- Does not lead to key recovery but only a keystream that encrypted a particular packet
- Sent again and again throughout the network.
- Solved by replacing TKIP with the AEC CCMP protocol.

CONCLUSIONS

- Security of Wireless Networks is a major concern.
- The WEP standard is not safe for secure communication because of weaknesses in the RC4 stream cipher.
- The WPA standard solves much of the problems by incorporating the use to TKIP and the Message Integrity Checks.
- Weaknesses have been observed in TKIP which can lead to further attacks on WPA.

REFERENCES

- 1. A. Bittau, M. Handley, and J. Lackey. The nal nail in wep's con. In Proceedings of the 2006 IEEE Symposium on Security and Privacy, pages 386{400, Washington,DC, USA, 2006. IEEE Computer Society.
- 2. S. R. Fluhrer, I. Mantin, and A. Shamir. Weaknesses in the key scheduling algorithm of rc4. In Revised Papers from the 8th Annual International Workshop on SelectedAreas in Cryptography, SAC '01, pages 1{24, London, UK, 2001. Springer-Verlag.
- 3. E. Tews and M. Beck. Practical attacks against wep and wpa. In Proceedings of the second ACM conference on Wireless network security, WiSec '09, pages 79-86,New York, NY, USA, 2009. ACM.
- 4. S. Vaudenay and M. Vuagnoux. Passive-only key recovery attacks on rc4. In Proceedings of the 14th international conference on Selected reas in cryptography, SAC'07,pages 344-359, Berlin, Heidelberg, 2007. Springer-Verlag.

THANK YOU