Introduction to Cryptography CS 355

Lecture 12

The RC4 Stream Cipher

Review

- One Time Pad (OTP) has perfect secrecy
  - requires key as long as plaintext
- Stream cipher approximates OTP by using PRNG
- A PRNG expands a short random seed into a long string that “looks random”
- A PRNG-based stream cipher has fundamental weaknesses
  - same stream cannot be used twice
  - highly malleable

The RC4 Stream Cipher

- A proprietary cipher owned by RSA, designed by Ron Rivest in 1987.
- Became public in 1994.
- Simple and effective design.
- Variable key size, byte-oriented stream cipher.
- Widely used (web SSL/TLS, wireless WEP).

The RC4 Cipher: Encryption

- The cipher internal state consists of
  - a 256-byte array S, which contains a permutation of 0 to 255
    - total number of possible states is 256! ≈ 2^{1700}
  - two indexes: i, j

```
i = j = 0
Loop
   i = (i + 1) (mod 256)
   j = (j + S[i]) (mod 256)
   swap(S[i], S[j])
   output (S[i] + S[j]) (mod 256)
End Loop
```

RC4 Initialization

- Generate the initial permutation from a key k; maximum key length is 2048 bits
- First divide k into L bytes
- Then

```
for i = 0 to 255 do
   S[i] = i
j = 0
for i = 0 to 255 do
   j = (j + S[i] + k[i mod L])(mod 256)
   swap (S[i], S[j])
```

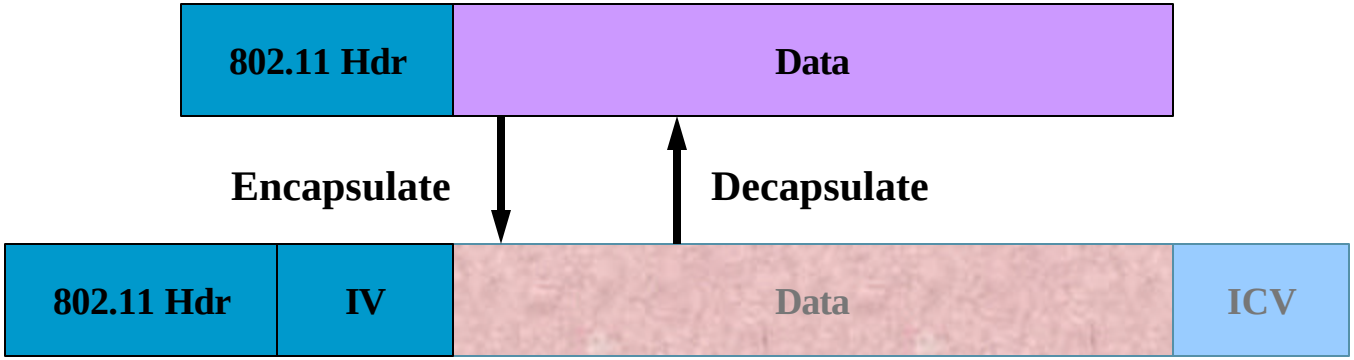
RC4 Cryptanalysis

- Known weaknesses:
  - Problem with init
    - the first byte generated by RC4 leaks information about individual key bytes.
    - best to drop first 256 bytes of output

802.11 Security

- Used between a Wireless Access Point and Wireless Ethernet Cards
- Existing security consists of two subsystems
  - A data encapsulation technique called ***W***ired ***E***quivalent ***P***rivacy (WEP)
  - An authentication algorithm called Shared Key Authentication
- Goals
  - Create the privacy achieved by a wired network
  - Simulate physical access control by denying access to unauthenticated stations

WEP Encapsulation



WEP Encapsulation Summary:

- A master key shared between the end points
- Encryption Algorithm = RC4
- Per-packet encryption key = 24-bit IV concatenated to a master key
- WEP allows IV to be reused with any frame
- Data integrity provided by CRC-32 of the plaintext data (the “ICV”)
- Data and ICV are encrypted under the per-packet encryption key

What Went Wrong in WEP?

- The space of IV is too small & IV is sent in clear.
- With two messages encrypted using the same IV, one can recover the key stream.
- The attack is made much easier by chosen plaintext attacks, which can be carried out in the environment where WEP is used.

Ways to Accelerate the Attack

- Send spam into the network: no pattern recognition required!
- Get the victim to send e-mail to you
  - The AP creates the plaintext for you!
- Decrypt packets from one Station to another via an Access Point
  - If you know the plaintext on one leg of the journey, you can recover the key stream immediately on the other
- Etc., etc., etc.

Coming Attractions …

- Block Ciphers, DES

- Recommended reading for next lecture:
  - Trappe & Washington: 4.1, 4.2