CH15 –Security & Crypto

Basics

- What if protection is “broken” by unauthorized user, or system is subverted
  - Crypting information can help
- Definitions of Cryptology
  - Cryptography, Cryptanalysis
- Model
  - Ciphertext = E(Plaintext,Ke)
  - Sent over unsecured channel
  - Plaintext = D(Ciphertext, Kd)
  - Cryptanalyst can see C, knows D and E, sometimes even Ke, and has “extra information”

Threats

- Ciphertext Only – The intruder can only see ciphertext. This is the easiest kind of attack to mount
- Known Plaintext – The intruder has some corresponding plaintext-ciphertext pairs.
  - Perhaps as the side information
- Chosen Plaintext – The intruder can find out the encryption of any arbitrary plaintext
  - Limited breakin ?

Some Design Principles

- Shannon’s Principles
  - Diffusion – spread correlations and dependencies between keys and strings so that length of plaintext needed to break the code is maximized
  - Confusion – make functional dependencies amongst related variables as complex as possible
- Exhaustive Search Principle

Classification of CrytoSystems

- Conventional
  - Geared towards languages
  - Caesar (E = M+k mod size of alphabet)
  - Substitution Cipher (size! keys)
  - Polyalphabetic (periodic sequence of substitution ciphers : vignere, onetime pad)
- Modern
  - Geared towards binary information
  - Private Key
  - Public Key

Private Key/DES

- Basic operations
  - Permutation: diffuse information by permuting bits
  - Substitution: replace an m bit input with an n bit output such that there is no simple relation between them to cause confusion
- DES works on 64 bit Data blocks using 56 bit key+8 parity bits (keylength an issue)

DES Steps

- Permute the 64 bits using IP
- 16 iterations of
  - $L_i = R_{i-1}$
  - Ri = L_{i-1} ***XOR*** $f(R_{i-1}, K_i)$