NETWORK SECURITY
E4.44/SO21

Dr Peter Beevor

Network Security Issues

- Information of value to attacker (passive attack)
- Information manipulated by attacker (active attack)
- Authorised user impersonated by attacker
- Value transaction repudiated by a fraudster
- Pay per view broadcasts available to non subscribers

Cryptographic Coding

$y = E_{k1}(x)$

x is the message

y is the encrypted message or ciphertext

E(.) is the encryption algorithm

k1 is the encryption key

Encryption should be reversible so that

$x = D_{k2}(y)$

Objectives

- Cryptographic techniques and their mathematical basis
- Use of cryptographic techniques to solve security problems
- Security systems to protect public and private networks

Course Content

- Cryptography
- Authentication
- Issues in Network Security
- Systems and Standards

Cryptography

- Symmetric key DES/IDEA/AES
- Modes of Operation ECB/CBC/CFB
- Hashes and message digests
- Public key RSA
- Diffie Hellman
- Elliptic Curve

Authentication

- Password
- Network Address
- Cryptographic
- Key Distribution Centres
- Certification Authorities
- Security Handshakes
- Strong password protocols

Issues in Network Security

- Security in public and private networks
- Security in OSI 7 layer model
- Denial of service attacks
- Perfect forward secrecy
- Public Key infrastructure
- Firewalls
- Security on the web

Systems and Standards

- Kerberos
- IPSec
- SSL/TLS
- PEM and S/MIME
- Pretty Good Privacy

Suggested Reading

- Network Security: Private communication in a public world.Kaufman, C, Perlman, R and Speciner, M. Prentice Hall 2002
- Applied Cryptography. Schneier, B. John Wiley, 1996

Private and Public Key Systems

$y = E_{k1}(x)$

$x = D_{k2}(y)$

In a symmetric key system k1 = k2 and $D = E^{-1}$

In a public key system k1 is the public key and k2 is the private key

Methods of Attack

- Ciphertext only
- Known plaintext
- Chosen plaintext

Ciphertext only attack

- Knowledge of original message statistics
- Exhaustive key search leads to recognisable plaintext
- Specific knowledge of type of encryption scheme used

Ciphertext Only Example

Cqrb rb j wng lxdabn rw wncfxat bnidarch

Known to be a Caesar cipher

Clues are in the one and two letter words

And in the letter frequency r,b,n (4), a,c (3)

This is a new course in network security

Authentication

- Cryptographic challenge / response
- A and B share key k and agree cryptographic function F(.)
- A sends random number n to B
- B returns $F_k(n)$ to A
- A compares B's return with his own $F_k(n)$
- Similarly B authenticates A

Message Authentication Code (MAC)

- Short code appended to message dependant on message and source identity
- Type of cryptographic CRC
- Typically length of message >> MAC
- Key component of financial security systems (e.g. S.W.I.F.T.)

Private and Public Authentication Systems

- Private systems use common key for creating and checking MAC
- Public systems use private key to create and public key to check
- In public key systems the MAC is known as a digital signature and provides non-repudiation.