Encryption and Key Distribution

Motivation

- ***More vital/secret data handled by distributed components.***
- ***Security: protecting data stored in and transferred between distributed components from unauthorised access.***
- ***Security is a non-functional requirement that cannot be added as a component but has to be built into all components.***

Why are Distrib. Systems insecure?

- *Distributed component rely on messages sent and received from network.*
- *Is network (especially WAN networks) secure?*
- *Is client component secure?*
- *Is client component who it claims to be?*
- *Are users of calling components really who they claim to be?*

Effects of Insecurity

- *Confidential Data may be stolen, e.g.:*
  - *corporate plans.*
  - *new product designs.*
  - *medical/financial records (e.g. Access bills....).*
- *Data may be altered, e.g.:*
  - *finances made to seem better than they are.*
  - *results of tests, e.g. on drugs, altered.*
  - *examination results amended (up or down).*

Need for Security

- *Loss of confidence: above effects may reduce confidence in systems.*
- *Claims for damages: legal developments may allow someone to sue if data on computer has not been guarded according to best practice.*
- *Loss of privacy: data legally stored on a computer may well be private to the person concerned (e.g. medical/personnel) record.*

Threats

- *Categorisation of attacks (and goals of attacks) that may be made on system.*
- *Four main areas:*
  - *leakage: information leaving system.*
  - *tampering: unauthorised information altering.*
  - *resource stealing: illegal use of resources.*
  - *vandalism: disturbing correct system operation.*
- *Used to specify what the system is proof, or secure, against.*

Methods of Attack

- *Eavesdropping: Obtaining message copies without authority.*
- *Masquerading: Using identity of another principle without authority.*
- *Message tampering: Intercepting and altering messages.*
- *Replaying: Storing messages and sending them later.*

Infiltration

- *Launch of attack requires access to the system.*
  - *Launched by legitimate users.*
  - *Lauchend after obtaining passwords of known users.*
- *Subtle ways of infiltration:*
  - *Viruses*
  - *Worms*
  - *Trojan horses.*

Cryptography

1 Introduction

2 Terminology

3 Encryption

4 Secret Keys

5 Public Keys and PGP

Introduction

- Cryptography: encode message data so that it can only be understood by intended recipient.
- Romans used it in military communication
- Given knowledge of encryption algorithm, brute force attempt: try every possible decoding until valid message is produced.
- Computers are good at this!
- Modern schemes must be computa-tionally hard to solve to remain secure.

Cryptographic Terminology

- *Plain text: the message before encoding.*
- *Cipher text: the message after encoding.*
- *Key: information needed to convert from plain text to cipher text (or vice-versa).*
- *Function: the encryption or decryption algorithm used, in conjunction with key, to encode or decode message.*
- *Key distribution service: trusted service which hands out keys.*

Encrpytion

- *Encrypting data prevents unauthorised access to the data (i.e. prevents eavesdropping).*
- *If encrypted data can only be encrypted with a matching key, this can be used to prove sender's identity (i.e prevents masquerading).*
- *Likewise, it can be used to ensure that only intended recipients can use the data.*
- *Two main ways: secret key & public key.*

Secret Keys

- *One key is used to both encrypt and decrypt data*
- *Encryption and decryption functions are often chosen to be the same*
- *Security should not be compromised by making function well-known as security comes from secret keys*

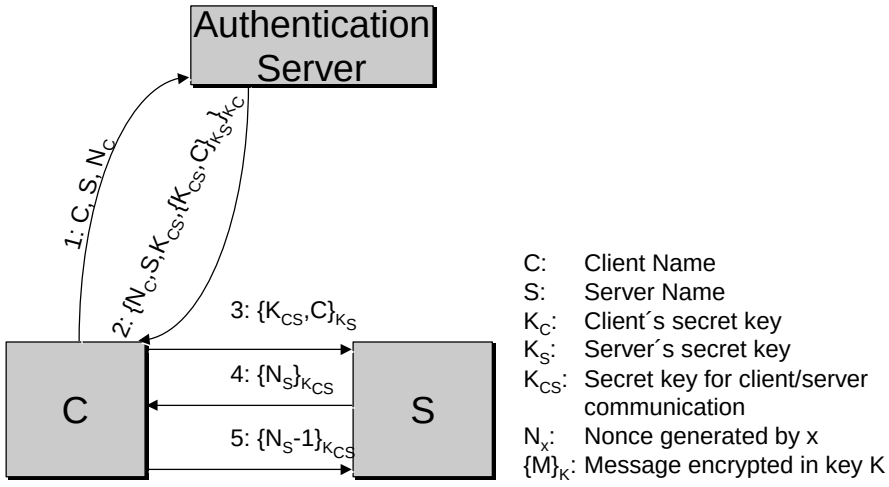
Using Secret Keys

- *Sender and recipient exchange keys through some secure, trusted, non-network based means.*
- *Sender encodes message using function and sends, knowing that only the holder of key (the intended recipient) can use it.*
- *Recipient decodes message and knows that only sender could have generated it.*
- *Message can be captured but is of no use.*

Needham/Schroeder Protocol

- ***Provides a secure way for pairs of components to obtain keys to be used during communication.***
- ***Based on an authentication server:***
  - ***maintains a name and a secret key for each component.***
  - ***can generate keys for peer-to-peer communications.***
- ***Secret keys are used for communication with server.***

Needham/Schroeder Protocol



C: Client Name
S: Server Name
K_C: Client´s secret key
K_S: Server´s secret key
K_{CS}: Secret key for client/server communication
N_x: Nonce generated by x
$\{M\}_K$: Message encrypted in key K

Public Keys

- *Gives 'one-way' security.*
- *Two keys generated, one used with decryption algorithm (private key) and one with encryption algorithm (public key).*
- *Generation of private key, given public key is computationally hard.*
- *Do not need secure key transmission mechanism for key distribution.*

Using Public Keys

- *Recipient generates key pair.*
- *Public key is published by trusted service.*
- *Sender gets public key, and uses this to encode message.*
- *Receiver decodes message.*
- *Replies can be encoded using sender's public key from the trusted distribution service.*
- *Message can be captured but is of no use.*

Pretty Good Privacy

- *PGP is example of public key system.*
- *Generally available, and can be used for*
  - *encryption of messages*
  - *digital signatures.*
- *Subject to legal problems since it uses idea of keys controlled by US government and patents.*