

Personal Authentication: What are the Options and How do you Choose?

Fred Piper

Codes & Ciphers Ltd
12 Duncan Road
Richmond, Surrey
TW9 2JD

Information Security Group
Royal Holloway, University of London
Egham, Surrey
TW20 0EX

The Basic Principle

- User identifies themselves to trusted body
- They agree an 'identifier'
- That identifier is then used to authenticate user

Note 1:

The authentication process merely confirms that the person producing the identifier is the person to whom it was issued

Note 2:

The identifier may be produced by the user (e.g. a password, token or biometric) or used by the user (e.g. a cryptographic key)

Impersonation Attacks

- Identity management is high on everyone's agenda
- 'Identity theft' is prevalent

Some Basic Questions

- What 'type' of identifier should be used?
- How is user identified **before** they are given the identifier?
 - Registration (enrolment) is important
- Where is identifier stored?
- How is identifier 'bound' to the user?
- Where is identity checked? (Is identifier transmitted across insecure channel?)
- Is the identification process manned or unmanned?

A VERY Important Question

Are you concerned about

- Authenticating the wrong person?

OR

- Rejecting the right person?

Basic Problem

Once a user has been 'assigned' an identifier, how does the system 'bind' that user's ID to that identifier?

- Infrastructure?
- Cryptography?

Verification

- Where is ID verified?
 - Centrally or at point of delivery
 - May need transmission over insecure channel
- Is complete ID information on token?
 - If not, may require central database of IDs with corresponding identifiers

Multiple Identities?

- For password and/or tokens a user may claim multiple identities with different identifiers
- It is asserted that the use of biometrics prevents users from claiming multiple identities
 - Not true if user's biometric is stored only on user's card
 - Needs central database for checking
 - Central database raises privacy issues

Keys as Identifiers

- It is the use of a cryptographic key, rather than revealing its value, that identifies a user

Asymmetric System

- Use of the private key acts as an identifier to 'everyone'

Symmetric System

- Use of a key identifies users only to those (trusted) people who share that key

Identification over the Internet

- Many applications use 2-factor systems that allow 'card not present' transactions
- Effectively a physical token is replaced by a virtual token which is nothing more than a card number

This is a 1-factor system

- In Singapore the FSA mandates use of genuine 2-factor authentication
- In UK banks are starting to issue customers with Chip and PIN 'readers'

OOB (Out of Band) Authentication

Requirement

- A user claims an identity over a computer network
- Host wants to use a second channel to confirm it is the genuine user
- Neither party is willing to pay for 'extra hardware'

Mobile Phones

- There is a move towards systems where the mobile phone is 'something you own'
- No reader required
- No extra cost (in the sense that most people have them)
- Use their own channel
- Security implications?

Some Basic Slides

Included for background information

Probably not discussed in presentation

User Recognition (1)

3 factors:

- 1) Something you know (Password/PIN/Cryptographic Key)
- 2) Something you own (Token)
- 3) Personal characteristic (Biometrics)

NOTE: Usually one-way authentication

Tokens and biometrics often require 'readers'

'Danger' of false 'readers'

Cost issues

User Recognition (2)

- Many systems rely on more than 1 factor
- For multi-factor systems compromise of 1 factor should not enable impersonation
- The PIN/magnetic stripe card for ATM networks is an example of a 2-factor system where each individual factor is 'weak'

Something You Know

- Password
- PIN
- Cryptographic key

Obvious observations:

- A PIN is a password with limited alphabet
- A cryptographic key may be regarded as a (secret) password which the user may use but probably not know
- Some keys need strong physical protection
- Policies for the management of PINs and Passwords are inconsistent

Cryptographic Keys

- It is the use of a cryptographic key, rather than revealing its value, that identifies a user
- Symmetric keys need to be kept secret
- Private keys in a PK system need to be secret
- Key management is difficult but crucial

Authentication Using Smart Tokens

- **Static Password Tokens**
 - Owner authenticates himself to token
 - Token identified owner to system
- **Dynamic Password Tokens**
 - Token generates new password
 - Owner activates token with PIN
 - Owner enters ID plus dynamic password
 - System knows which dynamic password to accept
- **Challenge-Response Tokens**
 - System generates challenges
 - Owner activates token with PIN and enters challenge
 - Token generates response (probably challenge encrypted with key that is unique to token)
 - System knows which response to accept

Comparing the 3 Factors (1)

Something known

- May be learnt by attackers
- May be forgotten by users
- Needs protection if stored
 - Cryptographic?
 - Physical?
- Can be changed if compromised

Comparing the 3 Factors (2)

Something owned:

- Can be stolen by attacker
- May be copied by attacker
- May be lost by user
- Stored information may be read by attacker
- May be replaced or changed

Comparing the 3 Factors (3)

Biometrics

- Difficult to 'copy'
- Difficult to recover from compromise
- Enrolment may be difficult (impossible?) for some users