Security in Computing & Information Technology

Lecture 4

Authentication

Lecture Schedule

Foundations

1. Introduction
2. Vulnerabilities, Threats, Attacks

Basic mechanisms

3. Security mechanisms, Elementary cryptography
4. Authentication
5. Access control

Major computing security areas

6. Operating systems
7. Databases
8. Networks
9. Web
10. Mobile computing

Applications

11. Privacy
12. Internet banking

Lecture Topics

- Concept of authentication
- Passwords
- Biometrics
- Electronic certificates

Identification

- Aim
  - Establish the identity of
    - a user
    - a communicating peer (e.g. sender of an email)
    - a process (who is running it)
- Problem
  - Difficult to verify
    - Physically not present
    - Characteristics, attributes cannot be observed
  - Even if established, may not be useful
- Solution: authentication

Authentication

- Verifying that the user (peer, origin of document etc) is who/what they claim to be
- Components
  - User
    - The person or process to be authenticated
  - Server
    - Authenticates the user for itself or for other services
    - Can generate an authentication ticket as evidence to be presented for obtaining services
- Forms
  - Attribute verification

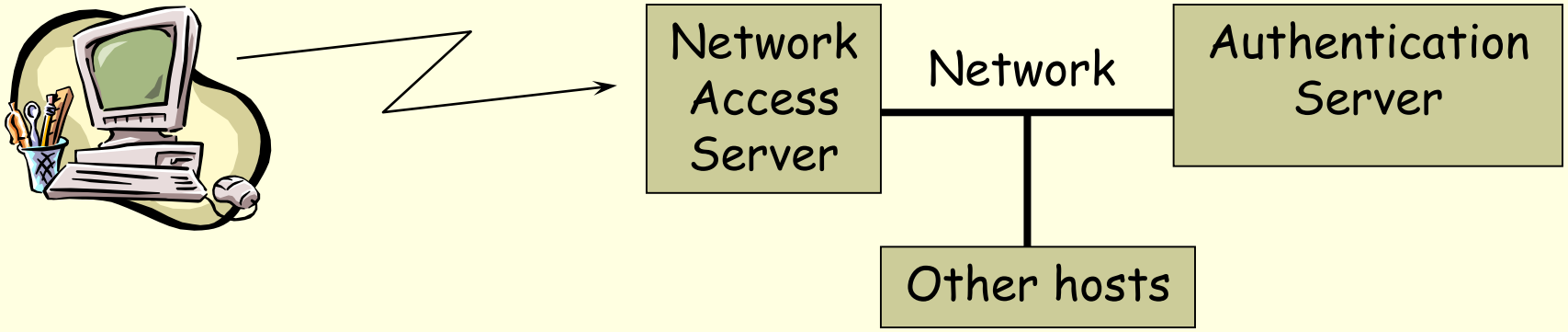
    E.g. biometrics, passwords
  - External affirmation

    E.g. certificates produced by authorities

Authentication Systems

- Requirement: protection against
  - Impersonation of a user or a server
  - Modification of data exchanged between user & server
  - Replay of a previous authentication

- Basic example



Mobile Phone Authentication System Example

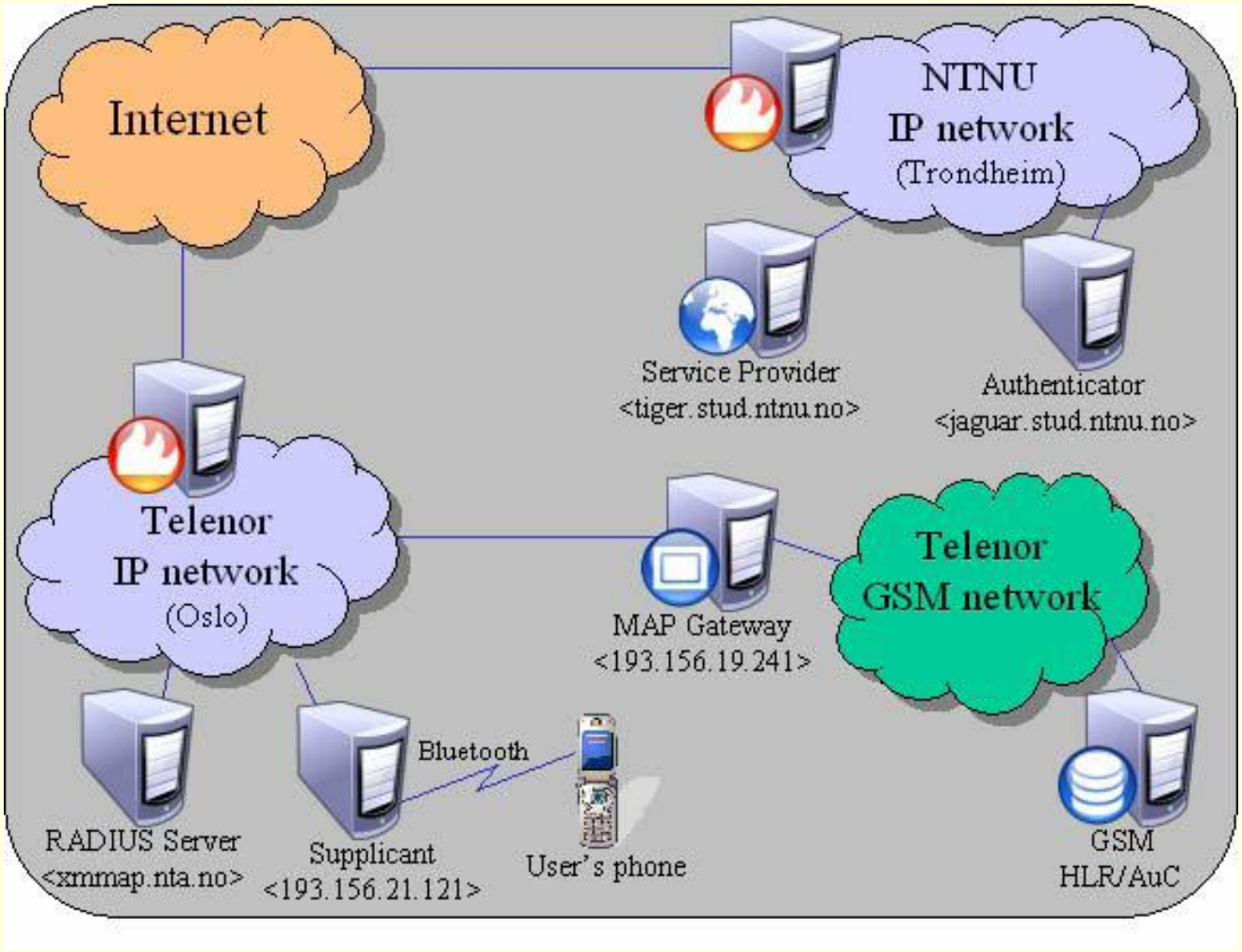


Image source: Wangensteen, A.; Lunde, L.; Jorstad, I.; van Thanh, D.; A Generic Authentication System Based on SIM,

Authentication Factors

- Main factors
  - Proof by knowledge (something you know)
    e.g. username & password
  - Proof by possession (something you hold)
    e.g. bank card
  - Proof by property (who you are)
    e.g. fingerprint
- Additional factors
  - Location (where you are)
  - Activity (e.g. your signature)
- Multifactor authentication
  More than one factor is needed
    E.g. banking ATMs: possession (bankcard) + knowledge (PIN)

Special Authentication Methods

- Mutual authentication

  E.g.

  - By communicating peers
  - Server & user (in TLS/SSL)
  - System & user
- Single sign-on (SSO, cascading authentication)
  - Process: User is authenticated once, subsequent authentications are re-using the result without user interaction
  - Method: Systems share the authentication database or exchange security assertions

Proof by Knowledge Challenge-Response Methods

- Server presents a challenge to the user, user answers the challenge
- If the answer is correct, the user is authenticated
- Challenge types
  - Password
  - Cryptographic methods

    E.g. user has to encrypt or produce the hash of the challenge

Passwords

- Most commonly used authentication token
- Advantage: easy to replace if compromised
- Commonly exploited
- Method
  - System stores password in hidden form
    E.g. encrypted, or its hash value
  - User enters password
  - System computes the hidden form
  - System compares the calculated value with the stored one
    - Match: authentication successful
    - Error: authentication fails

Password Transmission

- Some solutions forward the password in plain form
  - E.g. HTTP Basic, Telnet
- Reliable methods protect the password by
  - forwarding a hash only: HTTP Digest
  - encrypting the password: Kerberos
  - encrypting the whole communication channel: SSL/TLS/https, SSH

HTTP Authentication

Basic authentication

Features

- Not secure
  - Password is forwarded in plain form (not encrypted)
- No logout – the browser needs to 'forget' the information

Digest authentication

Features

- More secure
  - Only the digest (hash) is forwarded
- Supported by most (but not all) browsers

HTTP Authentication (Apache)

- Basic authentication
  - Create a password file

```
htpasswd -c my_dir/passwords user1
```

  - Configuration file: `.htaccess`

```
AuthType Basic
AuthName "Display this message"
AuthUserFile my_dir/passwords
Require user user1 user2
```

- Digest authentication
  - Create a password file

```
htdigest -c my_dir/passwords user1
```

  - Configuration file: `.htaccess`

```
AuthType Digest
AuthName "Private"
AuthDigestFile my_dir/passwords
Require user user2 user3
```

Password Attacks

- Password spoofing (phishing)
  - Screen imitates a real input page to collect authentication information
- Key logging
- Compromising the password file
  - Adding or modifying entries in the password file
- Password guessing
  - Intuitively
    - Date-of-birth, friend's name …
    - Dictionary attack: test every word of a dictionary

      The attacker needs the password hiding algorithm (encryption key, hash)
  - Exhaustive search (brute force)

Password Protection Methods

- Password strength
  - Should
    - be hard to guess
    - be long
    - mix upper, lower case letters, numbers and non-alphanumerical symbols
- Password ageing
  - Passwords should be regularly updated
- Password generation
  - Sounds good, but generated passwords are hard to remember
- Protective measures against attacks
  - Exponential backoff: increasing waiting time after every failed attempt
  - Blacklisting: locking the account after a certain number of consecutive incorrect guesses
  - Reverse Turing test: asking the user to perform a task only a human can do (tell humans and computers apart)

Password Management

Do

- Sending passwords to users should be done via secure channels
  - Use different channels (e.g. phone, SMS) to activate an account/password
- Use one-time passwords that the user has to update at first login
- Identify the user before communicating password (e.g. call back an authorised phone number)
- Re-setting passwords also needs care

  Although users are less likely to tolerate delays

Don't do

- Difficult passwords are written down, or replaced with easy ones
- Some very common passwords: 123456, Password, abc123

Bad Example: Sony's Password Lists

GTS Unix Server Privileged…tion Review - 07292013.xlsx	Oct 16, 2014, 7:24 PM	51 KB	Spreadsheet
Hold Codes- Passwords.xls	Oct 16, 2014, 7:49 PM	18 KB	Micros…ksheet
idm server storage migration.xlsx	Oct 16, 2014, 7:26 PM	16 KB	Spreadsheet
IFDS Passwords.xls	Oct 16, 2014, 7:46 PM	16 KB	Micros…ksheet
Important Passwords - TAAS, Outlook, Novell.txt	Oct 16, 2014, 6:36 PM	110 bytes	text
IP and Password.rtf	Oct 16, 2014, 6:06 PM	6 KB	rich text (RTF)
IT Security Assessment Questions for PRISM.xlsx	Oct 16, 2014, 5:40 PM	54 KB	Spreadsheet
ITPS Without Passwords 08_14_2014.xlsx	Oct 16, 2014, 7:56 PM	563 KB	Spreadsheet
karrie's Passwords.xls	Oct 16, 2014, 6:21 PM	15 KB	Micros…ksheet
Login and Passwords.xlsx	Oct 16, 2014, 7:43 PM	11 KB	Spreadsheet
Login_Password_Conne.txt	Oct 16, 2014, 7:33 PM	67 bytes	text
Logins and Passwords.xls	Oct 16, 2014, 7:33 PM	32 KB	Micros…ksheet
Master Application List.xls	Oct 16, 2014, 10:09 PM	177 KB	Micros…ksheet
Master Intern Password List.xls	Oct 16, 2014, 6:42 PM	15 KB	Micros…ksheet
Master Inventory.xls	Oct 16, 2014, 10:09 PM	737 KB	Micros…ksheet
Master Server List.zip	Oct 16, 2014, 7:21 PM	423 KB	ZIP archive
Master_Password_Sheet.xls	Oct 16, 2014, 7:36 PM	142 KB	Micros…ksheet
McAfeepassword.txt	Oct 16, 2014, 6:33 PM	509 bytes	text

Password Reset

- People forget passwords (esp. difficult ones)
- Systems usually offer a challenge question to avoid cumbersome procedures for password reset
  - Problems
    - Typical system questions are limited
      Make of your first car, name of your pet etc
    - Answers can be guessed
      Ford/Holden, most popular pet names available online…
- People lie to improve security – then forget

Password Crackers

- Numerous tools are available
  - Cain and Abel (Windows)
  - John the Ripper (Unix)
  - Airsnort (Wireless networks)
  - Some are free, others are commercial "password recovery tools/services"
- Difficulties
  - Passwords are usually encrypted with one-way functions (hard to reverse)
    - Solution: Crackers encrypt the guess and compare the result
  - Doesn't work with one-time passwords

One-Time Passwords (OTP)

- Valid for a single session or transaction

  Re-playing attacks do not work
- Delivery method
  - Via different channel

    E.g. using a separate device, printed on paper, etc
- Generating methods
  - Time-synchronised
    - A piece of hardware ('token') generates the password
    - Difficulties
      - The token needs an accurate clock synchronised with the server's clock
      - The algorithm must tolerate limited clock drift

One-Time Passwords (Continued)

- Generating methods (cont)
  - Mathematical algorithms
    - Each password is generated from the previous one by calculating the hash (MD5 etc) of the previous one

$$X_1 = H(S)$$
$$X_2 = H(X_1) = H(H(S))$$
$$\ldots$$
$$X_i = H(X_{i-1})$$

Calculate ↓ ↑ Use

    - Passwords are used one at a time, working backward through the list
    - An eavesdropper can learn Xi and consequently all subsequent (already used) passwords, but cannot guess the previous one in the list due to one-way hashing

Proof by Possession

- User has a token to prove authenticity
  - Bankcard
    - Most common, used in everyday banking

  - USB memory key
    - Software can turn an ordinary memory stick to a key

  - Subscriber identification module (SIM card)
    - Essential part of GSM mobile phones

  - Specific hardware: SecurID
    - Client & server clocks need to be synchronised

Proof by Property

- Problems
  - Can be used for authenticating human users only
  - Has to be
    - easy to measure: e.g. hand / eye properties
    - acceptable in form: non-intrusive
- Biometrics
  - *Physiological* (Face, fingerprint, hand, eye – retina print) commercially available
  - *Behavioural* (Signature, voice, keystroke dynamics) used mainly as an additional authentication factor

Biometrics

- Measure physical characteristics and evaluate them against a stored pattern (verification or identification)
- Advantage
  - Hard to forget
- Problems
  - Live tissue verification
  - Cannot be cancelled/replaced if data is compromised
  - Expensive equipment
- Reliability
  - False positive: accepting an unauthorised user
  - False negative: rejecting a legitimate user

Biometrics: Methods

- Major types
  - Fingerprints
    - Well developed technology, widely used
    - Can be used in clean environment only
  - Hand anatomy
    - Less frequently used
  - Iris pattern
    - Does not change in a lifetime
    - Measurement can be difficult
  - Face
    - E.g. e-passports

Fingerprints

- Has been used for more than a century
  - Forensic, government and civilian applications
- Sensing
  - Live scan
  - Traces
- Processing
  - Feature extraction
    - 3-step process: macrodetails, minutiae, dimensional attributes
  - Matching
- Problems
  - Low-quality images
    - Dirt, skin texture (mutilations)
  - Distortions (non-linear)
    - Pushing a finger against a surface
  - Connotations
    - Police / crime

Hand Anatomy & Related Methods

- Static methods
  - Veins in the hand
    - Method: Non-intrusive (uses infrared light)
    - Tolerates dirty hands

  - Hand geometry
    - Method: Length, width, thickness and curvature of hand & fingers
    - Reliability
      - Less distinctive than fingerprint
      - Hands may change due to injury, weight, etc

- Dynamic methods
  - Handwriting
    - Method: captures writing dynamics
    - Reliability: Affected by injury, fatigue, temperature, medical conditions
  - Keystroke analysis
    - Method: Typing speed, time a key is held down
    - Reliability: Not known (new method)

Iris Recognition

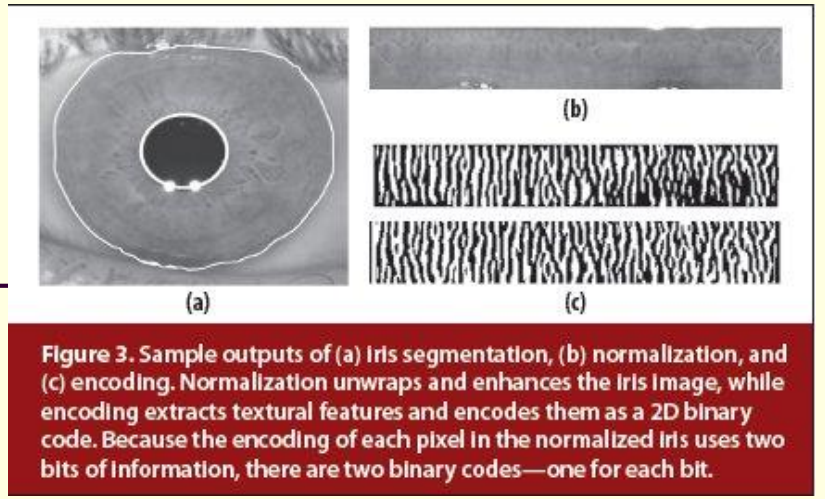


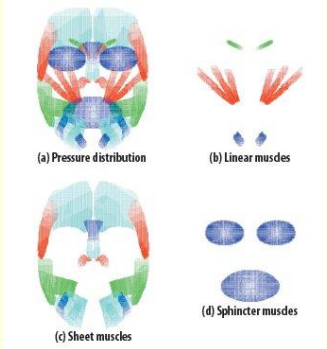
Figure 3. Sample outputs of (a) iris segmentation, (b) normalization, and (c) encoding. Normalization unwraps and enhances the iris image, while encoding extracts textural features and encodes them as a 2D binary code. Because the encoding of each pixel in the normalized iris uses two bits of information, there are two binary codes—one for each bit.

- Iris
  - In the eye in front of the lens, controls pupil size
  - Its textural complexity and variation across people postulates its uniqueness to individuals
- Iris recognition
  - Based on pattern matching

    Steps: acquisition, segmentation (isolating from the environment), normalisation, feature extraction (encoding), matching
  - Challenges
    - Acquisition: unfavourable lighting, large/variable distances, moving subjects result in poor contrast and blurred images
    - Segmentation: localise the iris position (head rotation, camera angle etc)
    - Matching: no effective theoretical model to quantify individuality

Face Recognition

- Motivation
  Basic method for identification by humans
- Approaches
  - Still face recognition
    - Principal component analysis, linear discriminant analysis, elastic graph matching
  - Video recognition
    - Temporal characteristics of facial motion, appearance changes
    - Often utilises images from multiple cameras
- Problems
  - Disguises
  - Illumination, facial expressions, natural aging



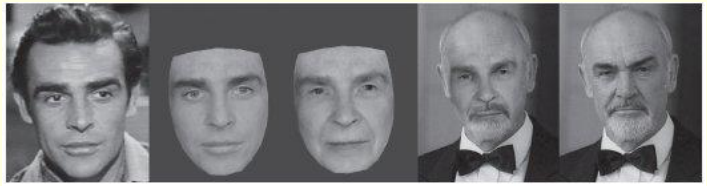
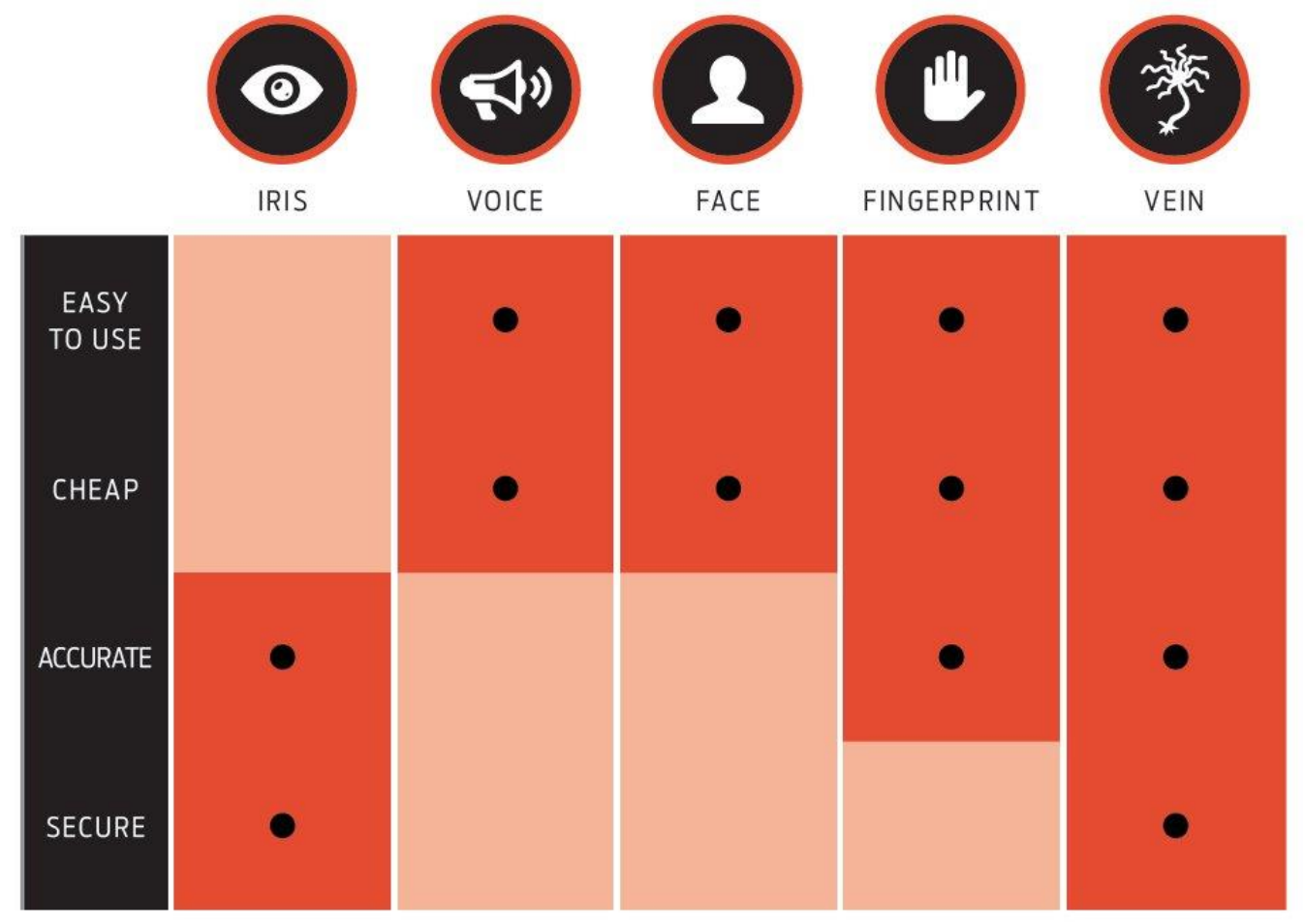


Figure 5. Sean Connery age-progressed from 25 to 70 relative to a photograph at 70. From left to right, the input photograph of Connery at age 25, the rendered input photograph from the projected hyperdimensional surface, the rendered aged Connery at 70 with the aged face superimposed onto a ground-truth background, and the ground-truth image of Connery at 70.

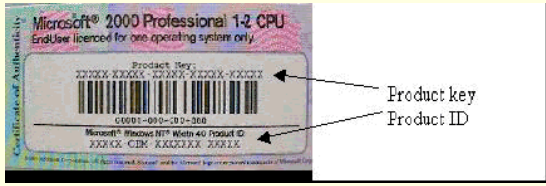
Biometrics: Summary



Certificates

- Documents stating the authenticity of a subject, product, item, art work etc
- Contain detailed information about the subject etc
- Issued by trustworthy authorities who are reputable themselves
- Come in different forms

  Labels, stickers (e.g Microsoft), electronic certificate



- Legally binding forms are very expensive (need thorough verification)

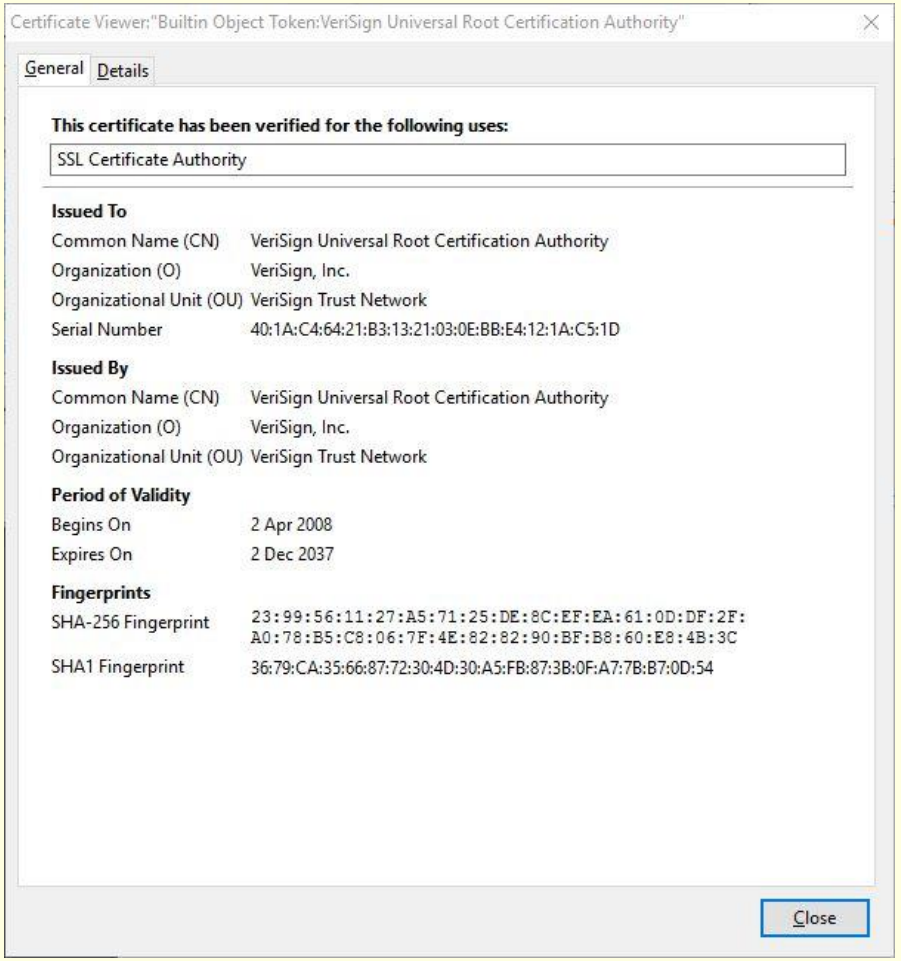
Electronic Certificates

- Electronic document to prove an identity or right to access certain resources
- Digitally signed document binding a subject to some information
  - Name certificates
  - Attribute certificates (access identity, charging identity, role, clearance…)
- Cryptographic methods (public key encryption) are used to
  - identify
    - the issuer
    - the subject
  - protect the content
- Issuer should be a Certificate Authority (CA) who
  - is reliable and trustworthy
  - verifies the content of a certificate

X.509 Certificates

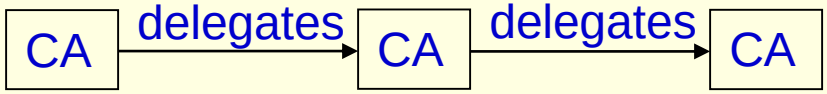
- The most widely used certificate type
- Structure

Version	*Version 1*
Serial number	*1988*
Signature algorithm ID	
Issuer name	
Validity period	
Subject name	
Subject public key info	
Issuer unique ID	*Version 2*
Subject unique ID	*1993*
Extensions	*Version 3*
Subject and issuer attributes	
Key usage and policies	*1996*
Certification path constraints	



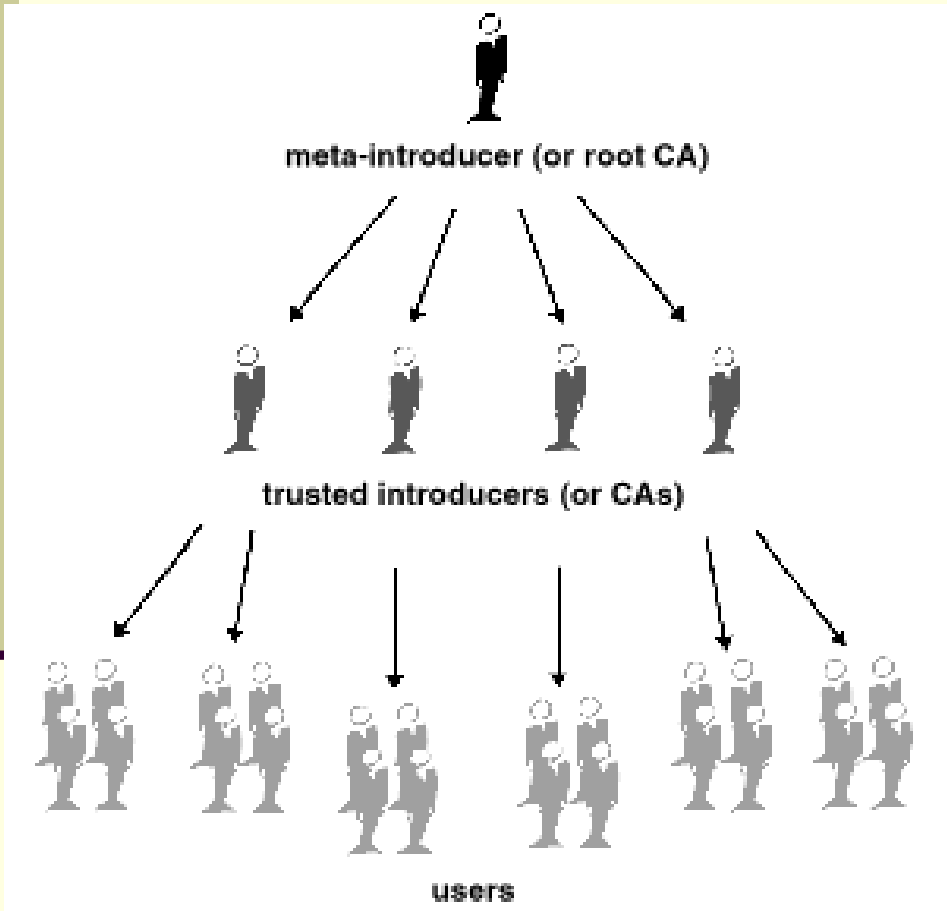
Public Key Infrastructure

- Certificate Authority (CA)
  - Trustworthy (checks the subject's details)
  - Has high availability
- Certificate chain
  - A CA delegates the right of signing certain type of certificates
  - The delegate can do the same



- Root certificate
  - A self-signed certificate
  - Issued by a universally trusted authority for itself
- Certificate revocation list (CRL)
  - List of invalid certificates
  - Can be subject to DoS attacks

Hierarchical Trust



Root certificate

Issuing CA certificate

User certificate

Image source: http://www.pgpi.org/doc/pgpintro/

Pretty Good Privacy (PGP)

- Uses certificates for credentials
- A certificate can have more than one signer
- Web of trust
  - There is no root certificate
  - Users start with a self-signed certificate
  - Users validate each other's certificate (including the public key)

Summary

- Proof-by-knowledge is the most frequently used way of authentication
  - Passwords are the typical form
  - Elaborated methods exist for attack and protection
- Biometrics is more reliable and also more complex/expensive
- Electronic certificates are the basis of a secure computing infrastructure