

# Authentication

Kjell Jørgen Hole  
NoWires Research Group  
Department of Informatics  
University of Bergen

last updated November 8, 2008

KJhole.com

## Outline

- Authentication defined
- Authentication techniques in client-server systems
- Privacy concerns

# Authentication defined

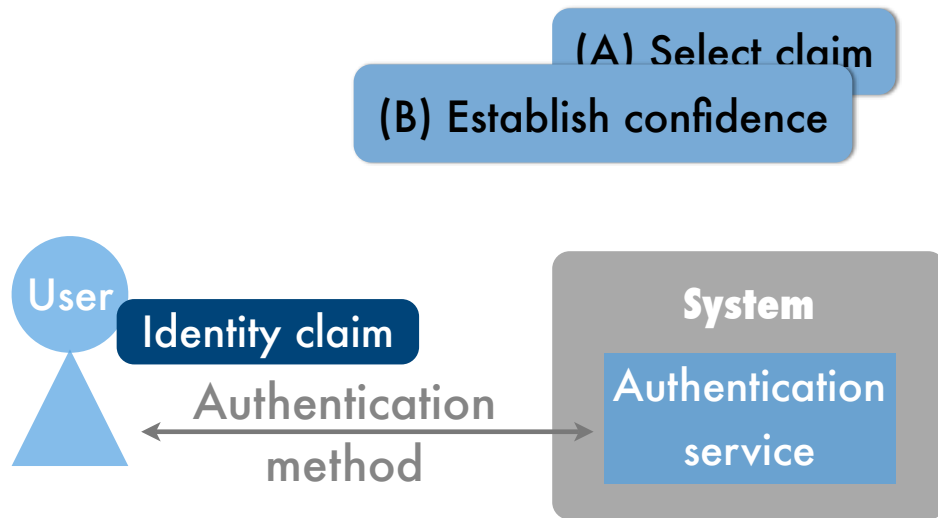
## General definition

KJhole.com

Authentication is the process of establishing confidence in the truth of some claim

- Examples of claims are:
  - “This individual’s name is ‘Matthew Gast’ “
  - “This person is less than 6 feet tall”

# Authentication illustrated



5

# Level of confidence

KJhole.com

- Authentication can only provide a **level of confidence** in a claim
- contrary to popular belief, authentication does *not prove* that a particular individual is who she claims to be

6

# Authentication parties

- Authentication systems involve parties who play three roles:
  - **issuer** generates credentials (e.g. driver's licenses)
  - **presenter** presents credentials
  - **verifier** determines the veracity of the credentials
- The issuer and verifier roles are often combined

7

# Example

- **Issuer:** the police issues passports to individuals in Norway
- **Presenter:** individual holding a passport
- **Verifier:** immigration agent

8

# Initial authentication

- The issuer often uses a separate system to perform an initial authentication of new credential holders
- a department of motor vehicles relies on birth certificates or passports

## Types of authentication

The following three types of authentication illustrate that authentication is not a simple concept

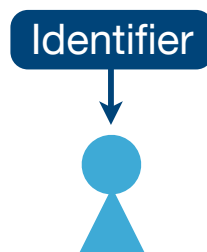
# Individual defined

- An **individual** denotes not only a human, but also nonhuman subjects such as organizations, identified computers, and other entities



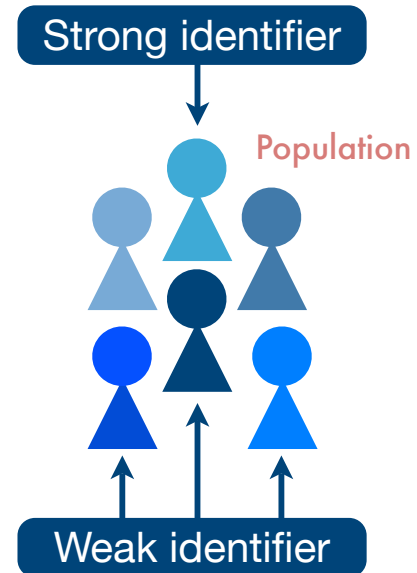
# Identifier defined

- An **identifier** points to an individual. Examples are
  - (personal) name
  - serial number
  - Social Security Number (SSN)



# Strong and weak identifiers

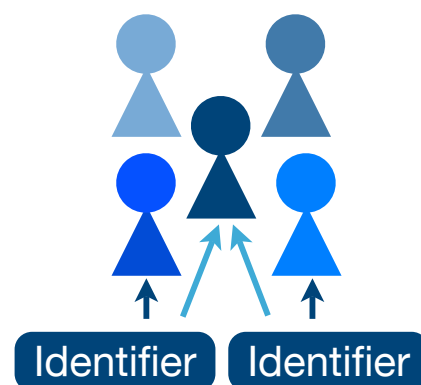
- An identifier is **strong** if it allows a unique mapping to a specific individual in a population
- The identifier is **weak** if it can be correctly applied to more than one individual in a population



13

# More on weak identifiers

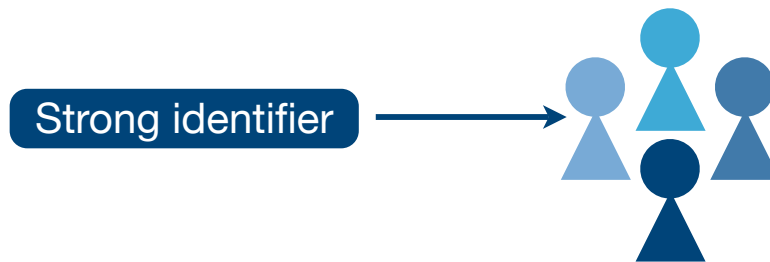
- A combination of weak identifiers can together identify a specific individual
- combination may be viewed as single strong identifier



14

# Individual authentication

Individual authentication is the process of establishing an understood level of confidence that an identifier refers to a specific individual



15

# Usage

- Individual authentication is needed when a user
  - is to be held *accountable* for his actions, or
  - when individuals have *different authorization*

16

# Identity defined

name      date of birth  
 address      nationality  
 gender      credit card number  
 driver's license number  
 pseudonym      favorite chocolate  
 . . .      . . .      . . .

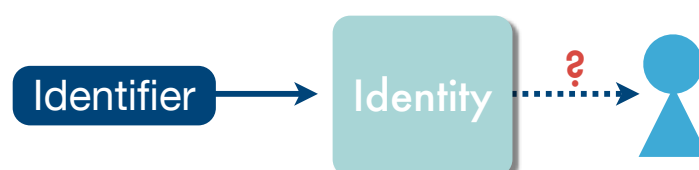
An **identity** is a set of information associated with a specific individual

17

# Identity authentication

**Identity authentication** is the process of establishing an understood level of confidence that an identifier refers to an identity

- The authenticated identity may or may not be linkable to an individual



18

# Example

- An example is the verification of a password (identifier) associated with a Hotmail account (part of identity)
- It may not be possible to link the account to any specific individual

19

KJhole.com

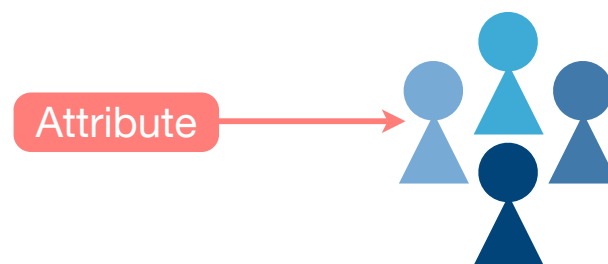
# Attribute

- An **attribute** is a property associated with an individual. Examples are
  - height
  - eye color
  - DNA profile
  - bus card is valid
  - entitlement to drive

20

# Attribute authentication

**Attribute authentication** is the process of establishing an understood level of confidence that an attribute refers to a specific individual



21

# Different from authorization

- **Authorization** is the process of deciding what an individual ought to be allowed to do
- Authentication establishes what an individual “is”, authorization determines what an individual “is allowed” to do
- observe that authorization depends on authentication

22

# Different from identification

- The processes of authentication and identification are related, but not equal
- **Identification** is the process of using observed attributes of an individual to infer who the individual is
- Authentication on the other hand verifies the linkage between an identifier and the individual

## Client-server authentication

# Two-way authentication

- When an individual accesses a service via his or her client device the client is the “presenter” and the server is the “verifier”
- To obtain a high level of security, the server must also authenticate itself to the client
  - in this case the server is the “presenter”

25

# Authenticating to authorize

- A client-server system may authorize individuals
  1. Individual submits request to access system resource
  2. Authorization is carried out by asking an authority, or policy decision point, for an authorization decision
  3. Individual is only allowed to access resource if the policy decision point grants the request

26

# Accountability (1)

- A client-server system may authenticate individuals to hold them *accountable* for their actions
- individuals' actions are usually stored in a log that can be search during an investigation
- Since inappropriate behavior must be tied to a *single* individual, personal identification is *eventually* necessary

27

# Accountability (2)

- **Example:**
  - a fingerprint or a DNA sample can be used to establish after-the-fact accountability
  - note than neither of these two types of evidence names the individual, but both provide means to verify the person's identity

28

# Accountability (3)

- If the the identifier associated with an individual is weak, then it may possible for a user of a system to successfully dispute the validity of the log by claiming that somebody else fooled the authentication system using the same identifier

# Authentication techniques

- Three classes of authentication techniques
  1. “something you know”
  2. “something you have”
  3. “something you are”
- Possible to combine techniques from different classes to obtain **multi-factor authentication**

# 1. Something you know

- One-way authentication with static passwords
- *Advantages* of password-based authentication:
  - cheap to implement
  - low training costs
- *Disadvantages*:
  - help-desk support for users who forget passwords
  - password-reuse in multiple systems

31

## Possible attacks

- Brute-force attacks
- Dictionary attacks
- Shoulder-surfing attacks
- Social engineering attacks
- Interception when password is transmitted in clear text
- One-way authentication allows for man-in-the-middle attacks

32

## 2. Something you have

- Authentication based on possession of (physical) token that is hard to forge or alter
  - driver's licenses make use of holograms as a deterrent to forgery
  - magnetic-stripe card
  - web cookie (needed because HTTP is stateless)
  - smart cards
  - USB storage tokens 33

## Possible attacks

- Steal token, e.g., credit card or cookie containing "secret"
- Trojan horse on client steals authentication information
- Denial-of-service attack simulating a large number of clients that transmit the wrong PIN to the server

## 3. Something you are

- Class of technologies utilizing biometrics to authenticate individuals
  - fingerprint recognition
  - voice analysis
  - iris scanning
  - facial image analysis
  - handwriting dynamics

35

## Biometric authentication (1)

- Biometric authentication, unlike the other authentication techniques, does not rely on secrets
  - register and match unique physical or behavioral characteristics of individuals
  - never exact because of "noise" in measurement process
- Offers only one-way authentication

36

## Biometric authentication (2)

- Technologies are prone to produce
  - **false negative**—individual is erroneously rejected
  - **false positive**—security failure allowing unauthorized access
- Trade-off between these two types of errors can be adjusted by changing threshold values used during the measurement process

37

## Multi-factor authentication KJhole.com

- Multi-factor authentication is often obtained by using techniques from two different classes
  - an example is a hardware token (something you have) activated by entering a PIN (something you know)
- **Remark.** The lectures on Internet banks showed that two-factor authentication does not always result in an acceptable level of security

38

# Centralized vs decentralized

- Some authentication techniques need an infrastructure while others do not
- No infrastructure:
  - static passwords and Secure Shell (SSH)
- Infrastructure:
  - PKI (Public Key Infrastructure) and Kerberos with a KDC (Key Distribution Center)

Privacy concerns

# Privacy defined

Privacy is the right of an individual to decide for himself when and on what terms his identity information should be revealed

# Privacy discussion

- Authentication by name, e.g. using a unique log-in name, enables *identity-based audit logs* and makes it possible to revoke access privileges and punish individuals
- Individual authentication with national unique identifiers makes it possible to determine who did what, where, and how

# Examples of tracking

1. Mobile phone networks authenticate mobile phones rather than handset users
  - however, databases are used to map from a handset identifier to the name of the individual paying the phone bill
2. Credit card transactions are information-rich:
  - a record is created that contains identifiers of both parties and the details of the transaction

43

# Privacy concerns (1)

- I. **Covert identification** Some authentication systems make it possible to identify an individual without the individual's consent or even knowledge
- II. **Excessive use of authentication technology**  
The public's desire for security has led to a rapid increase in installed security systems. Some of these systems can be used to authenticate people and collect personal information

44

## Privacy concerns (2)

### III. Excessive aggregation of personal information

The use of a single identifier (such as SSNs) or a small number of identifiers makes it possible to collect information about an individual from many repositories

- the introduction of a single national authentication system (using strong identifiers) may greatly reduce privacy

## Privacy concerns (3)

IV. **Chilling effects** Individual authentication introduces the possibility of strong social control

---

- **Important remark:** it is clearly very important to consider privacy issues when designing an authentication system

# Source

- National Research Council, *Who Goes There? Authentication Through the Lens of Privacy*. National Academies Press, 2003