

7. Pseudonymous Audit for a Privacy-Enhanced Intrusion Detection

7.1 Need for Pseudonymous Audit

Privacy Risks (conflict between accountability - privacy):

Increasing number of incidents, legal obligations for security audit

- ➔ Increasing commercial use of IDS processing large amounts of audit data
- ➔ Potential misuse of personal data in audit trails/ IDS-profiles/ anomaly reports

Example: Misuse for employee performance monitoring

- ➔ Implications:
stress, low job satisfaction, unfair decision making

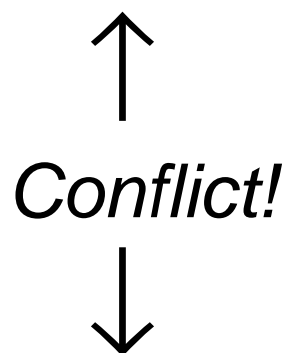
Legal obligations in Europe:

- Privacy legislation:
principle of necessity of data processing (Art. 6 EU-Directive)
- Labour legislation:
right of codetermination of works council

Conflict between Privacy and IT-Security

IT-Security as a technical mean to protect privacy:

e.g. Art. 17 EU Directive on Data Protection,
§ 9 BDSG + Annex



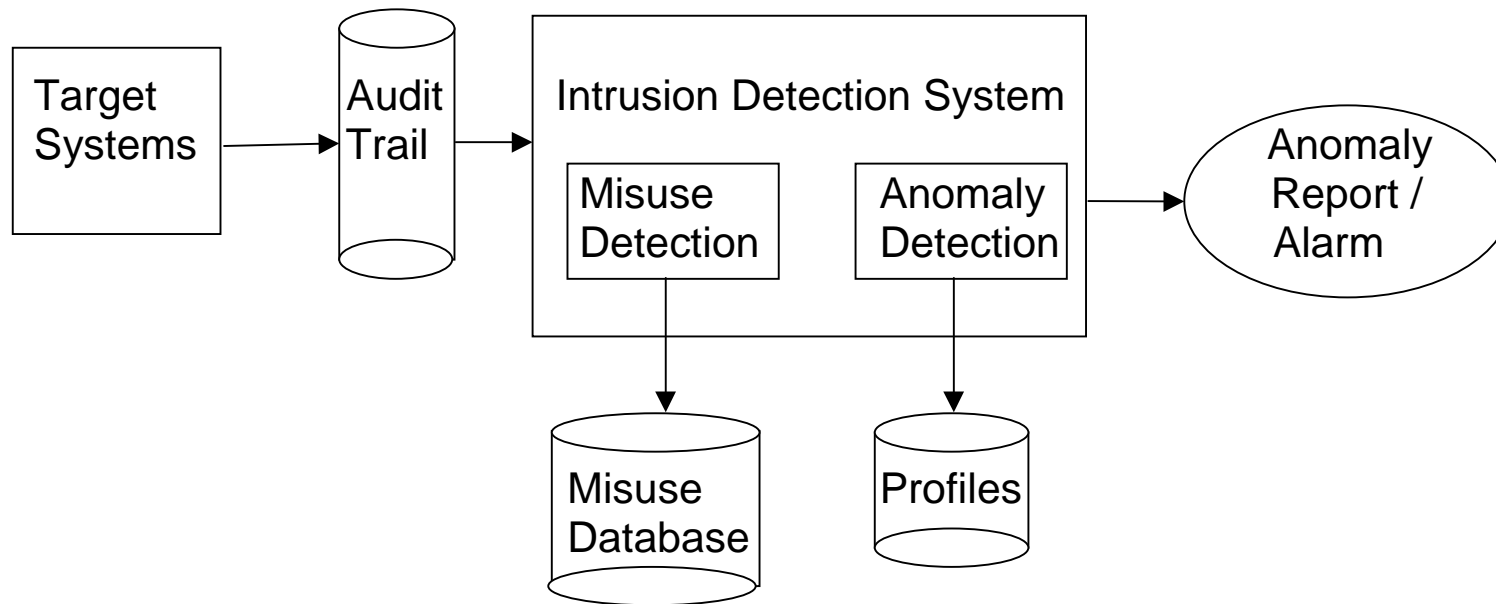
IT-Security as an invasion of privacy:

Security mechanisms use/collect personal control data
about users and data subjects

Example:

Auditing, Intrusion Detection Systems,
Biometrics, Location-based authentication

7.2 Architecture of an Intrusion Detection System (IDS)



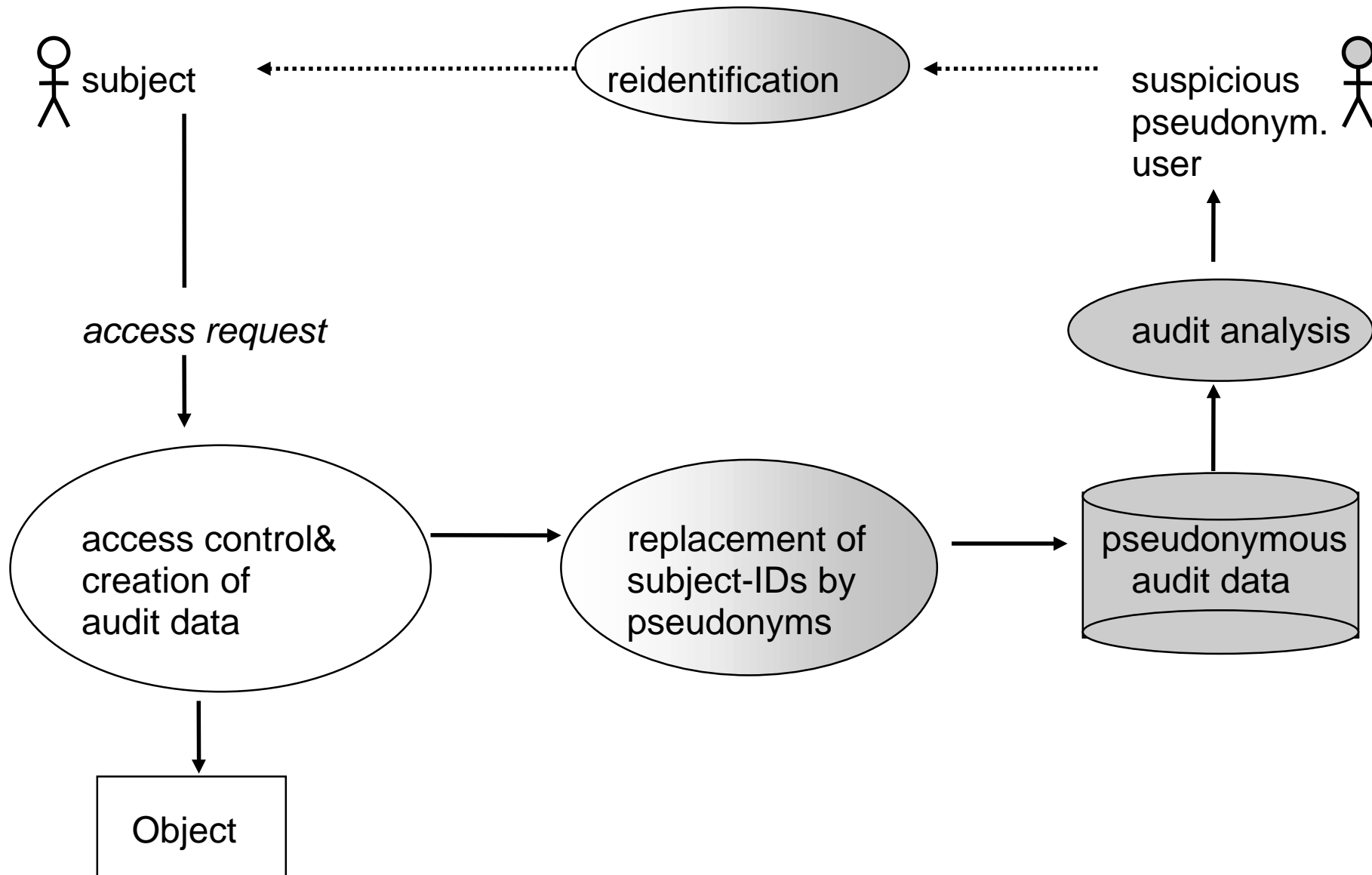
Anomaly Detection:

Statistical profiles of a user's normal behaviour are statistically compared with parameters of the current user session

Misuse Detection:

Parameters of the user's session are compared with known intrusion techniques / vulnerabilities

7.3 Concept of Pseudonymous Auditing



7.4 User-identifying Data in Audit Records

Information contained in audit records (e.g. Solaris 2.4):

Who accesses when, where, how, to which/whose resource ?

Example:

```
header,113,2,open(2) - read,,Mon Jan 22 09:34:32 1996,+650002 msec
      ^^^^^^0^^^^^^^          ^^^^^^^^^^^^^^^^^^^^^1^^^^^^^^^^^^^^^^^^^^
path, /home/richter/lib/libintl.so.1
      ^^^^^^^^^^^^^^2^^^^^^^^^^^^^^^^^^^^
attribute,100755,richter,rnks,8388638,29586,0
      ^^3^^^ ^^4^^^ ^^5^
subject,richter,richter,rnks,richter,rkns, 854, 639,0 0 romeo
      ^^6^^^ ^^7^^^ ^^8^ ^^9^^^ ^^10^          ^^11^
return,success,0
      ^^12^^^
```

Directly user identifying attributes:

- 6: audit ID
- 7: real user ID
- 8: real group ID
- 9: effective user ID
- 10: effective group ID
- 4: object owner
- 5: owner group

Indirectly user identifying attributes:

- 2: access path and object name
- 11: identifier of monitored host
- 1: date and time stamp
- 3, 0, 12: access rights + action + final action status

Problem:

Audit trail analysis is not possible with extensively pseudonymised audit records

Example:

Assume a user accessed his own file:

```
header,113,2,bcu8tH,,Mon Jan 22 0Aye.AK 1996,+650002 msec  
path, /ouin/ugGn/hu7uj/9jl9iyu  
attribute,100755, ugGn, Y9oK,8388638,29586,0  
subject,ugGn,ugGn,Y9oK,ugGn,Y9oK, 854, 639,0 0 C8Io  
return, MImoOIm
```

A certain user acted on his own account

(pseudonyms for audit ID and real user ID are identical)

and referred *somewhere, sometime, somehow* an own file

(subject ID's and object owner ID are identical)

Pseudonymisation of audit records should cover:

- All user ID's
- Location ID's
- Conditionally subdirectories and objects

7.5 Pseudonymisation techniques

- Reference pseudonyms
- Cryptographic pseudonyms
 - Operational separation of duties through:
symmetric encryption with key $k = k_1 + k_2$,
 k_1 is kept by security admin,
 k_2 is kept by data protection officer
 - Encryption keys should be changed after certain time intervals to prevent reidentification

7.4 A Holistic Approach

1. Technical /organisational measures

2. Legal measures

- purpose binding and necessity principle
- right of users to be informed / notified
- co-determination of works council

3. Ethical codices

4. Educational measures