Intrusion detection and privacy

Conflict: security mechanisms and privacy

- Security mechanisms are used to protect privacy;
- Security mechanisms use and/or collect personal private data about users and data they use;
- The data may be used to compromise privacy;

Examples:

- Audit, intrusion detection systems;
- Biometric

Audit and privacy

- During auditing events in a computer system a lot of sensitive information is recorded;
- When records are used for intrusion detection privacy is under potential threat
- As an example, consider a situation, when IDS has produced a false alarm, then a user, whose name is appeared in the corresponding record may be wrongly accused of the misuse;

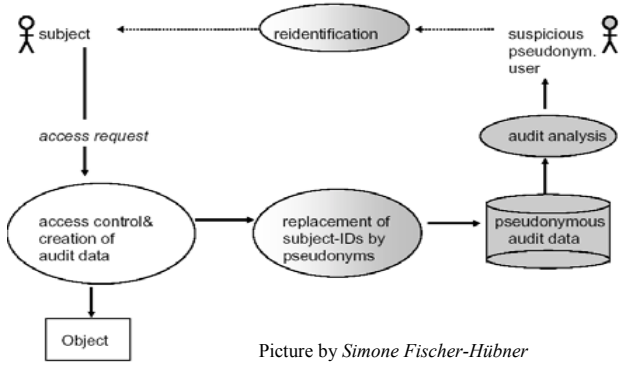
Accountability and privacy

- The conflict is inevitable:
  - On the one hand, when we are doing intrusion detection, there must be a way to connect events to a specific user (which could be held accountable)
  - On the other hand, if we want to protect privacy of users such connections should be hidden.

Anonymity and Pseudonimity

- Full anonymization of the audit records is not suitable because
  - there would be no way to recover real identities;
  - Intrusion detection requires often detection of a sequence of actions of the *same* user;
- Pseudonymity is a solution here. It allows
  - to protect privacy by using pseudonyms instead of true identities;
  - In case of suspicious behaviour it allows re-identify a user (find a true identity);

Pseudonymous audit



Picture by *Simone Fischer-Hübner*

Pseudonymization techniques

- Reference pseudonyms:
  - Database matching true identities and pseudonyms
- Cryptographic pseudonyms:
  - may use Separation of duties by:
    - Splitting the secret key k into two parts, e.g. k= k1 + k2;
    - k1 and k2 are hold by two different people, e.g SSO and privacy protection officer;
    - One part is not enough to restore true identity;

The issue of unauthorized re-identification

- The procedure of re-identification should be well specified in a security policy: who and under which circumstances can do it;
- There is problem of unwanted and unauthorized re-identification:
  - A person who knows well a system and its users, may re-idenify a person without an authorization, just using public information from audit records;
  - A real issue,especially for small systems/networks;

Re-identification

Re-identification can be based on the information about an event:

- Action and data/time;
- Action, access right, data/time;
- Host identifier;
- Etc

May be dealt with by creating the fake traffic, simulating normal behaviour of the users;

Legal and ethical issues

- Monitoring users behaviour may not be appropriate or even illegal, unless they are notified
  - They may be monitored
  - Information may be used to support prosecution or dismissal