Security models

TkL Markus Peuhkuri

2008-04-08

Lecture topics

- Security policy
- Security models
- Integrity models
- After this lecture, you know
  - structure of security policy
  - how trust builds (more methods later)
  - confidientility models
  - integrity models

Components in secure system

- A system has
  - subjects or principals: those who act on the system
  - objects that are manipulated by actions
  - transitions or actions that change the system state
  - states that are either secure or insecure
- Subjects have different *rights* to objects
  - read
  - write
  - own
  - transfer ownership
  - delete
  - create...

Security policy

- Statement that bisects states to
  1. authorised, secure
  2. unauthorised, insecure
- Different policies can have different sets of states
- Secure system
  - starts in authorised state
  - cannot enter to a unauthorised state
    if this happens, a *breach of security* occurs
- A security mechanism enforces some part of the security policy

  - entity (device, software) may allow only secure actions
  - procedure how the system is operated and actions taken

- Security model represents a policy or set of policies

- Policy description may include very detailed instructions. This is very common as security policies are updated every now and then, quite often after some incident. Policy is modified to avoid similar incidents in the future, but often people fail to see broader scope.

Different goals of security policies

- Information confidentiality
  - unauthorised disclosure causes damage
  - damages in integrity or availability can be overcame
  - military security policy
  - governmental security policy
  - executive privilege to access data
  - "what information can be disclosed"

- Information integrity
  - unauthorised change causes damage
  - confidentiality important, but non-critical
  - commercial security policy
  - trustworthiness of information
  - "who can modify information"

Example policy: TKK (2005)

TKK Computer Systems and Data Communication Networks Usage Policy

- Intention: motivation behind policy

  ...to offer students and staff a good access to information systems. ... Everyone should attend to matters related to security. All users have responsibility for the total security of the university's computer systems. ... into consideration the existing laws

- Scope: what systems it covers

  ...all information systems administered or maintained by the Computing Centre ... all data communication networks of the university

- What usage is allowed

  Students, researches and other staff have the right to use university's computer services in tasks related to studies, research and teaching. There are listed those *who* can use systems and *purposes* that systems can be used for. Thus it nor permitted for everyone and not for any use one would like to use.

- What usage is permitted

  Use of network services and email for private purposes is allowed to a limited extent. There is one woolly definition, thus it is left for after-the-fact interpretation.

- What usage is prohibited

  The use for commercial or political purposes, especially for election advertizing is strictly forbidden. One specific topic (there had been misuse event in this) is listed, as later commercial mass messages.

- Acceptance of rules

  A computer account is needed for the use of information technology services. The acceptance of these rules is a requirement for the use of a computer account.

Example policy: TKK (2005)

- Limiting authorisation and delegation

  User account and password are for personal use only.

- Requirement for authentication

  Access to outside networks is permitted only with user's personal account. The use of a false identity is forbidden while the use of anonymous servers is permitted.

- Terminology defined

  Misuse of information systems means every action that

  - *disturbs the use of information systems for the purpose it is meant for,*
  - *causes harm or damage in any data communication network or computer,*
  - *uses characteristics of the systems for purposes they are not meant for,*
  - *is prohibited by the administrators of the information systems*

- Retaining effect

  . . . following consequences can be applied:

  - *limitation or denial of usage*
  - *compensation for the misuse of resources, compensation for the investigation expenses,*
  - *transfer of the issue to the police authority and criminal court*

Do you ***trust***

- Does one understand the assumptions behind
  - security policy
  - security mechanisms
  - security procedures
- Understanding enables one to *evaluate effectiveness*

Example of trust: Internet banking

Is it safe to do bank transactions on net: assumptions

1. The bank correctly sent access codes and those were not exposed to any third party
2. The net bank server is at `https://online.bank.example` For most of Finnish banks the default main web page is insecure one `http://www.bank.example` that enables a set of attacks by providing a fake link (or login dialog) to net bank.

   OP-group redirects user to secure main page

   Sampo provides both secure and insecure, does redirect to unsecure one!

   Handelsbanken provides both secure[1] and insecure, does not redirect

   Nordea provides both secure and insecure, does not redirect

   Tapiola does not provide a secure page

   Ålandsbanken does not provide a secure page

3. DNS servers are not compromised
4. Protocol implements correct authentication and encryption
5. The security certificate is assigned to the right party by CA
6. The root certificate of CA is not compromised

[1] Serticate is for `www.handelsbanken.se`

7. The CA list in the browser includes only decent CAs
8. The browser or operating system integrity is not compromised: that is there is no viruses, trojans, backdoors, spy-ware or any security bugs in those
9. Security in the bank systems is sound

Access control

- Discretionary access control (DAC)
  - user (owner) can deny or grant access to objects
  - identity-based access control (IBAC)
- Mandatory access control (MAC)
  - access is determined by authoritative pronouncement
  - rule-based access control
- Originator controlled access control (ORCON)
  - bearer of data cannot control access
  - e.g. information is provided for use, but not for redistribution: Digital Rights Management (DRM)

Bell-LaPadula model

- Implements multilevel security (MLS)

  no read up a process cannot read data at higher level (NRU: simple security property)

  no write down a process cannot write data to a lower level (NWD: *-property)
- Subjects and objects have different security levels, e.g.
  - top secret
  - secret
  - confidential
  - public
- Confidential-level user can
  - read public — confidential
  - write confidential — top secret
- Data security level can only increase
  ⇒ need for *trusted subjects* to declassify
- In addition to levels, there are also compartments
  - enforces “need-to-know” principle

	personnel	financial	engineering
secret			
public			

Bell-LaPadula (and other) in real systems

- Blind write-ups are a problem as “low” may not learn that some data existed “high”: a black hole problem
- Enforcing the control across boundaries is hard
  - connecting two secure systems may result in one insecure system or one violating the policy
- Covert channels a difficult problem
  - a high-bandwidth system can easily leak 2048-bit key
- Program correctness
- Traffic analysis may be revealing
  - knowing that the data exists
  - learning nature of data: for example, if there are some $100-200$ bytes long packets sent every 20 ms, it is very probable that it is voice data.

Bell-LaPadula. . .

- Evaluating the whole system difficult
  - reference monitor that tracks every system call and decides if it violates security policy
  - data pump or data diode that copies data from “low” to “high”
  - many components in system manage all levels of data leading to very large system to analyse
- A common strategy is to have different systems for high and low
  - one computer for the Internet, another for classified work
  - files transfered with a removable media or by using some device that allows files to be transfered on command by an operator
- Security levels of data increase
  ⇒ overclassification of data
  ⇒ a need to change labels
- Data aggregation may result in more sensitive data than any of sources: for example a credit card number by itself has little value. It becomes more sensitive with the expiration date and the verification code. When this data is combined with the customer address record (user home address) that is not a very sensitive either, it becomes even more valuable. Also large databases are more sensitive than a single records.
- Security features are not used
  - capability exists, but not used
  - dedicated worker problem
- Implementing the *trusted path*

Trusted components

Trusted path who’s talking

- how a user knows which system(s) receives keystrokes
- WYSIWYS: What You See Is What You Sign?
- how a system knows its communicating with a human

Trusted distribution of information and devices

    - is the operating system and the applications genuine

Trusted Facility Management system administration

    - does a maintenance endanger information
    - is the system configuration correct

More on this in authentication lecture

Integrity of the information

- Important in commercial environment
- Principles:
    - separation of the duty: there are at least two persons who perform each one part of the critical function.
    - separation of the function: one developing new systems does not have access to the production system
    - auditing: any security breach will be detected and recovered — all actions have accountability.
- Classification is not set by a single authority
  ⇒ would result very large number of compartments
  ⇒ compartment management becomes a problem

Biba Integrity model

No write up a process cannot write data to a higher level

No read down a process cannot read data at a lower level

No execute up a process cannot execute process at a higher level

- Bell-LaPadula "upside down"
- Similar but opposite problems

Chinese Wall

- Bell-LaPadula: higher rank can access all
- Conflict of interest
    - accountant ⇔ financial advisor
    - design office with competing customers (advertising agency, consultant, financial advisor, . . .)
- If one has had an access (recently) to A's information, he cannot talk to B
- History of access matters

Medical records

- Both confidentiality and integrity

  Patient who records are about

  Personal health information is stored in medical records

  Clinician is one acting on health care. This includes doctors, dietitians, nurses, researchers. Those who treat patient *must* identify patient while other, like researchers developing a new drug, *may not* identify one to a person.

- Exhaustive list about who need information is not known *à priori*. It may not be your family doctor treating you after an accident. The doctor providing you the treatment may need to know, for example, if you are allergic to penicillin.

  ⇒potentially a large number of people may need to have an access

  - vulnerability to social engineering, curiosity
  - same applies for population register, tax records, call records, ...

- It is important to know medical history to avoid mistreatment or not to repeat laboratory tests. There is a need to optimise information flow without risking privacy. In US, for example, HIPAA legislation is intended to improve information exchange.

Medical records access principles

(designed for British Medical Association)

1. each record has an ACL[2] naming those individuals or groups who can read or append to records
2. clinician can create and open a record with patient and if there has been a referral with the referring clinician
3. one clinician has right to add other clinicians to ACL
4. patient must be informed who are on ACL and give permission new entries expect in emergency or statutory exemptions
5. records are immutable until they are deleted because of their age
6. *audit trail* of all access
7. information derived from one record may be appended to another record if the latter's ACL is subset of former's
8. patients must be notified if one person in their ACL has access to large number of records
9. computer systems must have a trusted subsystem to enforce above principles

Clark-Wilson

- Two classes of data items
  - constrained data items: those data items that are critical for correct operation (CDI)
  - unconstrained data items
- Integrity constraints
- Two classes of procedures
  - integrity verification procedures check that CDIs conform to integrity constrains
  - transformation procedures change state from one valid state to another valid state

An example would be a purchase: when goods arrive, they are checked to dispatch list, When a bill is received, it is compared to dispatch list, order, and to price list or offer. It is also validated that order was done according to policy, there is enough money to cover the bill and after that bill is accepted and payment done.

Depending on organisation, there are multiple persons acting on process to prevent single-person fraud. For example in TKK, a person who checks that a bill matches with the delivery, cannot accept the bill.

[2] Access Control List

How to enforce models

- Application
  - the most flexible access control
    - time-based, terminal-based
    - state maintained
  - only applicable selections shown
  - security depends on application correctness, that may be a difficult analyse because of large size of application
  - additional authentication for critical part
- Middle-ware, such as database, or application server
  - provides own, fine-grained, access control
  - because of performance, runs on single user permissions

How to enforce models

- Operating system
  - simple, but an efficient control, information in process structure
  - permissions are checked at start of file access
  - a change of rights may require user to re-login
- Hardware
  - provides feature or memory region protection
  - OS-controlled gates

How to allow access

- Let the user to log in
  - authenticate one
  - the user is mapped to some identifier
- For each item, list who has access to it and what kind of access
  - access control lists

```
-rw-r--r--  1 puhuri opetus   16469 2005-01-31 22:40 03models.tex
-rw-------  1 puhuri opetus    6400 2005-01-15 12:32 exams.txt
```

- Alternative: assign each user a list of rights for each object
  - also a capability model
  - e.g. cryptographic keys for a process to allow network access

Summary

- Security models try to formalise security policy
- Integrity and confidentiality may be conflicting
- Central access control rigid
- Distributed classification results large number of classes
  ⇒ difficult to verify if right persons have access
- Information confidentiality and availability

References