

## Lecture 18: Security and Privacy

### Information rights, obligations, control, and accountability

Data management is not just a technical problem.  
There are ethical and competitive considerations.

- security goals, threats and control measures
- discretionary, mandatory and role-based access control
- Australian privacy law
- (Privacy questions in *every* public service job interview!)

See [E&N Chapter 23]

<http://www.privacy.gov.au>

National Privacy Principles

## Security Goals - Integrity

- the database contains the information it *should* contain

## Security Goals - Integrity

- the database contains the information it *should* contain
- no improper modifications

## Security Goals - Integrity

- the database contains the information it *should* contain
- no improper modifications
- loss of integrity could result in

## Security Goals - Integrity

- the database contains the information it *should* contain
- no improper modifications
- loss of integrity could result in
  - incorrect or fraudulent payments (add some 0's to your bank balance)

## Security Goals - Integrity

- the database contains the information it *should* contain
- no improper modifications
- loss of integrity could result in
  - incorrect or fraudulent payments (add some 0's to your bank balance)
  - bad decisions (remove your mortgage from the recall list)

## Security Goals - Integrity

- the database contains the information it *should* contain
- no improper modifications
- loss of integrity could result in
  - incorrect or fraudulent payments (add some 0's to your bank balance)
  - bad decisions (remove your mortgage from the recall list)
  - nuclear strike!?

## Security Goals - Availability

- the database is available to be used by the people and systems it is intended for

## Security Goals - Availability

- the database is available to be used by the people and systems it is intended for
- at its full performance (eg ping-floods and other denial of service attacks)

## Security Goals - Availability

- the database is available to be used by the people and systems it is intended for
- at its full performance (eg ping-floods and other denial of service attacks)
- loss of availability could result in

## Security Goals - Availability

- the database is available to be used by the people and systems it is intended for
- at its full performance (eg ping-floods and other denial of service attacks)
- loss of availability could result in
  - waste of employee time

## Security Goals - Availability

- the database is available to be used by the people and systems it is intended for
- at its full performance (eg ping-floods and other denial of service attacks)
- loss of availability could result in
  - waste of employee time
  - loss of immediate business

## Security Goals - Availability

- the database is available to be used by the people and systems it is intended for
- at its full performance (eg ping-floods and other denial of service attacks)
- loss of availability could result in
  - waste of employee time
  - loss of immediate business
  - and thus perhaps ongoing business

## Security Goals - Confidentiality

- information is only disclosed to those with a right to know it

## Security Goals - Confidentiality

- information is only disclosed to those with a right to know it
- the Privacy Act (1988) specifies legal confidentiality requirements for personal information

## Security Goals - Confidentiality

- information is only disclosed to those with a right to know it
- the Privacy Act (1988) specifies legal confidentiality requirements for personal information
- loss of confidentiality could result in

## Security Goals - Confidentiality

- information is only disclosed to those with a right to know it
- the Privacy Act (1988) specifies legal confidentiality requirements for personal information
- loss of confidentiality could result in
  - embarrassment

## Security Goals - Confidentiality

- information is only disclosed to those with a right to know it
- the Privacy Act (1988) specifies legal confidentiality requirements for personal information
- loss of confidentiality could result in
  - embarrassment
  - loss of competitive advantage

## Security Goals - Confidentiality

- information is only disclosed to those with a right to know it
- the Privacy Act (1988) specifies legal confidentiality requirements for personal information
- loss of confidentiality could result in
  - embarrassment
  - loss of competitive advantage
  - prosecution under the Privacy Act

# Security Goals - Confidentiality

- information is only disclosed to those with a right to know it
- the Privacy Act (1988) specifies legal confidentiality requirements for personal information
- loss of confidentiality could result in
  - embarrassment
  - loss of competitive advantage
  - prosecution under the Privacy Act
  - compromise of national security

# Security Goals - Summary

- the right data is there

# Security Goals - Summary

- the right data is there
- the right people can use it

# Security Goals - Summary

- the right data is there
- the right people can use it
- *only the right people can see it*

## Security Goals - Summary

- the right data is there
- the right people can use it
- *only* the right people can see it
- bad things can happen if these goals are not achieved

## Security Goals - Summary

- the right data is there
- the right people can use it
- *only* the right people can see it
- bad things can happen if these goals are not achieved
  - **Publicity about security failures can harm an organisations reputation.**

## Security Goals - Summary

- the right data is there
- the right people can use it
- *only* the right people can see it
- bad things can happen if these goals are not achieved
  - Publicity about security failures can harm an organisations reputation.
- need ways to control threats to these goals

## Security Goals - Summary

- the right data is there
- the right people can use it
- *only* the right people can see it
- bad things can happen if these goals are not achieved
  - Publicity about security failures can harm an organisations reputation.
- need ways to control threats to these goals

## Security Goals - Summary

- the right data is there
- the right people can use it
- *only* the right people can see it
- bad things can happen if these goals are not achieved
  - Publicity about security failures can harm an organisations reputation.
- need ways to control threats to these goals

# Control Measures

The main measure for controlling these threats is

- access control

and this is what we will mostly discuss today.

# Control Measures

The main measure for controlling these threats is

- access control

and this is what we will mostly discuss today.

# Control Measures

The main measure for controlling these threats is

- access control

and this is what we will mostly discuss today.

However, there are others

- inference control

# Control Measures

The main measure for controlling these threats is

- access control

and this is what we will mostly discuss today.

However, there are others

- inference control
- flow control

# Control Measures

The main measure for controlling these threats is

- access control

and this is what we will mostly discuss today.

However, there are others

- inference control
- flow control
- encryption

# Access Control

Access control is about making sure the right *users* (represented by their *accounts*) have the right *privileges* (read or write access to part of the database schema).

# Access Control

Access control is about making sure the right *users* (represented by their *accounts*) have the right *privileges* (read or write access to part of the database schema).

- accounts, stored procedures are called *subjects*

# Access Control

Access control is about making sure the right *users* (represented by their *accounts*) have the right *privileges* (read or write access to part of the database schema).

- accounts, stored procedures are called *subjects*
- *objects* are things that can be accessed: special dbms commands (`CREATE SCHEMA`), database schemas, relations (including views), attributes, tuples, attribute values are called *objects*

# Access Control

Access control is about making sure the right *users* (represented by their *accounts*) have the right *privileges* (read or write access to part of the database schema).

- accounts, stored procedures are called *subjects*
- *objects* are things that can be accessed: special dbms commands (`CREATE SCHEMA`), database schemas, relations (including views), attributes, tuples, attribute values are called *objects*
- eg. some users may have `CREATE SCHEMA` access, others may only be able to read one restricted view.

## Access Control - Discretionary Control

The oldest and most commonly implemented mechanism is *discretionary control*

## Access Control - Discretionary Control

The oldest and most commonly implemented mechanism is *discretionary control*

- The DBA (database administrator) grants and revokes privileges to/from accounts at his discretion.

## Access Control - Discretionary Control

The oldest and most commonly implemented mechanism is *discretionary control*

- The DBA (database administrator) grants and revokes privileges to/from accounts at his discretion.
- no SQL support for control of access to special commands, each dbms does it its own way

## Access Control - Discretionary Control

The oldest and most commonly implemented mechanism is *discretionary control*

- The DBA (database administrator) grants and revokes privileges to/from accounts at his discretion.
- no SQL support for control of access to special commands, each dbms does it its own way
- each relation, attribute has an *owner*, who can grant privileges to it

## Access Control - Discretionary Control

The oldest and most commonly implemented mechanism is *discretionary control*

- The DBA (database administrator) grants and revokes privileges to/from accounts at his discretion.
- no SQL support for control of access to special commands, each dbms does it its own way
- each relation, attribute has an *owner*, who can grant privileges to it
- dbms maintains a *matrix* with a row for each subject, a column for each object, and an access level (read, write, update) in each cell

## Access Control - Mandatory Control

- subjects and objects are *classified*, ie assigned a classification in an ordered set, eg. top-secret  $\zeta$  secret  $\zeta$  confidential  $\zeta$  unclassified

## Access Control - Mandatory Control

- subjects and objects are *classified*, ie assigned a classification in an ordered set, eg. top-secret  $\zeta$  secret  $\zeta$  confidential  $\zeta$  unclassified
- user can read object iff  $class(user) \geq class(object)$

## Access Control - Mandatory Control

- subjects and objects are *classified*, ie assigned a classification in an ordered set, eg. top-secret  $\zeta$  secret  $\zeta$  confidential  $\zeta$  unclassified
- user can read object iff  $class(user) \geq class(object)$
- user can write object iff  $class(user) \leq class(object)$

## Access Control - Mandatory Control

- subjects and objects are *classified*, ie assigned a classification in an ordered set, eg. top-secret  $\zeta$  secret  $\zeta$  confidential  $\zeta$  unclassified
- user can read object iff  $class(user) \geq class(object)$
- user can write object iff  $class(user) \leq class(object)$
- *huh?* - that's right, otherwise we have a *covert channel* for higher classified material to reach lower classified users

## Access Control - Mandatory Control

- subjects and objects are *classified*, ie assigned a classification in an ordered set, eg. top-secret  $\zeta$  secret  $\zeta$  confidential  $\zeta$  unclassified
- user can read object iff  $class(user) \geq class(object)$
- user can write object iff  $class(user) \leq class(object)$
- *huh?* - that's right, otherwise we have a *covert channel* for higher classified material to reach lower classified users
- **further strangeness: inferred existence of higher classified value motivates *polyinstantiation* of the database [E&N §23.3]**

## Access Control - Role-Based Security

This is a “newer” form of access control (though it was used in mid-1990’s in an Australian Government department)

## Access Control - Role-Based Security

This is a “newer” form of access control (though it was used in mid-1990’s in an Australian Government department)

- in addition to subjects (users) and objects (data items, privileges), we also have *roles*
- roles are allocated the objects needed to perform them
- users are allocated to roles, and automatically get the associated access
- can be connected to human resources system so that users automatically have access needed to do their job (and only their job)
- why would you do it any other way?

# Privacy

When an organisation holds personal information about people, those people have rights with regard to that information. As a database worker, you must ensure these rights are upheld. As a citizen, you should be aware of these rights.

# Privacy

When an organisation holds personal information about people, those people have rights with regard to that information. As a database worker, you must ensure these rights are upheld. As a citizen, you should be aware of these rights.

The following document summarises the principles of Australian Privacy Law.  
National Privacy Principles