Security models

Partial orders applied

Prof Hans Georg Schaathun

Høgskolen i Ålesund

Autumn 2013 – Session 1/5 (2)

Security models

One of many approaches to information security

- Two sets

  Subjects S e.g. users

  Objects O e.g. files

- How do you manage access to files?
- Given $s \in S$ and $o \in O$
  - is s allowed to read o?
  - how do you know?

HØGSKOLEN I ÅLESUND
Aalesund University College

A naïve view

- This is just a relation $A \subset S \times O$
  - $(s, o) \in A$ if and only if s may read o
- Intractible.
  - You may have to store every element of A.

A naïve view

- This is just a relation $A \subset S \times O$
  - $(s, o) \in A$ if and only if s may read o
- Intractible.
  - You may have to store every element of A.

Security labels

The total order case

- We can assign security labels (from a set L):
  1. Top Secret
  2. Secret
  3. Confidential
  4. Unclassified
- Total order

$$\text{TopSecret} < \text{Secret} < \text{Confidential} < \text{Unclassified}$$

- Each subject has a security clearance $c : S \to L$
- Each object has an access level $c : O \to L$
- s may read o if $c(s) \geq c(o)$

HØGSKOLEN I ÅLESUND
Aalesund University College

The partial order case

- Same logic aswith the total order
  - s may read o if $c(s) \geq c(o)$
- If s and o are incomparable, there is no access

  Thus you can separate departments.

- There is no global 'Top Secret' clearance
- Labels from one department may be incomparable to those of another

One approach

- A set of departments: $G = \{\text{EE}, \text{Comp}, \text{Math}\}$
- A security label is a subset $L \subset G$
- Partial ordering: $\subset$
- For instance
  - $c(s) = \{\text{EE}, \text{Comp}\}$
  - $c(o) = \{\text{EE}\}$
  - $c(o) \subset c(s)$: access granted

Combination

Summary

1. Example of application
2. No details in this module
3. Reasoning over security models
4. Partial orders provide formalism

HØGSKOLEN I ÅLESUND
Aalesund University College