Computer Security

CIS 5370

Security Policies

1

Take-Grant Protection Model

- A specific (not generic) system
  - Set of rules for state transitions
- Safety decidable, and in time linear with the size of the system
- Goal: find conditions under which rights can be transferred from one entity to another in the system

2

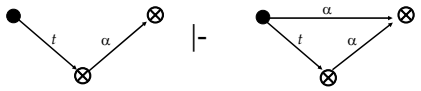
Take-Grant Notation

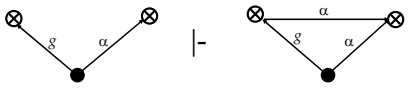
- ○: objects (files, …)
- ●: subjects (users, processes, …)
- ⊗ : either a subject or an object
- G |–$_x$ G': apply a rewriting rule *x* to G to get G'
- G |–* G': apply a sequence of rewriting rules to G to get G'
- R = { *t*, *g*, *r*, *w*, … }: set of rights

3

Four Rules in Take-Grant

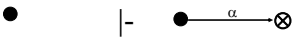
Take, grant, create, remove

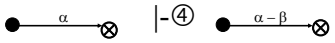
take 

grant 

4

More Rules

create 

remove 

These four rules are called the *de jure* rules

Rule sequences are called *witnesses*

5

Subjects and Objects

- Both subjects and objects can hold rights to objects
- Not sure what it means for an object to hold rights to another object (or to a subject)
- Only subjects can take or grant rights
  - See definition of take and grant
  - Important in later results

6

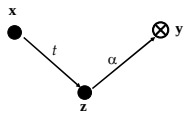
Transferring rights

- Two connected subject vertices may transfer rights in 4 ways:
  1. Take
  2. Grant
  3. Symmetric Take
  4. Symmetric Grant

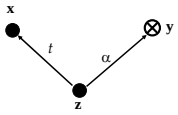
7

Symmetry

We know that if node z has α rights to y and x has take (t) rights to z, then x can gain α rights to y. This is the take rule.



What if x has no rights to z, and z has α to y, but has only take (t) rights to x? Can x gain α rights to object y?



Yes, but we will need a *witness!*

8

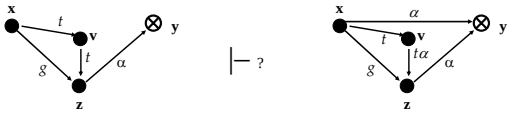
can•share Predicate

Definition:

- *can•share*(*r*, **x**, **y**, G_0) if, and only if, there is a sequence of protection graphs G_0, …, G_n such that $G_0 \vdash^* G_n$ using only *de jure* rules and in G_n there is an edge from **x** to **y** labeled *r*.

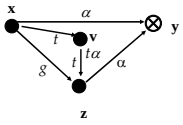
9

Can-share



Can subject x gain α rights to object y?

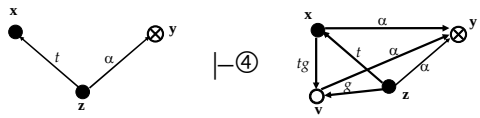
1. **v** takes (α to y) from z
2. **x** takes **(α to y) from v**



10

Symmetry

Can subject x gain α rights to object y?



1. **x** creates (*tg* to new) **v**
2. **z** takes (*g* to **v**) from **x**
3. **z** grants (α to **y**) to **v**
4. **x** takes (α to **y**) from **v**

11

Definitions

- tg-path: what you would think, path where each pair of connected vertices share at least one t or g edge
- tg-connected: two vertices are tg-connected if there is a tg-path between them
- island: subject-only subset of vertices in a protection graph that are ALL tg-connected

12

Exercise

- Prove that any right possessed by any vertex in an island can be shared with any other vertex in the island

13

Take – Grant Properties

- **Safety question is decidable in linear time on the complexity of the protection system**
- **In any Take-Grant protection system, there is an efficient algorithm to decide if a specific subject can gain a right to specific object**

14

Key Question

- Characterize class of models for which safety is decidable
  - Existence: Take-Grant Protection Model is a member of such a class
  - Universality: In general, question undecidable, so for some models it is not decidable
- What is the dividing line?

15