IT-Security

Access Control: Take-Grant Model

Volker Roth

Institut für Informatik
Freie Universität Berlin

Sommersemester 2009

Initial Remarks

In 1976, Lipton and Snyder presented a particular access control mechanism, the take and grant system, for which safety can be decided in linear time.

R. J. Lipton and L. Snyder.
"A linear time algorithm for deciding subject security."
Journal of the ACM, 24(3):455-464, July 1977.

Definitions

A *protection graph* is a directed graph G with two distinct kinds of vertices: *subjects* and *objects*. The edges are labeled with subsets of a finite set R of rights.

Subjects are *active* vertices (they represent e.g., processes or users); they can pass authority by invoking *graph rewriting rules.* We write

$$G \vdash G'$$

if the graph G' is produced from G by a rewriting rule. The symbol $\vdash^*$ represents zero or more rule applications.

Definitions

A *witness* is a sequence of graph rewriting rules which produce the predicate or condition being witnessed (e.g., the proof of a theorem).

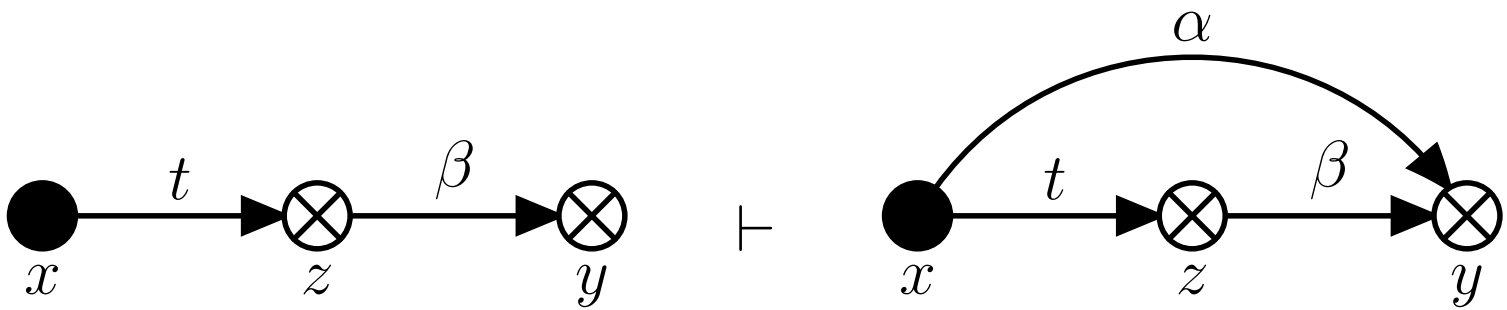
The set $\{t, g, r, w\} \in R$ of rights has special semantics which we describe next.

Take Rule

Let x, y, y be distinct vertices with x being a subject. Let $\alpha \subseteq \beta$ be a set of rights. Let there be an edge from x to z labeled γ with $t \in \gamma$. Then

$$x \text{ takes } (\alpha \text{ to } y) \text{ from } z$$

produces a new graph as shown below

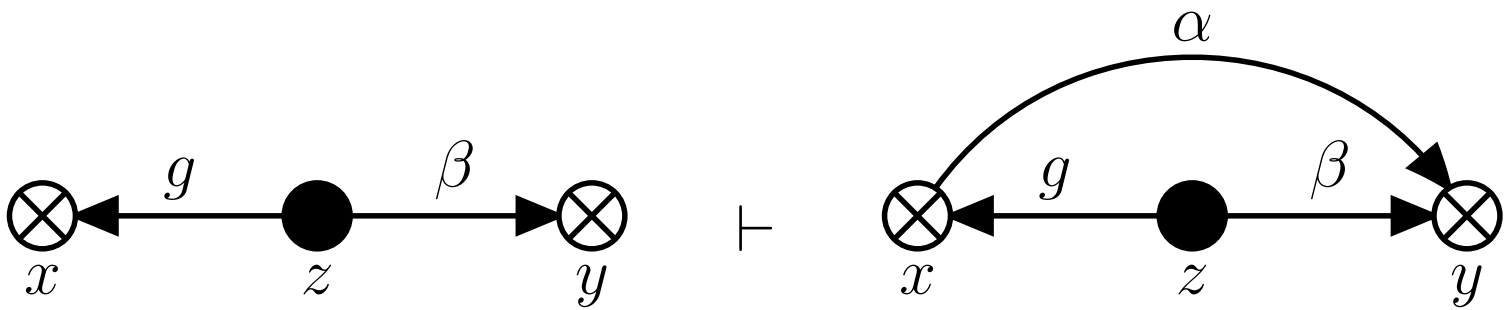


Grant Rule

Let x, y, y be distinct vertices with z being a subject. Let $\alpha \subseteq \beta$ be a set of rights. Let there be an edge from z to x labeled γ with $g \in \gamma$. Then

$$z \text{ grants}(\alpha \text{ to } y) \text{ to } x$$

produces a new graph as shown below



Create Rule

Let x be a subject in the protection graph and let $\alpha \in R$.

$$x \text{ creates } (\alpha \text{ to new vertex}) \; y$$

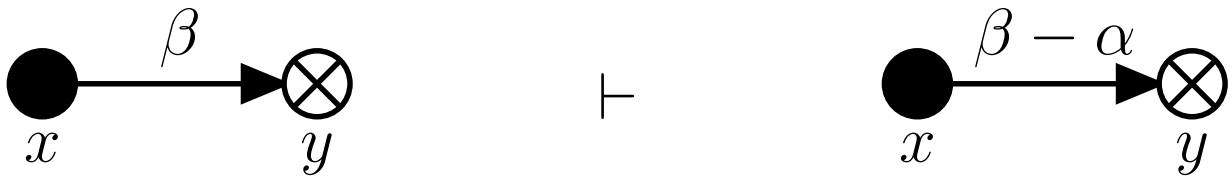
defines a new graph with an added vertice y and an edge from x to y labeled α, as shown below

Remove Rule

Let x, y be distinct vertices in a protection graph such that x is a subject. Let there be an explicit edge from x to y labeled β and let $\alpha \in \beta$.

$$x \text{ removes } (\alpha \text{ to }) \ y$$

defines a new graph by deleting α from β as shown below



If $\beta - \alpha$ is empty then the edge is deleted.

Rules Summary

The take and grant model has four *de jure* rules:

$$x \text{ takes } (\alpha \text{ to } y) \text{ from } z$$
$$x \text{ grants}(\alpha \text{ to } y) \text{ to } z$$
$$x \text{ creates } (\alpha \text{ to new vertex}) \ y$$
$$x \text{ removes } (\alpha \text{ to }) \ y$$

Remeber that **only subjects can act** i.e., in all rules, x is a subject. We need this later in the proofs.

Safety

We are again interested in the question of safety.

One concrete question to start with is, given a protection graph G, can a vertex x obtain α rights over another vertex y?

Sharing of Rights

Definition (can • share)

The predicate can • share(α, x, y, G_0) is true for rights α and vertices x, y in G_0 iff there exists a sequence $G_1 \ldots G_n$ 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 α.

To establish the conditions under which this theorem holds we need a few definitions and intermediate steps.

Definitions

Definition (tg-path)

A tg-path is a nonempty sequence $v_0 \dots v_n$ of distinct vertices such that v_i is connected to v_{i+1} for $0 \leq i < n$ by an edge with a label containing t or g.

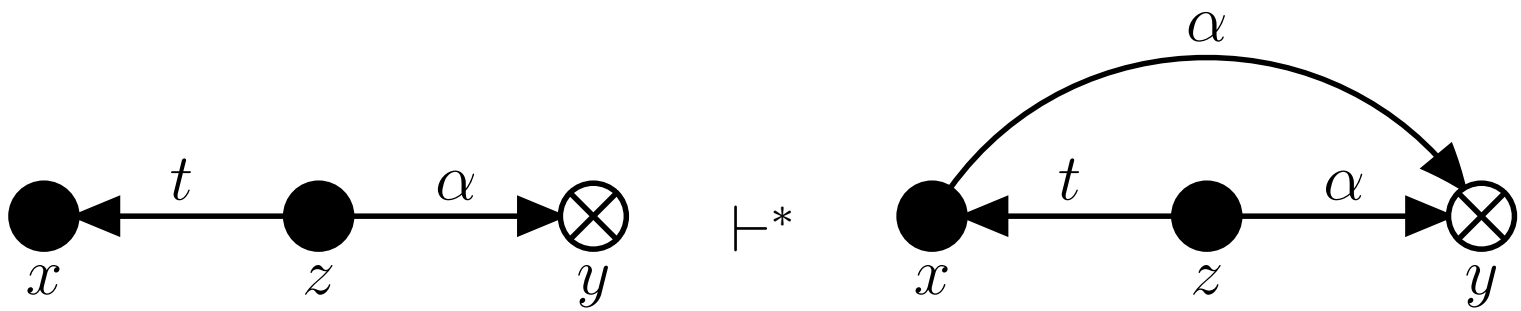
Definition (tg-connected)

Two vertices are tg-connected iff there is a tg-path between them.

Lemma 1

We can prove that any two subjects with a tg-path of length 1 can share rights. Four paths are possible and the *de jure* rules cover two of them.

Here is another one.

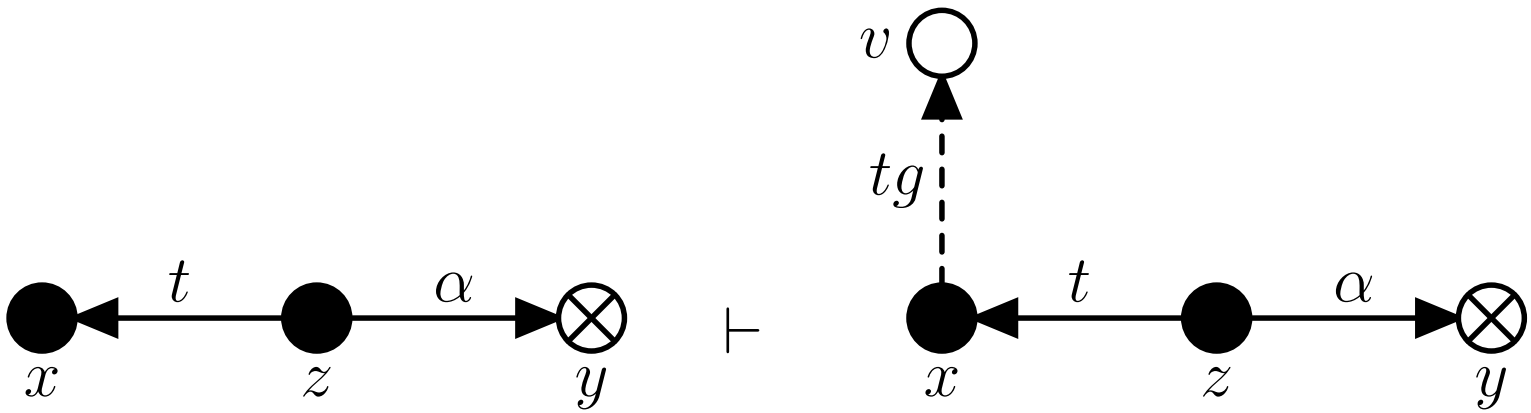


We prove this as a Lemma, next.

Proof of Lemma 1

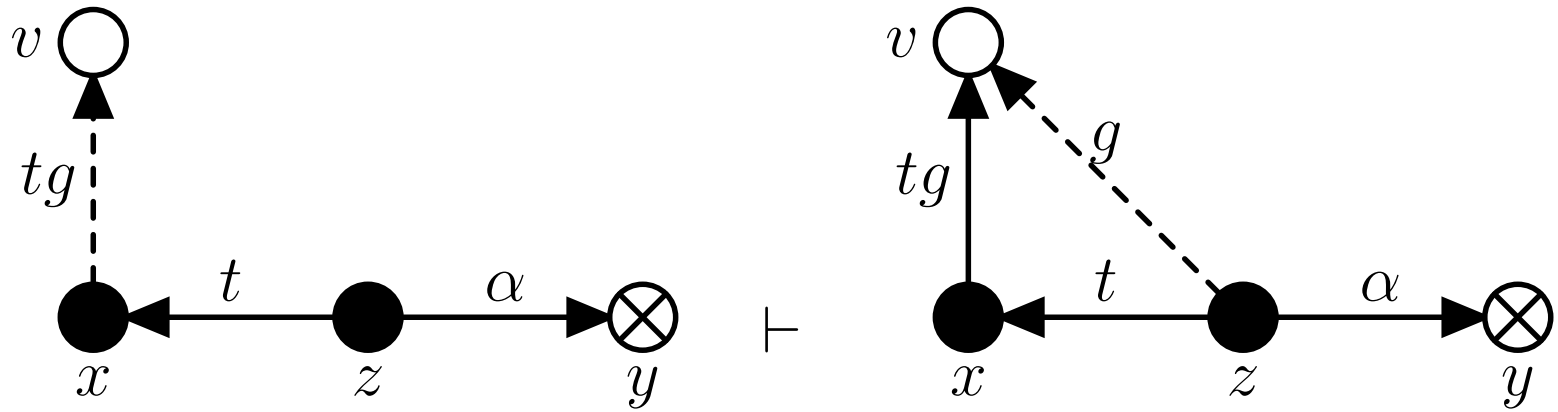
For ease of understanding, new edges are drawn as a dashed line when they are introduced.

x creates (tg to new vertex) v



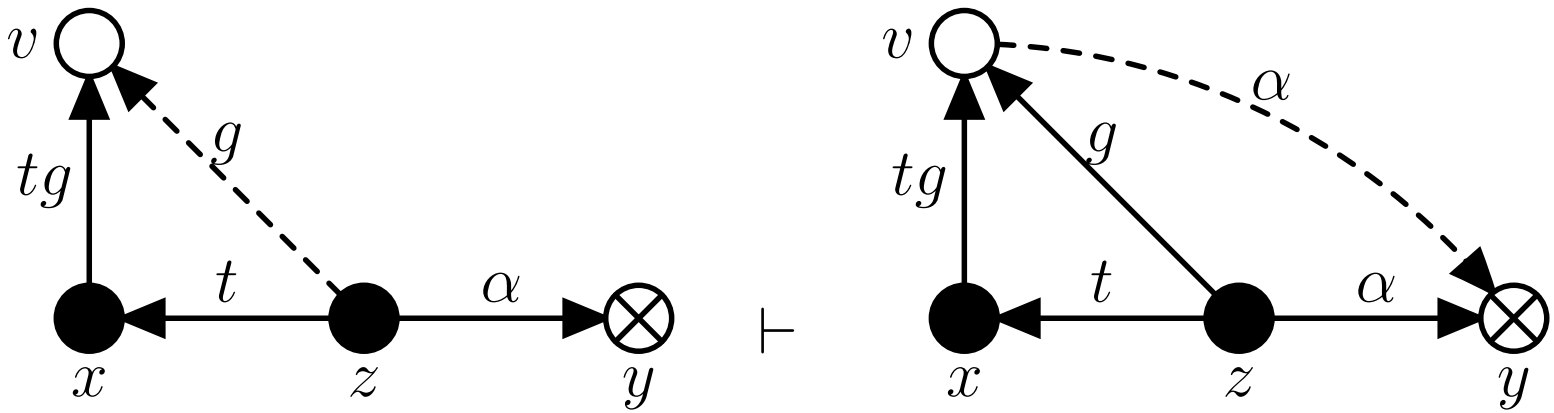
Proof of Lemma 1

z takes (g to v) from x



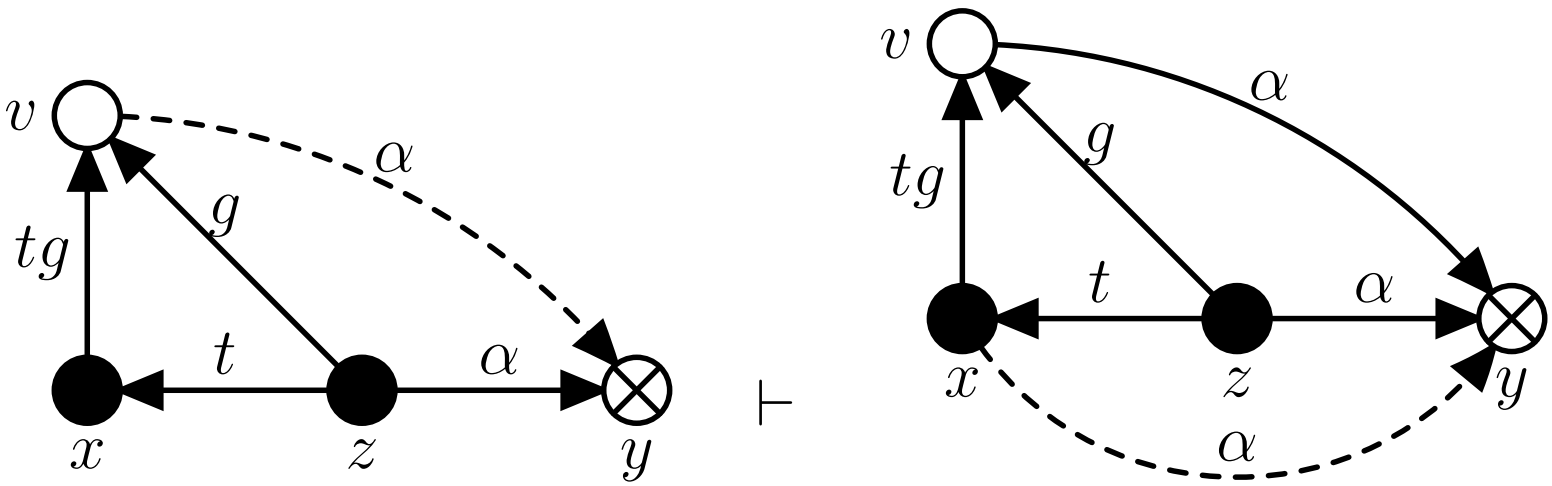
Proof of Lemma 1

z grants (α to y) to v



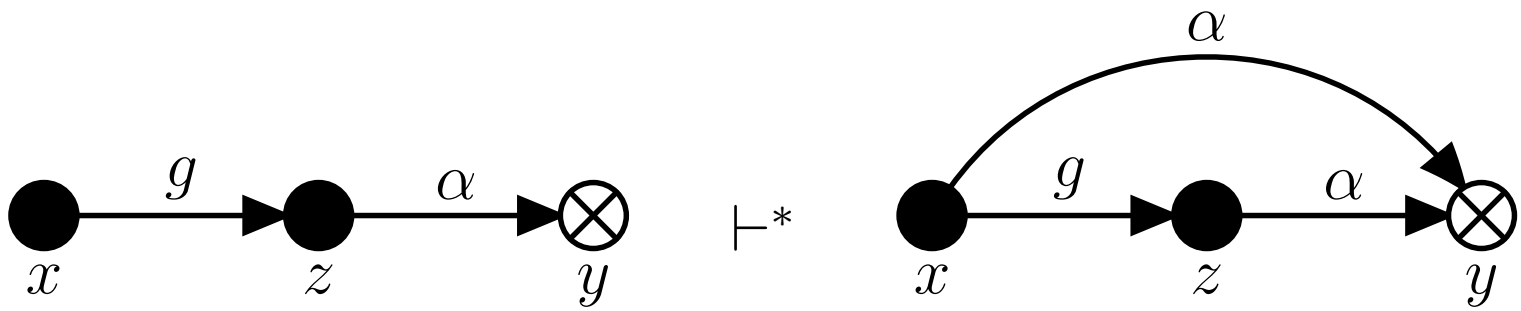
Proof of Lemma 1

x takes (α to y) from v



Lemma 2

In a similar fashion, the following Lemma can be shown



Can you do it?

Lemma 2

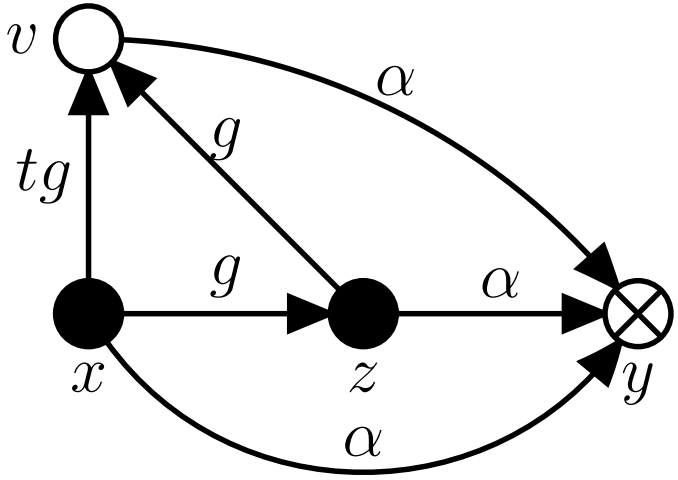
Answer

x creates (tg to new vertex) v

x grants(g to v) to z

z grants(α to y) to v

x takes (α to y) from v



Definitions

Definition (Island)

An *island* is a maximal tg-connected subject-only subgraph.

Corollary

Within an island, any right possessed by any vertex can be shared with any other vertex in the island.

Proof sketch: We know this is true for a tg-connected path of length 1. An induction can show that it is also true for paths of length $n > 1$.

Definitions

What if there are objects in between subjects?

Definition (Bridge)

A *bridge* is a tg-path with endpoints v_0 and v_n both subjects and the path's associated word is in $\{\overleftarrow{t_*}, \overrightarrow{t_*}, \overrightarrow{t_*}\,\overrightarrow{g}\,\overleftarrow{t_*}, \overrightarrow{t_*}\,\overleftarrow{g}\,\overleftarrow{t_*}\}$.

Note: All we need are bridges that are not islands.

Note: Since v_0 and v_n are subjects they can transfer rights from one endpoint to the other.

Sharing of Rights

Theorem (Subjects can share)

The predicate subject • can • share(α, x, y, G_0) *is true iff* x, y *are subjects and there is an edge from* x *to* y *in* G_0 *labeled* α*, or if the following hold simultaneously:*

1. *There is a subject* $s \in G_0$ *with an edge to* y *labeled* α*;*
2. *There exist islands* $I_1 \ldots I_n$ *such that* x *is in* I_1*,* s *is in* I_n*, and there is a bridge from* I_i *to* I_{i+1} *for* $1 \leq i < n$*.*

Question: If we show this, are we done yet?

Sharing of Rights

Because **subjects can act** and **objects cannot**, we need to cover the case that the transfer begins with a right possessed by an object and concludes by giving that right to another object.

Definitions

Definition

A vertex x *initially spans* to y if x is a subject and there is a tg-path between x and y with an associated word in $\{\overrightarrow{t_*}\,\overrightarrow{g}\,, \nu\}$.

Definition

A vertex x *terminally spans* to y if x is a subject and there is a tg-path between x and y with an associated word in $\{\overrightarrow{t_*}\,, \nu\}$.

Sharing of Rights

Theorem (Can share)

The predicate can • share(α, x, y, G_0) *is true iff there is an edge from* x *to* y *in* G_0 *labeled* α*, or if all following hold:*

1. *There exists* $s \in G_0$ *with an edge to* y *labeled* α*;*
2. *There is a subject vertex* $x' \in G_0$ *such that* $x' = x$ *or* x' *initially spans to* x*;*
3. *There is a subject vertex* $s' \in G_0$ *such that* $s' = s$ *or* s' *terminally spans to* s*;*
4. *There exist islands* $I_1 \ldots I_n$ *such that* x' *is in* I_1*,* s' *is in* I_n*, and there is a bridge from* I_i *to* I_{i+1} *for* $1 \leq i < n$*.*

Sharing of Rights

The proof is rather straightforward by showing for all four conditions that rights can be passed.

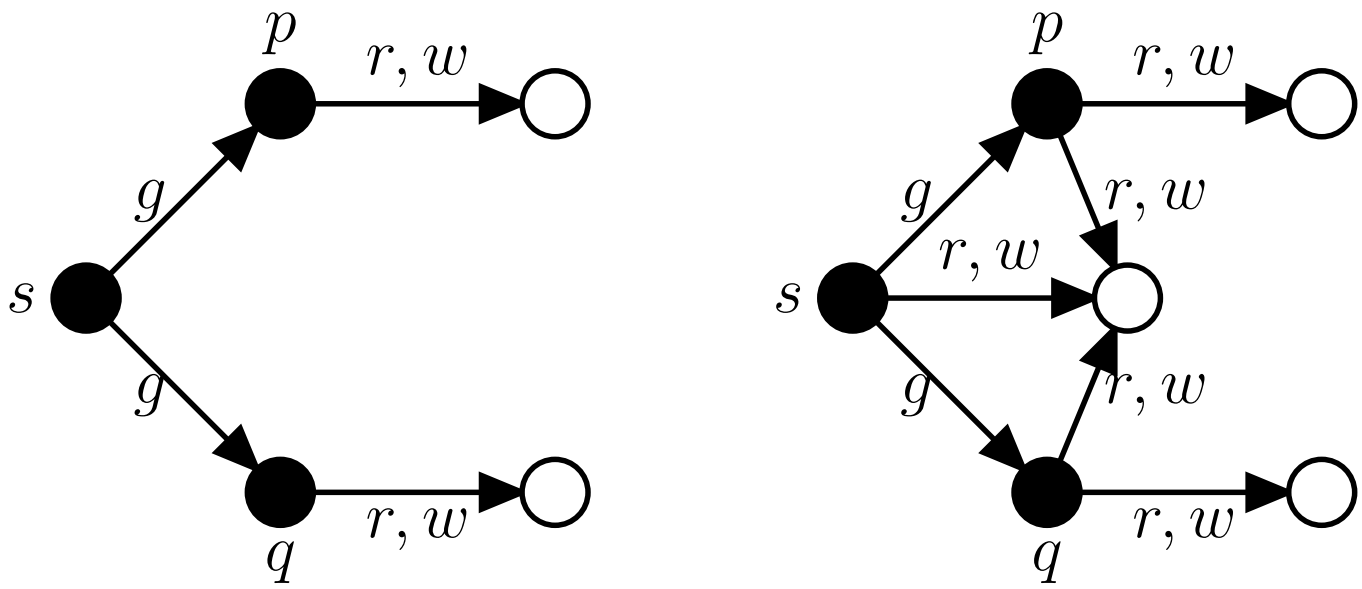
Corollary

There is an algorithm of complexity $O(|V| + |E|)$ *that tests the predicate can* $\bullet$ *share, where* V *is the set of vertices and* E *is the set of edges, in* G_0.

The algorithm finds a path between x and y and verifies that it matches the conditions.

Example

Suppose that two processes p and q communicate through a buffer b controlled by a trusted entity s. Each process has its own private information e.g., files u and v.



Example

Other notions of safety that were explored in this model:

- *Theft* (no owner of any right over an object grants that right to another)
- *Conspiracy* (what is the minimum number of actors necessary to transfer a right?)
- *Information flow* (Where can information go if no rights are transferred?)

Any questions?