TECHNISCHE UNIVERSITÄT DRESDEN

Department of Computer Science, Institute for System Architecture, Operating Systems Group

Paper Reading Group:

The Transfer of Information and Authority in a Protection System – Matt Bishop

Marcus Völp

Context

- `71 Butler Lampson:
  - Definition of Access Control Matrix
- `76 Harrison, Ruzzo, Ullman:
  - In the most general abstract case, security (leakage) is undecidable.
- `76 Jones, Lipton, Snyder:
  - Specific system in which leakage is decidable in linear time:
    - Take-Grant Protection Model
- **`79 Bishop, Snyder:**
  - De Facto leakage in the take grant model

- `84 Bobert, Karger: Unmodified capability systems cannot enforce * property (no write down)
- `88 Karger: Unmodified capability system cannot enforce confinement

A short side track – Undecidablility of Leakage

Idea: Implement Turing Machine with general ACM; Reduction to Halting Problem

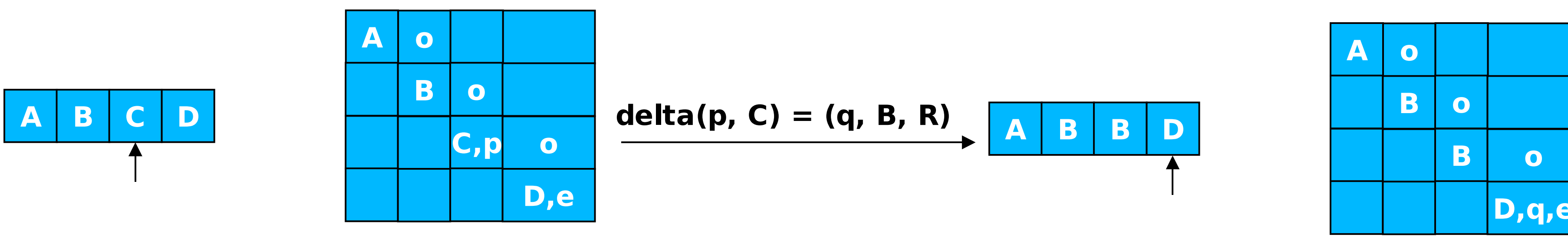
Turing Machine:

- K – States (p, q, ...)
- M – Type Symbols (A, B, ...)
- delta – Transition Function: K x M -> K x M x {L,R}

Subjects si = Cells of Tape

Access Rights:

- Type Symbols as Access Rights in si x si
- own in si+1 x si
- States as Access Rights in si x si iff head is at cell i



if own **in** a[si, si+1] **and** p **in** a[si, si] **and** C **in** a[si, si]
    delete p from a[si, si];
    delete C from a[si, si];
    enter B into a[si, si];
    enter q into a[si+1, si+1]

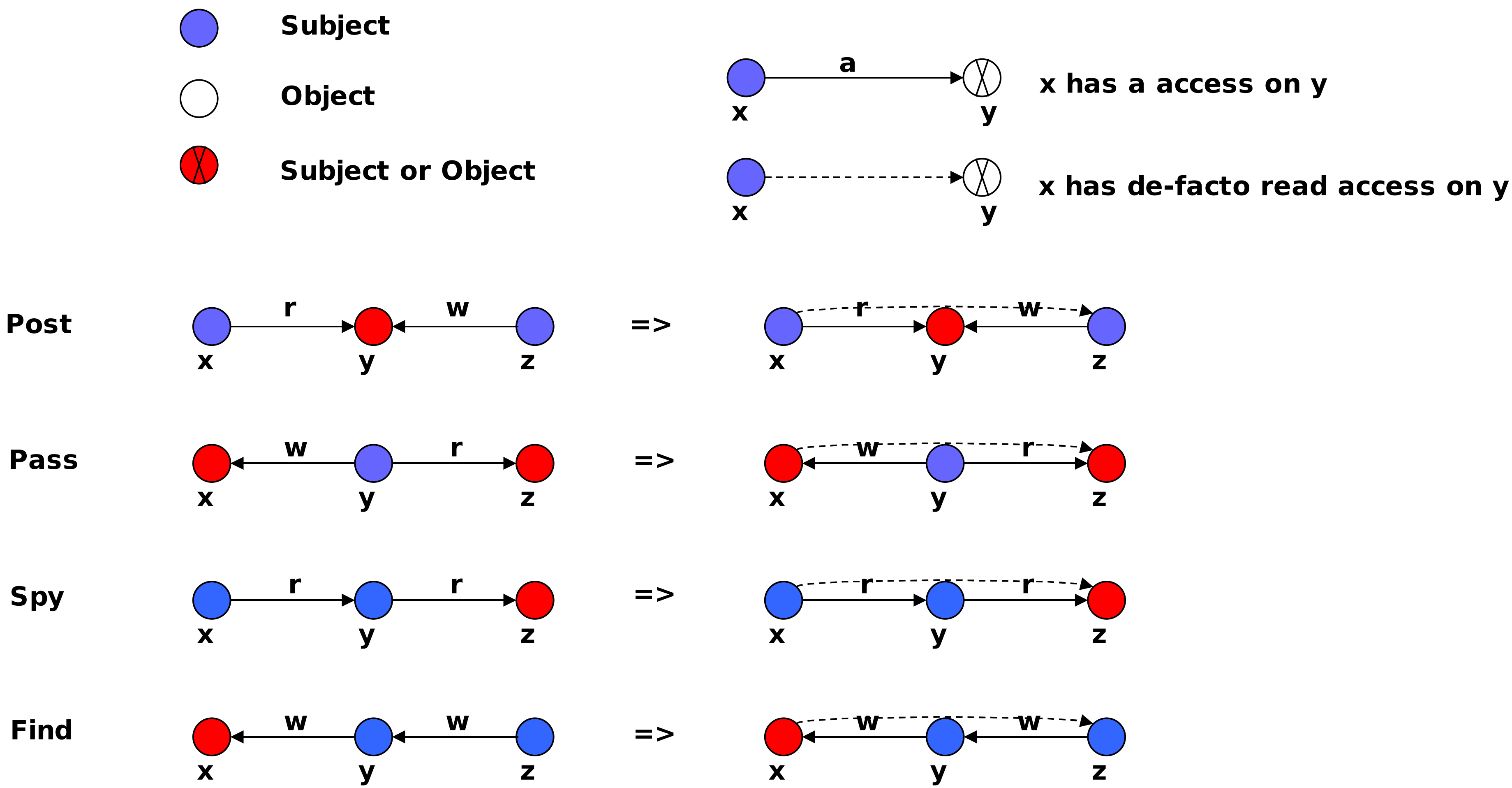
De facto vs. De Jure

- De Jure:
  - Obtain permissions to read an object

- De Facto:
  - Effectively read the content of an object

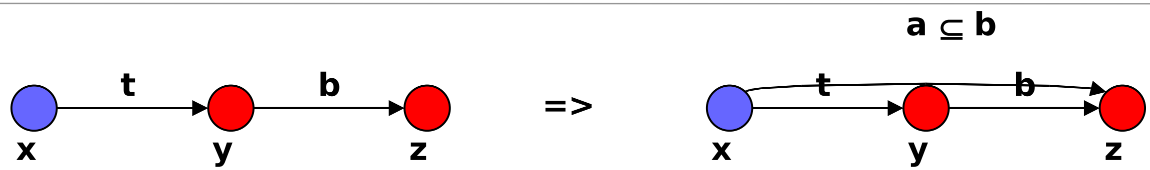
    - De jure => de facto
    - De jure gives right to obtain up-to-date information
    - De facto relies on transmitting agents
      (de jure in general also but only to obtain the right)

De facto rules

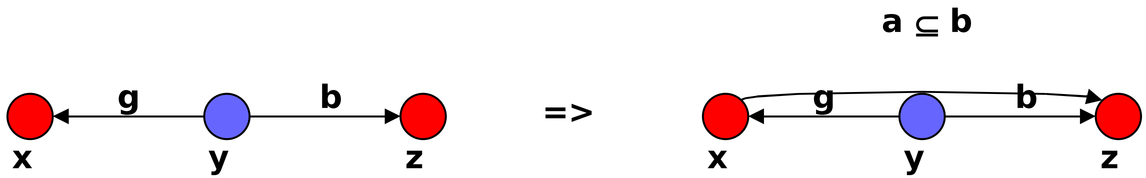


De jure rules

Take



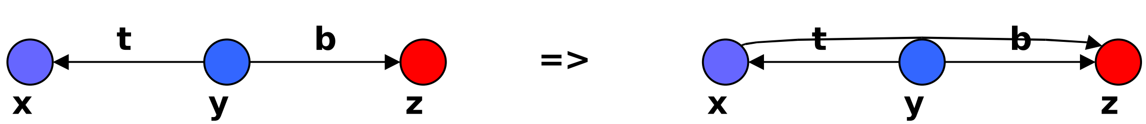
Grant

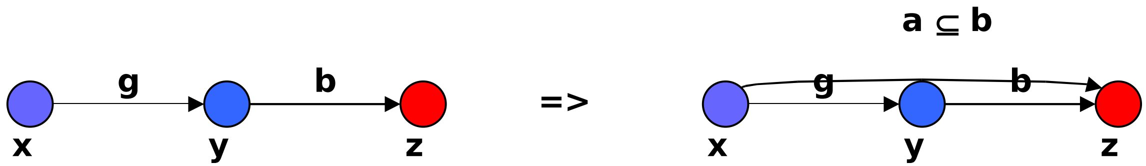


Create

Remove

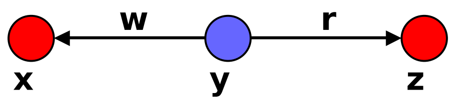
Sharing of Rights



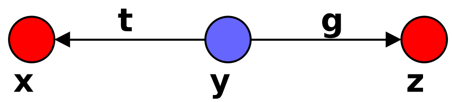


Paths, Spans, Islands, Bridges, Thiefs

- **RW-Path** – Sequence of vertices v0 ... vk; vi -> vi+1; r or w in Label(ei)



- **TG-Path**:



- De Facto Predicate:
  - p **can know** q in G0 ⇔
    - Exists Sequence of Graphs G1 ... Gn with

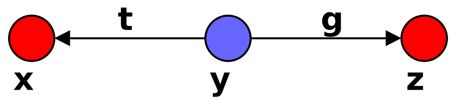
      DF
      Gi |- Gi +1

    - De Facto Edge p -> q in Gn
  - **admissible RW Path**
    - associated word ($\overrightarrow{r}$ u $\overleftarrow{w}$)* and
    - ai = $\overrightarrow{r}$ => vi-1 is subject; ai = $\overleftarrow{w}$ then vi is subject

<u>Can know ⇔ Exists admissible RW path</u>

Paths, Spans, Islands, Bridges

- **TG-Path**:



- **Island**
  - Maximal tg-conntected; subject only subgraph

- **Spans / Bridges**
  - v0 subject
    - initial span: $\{\vec{t}^{*}\,\vec{g}\}$ u {e}
    - terminal span: $\{\overleftarrow{t}^{*}\}$
    - bridge: $\{\vec{t}^{*}, \overleftarrow{t}^{*}, \vec{t}^{*}\vec{g}\overleftarrow{t}^{*}, \vec{t}^{*}\overleftarrow{g}\overleftarrow{t}^{*}\}$ and vk is subject

- De Jure Theorem:
  - p **can share** a with q in G0 ⇔
    - Exists s in G0 with s-to-q edge labeled a
    - Exist subject vertices p‘ and s‘ such that
      - p‘ initially spans to p
      - s‘ terminally spans to s
    - Exists islands I1, .. Iv‘
      - p` in I1, s‘ in Iv
      - Bridge from Ij to Ij+1

Thiefs

- **can share** relies on witness subjects in the Islands
- Can x obtain a even if some subjects don‘t cooperate?
- x **can steal** a on y in G0
  - Property:
    - No edge x to y labeled a
    - Sequence G1, ... Gn; x –a-> y in Gn
      - Gi |-pi- Gi+1
      - Forall vertices v, w in Gi-1

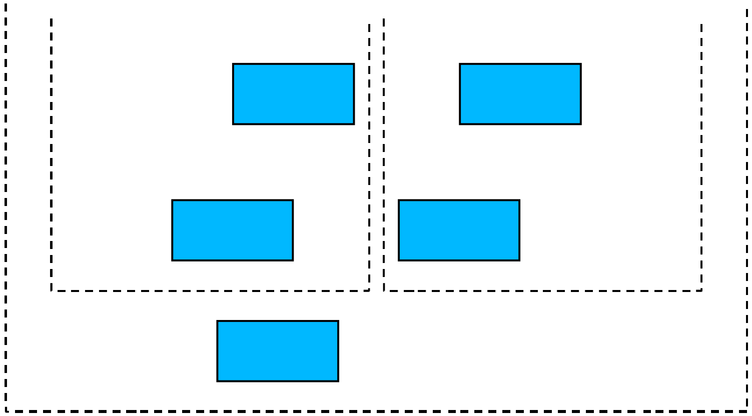
        Exists v-to-y in G0 labeled a =>

        pi is not: v grants (a on y) to w
  - Theorem:
    - there is no edge from x to y labeled a in G0
    - Exists subject x‘: x = x‘ or x‘ initially spans to x
    - Exists vertex s with edge labeled a to y in G0 and for which **can share** (t, x, s, G0) holds.

Stars and Confinement

- * property – no writes to lower objects

- Confinement
  - Shapiro: Confined process should not be able to affect any non-authorized entities outside confinement boundary.



  - No take outside confinement boundary
    (EROS: weak attribute allows take of read only, caps)

  - Parent does not grant into confinement

The End

- **I like this stuff:**
  !!! Weird Math by Drawing Pictures !!!

- Things to Discuss / Open Issues from my point of view
  - How do Confinement, de Facto Knowledge and Noninterference interact?
  - More on trusted servers
    - How to formulate proper object reuse:
      Grant access to C2 after access is being revoked from C1.
  - Security / Resource Policies based on Identity
    - Do we need them?
    - Can we build a pure capability system?
      - No quotas but caps on resources
      - No names
      - Everything is authorized through capabilities