**Bài 1:** *(2điểm)* Alice và Bob sử dụng giao thức sau đây để trao đổi khóa/thông điệp cho nhau:

1. Alice gửi cho Trent: Alice, Bob, {K}KAT
2. Trent gửi cho Bob: Alice, Bob, {K}KBT
3. Bob gửi cho Alice: {Hi, Alice. I am Bob}K

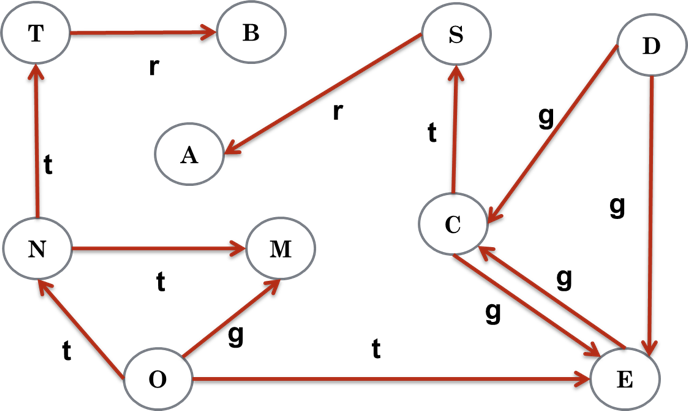
Giao thức trên có điểm yếu, anh/chị hãy đóng vai trò là Malice để đưa ra 2 phương pháp tấn công vào giao thức trên.

*Phương pháp 1:*

*Phương pháp 2:*

**Bài 2:** *(1điểm + 1điểm bonus)* Quản lý truy cập theo DAC dựa vào mô hình Take-Grant. Xét đồ thị sau

Trong đó: r là quyền read, t là quyền take, g là grant.

Giả sử rằng các subject ***không có quyền*** tạo ra các object/subject mới.

Sinh viên hãy trình bày các câu lệnh take và grant để trả lời các câu sau (Nếu câu trả lời là ***không thể*** hãy giải thích ngắn gọn)

1. M có đọc được B không?

1. E có đọc được A không?

1. D có đọc được A không?

1. N có đọc được A không ?

# BÀI TẬP (2đ)

* 1. **[Bắt buộc]** Trạng thái hiện tại của hệ thống được biểu diễn bằng *mô hình Take-Grant* bên cạnh. Cho biết mọi *subject s* trong hệ thống đều có quyền tạo *object o* với lệnh **create objectp {s, o}** và **s** sẽ có tập quyền **p** trên **o**, với *p = {take, grant, read, write*}. Hãy viết các lệnh để E có được quyền write trên A. **(1đ)**

Đáp án:

1. Grant (w, B, C, A) (hoặc Take (w, C, B, A)).
2. Create objectp {E, O}.
3. Take (g, C, E, O).
4. Grant (w, C, O, A).
5. Take (w, E, O, A).
   1. Cho ***quan hệ đa mức*** Employee như bảng dưới:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Name** | **CName** | **Department** | **CDepartment** | **Salary** | **CSalary** | **TC** |
| Bob | S | Dept1 | S | 10K | S | S |
| Ann | S | Dept2 | S | 20K | TS | TS |
| Sam | TS | Dept2 | TS | 30K | TS | TS |

Trong quan hệ đa mức theo cơ chế bảo mật MAC, tác vụ UPDATE được thực hiện với quy luật sau:

* Mỗi dòng thỏa điều kiện UPDATE sẽ được thay bằng 1 dòng t’ được xác định như trong biểu thức (1).
* Đồng thời, để tránh convert channels, 1 dòng phụ t” **có thể** được thêm vào để che giấu những thay đổi này khỏi các user có mức bảo mật thấp hơn mức bảo mật của user thực hiện tác vụ UPDATE. Cụ thể hơn, dòng t” sẽ được thêm vào khi thuộc tính nằm trong mệnh đề SET có mức độ bảo mật thấp hơn mức độ bảo mật của user thực hiện tác vụ UPDATE. Dòng t” được xác định như trong biểu thức (2).

Trong đó,

* : thuộc tính với mức bảo mật tương đương là của dòng t.
* : giá trị mới thay thế cho thuộc tính
* : mức bảo mật của chủ thế thực hiện tác vụ UPDATE
* : mức độ bảo mật của khóa biểu kiến trong dòng t
* : mức độ bảo mật của thuộc tính trong dòng t1 user có mức độ bảo mật TS, thực hiện tác vụ UPDATE như bên dưới, hãy cho biết kết quả trả về *ở mức độ bảo mật TS:*

**UPDATE Employee**

**SET Department = “Dept1”**

**WHERE Name = “Ann”**

🡺 Kết quả trả về (ở mức độ bảo mật TS)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Name** | **CName** | **Department** | **CDepartment** | **Salary** | **CSalary** | **TC** |
| Bob | S | Dept1 | S | 10K | S | S |
| Ann | S | Dept1 | TS | 20K | TS | TS |
| Ann | S | Dept2 | S | - | S | S |
| Sam | TS | Dept2 | TS | 30K | TS | TS |