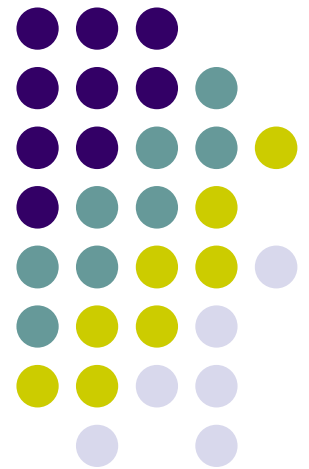
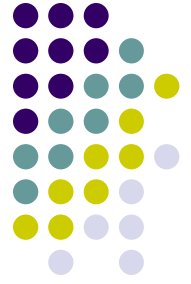


CS4236 Tutorial 8

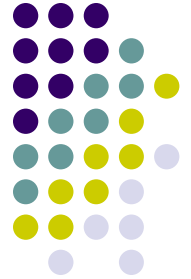
Question 2
By Cai Guan Yan





Question 2

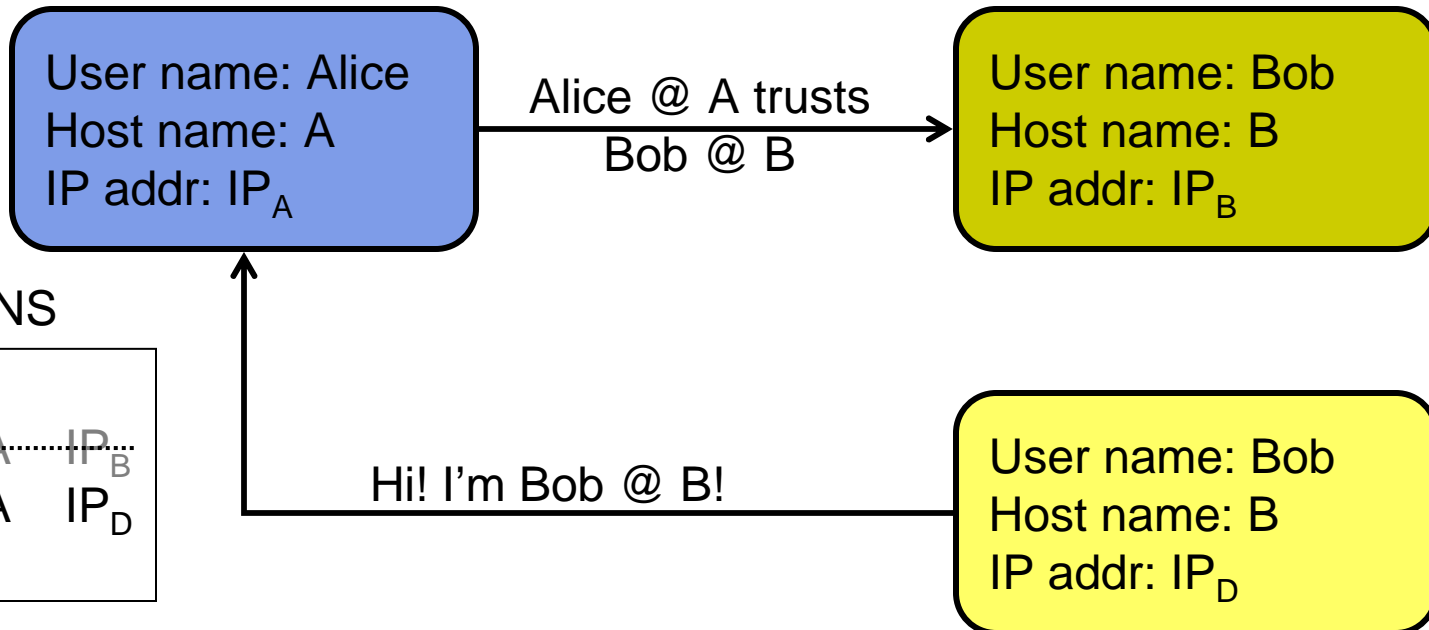
- Suppose that user applications did not establish ***trust relationships*** based on host names; rather they used IP addresses for describing trust relationships in their configuration files. **Would that prevent the kind of DNS attack described in class?** Why or why not? (1.5 marks)



DNS Attack mentioned in class

~alice/.rhosts

```
...  
B Bob  
...
```



Altered DNS

```
...  
B IN A IP_B  
B IN A IP_D  
...
```

rlogin, trust IP address helps



- For the issue with rlogin, trusting IP address may solve the problem
- Because the IP address uniquely identifies the host
- The solution is inelegant and problems are shown in page 30 of the following paper:
- Christoph Schuba, ***“Addressing the Weaknesses in Domain Name System Protocol”***, July 1993

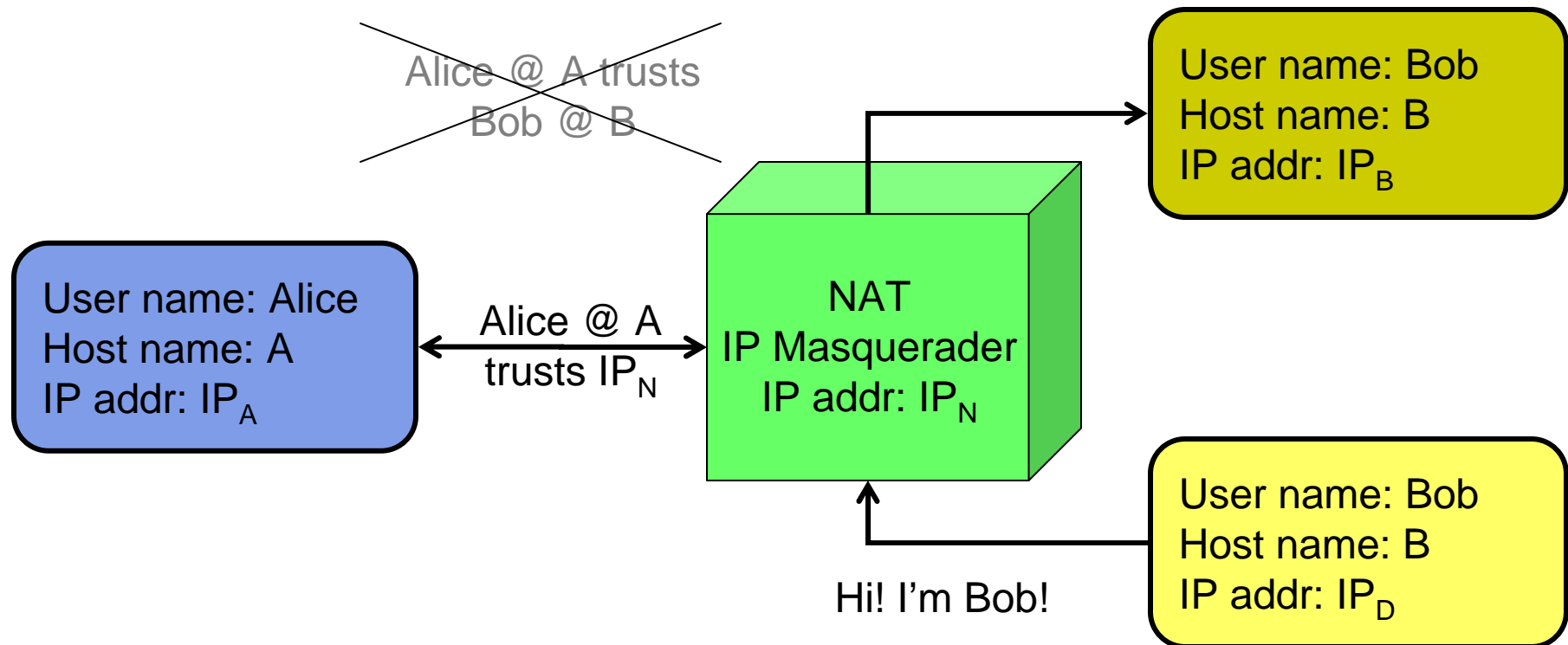


However...

- There are cases when the **IP address does not reflect the actual host**
- E.g. **IP masquerading** behind a Network Address Translator (NAT)



An attack based on IP address



!!! Problem with trusting hostname: trusting B \rightarrow trusting ~~IP_B~~ IP_D

!!! Problem with trusting IP address: trusting $IP_N \rightarrow$ trusting IP_B and trusting IP_D