Attack Trees

Matthew Edwards

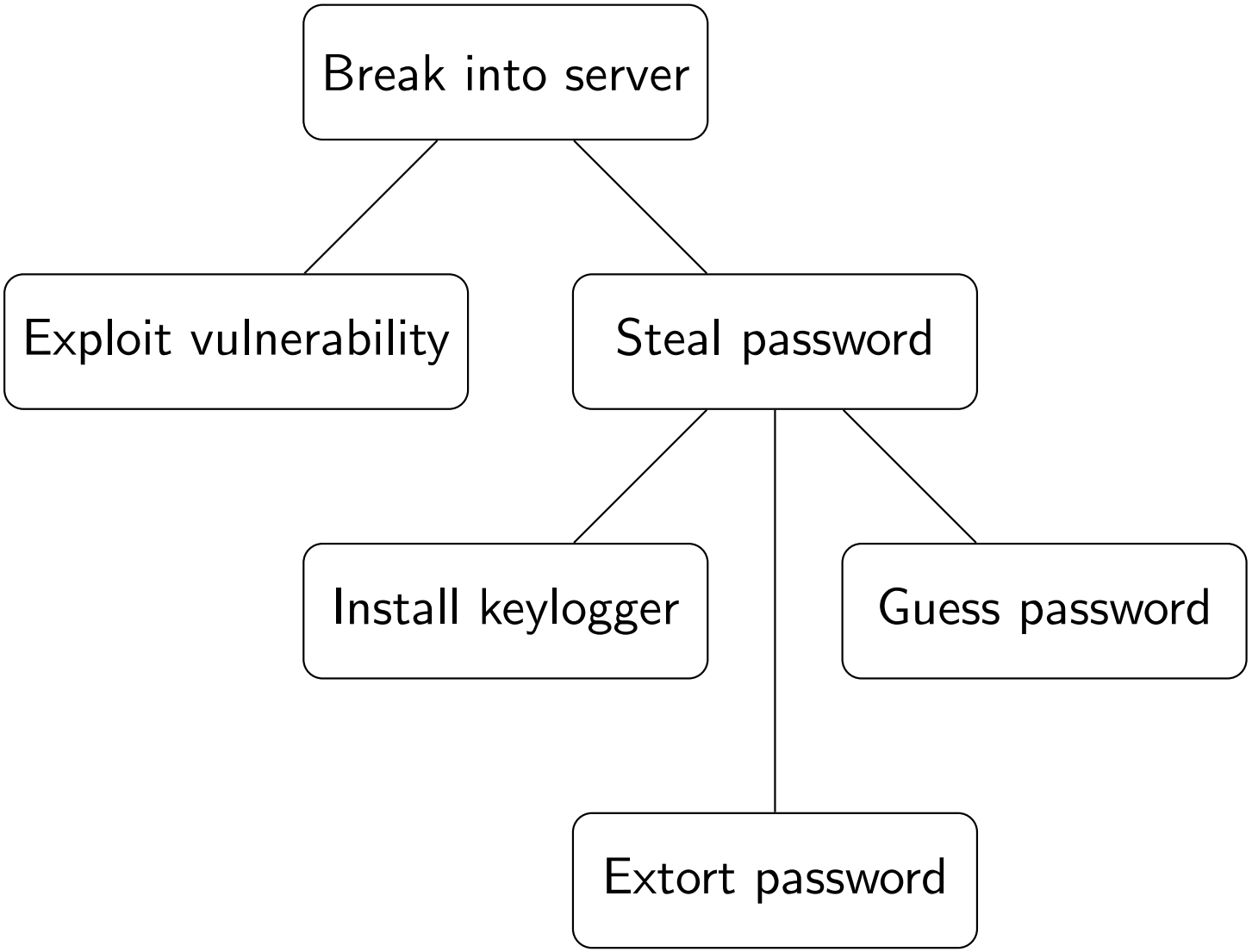
Focus: Threat Modelling

September 9, 2020

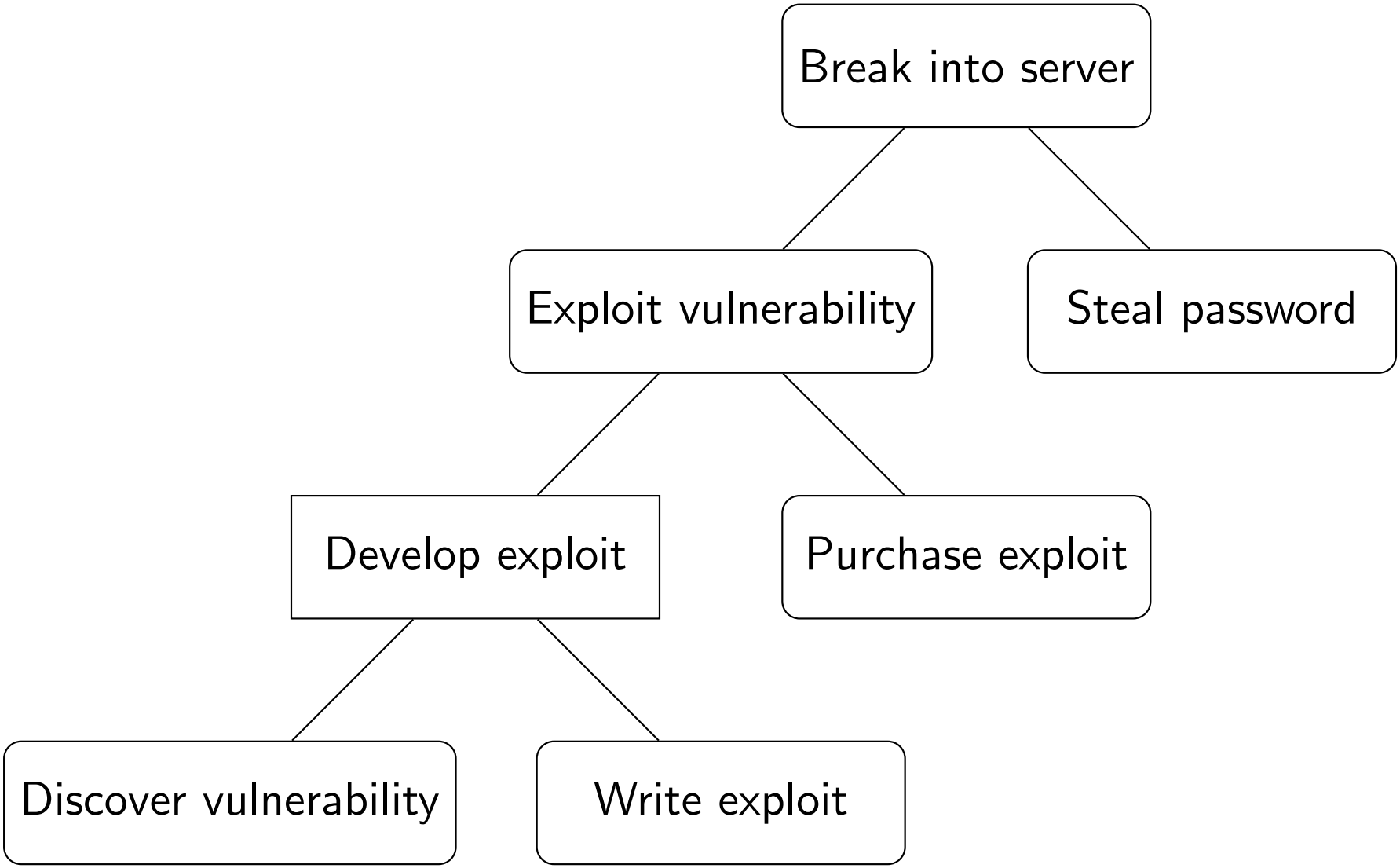
Improving on the cyber-killchain

One of the problems with the cyber-killchain is it can be too prescriptive, baking in assumptions about the attacker.
We sometimes need a more general, flexible model.
Enter: the **attack tree**.

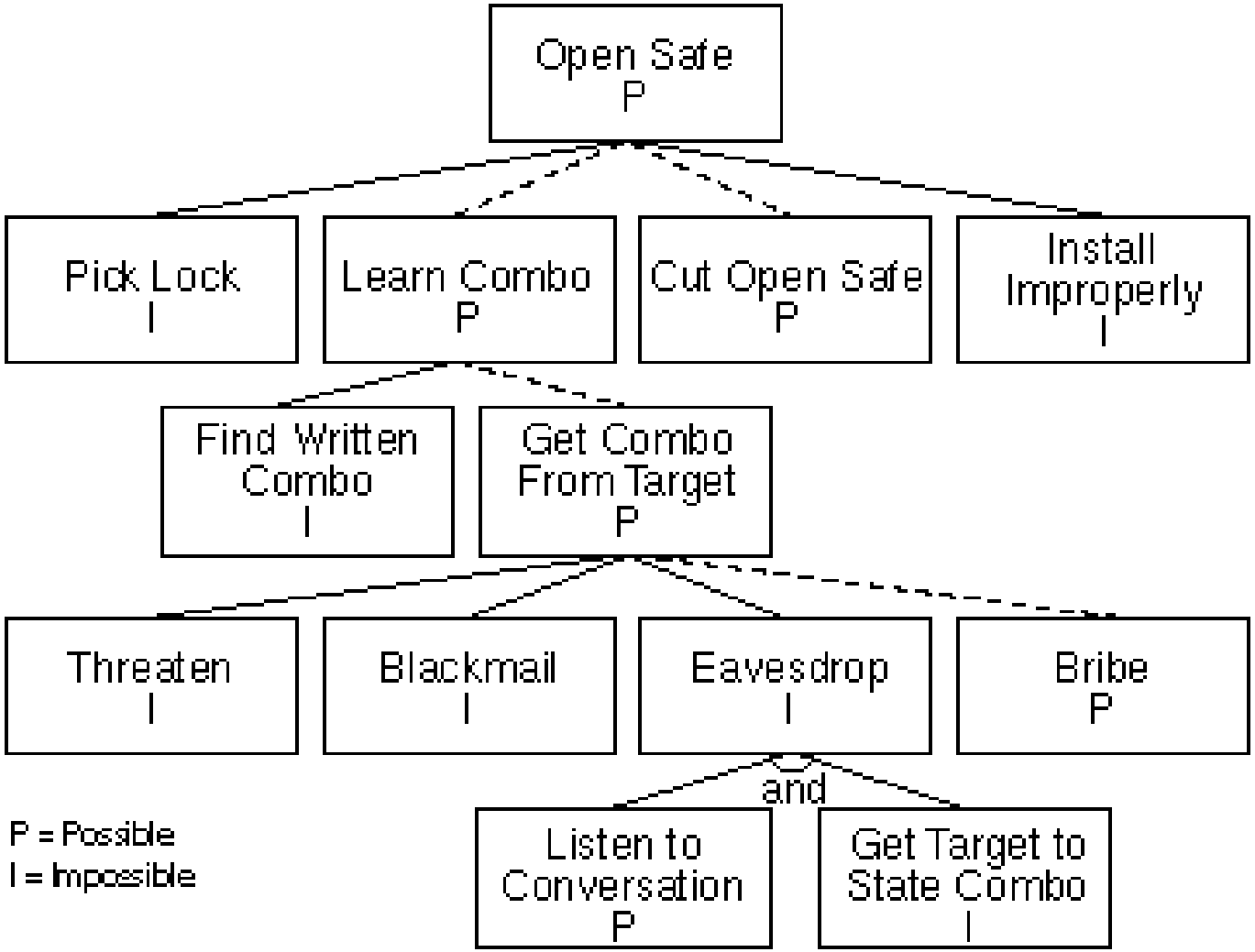
A simple attack tree



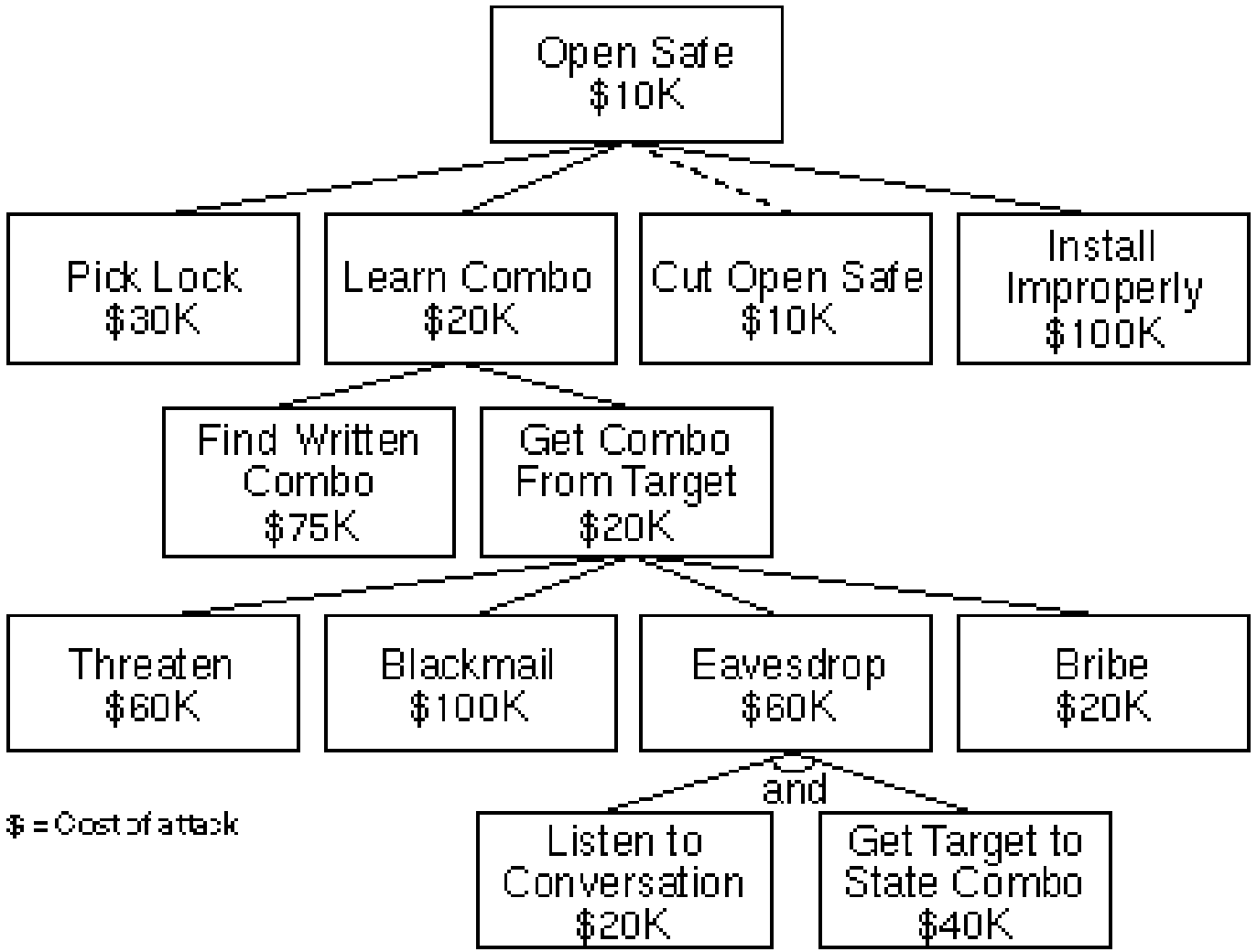
AND vs OR nodes



Annotating Trees



Continuous Annotation



What we need to know

About the attacker:

- What they want;
- The skills they have;
- The risks they are willing to take.

About our system:

- How it works;
- The ways it could fail.