Automated Generation of Attack Routes for Service Security Analysis – A Preliminary Report

Tong Li
Lin Liu
Tsinghua University

Golnaz Elahi
Eric Yu
University of Toronto

iStar 2010 - The 4th international i* workshop
Hammamet, Tunisia. June 7-8, 2010

Motivation & Approach

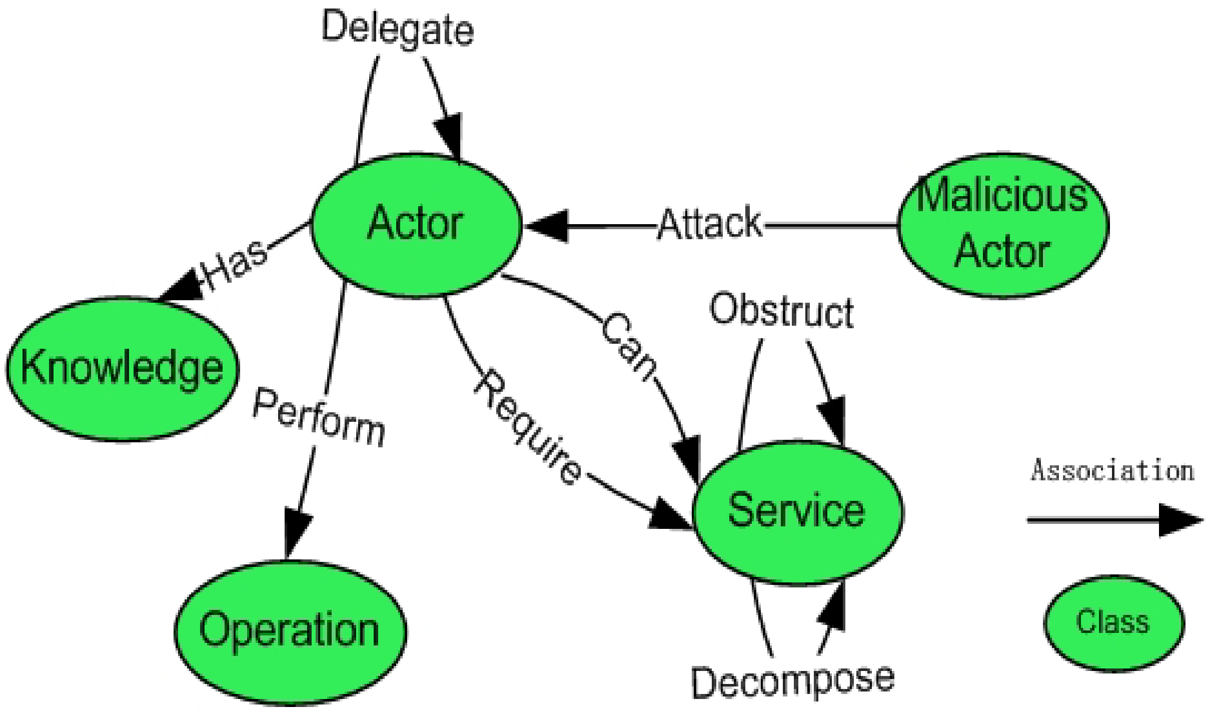
- In a service-oriented computing environment …
  - Services are constructed through composition and delegation
  - Risks arise due to compositions and delegations
  - Attackers can also use service composition and delegation
- Approach
  - Use agent-oriented modeling to represent the service environment, including attackers
  - Automatically generate all possible attack routes using a Knowledge Base and Rule Set
  - Prune attack routes space by
    - Evaluating their feasibility
    - Assessing attack costs, probability
  - Generate counter-measures to defend high-risk attack routes (future work)

Outline

- Motivations and Approach
- Service Security Modeling Framework
- Analysis Method
- Example
- Related Work
- Conclusion and Future Work

Service Security Modeling Framework (SSMF)

- Service Security extension of the i* framework



Security Related Concepts in SSMF

- A = set of actors
- S = set of services

- *$MA = \{m_1, \ldots, m_n\}$ is a set of Malicious Actors.*
- *$AT \subseteq MA \times S \times A$*, is a set of *Attack* relations.
- *$OB \subseteq S \times S$*, is a set of *Obstruct* relations.

Analysis Process

- Service environment modeling
- Attack goal identification
- Reasoning from attacker’s viewpoint *
- Attack identification and assessment

We focus on this step !!

- Focusing on Availability only

Rule Set

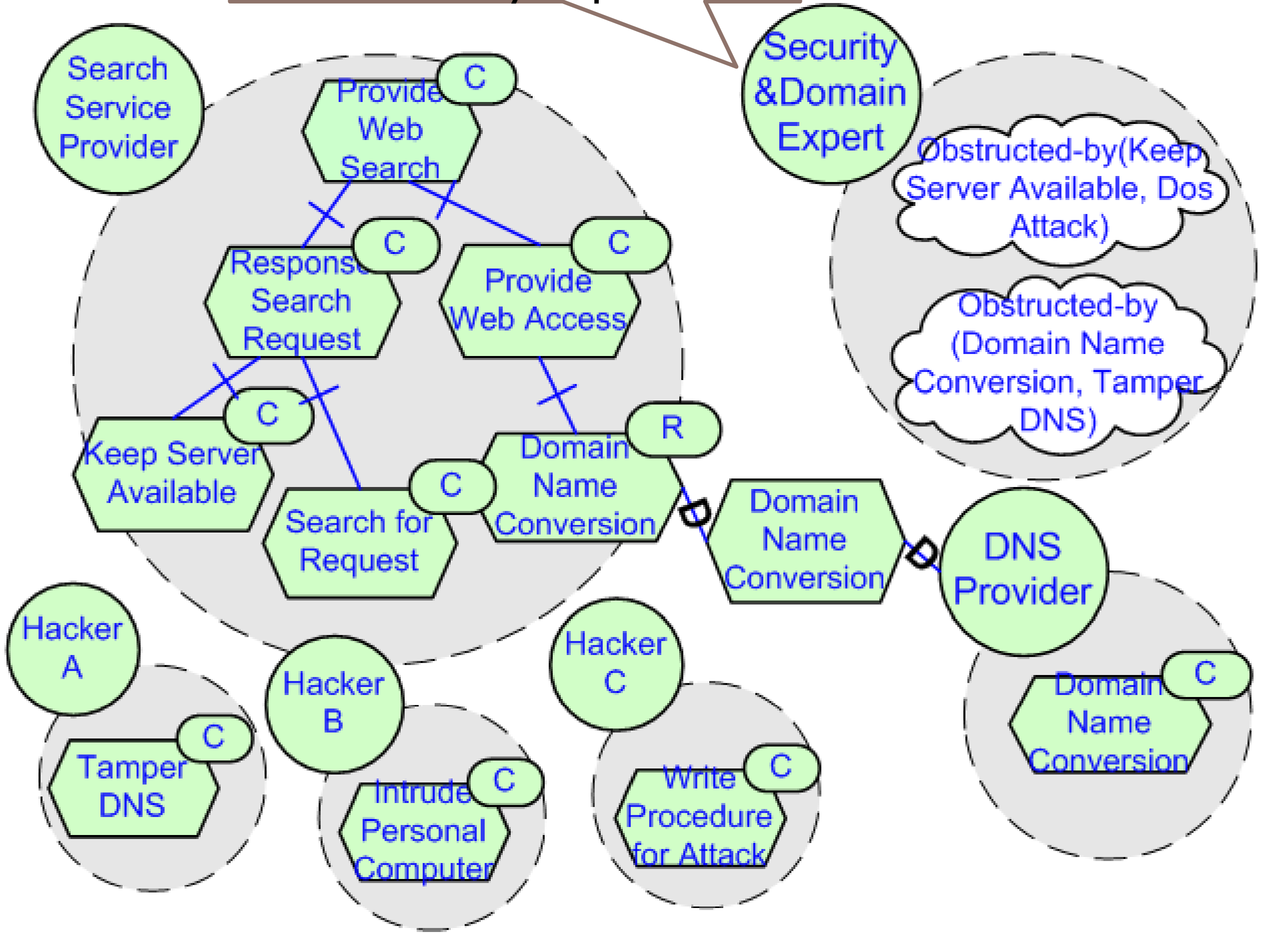
MActor(m) ∧Service(s) ∧Service(anti-s) ∧Service(os) ∧ require(m, anti-s) ∧ know(m, obstruct(s, os))
=> or-decomposition(anti-s, os) ∧ add(know(m, obstruct(s, os)), set)

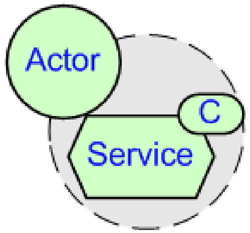
- Rule 1: Attack Strategy Identification
  - If the malicious actor knows about a service, like *os, which can obstruct the service s, then os is a* concrete way to accomplish "anti-s".
- Rule 2: Attack Decomposition
  - if his anti-service is not satisfied, he may decompose the anti-service into finer grained anti-services in the same way that the target actor decomposes the target service.
- Rule 3: Attack Delegation
  - If the attacker discovers that an actor in the service environment provides the required services that meet the attackers' requirements, he can delegate those services to the actors.
- Rule 4: Satisfaction Propagation
  - For or-decomposition: if one of the subservices has been satisfied, then the parent-service would be satisfied as well.
  - For and-decomposition, if all of the sub-services have been satisfied, then the parent-service would be satisfied.

A Web Attack Example

Modeling the Service Environment

That is the person who have relevant domain knowledge. Generally, he is a security expert.

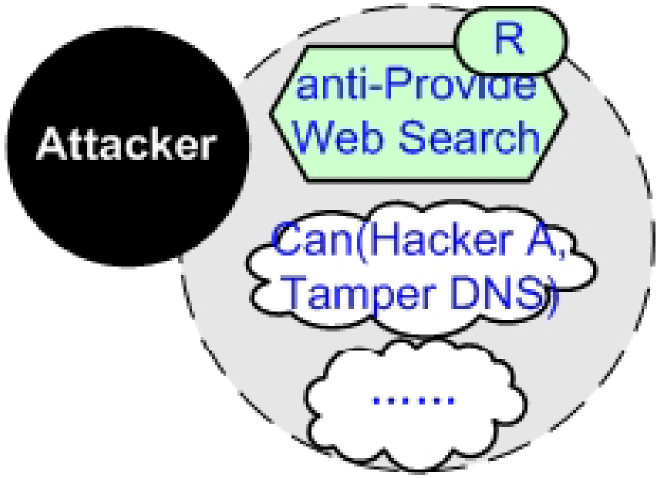


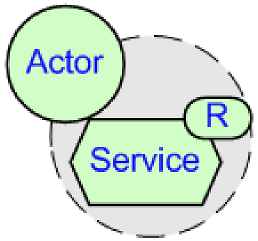


The actor can provide the service

Now consider the Attacker

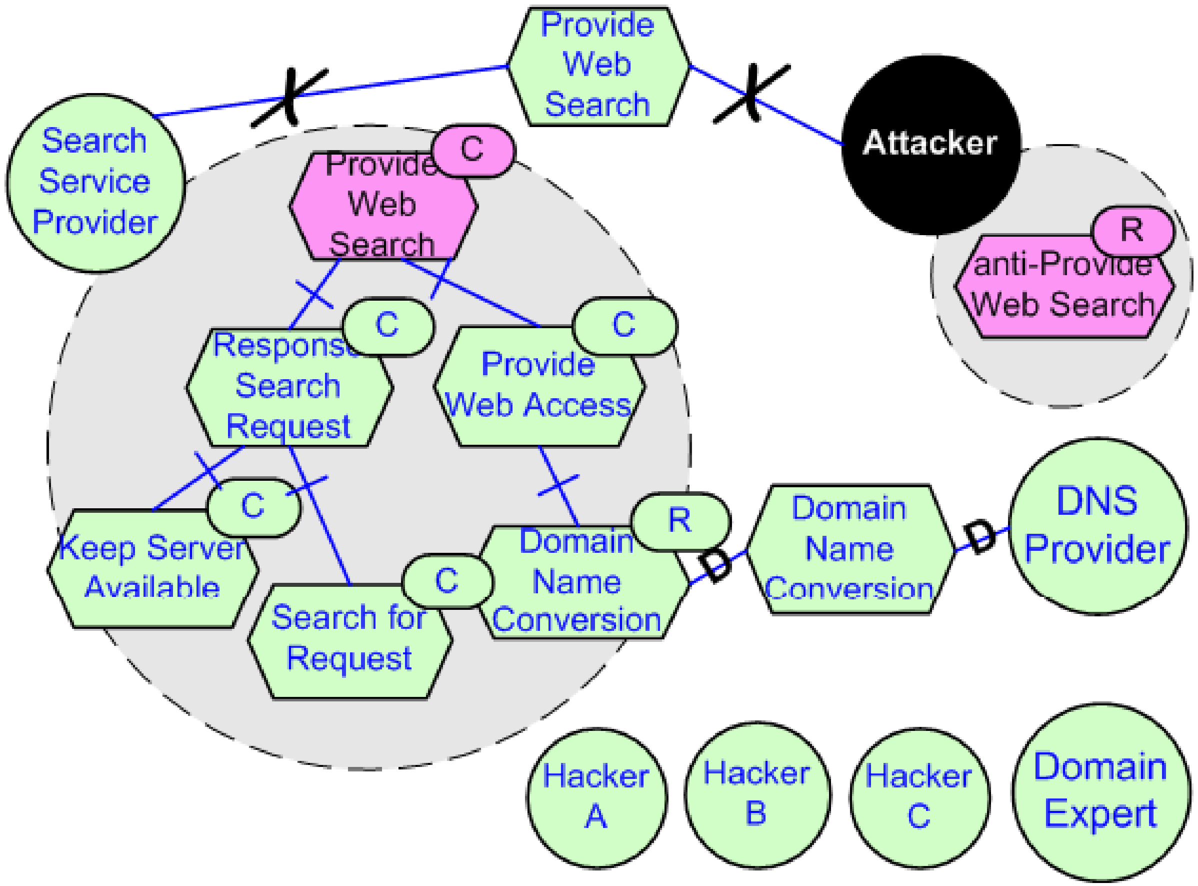
- Attack Goal Identification



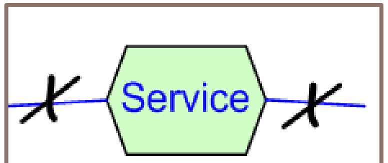


The actor requires the service

Reasoning from Attacker's Viewpoint

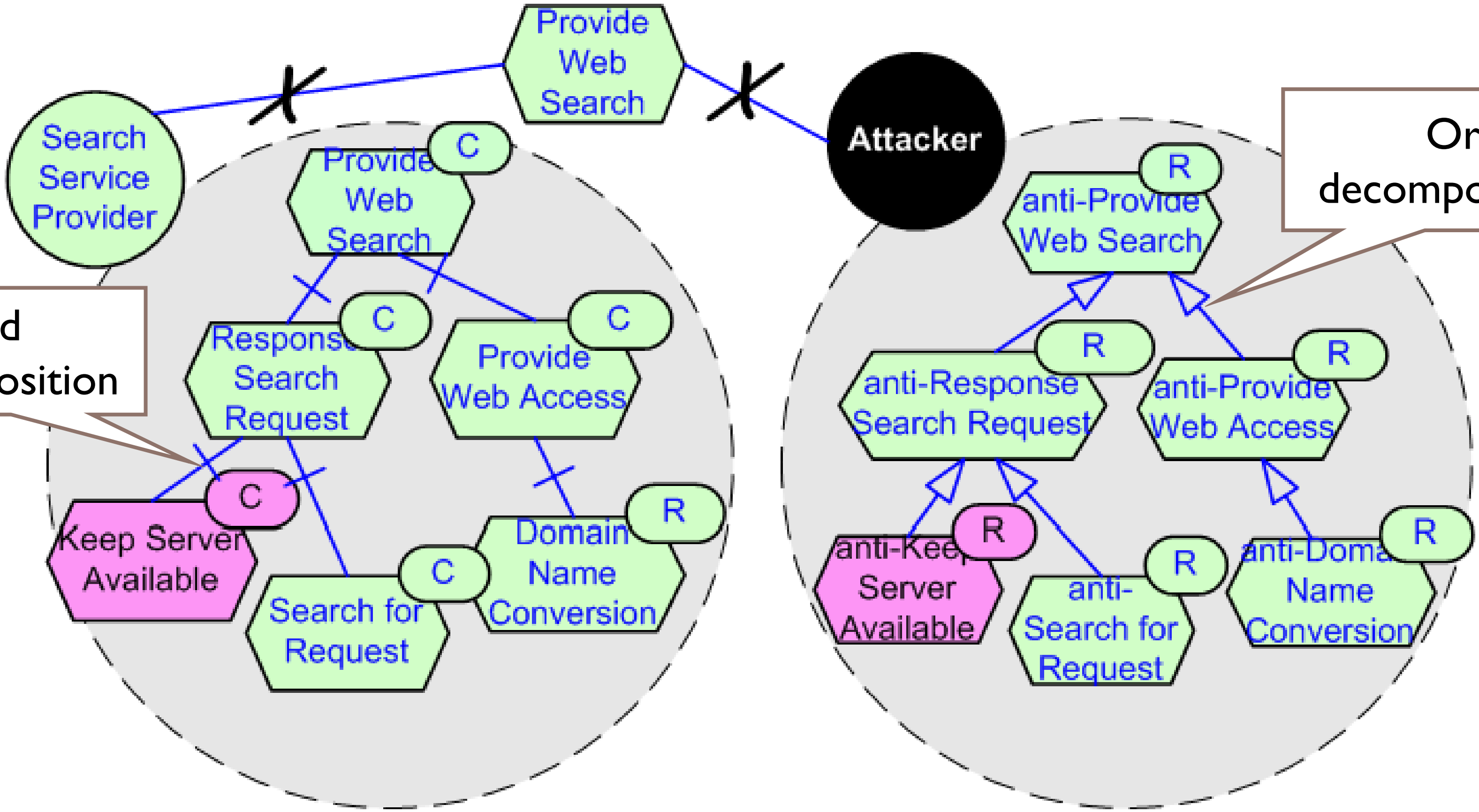


Step1. Build initial model of target service



The service is under attack from an attacker

Step2. Goal refinement on attacker side



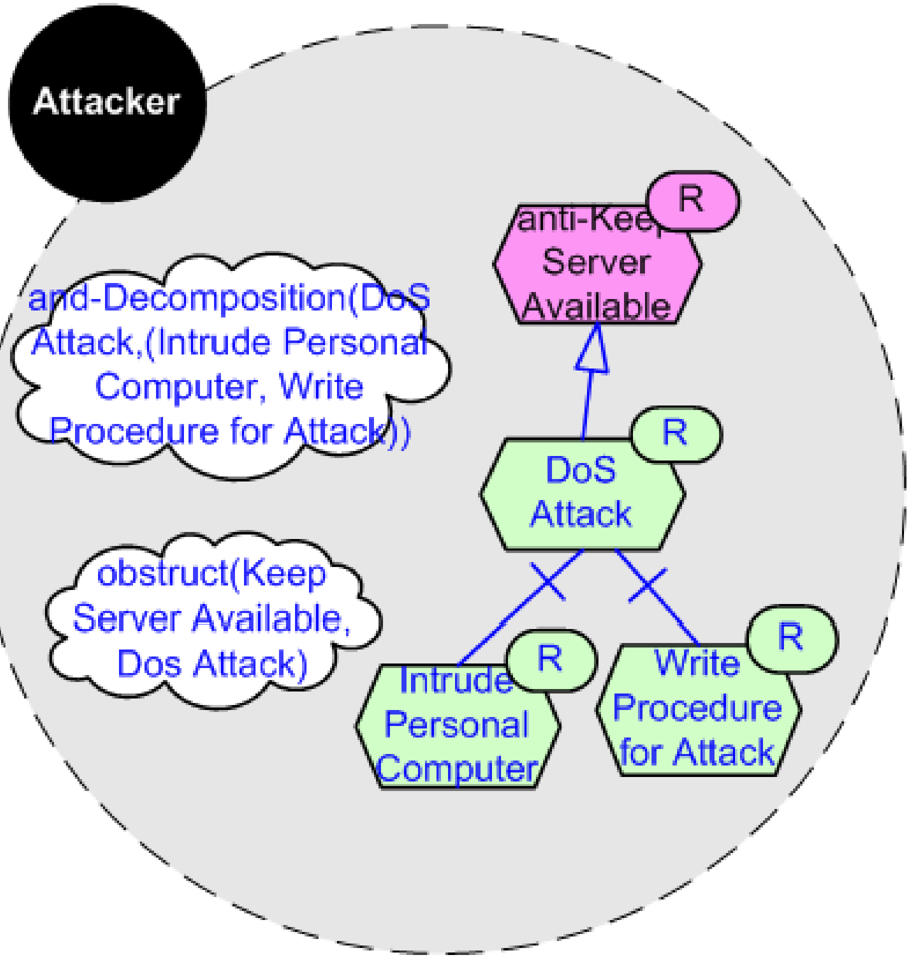
And decomposition

Or decomposition

- Apply Rule 2: Attack Decomposition

Decompose attacker goals until they can be met

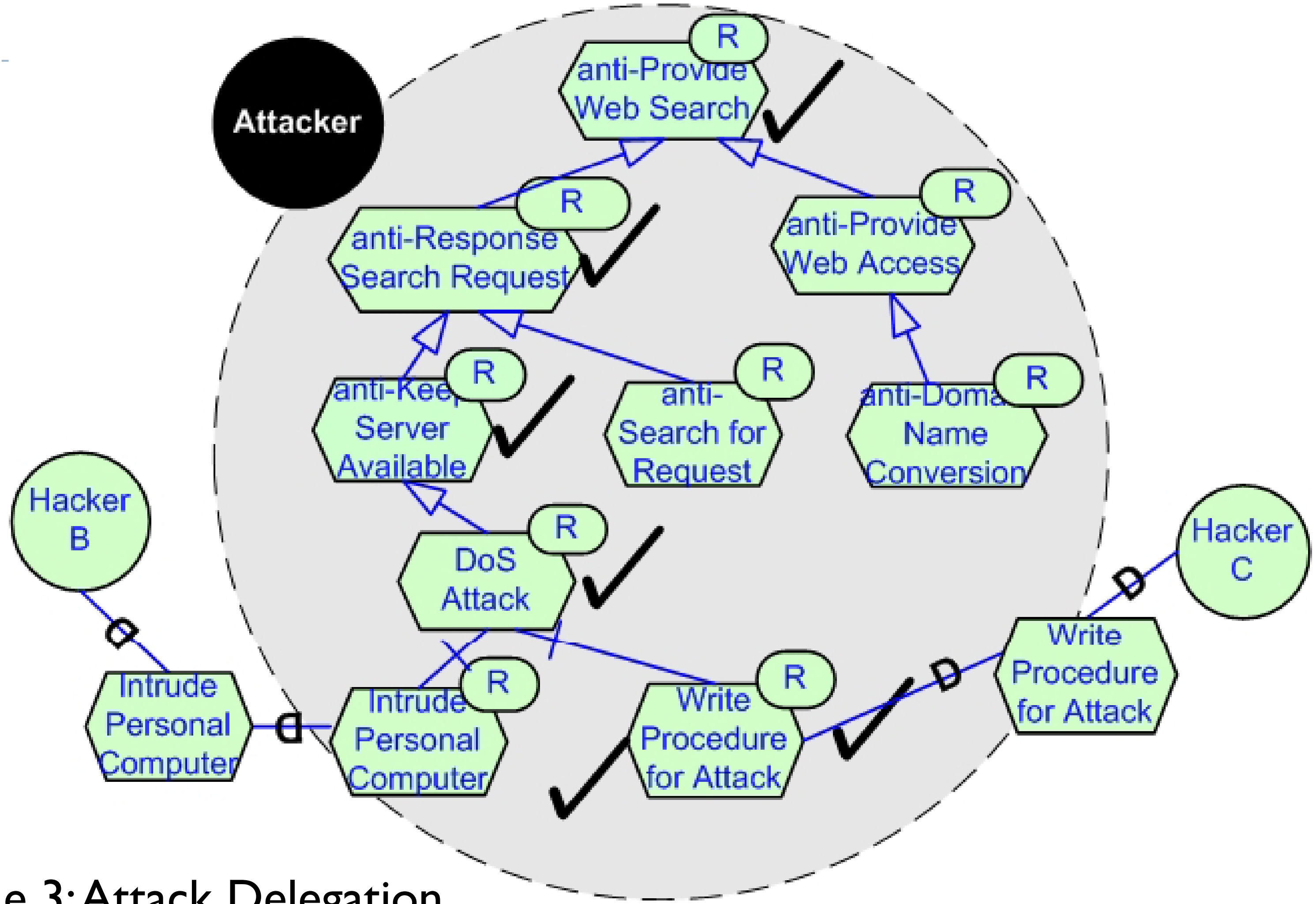
Step3. Relate anti-goals to attack tasks through knowledge in KB


Attacker
and-Decomposition(DoS Attack,(Intrude Personal Computer, Write Procedure for Attack))
obstruct(Keep Server Available, Dos Attack)
R
anti-Keep Server Available
R
DoS Attack
R
Intrude Personal Computer
R
Write Procedure for Attack

- Apply Rule 1: Attack Strategy Identification

Attacker got knowledge from domain experts or other sources, stored in KB

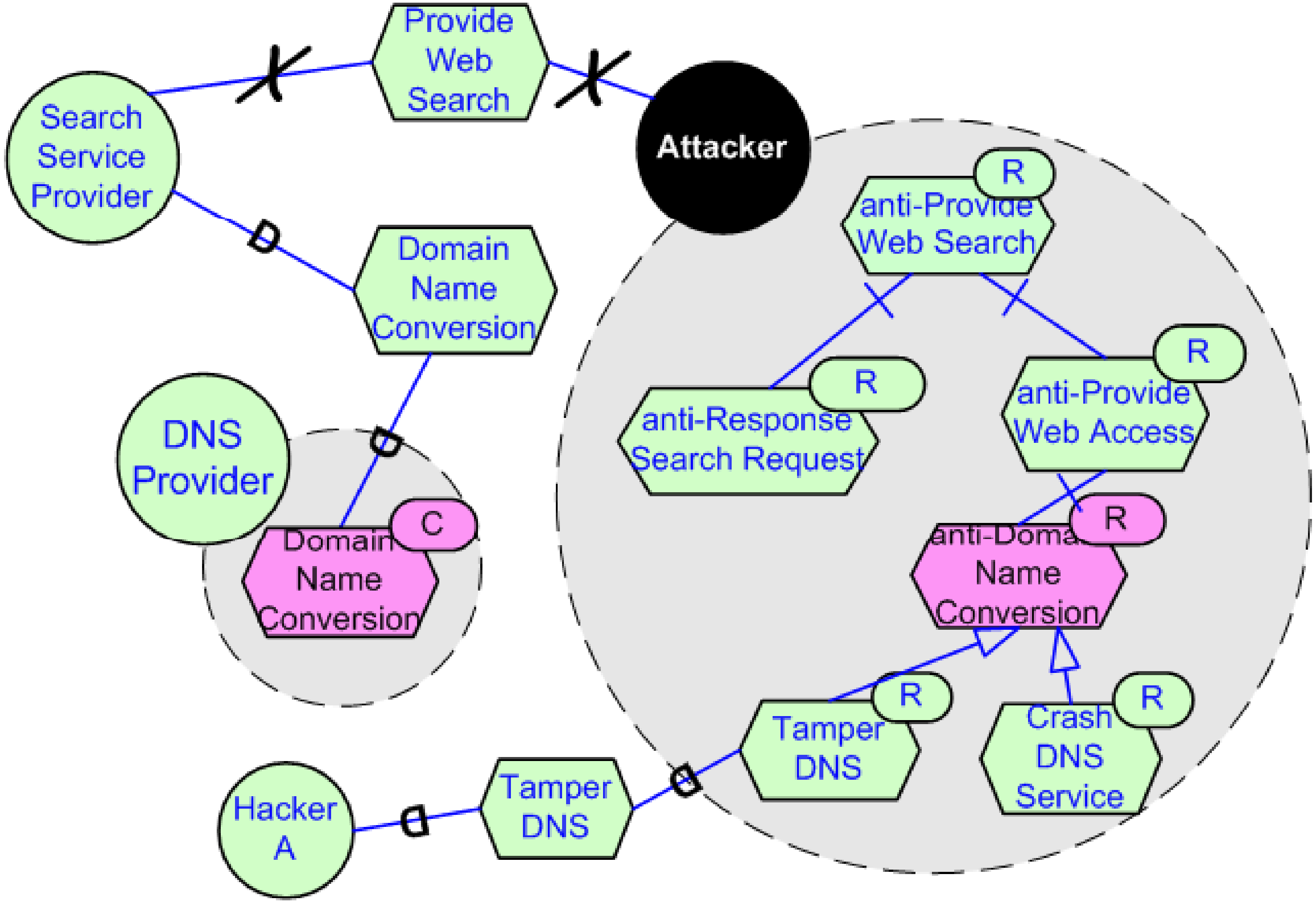
Step 4. Delegate and evaluate the attack tasks


Attacker
anti-Provide Web Search
R
anti-Response Search Request
R
anti-Provide Web Access
R
anti-Keep Server Available
R
anti-Search for Request
R
anti-Domain Name Conversion
R
Hacker B
DoS Attack
R
Hacker C
D
D
D
D
Intrude Personal Computer
Intrude Personal Computer
R
Write Procedure for Attack
R
Write Procedure for Attack
✓
✓
✓
✓
✓
✓
✓

- Apply Rule 3: Attack Delegation
- Apply Rule 4: Satisfaction Propagation

Evaluation is through binary logic in AND/OR tree

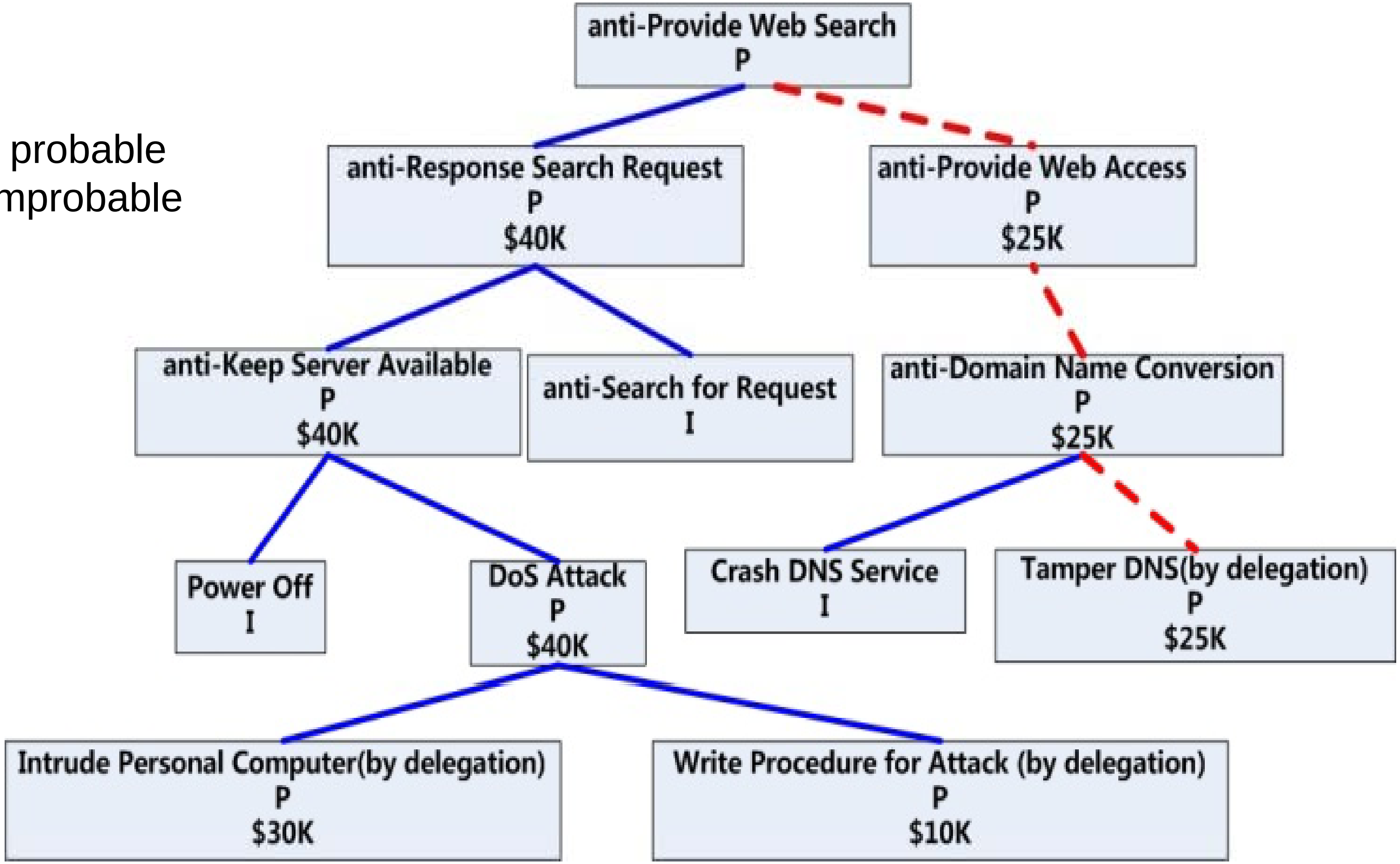
Step 5: Repeat on all alternative attack routes …



Are the risks high enough to take defensive measures?

Do attack cost and probability assessment

P = probable
I = improbable


anti-Provide Web Search
P
anti-Response Search Request
P
$40K
anti-Provide Web Access
P
$25K
anti-Keep Server Available
P
$40K
anti-Search for Request
I
anti-Domain Name Conversion
P
$25K
Power Off
I
DoS Attack
P
$40K
Crash DNS Service
I
Tamper DNS(by delegation)
P
$25K
Intrude Personal Computer(by delegation)
P
$30K
Write Procedure for Attack (by delegation)
P
$10K

Related Work

- A. van Lamsweerde, and E. Letier, Handling Obstacles in Goal-Oriented Requirements Engineering. IEEE Transactions on Software Engineering, Special Issue on Exception Handling, 2000. 26(10): p. 978-1005.
  - goals and goal refinements within one jurisdiction
- L. Liu, E. Yu, and J. Mylopoulos Security and privacy requirements analysis within a social setting. RE'03.
  - Only considers stakeholders' malicious effects to the specific project, but has left out other agents in the environment.
- J.D. Meier, Carlos Farre, Jason Taylor, Prashant Bansode, Steve Gregersen, Madhu Sundararajan, Rob Boucher.

  Improving Web Service Security. Microsoft .
- OASIS. WS-Security standard.

Conclusion

- Security analysis is more complicated in the service environment due to service compositions and delegations.
  - Focusing on goals and goal refinements within a single actor is not enough
- We use Service Security Modeling Framework (SSMF, an i* extension) to model services, attackers, and attack routes.
- We automatically generate the attack routes using rules and KB.

Limitations and Future Work

- Develop rules to automatically discover countermeasures
- Include non-security goals; trade-offs with countermeasures.
- Include integrity and confidentiality goals, and define related rules.
- Show how automation greatly reduces analysis effort when services change.

Thank you !

- Tong Li

litong08@mails.tsinghua.edu.cn

- Lin Liu

Linliu@tsinghua.edu.cn

- Golnaz Elahi

gelahi@cs.toronto.edu

http://www.cs.toronto.edu/~gelahi

- Eric Yu

http://www3.ischool.utoronto.ca/~yu