Amenaza Technologies Limited

We model the unthinkable.

Vulnerability Analysis

The Traditional Approach to Risk

Risk ≡ Event Probability x Resulting Damage

Good for natural events but can't cope with malice

- Statistics require many measurable events
- Adversary's behavior is adaptable
- Can't deal with irrational people
- High Prob/Low Impact ≠ Low Prob/High Impact

Vulnerability Analysis

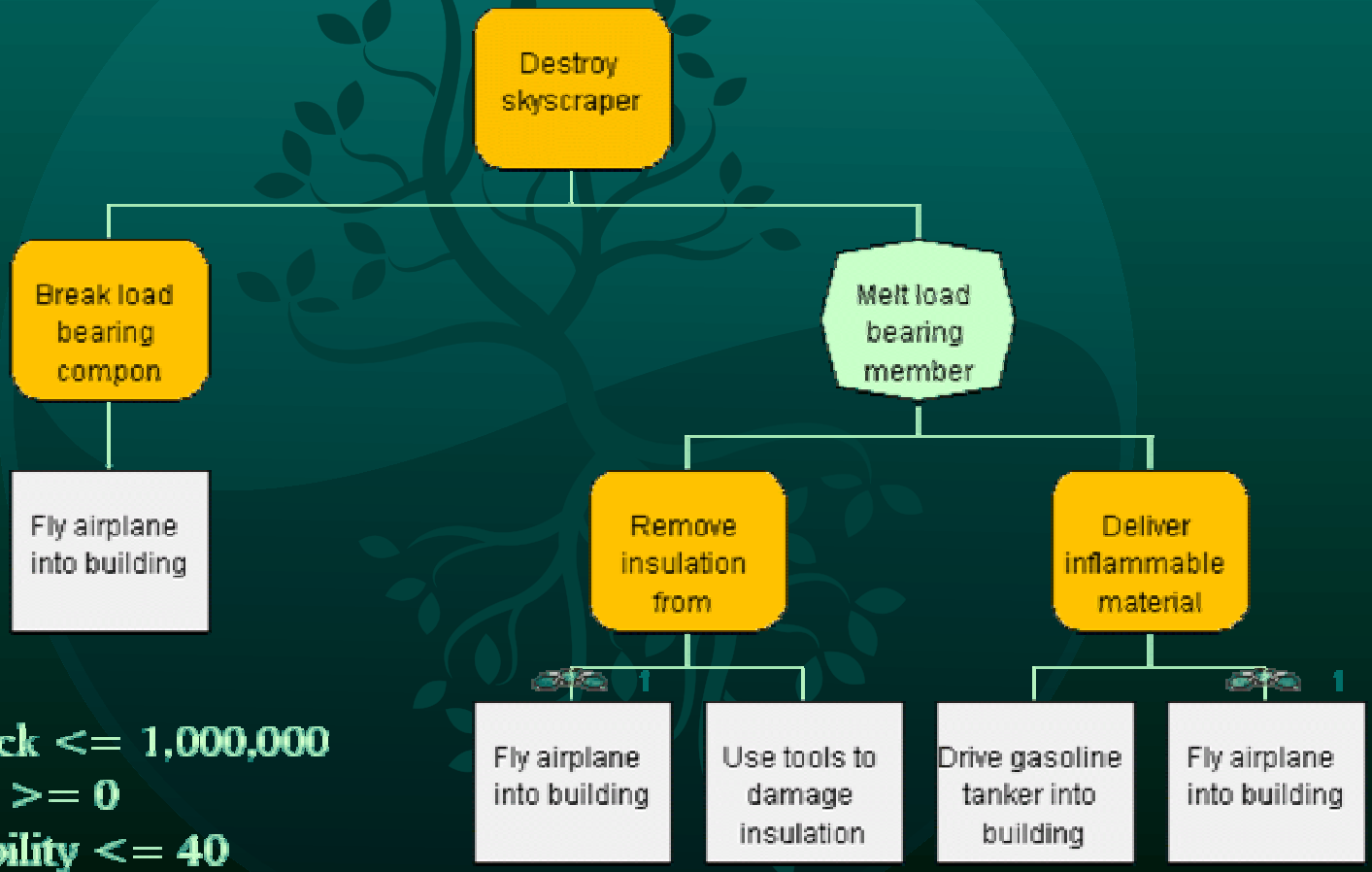
Attack Trees - Capability-Based Approach

Attack Prediction

Capabilities-Based

- Even lunatics & fanatics are resource constrained
- Choose resources that influence human behavior
  - Cost, Technical ability, Materials, Escapability
- Compare resources required for each (leaf) attack with capabilities of attackers
- Remove infeasible attacks from model
  - Remaining attacks are areas of concern
  - It helps to have a tool – **Secur/Tree**

Attack Prediction



Cost of Attack <= 1,000,000
Escapability >= 0
Technical Ability <= 40
Probability of Getting Stopped <= 0.15

Assumptions

- If they Can, They Will
  - ≈ true for sufficiently large groups of people
- The analyst is as smart as the enemy
  - Mustn’t forget any attacks
- Must know what resources constrain the enemy
- Reasonably accurate attack resource estimates

Conventional vs Capabilities

Conventional Risk Assessment gives you . . .

1. Avoid - you get to do something about it
2. Assign - somebody else gets to do something about it
3. Accept - nobody does anything about it

Capabilities-based Attack Tree

Easy to understand graphical output

- If isolated vulnerabilities then try a point sol'n
  - Raise attacker's resource requirements
- Vulnerabilities on one subtree may suggest an architectural solution
  - Create an AND node with a secure system
- Unfixable vulnerabilities?
  - Reduce attacker's resources (Bush & Iraq)
  - Create unbearable attack cost (Cold War and MAD)

Leverage Expert Skills

Knowledge reuse

- Tree structure suited to subdivision of tasks
  - Independent work can be combined later if care used
- Trees built by experts can be reused
  - Experts are scarce
  - Less knowledgeable people can tweak a template
- Combine expertise from diverse fields in trees

We model the unthinkable.

Amenaza Technologies Limited
Suite 550 1000 8th Ave SW
Calgary, AB Canada T2P 3M7

www.amenaza.com
1-888-949-9797 toll free
403-630-5931