iCAT: A Probabilistic Risk Assessment Toolkit for 3G Networks

Kameswari Kotapati, Peng Liu, and Thomas F. LaPorta

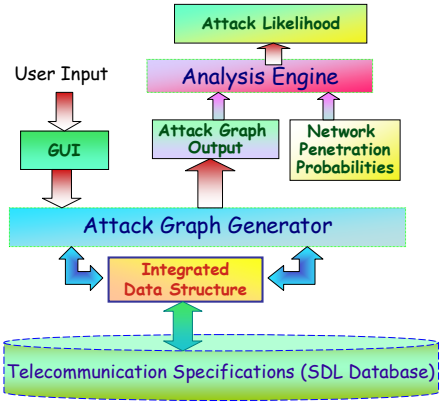
Overview

- iCAT is a graphical tool for assessing and verifying the likelihood of cascading attacks in 3G networks.
- iCAT uses 'probabilities of network penetration' obtained from network operators to compute these likelihoods.
- iCAT is an extension of CAT. CAT is a vulnerability assessment toolkit which uses SDL specifications to identify cascading attacks of 3G networks.
- CAT presents these attacks in the form of attack graphs.
- iCAT computes the attack likelihoods using these attack graphs.

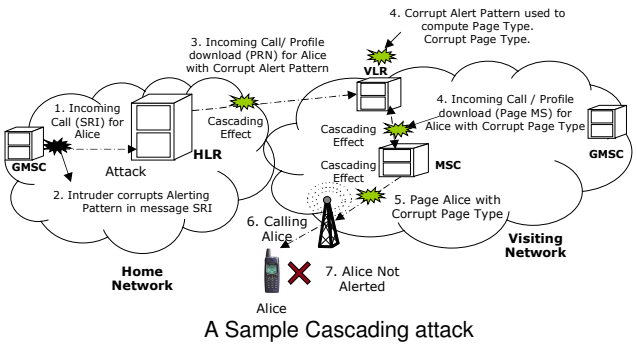
Objectives

- iCAT computes the likelihood of occurrence of every stage of the attack based on defenses in the network.
- iCAT identifies `hotspots areas' in the network which when properly protected reduces the likelihood of a majority of attacks.
- iCAT verifies if the actual defenses used to protect the network are truly effective.

iCAT Architecture



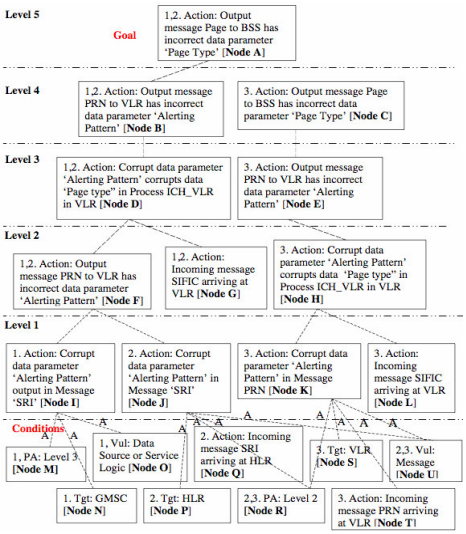
Cascading attacks



A Sample Cascading attack

- Cascading attacks are a new class of attacks where data corruption of one or two low key data items will result in propagation of corruption to remote service nodes.
- This attack can be specially hazardous to the 3G network due to:
  - Exchange of signaling messages.
  - Dependencies between data items.
  - Cached data items.
  - Shared databases.

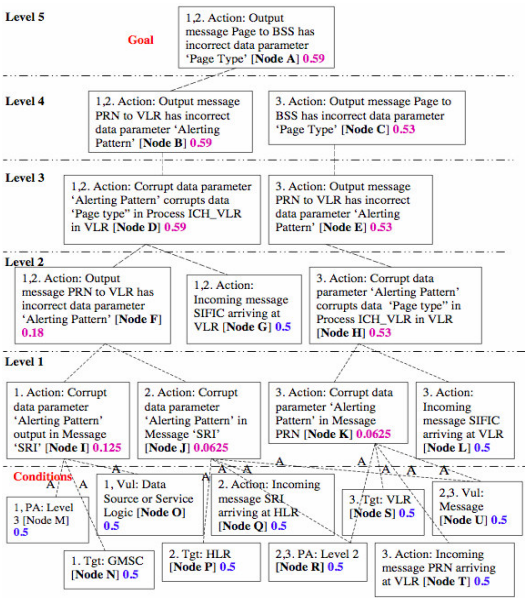
Attack Graphs



- Nodes indicate Network states.
- Network states include conditions for attack to occur, actions (network or adversary), and goals.
- Edges indicate Network State transitions.
- State transitions may be due to normal network activity or adversary action.

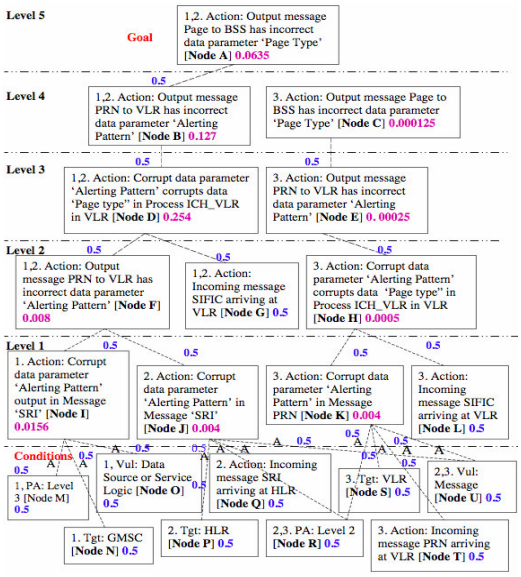
Likelihood Analysis & Results

Defenseless Network



- In a defenseless network, we assume that once corruption occurs there are no defenses to prevent its propagation.
- Hence we assume defenses exist to prevent an attack from happening (shown at conditions level).
- The likelihoods of other network states are computed using using the likelihoods of previous levels

Defensive Network



- In a defensive network, we assume that defenses exist not only to prevent an attack from happening but also to prevent corruption from propagating.
- The probabilities shown in on the edges of the attack graph indicate the defenses that prevent the attack from propagating.
- The rest of the likelihoods are computed using Bayesian conditional probabilities