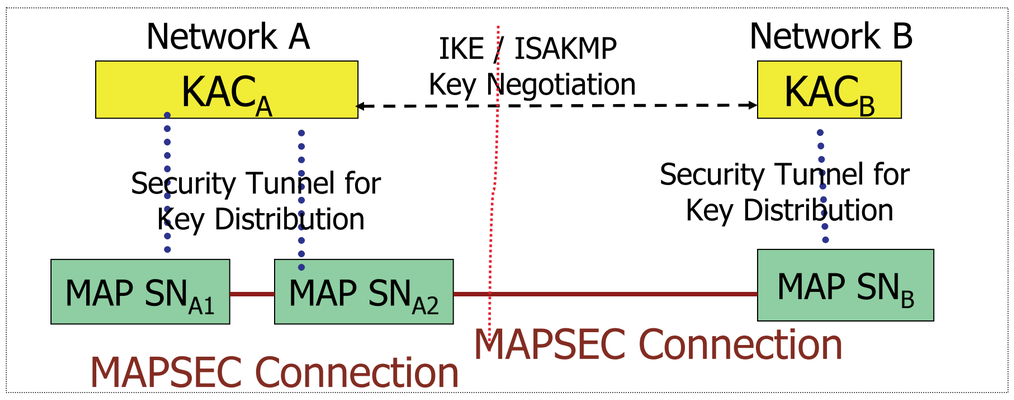
Evaluating MAPSec using Marked Attack Graphs

Kameswari Kotapati, Peng Liu, Thomas F. LaPorta

Overview

- MAPSec a new security protocol was introduced as a solution for mobile telecommunication network vulnerabilities.
- We designed **eCAT - Cellular Network Vulnerability Assessment Toolkit for Evaluation** to evaluate the design principles of MAPSec and find:
  - Exact coverage of MAPSec
  - Other kinds of security protocols required in addition to MAPSec
  - Most vulnerable network areas (hot-spots)
- eCAT is graph based and uses boolean probabilities and Coverage Measurement Formulas (CMF).
- Results from eCAT's evaluation of MAPSec reveals MAPSec's effectiveness and provide insights into overall networks vulnerabilities.

MAPSec

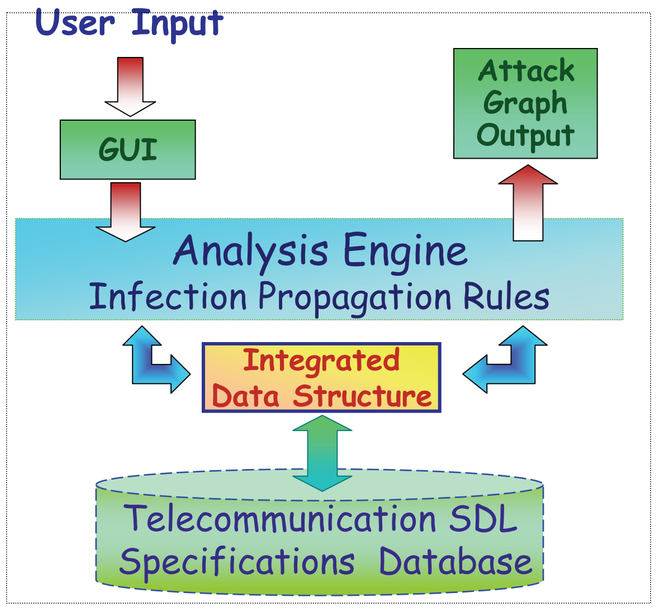


- MAPSec is developed to provide for link security to cleartext wireline messages in the network.
- It provides message data authentication origin authentication, and message confidentiality.
- MAPSec uses the ISAKMP/IKE framework to negotiate security associations (distribute the keys, algorithms, protection profiles and lifetimes)

eCAT Workflow for Evaluation of MAPSec

Step 1: Capture Network Wide Scope

Attacks & Effects: Attack Graphs

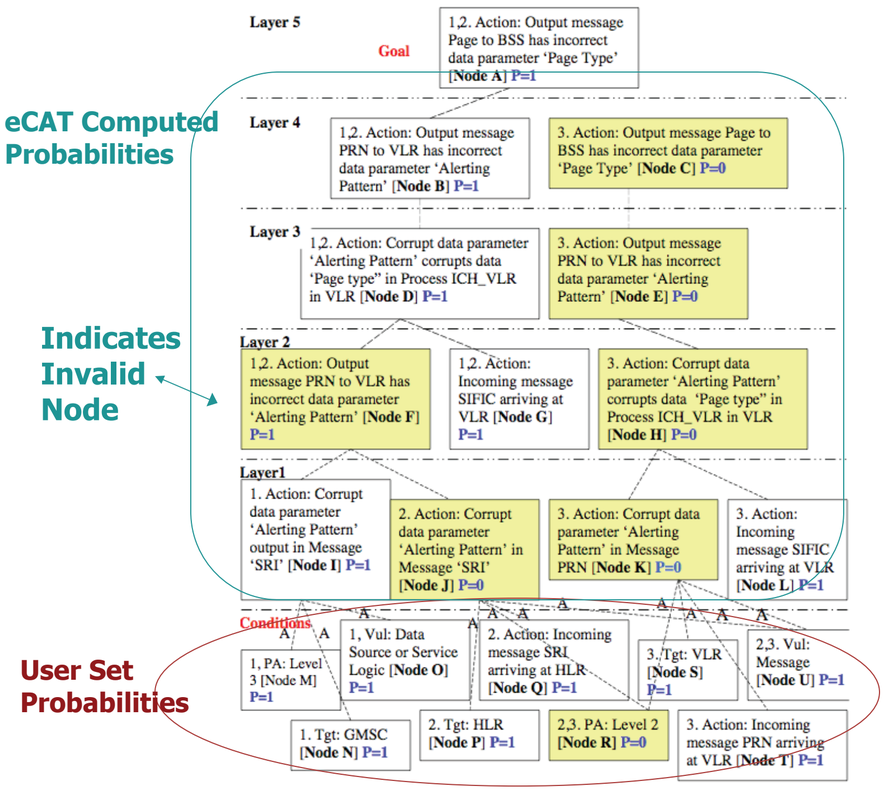


- Generate attack graphs to capture attacks & effects.
- System input
  - Telecommunication Specifications written in Specification and Description Language (SDL).
  - Network Dependency Model – show relationship between processing and data
  - Infection Propagation Rules

Step 2 : Extract the coverage of MAPSec

Boolean probabilities

- Set boolean probabilities for Layer 0.
- eCAT computes the boolean probabilities for other layers.
  - 0 : indicates conditions eliminated by MAPSec
  - 1 : indicates conditions not eliminated by MAPSec



Step 3: Quantify Coverage of MAPSec

Coverage Measurement Formulas

- Effective Coverage: Captures the average effective number of attacks eliminated.
- Deployment coverage: Captures % of total vulnerabilities protected.
- Attack Coverage: Capture the attack reduction effect of the protocol.
- Good Measure CMF: High Effective Coverage, Low Deployment coverage, High Attack Coverage

A. Location Update Service

MAP_Message_Name	# Attacks Prevented	Total # of Possible Attacks	Effective Covergae	Deployment Coverage	Attack Coverage
MAP_UPDATE_LOCATION_AREA	2	8	2	0.06	0.25
MAP_UPDATE_LOCATION_AREA-ACK	1	4	1	0.06	0.25
MAP_SEND_IDENTIFICATION	3	12	3	0.06	0.25
MAP_SEND_IDENTIFICATION-ACK	3	13	3	0.06	0.23
MAP_SET_CIPHERING_MODE	2	8	2	0.06	0.25
MAP_SET_CIPHERING_MODE-ACK	0	0	0	0.06	0
MAP_FORWARD_NEW_TMSI	1	4	1	0.06	0.25
MAP_ FORWARD_NEW_TMSI -ACK	0	0	0	0.06	0
MAP_UPDATE_LOCATION	8	30	8	0.06	0.27
MAP_UPDATE_LOCATION-ACK	2	8	2	0.06	0.25
MAP_CANCEL_LOCATION	3	9	3	0.06	0.33
MAP_CANCEL_LOCATION-ACK	0	0	0	0.06	0
MAP_INSERT_SUBSCRIBER_DATA	26	40	26	0.06	0.65
MAP_INSERT_SUBSCRIBER_DATA-ACK	6	18	6	0.06	0.33
MAP_AUTHENTICATE	2	6	2	0.06	0.33
MAP_AUTHENTICATE-ACK	1	3	1	0.06	0.33
All Messages	60	163	3.75	1	0.37

- MAPSec has an average attack coverage of 33%, with a maximum of 65%, and a minimum of 0%.

Results from Evaluating MAPSec

- Message corruption accounts for 33% of attacks: MAPSec can protect them all.
- Effective Coverage provided by MAPSec for a single message can be a high of 26 to a low of 0.
- Risk level of Message based attacks is high due to message traversal through untrusted networks.
- MAPSec is successful only when all service providers deploy it.
- While MAPSec provides link security it cannot prevent a successfully launched attack from propagating.
- Hot-Spots: Data Sources & Service Logic: High amplification effect: MAPSec does not protect them
- Hence data source and service logic protection must be deployed.

Funded by Raytheon and NSF/DHS Grant no. 0335241