

# **Security Evaluation of Software Architectures using ATAM (ESAM as a case study)**

By

**Asad Raza**

**&**

**Haider Abbas**

# Agenda

- Research Question
- Security challenges in developing countries
- ATAM
- ESAM (as case study)
- Quality Attributes Characterization
- Security Characterization
- Conclusions

# Research Questions

- How to do security evaluation using ATAM?
- How to promote time/cost-effective security evaluation of Software Architectures in developing countries?
- How to Identify security risks and threats in the requirement & design phase of SDLC?

# Security challenges in Developing Countries

- Security is all about CIA (Confidentiality , Integrity and Availability)
- ICT assets include hardware, software, information exchanged and critical assets.
- Unawareness of ICT related threats.
- Lack of ICT policies and procedures.
- No security evaluation at requirement and design level.
- More focused towards the functional requirement.
- Limited resources/constraints.

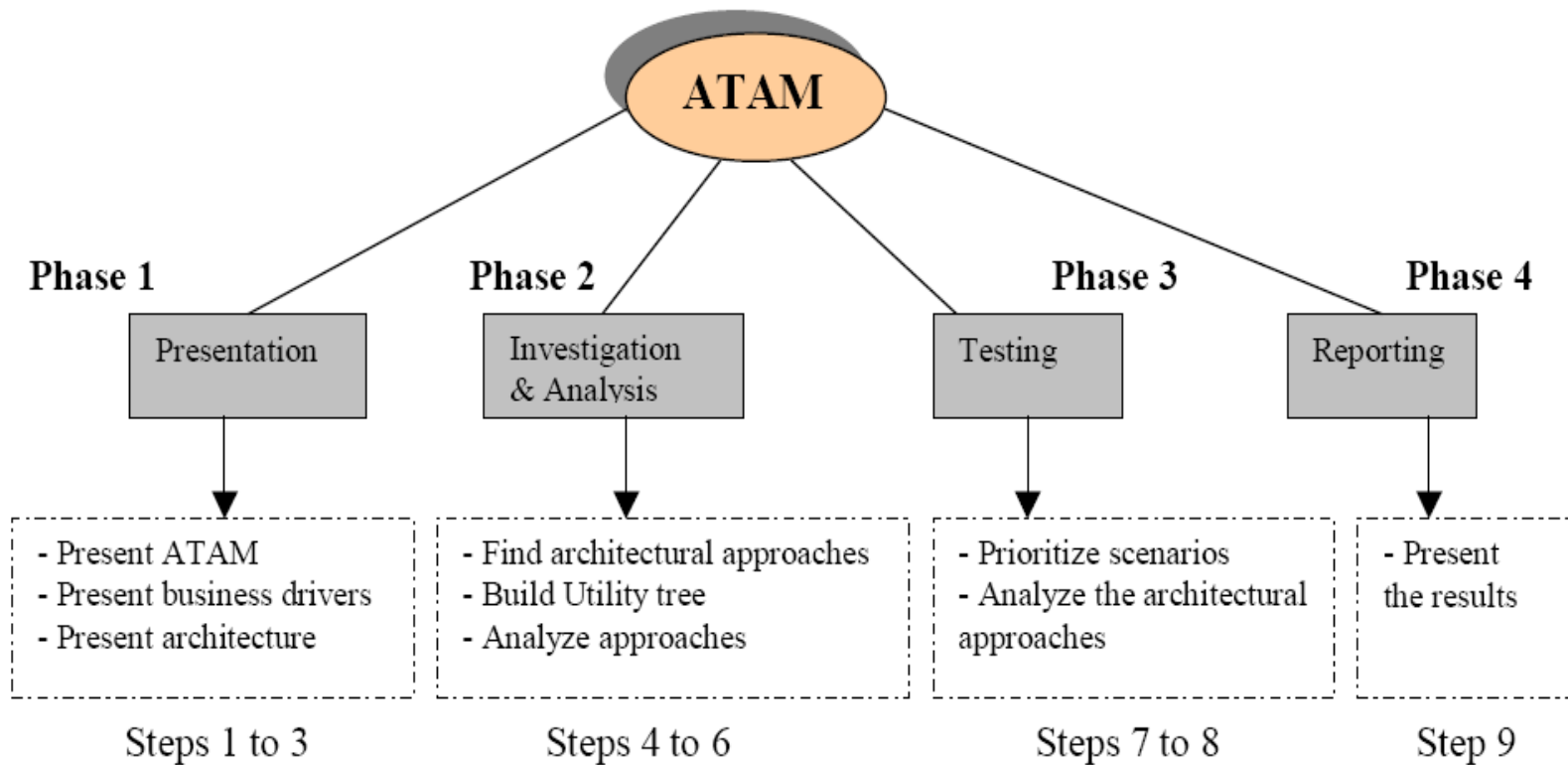
# Security challenges in Developing Countries

- Security is addressed too late in a software development process.
- It is not considered as a risk to achieving business goals.
- Security is considered as an overhead from the cost perspective.
- Considered as the technical problem.
- Systems are more vulnerable ICT threats.
- Poor documentation (hindrance in CC evaluation)

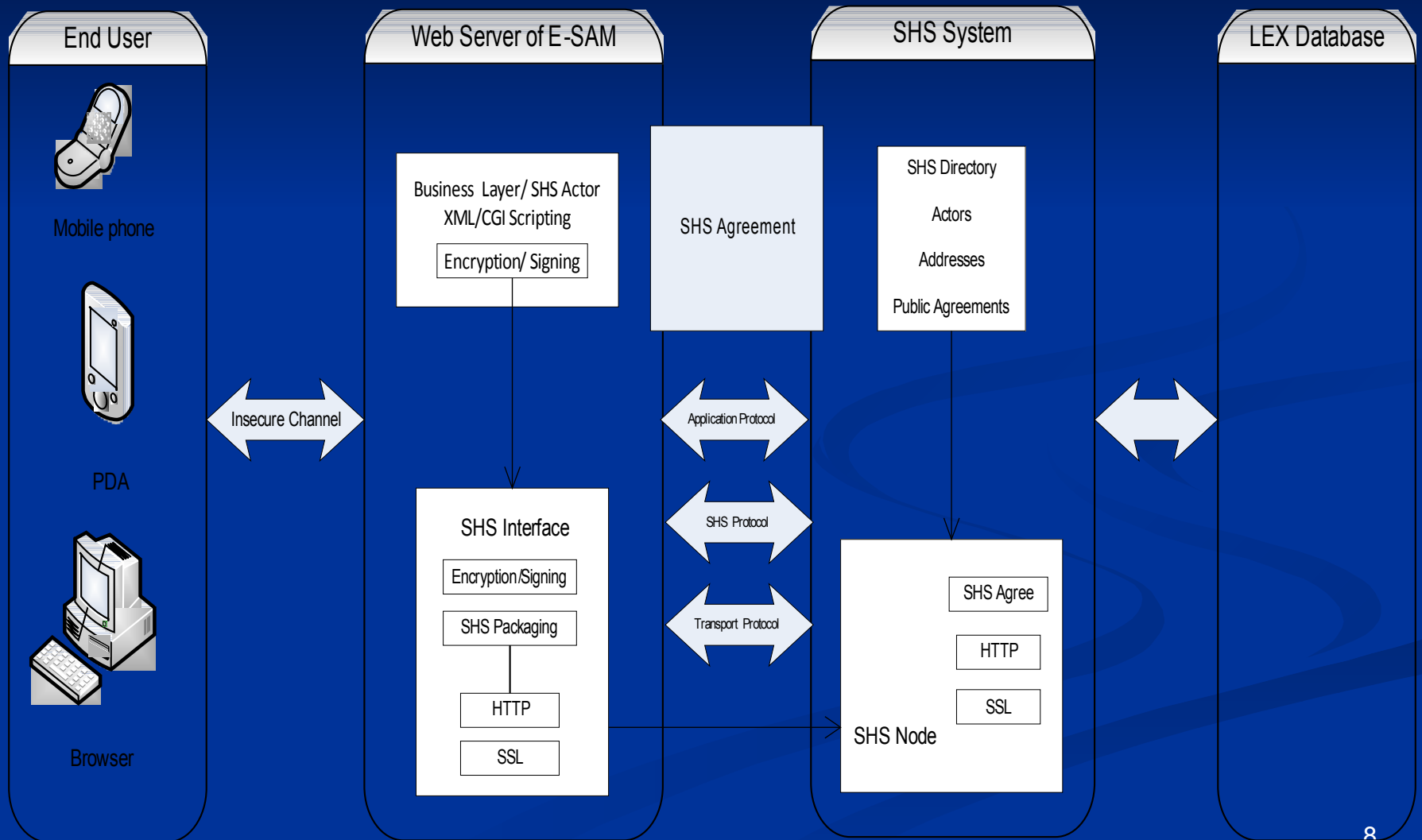
# ATAM

- Purpose of ATAM?
- Aimed to locating and analyzing tradeoffs, risks and sensitivity in software architectures
- Multiple Quality Attributes
- Scenario based
- Early Phase of SDLC
- Determines where an attribute is affected by architectural decisions

# ATAM



# ESAM Framework



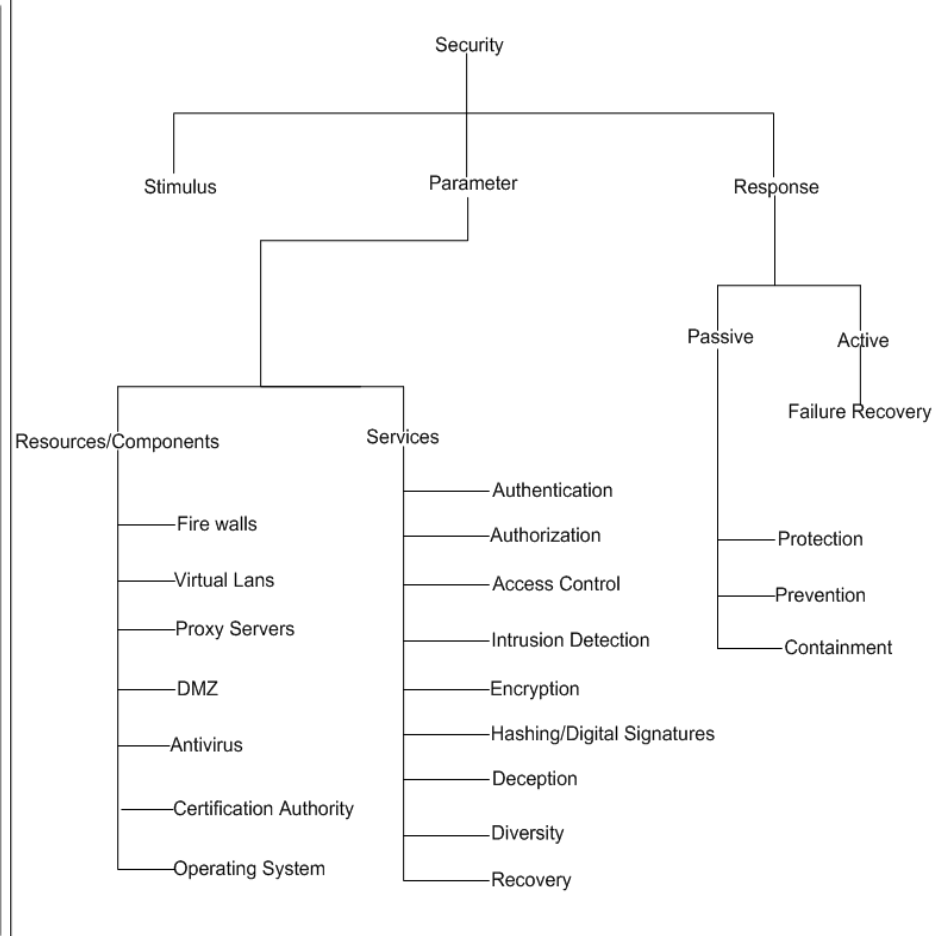
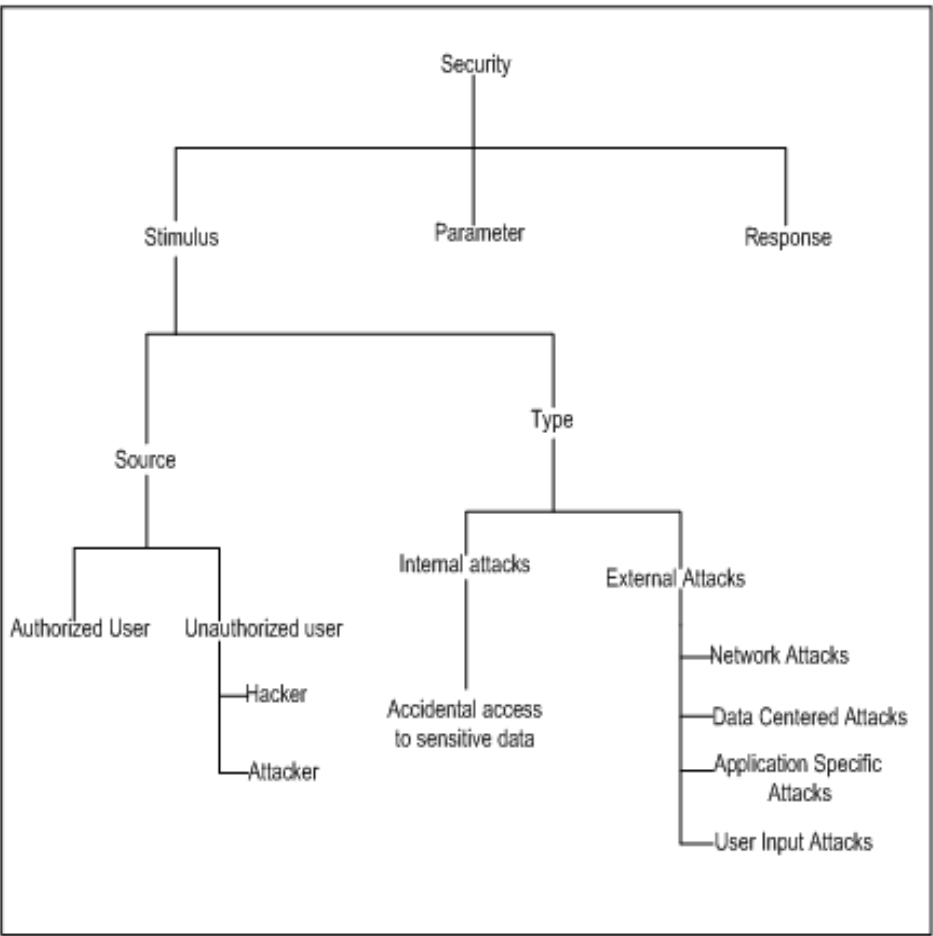
# Quality Attribute Characterization

- Evaluating architectural design against the quality attributes requires characterization of those quality attributes.
- It is the Starting point for ATAM
- Scenario generation depends upon QAC
- Quality attribute characterization is divided into three categories
  5. Stimuli
  6. Architectural decisions
  7. Responses

# Security Characterization

- ATAM provides characterization of Performance, Modifiability and availability
- Our contribution: plug-in in ATAM process for security evaluation of architectures.
- This characterization will serve as the milestone for security scenarios elicitation.
- Not an exhaustive taxonomy
- Offers a rationale for asking elicitation questions

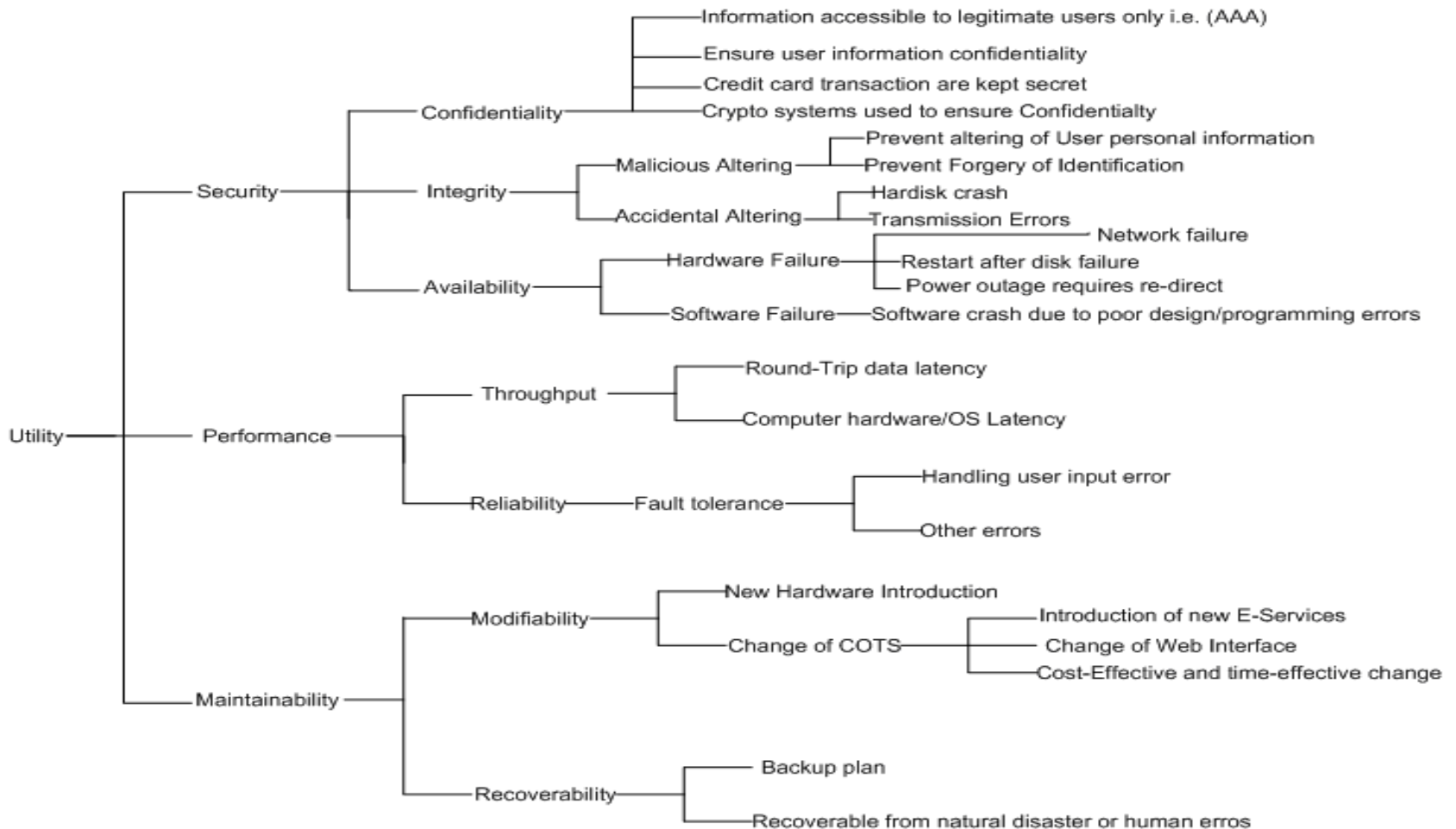
# Security Characterization



# Sample Security Scenarios

1. The intermediary SHS server forwards a message to the ultimate receiver on behalf of an initial sender. The sender/ultimate receiver wishes to enforce the non-repudiation property of the route. The intermediate message service handler that appends a routing message must log the routing header information. Signed routing headers and the message sender/readers must be logged at the message handler which passes the message to the ultimate sender/receiver to provide the evidence of non-repudiation.
3. In ESAM a sender and receiver may wish to be able to determine if a message has been modified in transit if the point-to-point encryption is not appropriate because of intermediaries or system architecture choices. In this scenario the ESAM system either signs the arbitrary portion of document or uses digital signature to guarantee that the message has not been modified during the transit.

# Utility Tree



# Conclusions

**We believe that our research will encourage the security evaluation of at Architecture level in developing countries due to the following stand points**

- Security Evaluation using ATAM is less expensive as compared to CC Evaluation.
- Can be done in 3-4 weeks (CC Evaluation can takes 12-14 months)
- Can be started with minimum input due to the interactive nature.
- Security risks and tradeoffs are identified in the early stages of software development process.
- Decrease the maintenance cost.
- Brings all the stakeholder at one table which results in the improved quality product.
- Does not require much resources.
- Our Security characterization will help in security scenarios elicitation