

Project Proposal

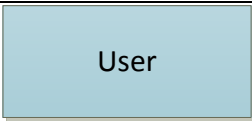


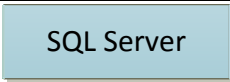
Automated Thread Analysis for distributed systems

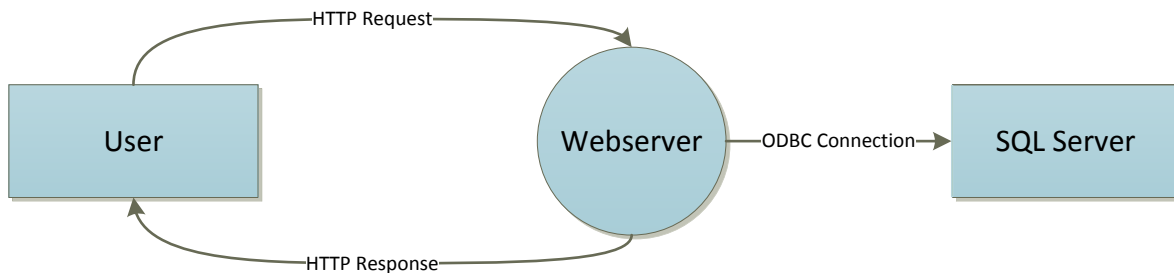
Vision

Applications are distributed over several workstations and server applications. For example a rich client application may run on a workstation and use web services over the internet or LAN. The web service endpoint is hosted on a web server. The business logic and a database may run on an application server. The vision is to put the topology into a prolog application. The system administrator may ask the PROLOG application to find possible vulnerabilities and effected nodes.

Topology

I assume that the system topology is already known. The analysis is based on a simple data flow diagram. There are 4 different types of nodes.

	External Entity like people, external events etc.
	Process: Web service, component, application server, etc.
	Dataflow: method call, request and response from a webserver, etc.
	Datastore: Database, file, message queue



For example a simple web application where a client requests a page from the server. The server gets data from the SQL server and builds the new webpage. Last the webpage is returned to the client.

Threats

There are several threats that may occur in a distributed system. The most common threats are defined as STRIDE : Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of privilege.

Project Goal

Project goal is to define syntax (predicates) to model the topology and threats.