Contribution ID: **349** Type: **oral presentation**

Role of Digital Forensics in Service Oriented Architectures

Monday, September 3, 2007 5:50 PM (20 minutes)

Security requirements of service oriented architectures (SOA) are reasonably higher than the classical information technology (IT) architectures. Loose coupling –the inherent benefit of SOA –stipulates security as a service so as to circumvent tight binding of the services. The services integration interfaces are developed with minimal assumptions between the sending and receiving parties. This services aggregation approach is highly beneficial for achieving higher performance level; however, bookkeeping and logging of various events of such dynamic architecture are very complex issues. Security architecture requires these trails of events to establish clearly what happened and why in the post-accident scenario. The techniques employed to determine the reasons of security architecture's failure to prevent an incident are collectively known as Digital Forensics. It is necessary to develop digital forensics techniques for SOA so that necessary actions can be taken in the wake of a security breach. In this article we explore the role of digital forensics in SOA especially in the mission-critical SOA applications. We envision digital forensics as a sub-service of the security service in SOA. We propose the use of a monitoring service to generate these logs. We then present a mechanism of efficiently managing the logs of various actions based on the lifecycle of these logs. We finally conclude with the open issues and areas for further improvements.

Primary author: Dr NAQVI, Syed (CoreGRID Network of Excellence)

Co-author: Prof. RIGUIDEL, Michel (TELECOM PARIS)

Presenter: Dr NAQVI, Syed (CoreGRID Network of Excellence)

Session Classification: Grid middleware and tools

Track Classification: Grid middleware and tools