WG Critical Systems: On Protecting Networks of Services

Hong-Linh Truong, Schahram Dustdar

Distributed Systems Group, Vienna University of Technology

{truong,dustdar}@infosys.tuwien.ac.at

In our view, today's and future critical ICT infrastructures are managed by networks of software services belonging to possibly different organizations. We consider that such networks of software services are (parts of) critical systems. Examples of these networks include critical information systems supporting crisis managements, sensor Web for monitoring environments, collaboration services for networked enterprises. Although services can be provided in various forms, we believe that the mainstream of critical systems will be built around Web services technologies.

To protect critical systems equals protecting networks of software services. We believe protecting critical systems is not only to protect the software (to ensure the software functions as in its design) but also to integrate human in the loop because there are various tasks which cannot be done by software in critical situations. In this sense, critical systems will include also humans, constituting the so called "mixed systems of humans and software services". Furthermore, we believe that we should not focus solely on the "defense" of critical systems but also on the response to the crisis of critical systems. Networks of software services in critical systems typically are managed by different organizations. Thus, the protection of critical systems should be coordinated across the boundaries of single organization because a critical system can be attacked from any point in the system's network.

We, therefore, propose this working group to focus on the following topics

- To develop software engineering techniques supporting the design of critical systems to work on failure conditions. The services in critical systems and the systems themselves should be self-managed. This requires a multi-disciplinary effort as we need to provide techniques at multiple levels, from networks to middleware to applications.
- To develop monitoring techniques and infrastructure for large scale networks of services across various organizations. The prerequisite for this is that services must be monitorable at runtime. The monitoring of such networks require standardized data presentations, protocols, large scale and distributed storage, access controls, to name just a few. Here we stress that the monitoring is not only at the network level but also at the application level and we should target to the monitoring of large scale networks of Web services with the focus on providing information for threat management.
- To develop tools and policies to support the correlation and mining of monitoring data of critical systems on the fly. We need to detect threats and patterns of threats which are associated with services and humans based on different types of interactions such as service-to-service, human-

to-service, and human-to-human. The key challenge here are the technique and policy to support the correlation monitoring data gathered from different organizations.

- To develop techniques and tools for supporting the response to the crisis of critical systems. We need crisis management systems and tools to support collaborative works in crisis situations. Furthermore, we need a mechanism to integrate humans into critical systems, making humans as a part of critical systems who can readily react to and solve activities that software services cannot do in critical situations