

Qualification Statement *

Vipin Swarup
The MITRE Corp, MS W424
7515 Colshire Drive.
McLean, VA 22102
swarup@mitre.org

January 31, 2002

The security of computer systems and networks is based on the principle of “Defense-in-Depth”. This principle states that security improves when defenses are built in layers so an intruder who penetrates a single defense (e.g., a firewall) does not gain complete access to the assets protected by that defense; rather, the intruder must successfully penetrate a series of layered defenses in order to compromise a system. This principle is just as applicable to survivability architectures. I have explored this connection over the past year and am developing a framework for applying the defense-in-depth principle to survivability architectures. This work qualifies me to provide a holistic perspective of survivability and contribute to various discussions.

Two topics that have emerged during my work that I believe should be addressed at the workshop are:

1. *Survivability requirements (“Protection Profiles”)*: I believe that a critical impediment to the design, construction, and deployment of survivable systems is the lack of standards for survivability requirements (ala the Common Criteria for information assurance requirements). We need to develop an analogue to the Common Criteria that provides an extensive catalog of survivability requirements and a standardized format for communication among stakeholders and other players.
2. *Architectural patterns for survivability*: Decades of experience in security engineering has resulted in the development of several informal patterns for building secure systems (e.g., the defense-in-depth paradigm, trust boundaries and boundary controllers, etc.). The survivability community lacks such tried-and-tested patterns which are essential to design and construct practical survivable systems.

*This work is supported by DARPA through US Army CECOM contract DAAB 07-01-C-N200.