

Summary Panel 2

Yvo Desmedt: moderator

1. What is the discipline

Definition 1 *Information survivability is the capability to deliver desired variable properties (such as security and reliability) for a given mission as a function of:*

- *variable information resources, and*
- *faults (malicious and accidental),*

as these evolve in time.

Essential aspects:

variability in time: e.g. adapting performance to the circumstances (such as attacks or failures), increase/decrease security aspects (e.g. privacy), etc.

accidental and malicious faults: need to deal with both

scale of the mission: small to broad (e.g. financial transactions).

2. Research goals

High Level:

- (a) identification and assessment of critical and vulnerable subsystems in the presence of knowledgeable adversaries, who may be more/less knowledgeable than the user.
- (b) understand threats in function of time, skills, knowledge, ...
- (c) management and protection of (e.g. large scale) distributed systems in the presence of a faults (malicious, accidental).
- (d) interaction of the 3 items above.

3. How to attract funding

We were very concerned that:

- at a high level one is unaware of the severity of the issue,
- there is a need for a long term study of which the need is not understood at a high to very high level,
- some do not understand the need of the “R” aspect in the “R&D”.

- some do not understand the need of the “R” aspect in the “R&D”. There is a need for:
 - (a) long term research
 - (b) short term research
 - (c) development

Without the first two we will never approach the goal, but many seem to be unaware of this.

- We do not want to be blamed for the lack of an appropriate approach due to the fact high level funding administrations do not understand what needs to be done.