Towards Cyber Resiliency in the Context of Cloud Computing

Anoop Singhal
Senior Scientist
Computer Security Division
National Institute of Standards and Technology
Email:psinghal@nist.gov

Peng Liu and Xiaoyan Sun
Pennsylvania State University

Cyber Resilience (1)

Cyber resilience:

the ability to recover and adapt to adverse conditions or cyber attacks on systems

Cyber Resilience (2)

Cyber resiliency is a capability depending upon multiple factors:

- a business process could involve tasks which could be running on any part of the enterprise network
- any security measure deployed on the enterprise network could help mitigate the impact on the business process.
- data dependencies and control dependencies could exist between this business process and some other business processes.

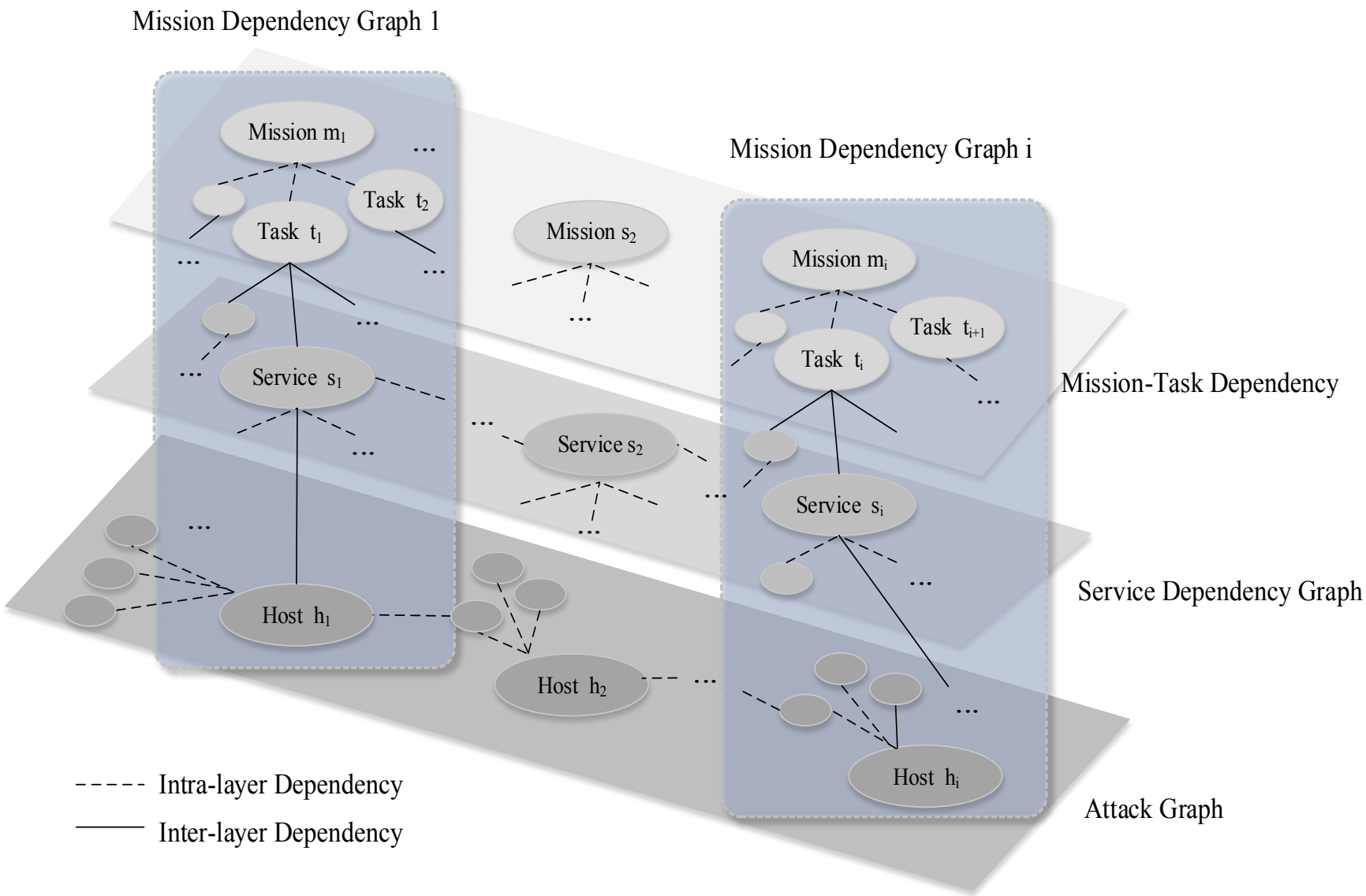
Overlooked Gap between Mission Impact Assessment and Cyber Resilience

- Existing cyber resilience techniques are unfortunately *not mission-centric*
- Mission impact assessment results *cannot be automatically used to make mission-centric recommendations*
- Mission impact assessment techniques do not consider the dimension of service dependency

Towards Bridging the Gap (1)

The strategy we take is to integrate mission dependency graphs and attack graphs into a unified graphical model.

Towards Bridging the Gap (2)



Mission Impact Assessment Framework (1)

The Framework is composed of:

- a new graphical model named *mission impact graph* to integrate mission dependency graph, service dependency graph, and attack graph;
- the applicable metrics on top of the graphical model to actually measure the impact

Thank you!