The Survivable Network Analysis Method:

Assessing Survivability of Critical Systems

CERT/Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Sponsored by the U.S. Department of Defense

Mission Survivability

Changing Environment

- System Evolution
  - expanding network boundaries
  - additional participants with varying levels of trust
  - numerous point solutions: Public Key Infrastructure, Virtual Private Networks, Firewalls
  - blurring of Intranet and Extranet boundaries
  - new technologies -- directory services, XML
- The impact of attacks is on organizations, and hence on the applications which support the organization's mission

Impact on Analysis

- Lack of complete information
  - physical and logical perimeters
  - participants, untrusted insiders
  - software components --- COTS Java, etc.
- Mix of central and local administrative control
- Critical components more exposed
- An attack could impact essential business services

Survivability Defined

Survivability is the ability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents.

Key properties

- Mission Focus
  - Identification of risks and trade-offs
  - Alternative means to meet mission
- Assume imperfect defenses

The "Three Rs"

- *Resistance*
  - Capability to deter attacks
- *Recognition*
  - Capability to recognize attacks and extent of damage
- *Recovery*
  - Capability to provide essential services/assets during attack and recover full services after attack

Techniques and Methods

- Traditional Security
  - fortress model: firewalls, protection, security policy
  - insider trust
  - encryption, authentication, passwords
  - resistance and recognition with recovery secondary

- Survivability is enhanced by
  - security techniques where applicable
  - redundancy, diversity, general trust validation, etc
  - automated recovery support

Example

- E-mail
  - E-mail content tunnels through firewalls
  - Always time lag between initial discovery and upgraded virus signatures required for scans
  - Enhanced e-mail functionality
    - Attachments (Word macros)
    - Rich content such as HTML, Javascript
  - Resistance and recognition limited. Recovery strategies essential.
  - Significant impact on services other than e-mail.

The Survivable Network Analysis Method

- Focus
  - early phase of life cycle
  - applications as well as system infrastructure
  - tailorable depending on stage of development.

- Three options for SNA analysis
  - survivability architecture
  - survivability requirements
  - mission lifecycle

Architectural Focus

- Capture assumptions such as boundaries and users
- Support system evolution as requirements and technologies change
  - evolving functional requirements
  - trend to loosely coupled
  - requirements for integration across diverse systems
- Assist with product selection and integration with respect to rapidly changing security product world

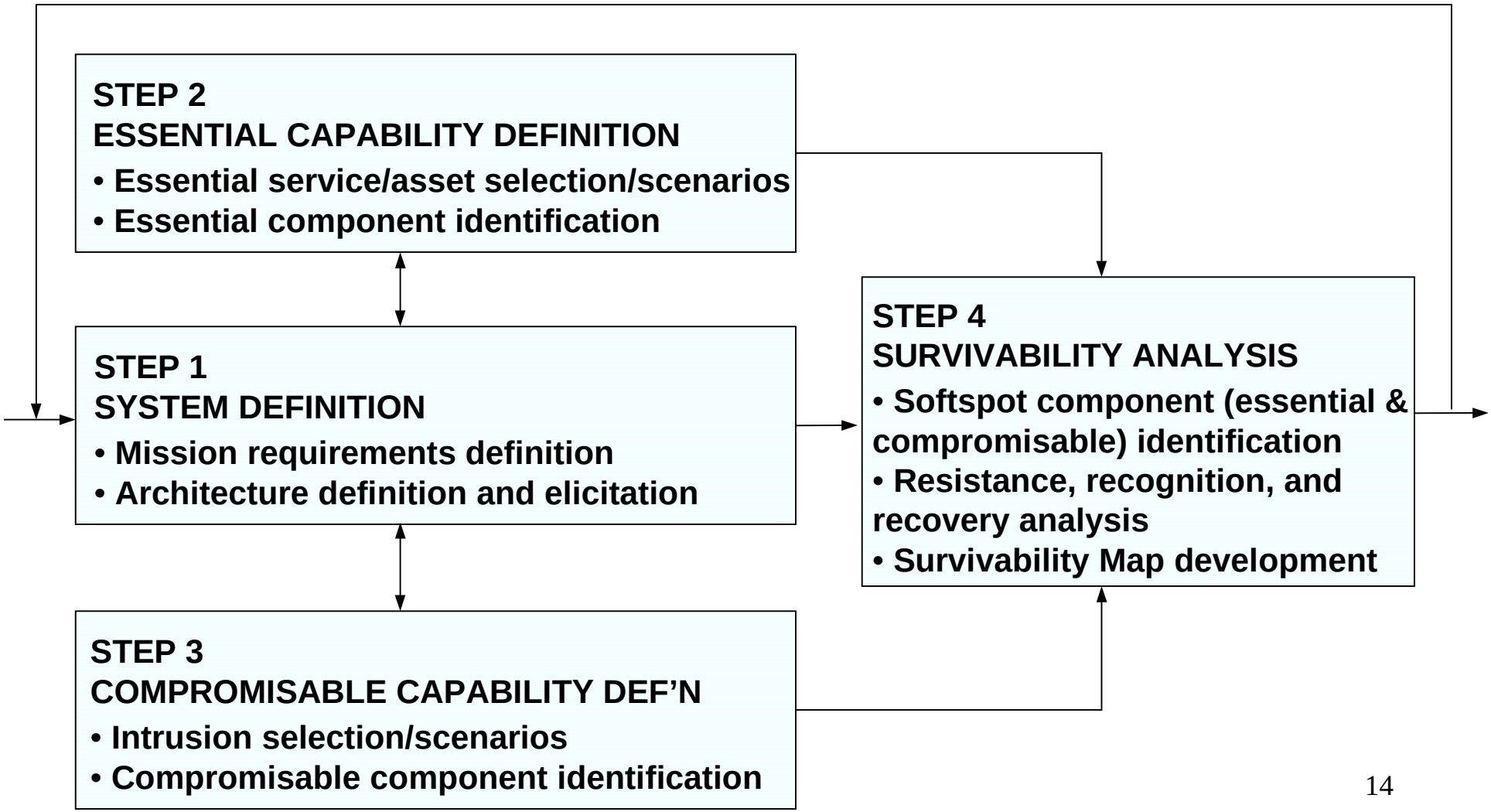
General Method

- Identify essential services with normal usage.
- Generate intrusion scenarios which are use cases for intruder
- Evaluate system in terms of response to scenarios
  - Requirements: propose response to intrusions
  - Architecture: evaluate system and operational behavior
- Mission impact
  - applications as well as system components
  - stakeholders input essential

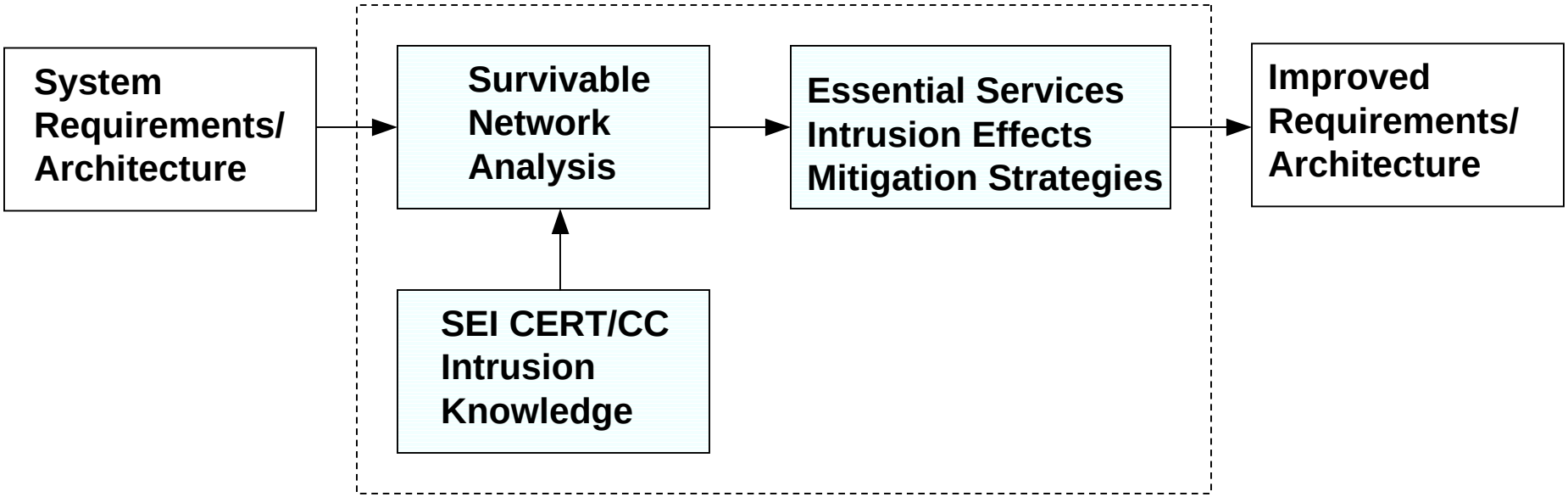
Survivability Architecture

- Make recommendations for survivability improvements
- Identify decision and tradeoff points - areas of high risk
- Identify trade-offs with other software quality attributes
  - safety, reliability, performance, usability

The Survivable Network Analysis Method



Determining Survivability Strategies



Survivability Map

Intrusion Scenario	Softspot Effects	Architecture Strategies for	Resistance	Recognition	Recovery
(Scenario 1) …		Current			
		Recommended			
(Scenario n)		Current			
		Recommended			

- Roadmap for management evaluation and action

Option: Survivability Requirements

- Identify requirements for mission-critical functionality
  - minimum essential services
  - graceful degradation of services
  - restoration of full services

- Identify explicit requirements for
  - recovery
  - recognition
  - resistance

Option: Mission Lifecycle

- Factor survivability into the development and operational lifecycle
- Capture security and survivability assumptions
  - boundaries, users
- Identify survivability decision points
  - impact of changes on recovery, intrusion detection, etc.

Benefits of the SNA

- Clarified requirements
- Documented basis for system decisions
- Basis to evaluate changes in architecture
- Early problem identification
- Increased stakeholder communication

Additional Information

- SNA Case Study: The Vigilant Healthcare System
  - IEEE Software: July/August 1999
- Survivability: Protection Your Critical Systems
  - IEEE Internet Computing: Nov/December 1999
- Web site: IEEE article and other reports

  www.sei.cmu.edu/organization/programs/nss/surv-net-tech.html