Survivable Network Analysis

Changpeng Ti
CS616 Software Engineering
Apr 21 2009
Network System Survivability

- Where do we need survivability
  - large-scale distributed systems
    - Banking
    - Telecommunications
    - E-commerce
- Why do we need survivability
Network System Survivability

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

- **Focus**
  - Delivery of essential services
  - Preservation of essential assets
  - Timely recovery of full services/assets
Network System Survivability

- Key system capabilities
  - 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
Network System Survivability

- Fundamental assumption
  No individual component of a system is immune to all attacks, accidents, and design errors.

- Fundamental goal
  The mission must survive
  - Not any individual component
  - Not even the system itself
Survivability Requirements

- Classification
  - System/Survivability Req'ts
  - Usage/Intrusion Req'ts
  - Development Req'ts
  - Operations Req'ts
  - Evolution Req'ts
Survivability Requirements

- Phases of intrusion
  - Penetration Phase
  - Exploration Phase
  - Exploitation Phase
Survivability Requirements

- Requirements definitions
  - Resistance Service Req’ts
    -- penetration and exploration
    Firewalls, authentication, encryption
    Diversification
  - Recognition Service Req’ts
    -- all 3 phases of attack
    Intrusion detection, logging & auditing
    Self-awareness, trust maintenance, black-box reporting
  - Recovery Service Req’ts
    -- exploration and exploitation
    Replication of critical info, fault-tolerant designs, backup systems
    Dynamic system adaptation
The Survivable Network Analysis Method

Step 1: System Definition

Step 2: Essential Capability Definition

Step 3: Compromisable Capability Definition

Step 4: Survivability Analysis
The Survivable Network Analysis Method

- Step 1: System Definition
  - Mission requirements definition
  - Architecture definition and elicitation
The Survivable Network Analysis Method

- Step 2: Essential Capacity Definition
  - Essential service/assets election/scenarios
  - Essential component identification
The Survivable Network Analysis Method

- Step 3: Compromisable Capacity Definition
  - Intrusion scenario selection
  - Compromisable component identification
The Survivable Network Analysis Method

- Step 4: Survivable Analysis
  - Softspot component (essential and compromisable) identification
  - Resistance, recognition, and recovery analysis
  - Survivability Map development
Thank you~