Introduction

This introduction is based on various resources, including

- [Ellison99] Survivable Network Systems: An Emerging Discipline

Note that the CMU/SEI group had many papers on the subject. Here we start with an early paper and will look at newer work afterwards.

Whereas more than 10 years have passed, most of the general arguments still hold.

Introduction

- Survivability
  - builds on related fields
    - security
    - fault-tolerance
    - safety
    - reliability
    - reuse
    - performance
    - verification
    - testing
Introduction

- **Bounded and Unbounded Networks**
  - bounded network
    - all of the systems parts are controlled by unified administration and can be completely characterized and controlled
  - unbounded network
    - radical new levels of organizational integration
    - integration obliterates traditional organizational boundaries and transforms local operations into components of comprehensive network-resident business processes
    - example, commercial organizations are integrating operations with business units, suppliers, and customers through large-scale networks that enhance communication and services. These networks combine previously fragmented operations into coherent processes open to many organizational participants.
    - this new paradigm represents a shift from bounded networks with central control to unbounded networks

- unbounded network (cont.)
  - there is no unified administrative control over its parts
  - each participant has incomplete view of the whole
    - must depend on the trust information supplied by its neighbors
    - cannot exercise control outside of its local domain

*Figure 1: An Unbounded Domain Viewed as a Collection of Bounded Systems*
Introduction

- Survivability
  - fulfill the mission, in a timely manner, in the presence of attacks, failures, or accidents.
    - Note, this is only the CMU definition.
  - Mission
    - not just the military definition
    - example of financial system
      - shutdown (12h) during a power outage caused by hurricane
      - if the system is down, but preserves integrity and confidentiality of its data and resumes essential services after the environmental stress is over, then the mission is fulfilled
      - if the same system is down 12 hours during normal conditions than the mission has failed

- Attack
  - events orchestrated by an intelligent adversary
  - includes intrusion, probes, denial of service
  - system that assumes defensive positions because of a threat may reduce its functionality and divert additional resources for monitoring and protection

- Failure
  - may be due to
    - software design error
    - hardware degradation
    - human error
    - corrupted data

- Accident
  - broad range of randomly occurring and potentially damaging events such as natural disasters
**Introduction**

- Survivability trademarks
  - must react to damaging effect
  - must recover
  - reaction and recovery may take place before underlying cause is identified
  - cause may never be determined!
  - mission fulfillment must survive, not any particular subsystem or component
  - mission must survive even if significant portions of the system are damaged or destroyed

- Characteristics of Survivable System
  - deliver essential services in the face of attack, failure, or accident
  - maintain essential properties
    » specified levels of integrity, confidentiality, performance
  - maintain balance among multiple quality attributes
    » performance,
    » security,
    » reliability,
    » availability,
    » fault-tolerance,
    » modifiability,
    » affordability.
Introduction

- **Characteristics of Survivable System (cont.)**
  - What are essential services and properties?
    - for military
      - essential services:
        - maintain overwhelming technical superiority
      - essential properties:
        - integrity, confidentiality, level of performance
    - for public sector
      - maintain integrity, confidentiality, availability of essential information and financial services in the presence of intrusions/attacks
  - Example: Key question:
    - *What are the essential services within the operational system?*

- typically there are many services that can be temporarily suspended when a system is dealing with an attack or environmental condition
  - suspension can help isolating areas affected by intrusion
  - the mission must survive:
    - if an essential service is lost it can be replaced with another service that supports mission fulfillment in a different **but equivalent** way
    - essential services should include alternate sets of essential services that
      - need not be simultaneously available
      - could be mutually exclusive
Introduction

What is the difference between
- Survivability and Security?
- Survivability and Fault-tolerance?
Introduction

◆ Survivability and Security
  - Security (typical def. w.r.t. confidentiality, integrity, availability & authenticity, non-repudiation)
    » the system is either safe or compromised
    » goal:
      ■ prevent intrusion from happening
      ■ detect intrusion if it occurred
    » largely ignores
      ■ aspects of recovery
      ■ aspects of maintaining services during and after an intrusion
  - Survivability
    » components collectively need to accomplish their mission even under attack and despite active intrusions that could effectively damage significant portions of the system
    » robustness under attack is at least as important as hardness, or resistance to attack

hardness contributes to survivability, BUT
robustness under attack and recoverability are the essential characteristics that distinguish survivability from traditional computer security
survivability benefits from computer security research and practice
survivability can provide a framework for integrating security with other disciplines
Introduction

Survivability and Fault-Tolerance
- Fault-tolerance relates to the statistical probabilities of an accidental fault or combinations of faults
- Example
  - assume triple redundant system
  - probability that all 3 components fail may be statistically small
  - this assumes independence of faults!
  - malicious faults are statistically the least likely

- however, under malicious attack with knowledge of the systems internal functions, the independence assumption may not be valid anymore
- the faults are not benign anymore and we expect malicious behavior
- Redundancy can contribute to survivability
  - may be insufficient if redundant copies are identical
  - would imply susceptibility to same attack strategy

whereas fault-tolerance is fairly well defined, there is no unique definition of survivability or the differences between both
- e.g. "Survivability is a requirement that the system must meet with a high probability. Fault tolerance is a mechanism for dealing with the major causes of system failure, namely faults arising in the system." from http://www.cs.virginia.edu/~survive/faq.html

- Related terms:
  - The term Intrusion Tolerance has been derived from Fault Tolerance
  - Is intrusion tolerance different from survivability?
    - some people might argue so, but for our purposes they address the same sentiment
Introduction

- Current State (ref. late 90s) of Practice in Survivable Systems
  - mainly “security-based” view of defense against intrusions
    - this view is dangerously incomplete
    - focus is almost exclusively on hardening of system to prevent break-in or other malicious attack
  - affordability is important factor in design, implementation and maintenance
    - has implications on national infrastructure (e.g. power grid, public switched communication networks, financial networks) and national defense
  - trend towards reusability - (opening a can of worms)
    - COTS introduces exploitable bugs
    - problem when used as part of larger system

Introduction

- Realities
  - no practical systems can be build that are invulnerable to attack
  - traditional view of information systems security must be expanded to include survivability concepts,
    - i.e., survive in spite of active intrusion
  - systems can and will be broken (into)
  - survivability must be designed into the system
    - survivability as part of the design strategy
    - analogy with VLSI and “design for testability”
      - What was that all about?
      - let’s call it “Design for Survivability”