Basic Concepts & Taxonomy for Dependable & Secure Computing
Algirdas Avizienis, Jean-Claude Laprie, Brian Randel, and Carl Landwehr

Presenter: Aly Farahat

Contents

• Basic Concepts
• Dependability & Security
• Threats:
  – Faults
  – Errors
  – Failures
  – Relationship
• Means to attain Dependability & Security
  – Fault Prevention
  – Fault Tolerance
  – Fault Removal
  – Fault Forecasting
• Conclusion

Basic Concepts

• System
  – Function
  – Structure
  – Behavior
  – State
    • Internal
    • External
  – Service
    • Service Interface
    • User
Dependability

• Original Definition:
The ability to deliver a service justifiably trusted

• Alternate Definition:
The ability to avoid service failures that are more frequent or more severe than accepted

Q: What is the relationship between both definitions?

Dependability & Security Attributes

Attributes (cont.’d)

• Availability: readiness for correct service
• Reliability: continuity of correct service
• Safety: absence of catastrophic consequences on user & environment
• Integrity: absence of improper system alterations
• Maintainability: ability to undergo modifications & repairs
• Confidentiality: absence of unauthorized disclosure of information
Threats to dependability & security

- Failure: event that occurs when the delivered service deviates from the correct service (at the service interface)
- Error: part of the system state having a value that may lead to a failure (illegitimate state)
- Fault: event that may cause an error

Q: Is it possible to have a legitimate state, though, have an error? Think about violating the specification

Pathology of Fault, Error, Failure

Faults: A taxonomy
Failures

- Service Failures
- Development Failures
- Dependability & Security Failures (second definition)
Failures (Cont.’d)

Errors

- Same domain classification as failures
- Can either be:
  - Detected or
  - Latent

The Means to attain Dependability & Security

- Fault Prevention: prevent the occurrence of faults
- Fault Tolerance: avoid service failures in the presence of faults
- Fault Removal: reduce the number and severity of faults
- Fault Forecasting: estimate the number, future incidence and likely consequences of faults
Fault Prevention

- During Development Phase
- Software:
  - Strongly Typed Languages
  - Development Methodologies
  - Modularization
  - Encapsulation
- Hardware:
  - Design Rules

Fault Tolerance

- Error Detection
- System Recovery

Fault tolerance techniques
Fault tolerance implementation

- Replication (*Physical Independent Faults*)
- Design Diversity (Solid Development Faults)
- Effectiveness (*Coverage*)
  - Problem in fault tolerance mechanism
  - Incorrect fault assumptions

Q: Where are fault-tolerance formal techniques located in the previous slide’s tree?

Basic Strategies for Implementing fault tolerance

Fault Removal

- During Development
  - Verification
  - Validation
- During Use: *corrective maintenance*
Verifications Strategies

Verification

System not exercised

Static authentication

Static analysis

Theorem proving

System exercised

Dynamic verification

Behavioral inputs

Model checking

Symbolic inputs

Symbolic simulations

Actual inputs

Testing

Q: How fault prevention, fault handling and verification are differentiated?

Fault Forecasting

• Qualitative Evaluation: *classify failure modes and rank them*

• Quantitative Evaluation:
  – Stochastic Modeling
  – Reliability growth models

Summary

Q: How are dependability & security attributes quantitatively influenced by threats?
Thank you!