A Case for Survivability

A Worthy Research Problem

O. Sami Saydjari
28 June 2002

Definition

- Survivability – see dependability (ability to deliver service that can justifiably be trusted)
- Case for Survivability – a convincing argument that a system meets its survivability specification (desirable survivability properties, like confidentiality)

Case for a Case

- Because Assurance is hard, trend toward functionality without the assurance
- Survivability functionality without assurance can actually be worse than nothing at all
  - Example: confidentiality labeling just tells attackers where the good stuff is
- Risk is uncertain without a case
- Lack basis for survivability trade-offs

Properties of a Case

- Socially Refereeable
  - Clear, concise, modular & composable
- Maintainable
  - Argument needs to keep up with spec
- Validatable
  - Explicit and testable premises
- At the Right Abstraction Level
  - Mappable all the way to implementation
- Expressive of Realistic User Needs
  - Can handle large complex systems
  - Example - *-property

Some Useful Historical Mistakes

- Ignoring Application Assurance in Computer Security – Orange Book
- Enshrining techniques without a deep understanding of their assurance value
- Overly-narrow focus on subsystem properties and assurance – Crypto
- Over promise of verification technology –
- Unrefereeable assurance evidence - LOCK
- Creating Sub-useful systems – Multics, Guards

Lessons for School of Hard Knocks

- Theories of Security Come from Theories of Insecurity – *Rick Proto*
  - Must achieve coverage of the attack space
- They Come at you Through the Weeds – *Earl Boebert*
  - Implementations and interfaces matter
- Consider the Spherical Chicken
  - Models need to be accurate
  - Attackers need find only one path; defenders must find all
- Non-steady state matters – don’t assume secure initial state

Security Assurance: Criteria

- Operational Assurance
  - System Architecture – TCB in own domain, layering
  - System Integrity – health checks
  - Covert channel Analysis – ***formal*** search, estimate
  - Trusted Facility Manual – role separation
  - Trusted Recovery – no compromise
- Life Cycle Assurance
  - Security Testing – find all flaws, resist penetration
  - Design Specification and Verification –
    - Model, FTLS, DTLS, Spec-to-Code maps, formal proofs
  - Configuration Management – design, dev, maintenance
  - Trusted Distribution – mapping master to cur version

Related Cases

- Safety Cases
- Dependability Cases
- Formal Testing Methods
- Hazard Analysis
- Work Factor/ Red Team Work Factor
- Criteria Compliance Cases

What do we need

- Framework/Unification of techniques
- Accounting framework for Evidence
  - Mixed evidence, testing, formal proof, inspection, etc.
- Ways to compose the evidence
- Statements about properties that matter to customers
  - Can it withstand 5 yrs of attack by nation-state
  - What is probability my secrets will leak
- Residual risk statements from evidence