

Software Survivability

Ansatz zur Quantifizierung der
Überlebensfähigkeit von
Softwaresystem

Andreas Rascher

Seminar: Web-Qualitätsmanagement

Sommersemester 2004

Gliederung

1. Einleitung
2. Survivability
3. Software Survivability – Definition
4. Quantifizierung von Software Survivability
5. Attribute
6. Metrik für einen Survivability Index
7. Ausblick

Einleitung

- Absolute Sicherheit ist nicht erreichbar
- Konstant steigende Zahl bekannter Schwachstellen
- Systeme müssen so entwickelt werden, dass sie mögliche Bedrohungen bewältigen

Einleitung

- Bisherige Ansätze:
 - security
 - availability (Verfügbarkeit)
 - reliability (Ausfallssicherheit)
 - Fehlertoleranz
- Forschungsgebiet der Survivability
 - Entwicklung und Verbesserung von Systemen, die in der Lage sind Dienste anzubieten, sogar nachdem Sicherheitsmaßnahmen versagt haben

Survivability

- survive what?
 - Naturkatastrophen
 - Feuer, Flut, Erdbeben, Stürme
 - Künstliche Unfälle
 - Kabelschnitte, Bediehnungsfehler
 - Hardware/Software Fehler
 - Bugs, Hardwareversagen
 - Böswillige Attacken
 - Denial of service, Computerviren

Software Survivability - Definition

- Viele Definitionen aus intuitiver Sicht
- Eckpunkte des allg. Verständnisses
 - ‚Etwas‘ das zu funktionieren hat
 - Die ‚Bedrohung‘, welche das ‚Etwas‘ am Funktionieren hindern will
 - Der Fakt, dass die ‚Bedrohung‘ von einer intelligenten Kraft betrieben wird
- Definition:
 - Die Eigenschaft von (Teil-) Systemen, Ausstattung, Prozess oder Prozedur, die einen bestimmten Grad an Sicherheit bietet, so dass die genannte Entität ihre Funktionsweise fortsetzt - während sowie nach natürlichen oder künstlichen Störungen

Quantifizierung von Software Survivability (1)

- Warum?
 - Aktueller Stand
 - Einfluss von Änderungen am System
 - Erfolg/Misserfolg von Verbesserungen
 - Während des Design-Prozesses -> Entscheidungen

Quantifizierung von Software Survivability (2)

- Ansatz: Zerlegung der Software Survivability
 - Aufspaltung des Systems in Teilkomponenten
 - Kleinste Komponente = Modul
 - Modul ist die kleinste messbare Einheit
 - Auf Softwareebene ist Modul äquivalent zu einer Funktion (z.B. in C)

Quantifizierung von Software Survivability (3)

- Beispiel:
 - C - Funktionen: memcpy, strcpy machen keine Begrenzungsprüfung, wenn sie in den Arbeitsspeicher kopieren, überschreibt andere Speicherbereiche
 - Folge: Änderungen im Verhalten der Anwendungen

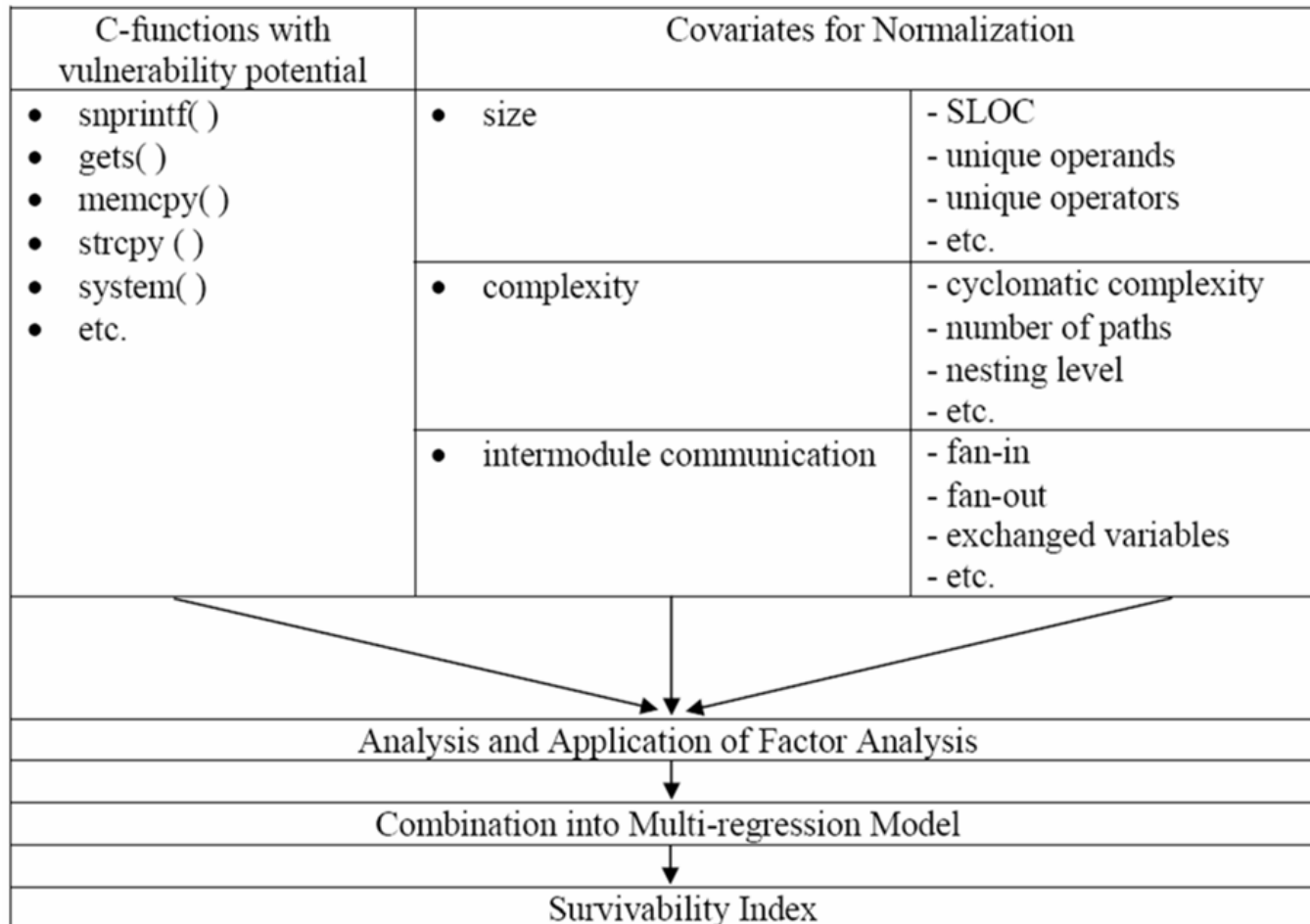
Attribute (1)

- Die Idee einer Survivability – Metrik:
 - basiert auf dem Fakt, dass bestimmte Code - Konstrukte den Quellcode verletzbarer gegenüber böswilligen Inputs machen
- Spezielle Schlüsselwörter und Sequenzen können gezählt werden
- Survivability wird besonders an den Schnittstellen gemessen
 - Anzahl von Input/ Output – Operationen
- Komplexe Software ist potentiell anfälliger für böswilligen Input

Attribute (2)

- Normalisierung und Gewichtung
 - Software mit den beschriebenen Code-Konstrukten ist nicht automatisch verwundbarer aber die Wahrscheinlichkeit steigt mit einer höheren Anzahl
 - Mehr gezählte Konstrukte \neq höhere Verwundbarkeit
 - Ausgleichende Maße werden benötigt
 - Zum Normalisieren (z.B. LOC)
 - Zum Gewichten (z.B. Code Größe, Komplexität und Informationsfluss)

Metrik für einen Survivability Index



Ausblick

- Dynamische Survivability
 - Echtzeitmessung von Survivability
 - gezielte Aktionen sobald Indexwert einen kritischen Punkt unterschreitet z.B.:
 - Zuschalten von weiteren Sicherheitsmaßnahmen
 - Abschalten bestimmter Dienste
 - Einfluss bestimmter Aktionen im System auf die Survivability messen