Prüfungsprotokoll Vertiefung - Freiling geb. Gärtner
Verlässliche verteilte Systeme I+II (je V4), Information Warfare (V2), Fallstudie von Apollo bis Space Shuttle(V2)

14. Juli 2005

Beisitzer war Martin Mink. Note: 1.0.

1 VVS II

Einleitend kam die Frage womit ich anfangen wolle, ich entschied mich für CHT.

- Zunächst: wie zeigt man denn das ein Fehlerdetektor schwächer ist als ein anderer? *(man hat Algorithmus gegeben der ein Problem mit einem Fehlerdetektor FD löst und zeigt das man damit den fraglichen Fehlerdetektor emulieren kann)*
- Wie funktioniert denn CHT? *(CHT komplett erklärt)*
- Wo werden denn die Eigenschaften von Consensus im Beweis benutzt? *Agreement: ? (anscheinend wird es im Anhang des Papers benötigt, um zu zeigen, daß auch wenn c_k bivalent ist der ausgegebene Prozess korrekt ist), Validity: c_0=0-valent, c_n=1-valent $\rightarrow$ es gibt c_k, Termination: es wird auf jedem Pfad nach endlicher Zeit ein Wert entschieden (fürs tagging)*
- Was hat man denn jetzt für die Praxis davon, das Omega der schwächste Fehlerdetektor ist? *(besser als P? (bringt in der Praxis wenig, soll helfen Komplexität von Algorithmen zu vergleichen und ein Gefühl für die Schwere zu bekommen))*
- Synchronität? *(asynchron, eventually synchron, synchron)*
- Kann man mit omega im eventually synchronen system etwas für die Praxis anfangen? *(nein, weil ich nicht weiß ab wann ich omega vertrauen kann)*

2 VVS I

- Gibt es denn in der Praxis synchrone Systeme? *(Nein)*
- Wir hatten den Begriff der Überdeckung, was war das? *(Erbringung der Leistung außerhalb der Spezifikation / Wahrscheinlichkeit das das System auch außerhalb der Spezifikation läuft)*
- Nehmen wir an wir hätten einen Consensus Algorithmus der für ein asynchrones System ohne Fehlerdetektor implementiert wurde. Wie ist dann die Überdeckung in der Realität? *(die ist 1)*
- Wir haben ja den Bereich security sehr hervorgehoben in der Vorlesung, was ändert sich denn dann bei meinen Fehlerannahmen? *(Probleme sind nicht ohne weiteres Übertragbar; Byzantine-Annahmen wie wir sie hatten reichen nicht aus; Angriffe sind nicht statistisch unabhängig; z.B. non-interference security ist weder safety noch liveness)*
- Wie kann man denn z.B. die Integrität von Informationen sicherstellen? *(zum Beispiel mit tripwire, um überhaupt erstmal Veränderungen am System feststellen zu können)*
- Wie funktioniert denn Tripwire? *(es werden cryptographische Checksummen über Dateien in einer Datenbank gespeichert, außerdem kann z.B. noch angegeben werden das sich bestimmte Dateien nur vergrößern (logdateien) und Verzeichnisse nicht verändern dürfen (/etc, /bin) – das ganze kann aber nur funktionieren, wenn sowohl die Datenbank als auch das binary auf einem read-only Dateisystem gespeichert ist)*
- Wie kann man denn Tripwire umgehen, wenn man auf einem Computer eingebrochen ist, und Datenbank und binary beschreibbar sind? *(z.B. das binary ersetzen, oder Systemcalls so ändern das bestimmte Verzeichnisse nicht angezeigt werden)*

3 Information Warfare

- Wie wird denn InfoWar definiert? *(Operationen auf Informationsressourcen mit Ziel „Erhöhung Verfügbarkeit für Offense…“)*
- Wie ist denn der Zusammenhang zwischen Safety, Liveness und Non-Interference security aus VVS2 mit diesen Zielen *(Verringerung der Verfügbarkeit für Defense → Verletzung von Liveness; Verringerung der Integrität → Verletzung von Safety; Erhöhung der Verfügbarkeit für Offense → Verletzung von non-interference security)*

4 Fallstudie: Apollo bis Spaceshuttle

- Jetzt ist ja das Thema Shuttle wieder aktuell, und man hört in Dokumentationen immer das es nicht gehalten hätte, was es versprach? Kannst du dem zustimmmen? *(Ja, das liegt aber daran das zu viel versprochen wurde, und die NASA die Kosten und Starts pro Jahr schönrechnen mußte, um* *das Shuttle überhaupt bauen zu können; Außerdem waren die Anforderungen an das Shuttle auch sehr vielseitig, es sollte zum Beispiel nicht nur schwere Lasten transportieren können sondern auch als „mobiler Spionagesattelit“ dienen; Und nach der Budgetüberziehung von Mercury, Gemini und Apollo hätte man auch beim Shuttle damit rechnen können)*

- Hätte man denn das Columbiaunglück verhindern können, nach der Challenger Katastrophe? *(nein, Columbia war nicht vorhersehbar, außerdem waren die Astronauten ja im Weltall und runterkommen müssen sie – bei der Challenger gab es vorher Diskussionen über die Sicherheit, die aber durch die Managementstruktur bei der NASA dann ignoriert wurden)*

- Ist denn die Einstellung gegenüber der Sicherheit von Technik jetzt größer geworden? Oder wie war die denn nach Apollo? *(Nach Apollo gab es ja die Euphorie, das technisch alles machbar ist. Da hatte man aber auch Geld um sich Sicherheit zu kaufen. Nach der Challenger Katastrophe wurde die Managementstruktur überarbeitet und das Verhältnis von Ingenieuren und Astronauten verbessert. Außerdem wurde die Mentalität „Wir sind bei der NASA also bauen wir sichere Hardware“verändert.)*