Thesis Project Structure:

## Intrusion Recovery for PaaS using Redo

Quero um sistema que faz rewind e redo das accoes do utilizador para conseguir recuperar os dados que foram comprometidos em caso de intrusao. O sistema poderia ser também aplicado em outros casos, caso paper das faults. O foco é a recuperação aplicacional e multi-layer. A recuperação ao nível do SO tira proveito de PaaS exigir imagens das máquinas que estão limpas e podem substituir SO comprometidos.

Não usamos Selective Undo (backward recovery) tem falsos negativos que implicam a perda de dados e não suportam que o software mude porque assumem apenas as dependencias originais. Usamos rewind e redo porque assim podemos mudar o software (patch), não temos de saber qual o erro original porque tudo é rolled-back (ainda que possa memorizar as response e ajudar a determinar se houve intrusion) e como a cloud dá escalabilidade para usar 1000 servidores durante 1 hora, o processo deixa de ser custoso em termos temporais.

As dependências deixam de ser usadas para Selective Undo, passam a servir para ligar requests entre si. Para aumentar o nº de requests em paralelo.

As dependencias são nível da base de dados (assume que computation tier é stateless e pedidos não comunicam sem ser pela BD) e formar grafos independentes de pedidos. Como os pedidos são geralmente indepentes entre utilizadores, podemos executar mais pedidos em paralelo. Falsos positivos deixam de ser problema, apenas atrasam o redo.

# Introduction

*Existem várias soluções para problemas especificos, vou integrar várias: Redo, Intrusion Recovery e Paas.*

* Explicar o que é PaaS mais resumidamente - Caracteristicas: Custo computação on Iaas, containers e abstracção ao programador.
* O problema a resolver: Intrusões nestes sistemas: Porque são um problema? Quais as causas?
* Como é que vou resolver o problema?
* Contribuiçoes que a solução oferece ao problema proposto

# Fault Characterization

* O que são faults? Como ocorrem?
* O que são intrusion, parte das faults…

Técnicas de suporte: Detection, Prevention porque não funcionam no caso das intrusion? Explicar as fases de fault recovery e qual é a fase em que nos estamos a focar e dizer que os trabalhos mais comuns assumem a detection por outra entidade.

# Intrusion Survivability Techniques

* Intrusion tolerance techniques: papers do professor e Verissimo para explicar mecanismos como byzantine, fault removal (Dare), proactive recovery (restarts). Esta é a approach que uso para o nível do SO.
* Não é suficiente, as máquinas podem ser atacadas e o sistema pode não conseguir tolerar por isso temos de recuperar
* Recover oriented Software (Intrusion recovery): O que é o paradigma?

# Recovery based on Undo and Redo

*Experience with Evaluating Human-Assisted Recovery Process – Porque usar o redo para recovery?*

* Porque recuperar baseado em Undo (Selective/Backward Recovery) vs Rewind (Forward Recovery): explicar o conceito e a diferença entre Undo e Rewind.
* Explicar o conceito de dependencia de pedidos: taint para conseguir saber quais os pedidos que queremos remover quer seja Undo quer seja Redo
* Recuperação da base de sistemas operativos (file systems)
  + Dependencias de SO level, memory and system calls: Aspectos de granualidade
* Recuperação de Bases de Dados
  + Dependecias ao nível das transacções: WR Set is the only way?
* Recupearação ao nível Aplicacional
  + Dependencias multi-tier
  + Dependências ao nível do Código: que servem para determiner se os path tiveram efeito
  + Consistência externa: como é que o utilizador é informado das mudanças? Poucos abordam isso

Comparação das vantagens e desvantagens entre as várias soluções numa tabela.

# Platform as a Service Model

* Caracterizar o que é PaaS, a arquitectura tipica. Para facilitar compreender o resto
* PaaS providers e as suas caracteristicas e comparação entre eles

# Architecture

## Shuttle Architecture

* Conceito: rewind and redo
* Listagem dos modulos
* Como é que os modulos funcionam entre si quando online
* Como é que os modulos funcionam entre si quando recovery mode

# Evaluation

# Schedule

# Conclusion

**Rewind/Forward Recovery**

* Rolls the system state back to the most recent clean snapshot and selectively applies the non-contaminated redo operations to keep useful work.
* Mais lento a reparar a não ser que o sistema faça vários checkpoints

**Undo/Backward Recovery/Selective Undo**

Rolls the current system state by undo contaminated operations until the entire system is clean.

Avoid the overhead of checkpointing and the repair time is proportional to the duration before intrusion or mistakes are detected.

Intrusion Tolerance vs Intrusion Recovery

Intrusão é a prática de explorar uma vulnerabilidade e através dessa prática passar o sistema para um modo incoerente.

Recuperar das intrusões implica passar o sistema de um estado incoerente para um estado coerente, que é o que este trabalho faz. Se essa mudança for realizada sem que o utilizador externo se aperceba do estado incoerente, então conseguimos tolerar a intrusão.