the fuzz factor

Robert Svensen,
Jacob Nordgren
Presentation av projektspec.
DD143X
9/2 -10

Fuzzing

- Automatisk säkerhetstestning
- Historia
- SPIKE,Sulley, Peach

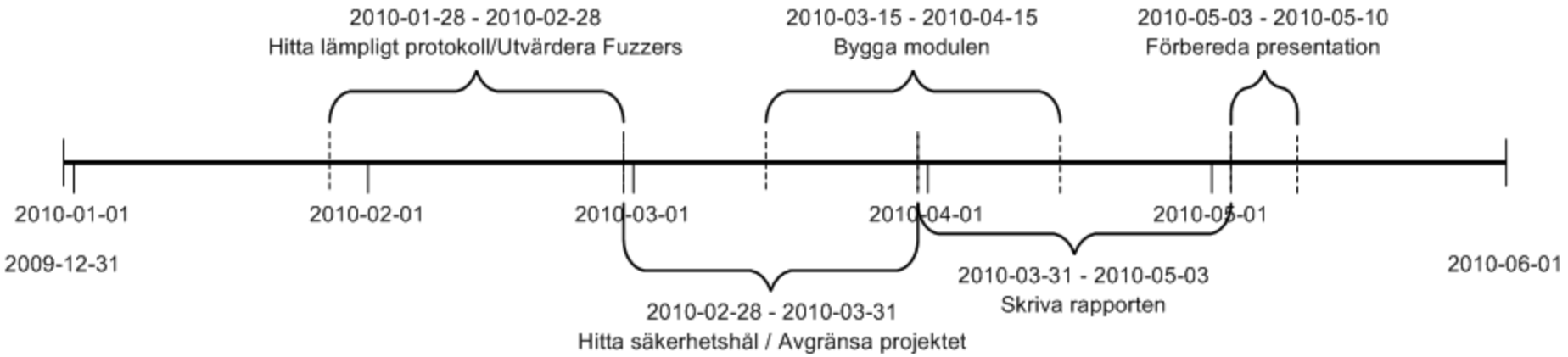
- Film: http://www.d.kth.se/~jacobnor/kand/presentation%201/CSS_DIE_FF_V2_REDIGERAD.wmv

Problem

- Problem med icke automatisk test
  - Dyrt
  - Tråkigt
  - Lätt att göra misstag
  - Kunskapsbrist
- =Bygg en fuzzingmodul

- Svagheter med fuzzing
  - Inga garantier
  - Tar lång tid
  - Kräver mycket resurser
  - Svårt att bygga bra moduler

Planering


2010-01-28 - 2010-02-28
Hitta lämpligt protokoll/Utvärdera Fuzzers
2010-03-15 - 2010-04-15
Bygga modulen
2010-05-03 - 2010-05-10
Förbereda presentation
2010-01-01
2009-12-31
2010-02-01
2010-03-01
2010-04-01
2010-05-01
2010-06-01
2010-02-28 - 2010-03-31
Hitta säkerhetshål / Avgränsa projektet
2010-03-31 - 2010-05-03
Skriva rapporten