Notes from seminar topic “Practical reports on dependability”

Presenter: Arlene Pearce
Time: 2. Lecture on the 12th of February
Note taker: Morten Lindeberg

Presentation

Arlene’s presentation was based upon the article “*Causes of Failure in Web Applications*” by Pertet et. al. This article was a practical report with statistics found in several newspaper articles written on the topic of failures on commercial web applications.

The article focused on non-malicious failures, and classified them into four categories:

- Site unavailability
- System exception
- Incorrect result
- Data loss / corruption

Further on, Arlene presented statistics from the article showing that 80% of downtime on web applications is actually planned. This means that only 20% of the downtime is unplanned. Out of the unplanned downtime, 80% of the errors are caused by software (40%), and human (40%) errors. Roman pointed out that the hardware has become way more reliable than in the 80ies, although at Google, they claim that their super cluster undergoes a hardware malfunction each hour. Because of redundancy, this although is not notable for the end-user.

Triggers of failures were:

- Resource exhaustion
- Logical errors
- System overload
- Recovery code
- Failed upgrades

Arlene then presented methodology for the duration of failures, e.g., permanent failures, transient failure and intermittent failures, and also fault chains. Fault chains, are series of component failures either uncoupled, or tightly coupled.

As example of one the failures described in the survey, Arlene presented an occasion where “Danske bank” during the routing maintenance changed a malfunctioned disk leading to 3 days of downtime. During the disk switching, several unpredicted errors occurred, which was the actual reason for the drastic amount of downtime.

Arlene claimed the main contribution of the article to be the finding of the fact that 80% of unpredicted downtime is caused by software / human errors. As pointed out by Roman, this is the a great motivation for having autonomic web-servers; “to get humans out of the loop." Another conclusion to draw from this is that web-servers in general lack redundancy in presence of human errors.

Questions and Discussion

As a first question, Roman questioned the 404 failures, since they in the article is said to be caused by "site unavailability." What about links with errors? Arlene stated that the article lacks statistics showing this kind of error. Roman also asked for more statistics on the duration of recoveries. In response, Arlene questioned the statistical quality of the data the article was based upon, since the sources are newspaper articles rather than results found in scientific papers. Although she found the fact that 80% of the unexpected downtime was due to software / human errors to be quite a contribution.

Frank remarked the need of self-configuring solutions since so many errors is caused by miss-configurations.

Tommy claimed the article to lack focus on solutions, and Morten (me) thought it would be nice to include also statistics based upon errors caused by malicious attacks, e.g. DoS and viruses. In response to Tommy's claim on the lack of focus for solutions, Anh agreed, and stated it seemed that limiting the input of the user to perhaps be one possible solution to the errors caused by software / human.

In the direction of limiting user input, Eli commented on the fact that in-air collision avoidance systems in aircrafts overrides control tower personnel in emergency situations. This meaning each and one of us (at least those of us that have ever been on an airplane) trust computer decision support with our lives. An article describing the system can be found here:
"http://en.wikipedia.org/wiki/Traffic_Collision_Avoidance_System."

The trustfulness of the cause of errors presented in the articles was also questioned, since the error descriptions might originate from corporate press releases. As Arlene stated, "it might be a lot more to it", referring to the error reports. Frank stated "some companies might preserve many details, especially banks".

Aida remarked that the article, like they don't do in risk analysis, looks at consequences without looking at the cause. Meaning they should have argued wetter or not to reason the linkage between consequences and their causes.

Conclusion

To draw a conclusion, the main contribution of the article can be said to deal with the fact that most errors is caused by human operators. These errors seems harder to mask than other errors, which can be easily hided by the use of redundancies. The amount of human errors is clearly a motivation for autonomous systems, which in addition should be self-adaptive.