(Some remarks about)
Dependability of large networked computer systems

Jean-Claude Laprie
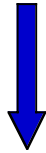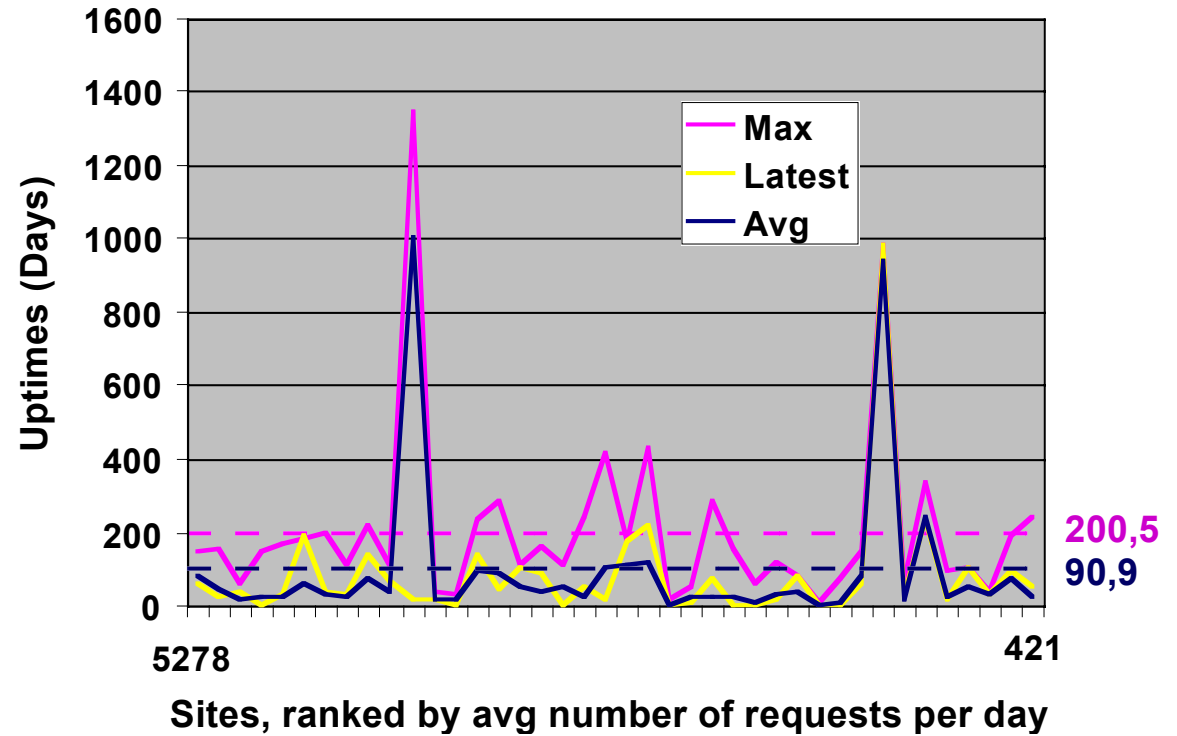
Findings

Availability Drop

99.999% - 99.99%

(wired telephone,

computer systems in the 90's)
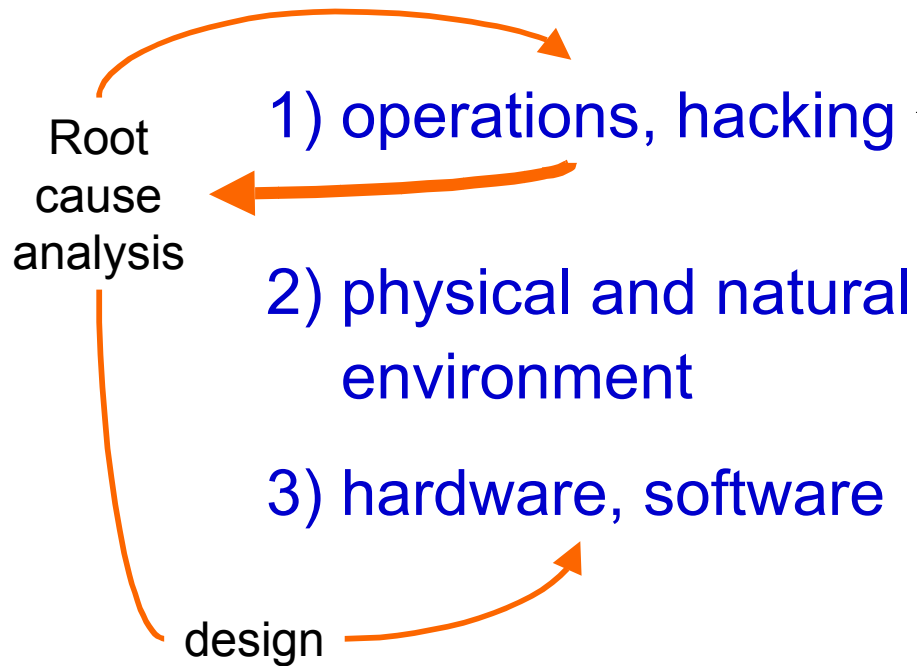
⬇

99% - 90%

(cellular phone,

Web-based services)

Uptimes of the 40 most requested sites (netcraft.com)

Legend: Max, Latest, Avg

Y-axis: Uptimes (Days), 0 to 1600

Dashed lines: 200,5 (Max), 90,9 (Avg)

X-axis: 5278 to 421

Sites, ranked by avg number of requests per day

Causes?

? Surface: ignorance, velocity

? Deeper: complexity-related, hackers

Causes of failure

Challenges

(Some) Remedies

Root
cause
analysis

1) operations, hacking

human activity
and system co-
design

2) physical and natural
environment

3) hardware, software

diversity

design

☞ Likely to hold for
networked embedded
systems

Some Gaps

composability

metrology

☞ Co-design of human activity and system

- ➢ Absence of exploitation of findings by cognitive ergonomists
- ☞ From task allocation to reciprocal monitoring and recovery

☞ Diversity

- ➢ Decreasing natural robustness of hw and sw ➟ fragility of systems based on uniform solutions
- ☞ Revisiting diversity at all system levels

☞ Composability of dependability (logical) properties

- ➢ Performed on a largely ad-hoc basis
- ☞ Formalisation for transferability, durability, scalability

☞ Metrology

- ➢ Prerequisite for substantiating current and future research (current gaps? expected future threats?, identified from exploitation of measurement trends)
- ☞ Need for widely accepted basis for data collection and measurements of accidental and malicious events

Survey on computer damages in France

- ➢ Year 2000
- ➢ Representative sample of 450 organizations (size, activity domains)
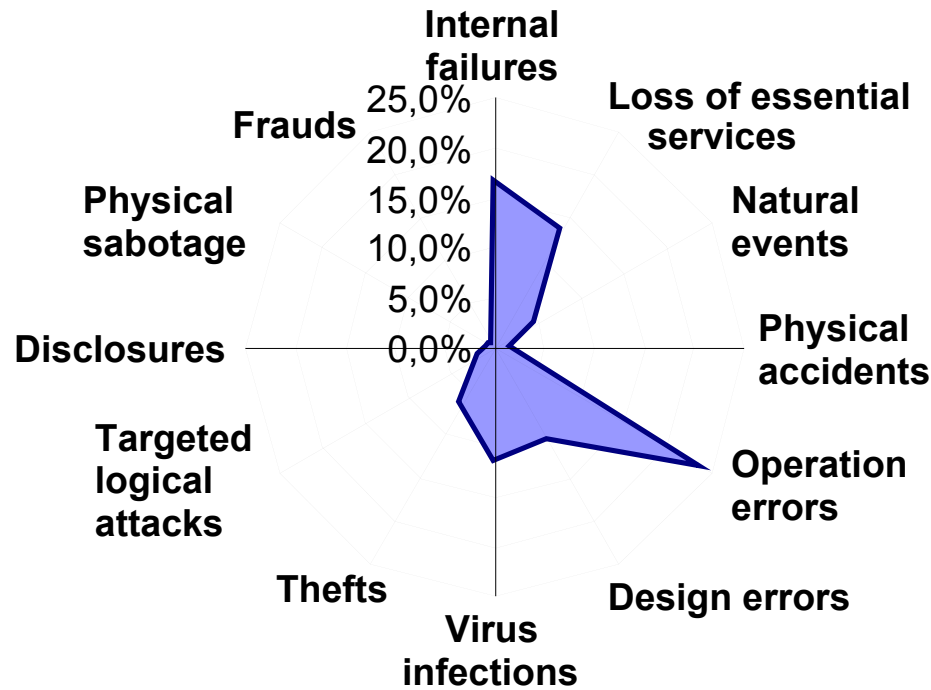
Damage occurrences
(percentage of affected organizations)

Perceived risks