Softwaretechnik

Vorlesung 01: Einführung

Peter Thiemann

Universität Freiburg, Germany

SS 2008

Inhalt

Einführung

Software Engineering

- programming in the large
- principles, models, and techniques for development and maintenance
- emphasis on engineering techniques
- Goals:
  - cost reduction for development and maintenance (often 80 %)
  - delivery dates
  - high quality
  - efficiency

Software Crisis

- coined 1965, NATO meetings 1968/69
- programs hard to maintain (punch cards, mag tapes, restricted machines)
- documentation absent or obsolete
- overrunning cost and deadlines

Characteristics of Software

“Software is soft”

- immaterial: no wear and tear, no physical limitations, no spare parts, hard to measure, easily changeable
- aging

Software Development Today

- Hardware not an issue
  - cost for development and maintenance more important than efficiency (Moore's law)
    cost of software $\nearrow$, cost of hardware $\searrow$
  - more complex systems
- teamwork essential ($\rightarrow$ decomposition, interfaces, contracts)
- two kinds of developers/applications

Two Kinds of Applications

applications with short time-to-market

base functionality more important than correctness, robustness
$\longrightarrow$ accelerated design process

safety critical applications

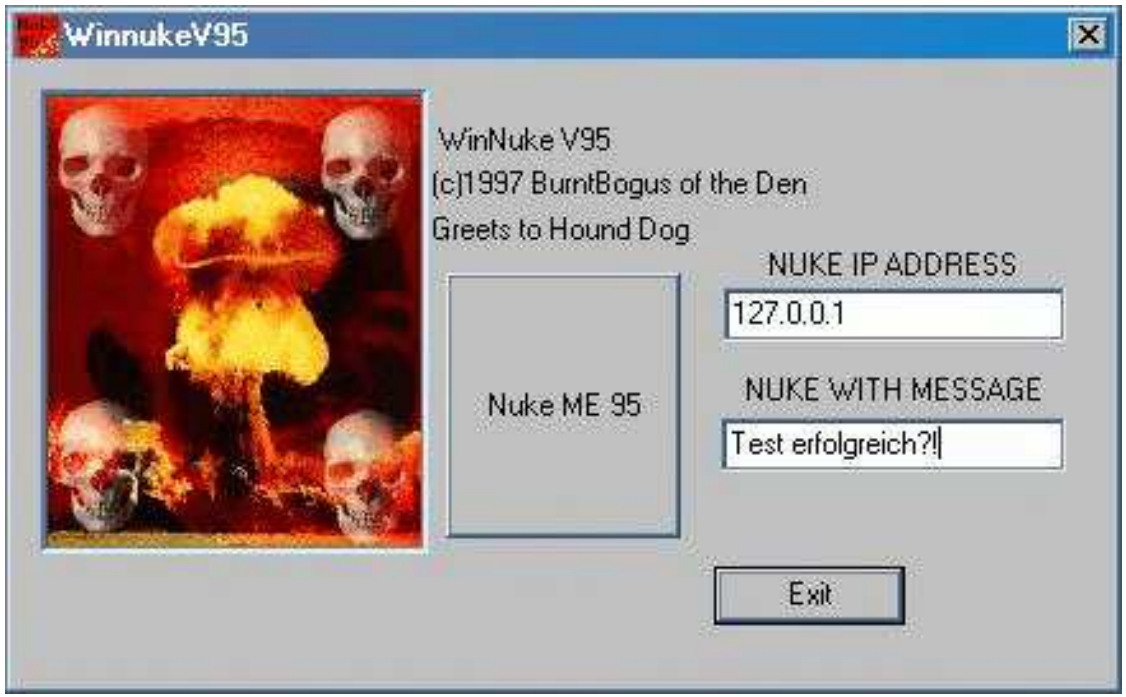
correctness essential for functionality
$\longrightarrow$ (semi-) formal methods, verification

Software Crisis Today . . .

Bugs can be funny

In September 1997, a crew member of the cruiser USS Yorktown mistakenly entered a zero for a data value, which resulted in a division by zero. The error cascaded, crashed every computer (WinNT 4.0), and eventually shut down the ship's propulsion system. The ship was dead in the water for 2 hours 45 minutes.

Bugs make you vulnerable



A faulty implementation of Window's NetBEUI (Win95, WinNT) crashes the whole system if there are some unresolveable characters received at port 135 or 139. A tool (malware) to exploit this error was WinNukeV95, which sends a message to the victim before crashing the computer.

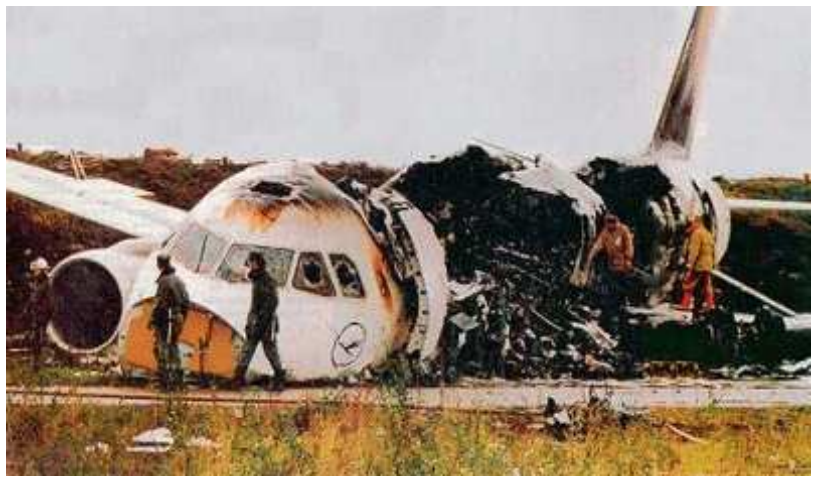
Bugs can be expensive

Customers of the Postbank using a "Sparcard" to withdraw money in January 2002 at another bank didn't have to use their PIN to do so, and there was also no charge on their accounts. This failure was introduced by changes made to adopt to the Euro. Fortunately there was only one exploit of this failure.

In the first night of operation of a new system 28 billion dollars were wrongly transferred to other banks. Only 24 billion dollars could be returned, the remaining money was untraceable.

Bugs can be fatal

In September 1993 an A320 skidded off the end of the runway during landing. The aircraft touched down with sink rate low enough that the onboard flight computers did not consider it to be “landing”, which inhibited thrust reverse and brake application for nine seconds.



The failure was caused by adopting two unnecessary preconditions to landing (weight on wheels, wheels spinning). They were introduced because of an earlier accident (Lauda Air) where reverse thrust was applied during normal flight, wrongly assuming the plane was about to land.

Neverending Stories . . .

In the meantime the modules in the trucks (On Board Units - OBU) aren't the worst havoc to the engineers anymore. Software problems have grown more serious. The billing system for example works so clumsy it will break down under real conditions. [. . .] The final OBU-software shall go into action on Jan, 1st 2006 . . . [Quelle: BBV-NET]

Plan for a software engineering course

- No consensus on "what is software engineering"
- No simple (or single) answer ("No silver bullet", Fred Brooks)
- But there are *techniques*, *methods*, and *tools*, that can reduce the complexity of constructing systems
- There are also techniques for building specific kinds of systems with high degrees of reliability

Approach

- It is not possible to present and practice the full spectrum of approaches to software engineering in one class
  - industrial setting is completely different from a University
  - insufficient time for development in the large
  - different problems demand different techniques

$\Rightarrow$ We survey central concepts and experiment with selected approaches

$\Rightarrow$ Emphasis on techniques for safety critical systems

- Specialized techniques presented in depth in advanced courses

Our View on Software Development Methods

1. Specification with types
   - type systems
   - type soundness
   - uses of type systems
2. Specification with logics
   - design by contract
   - monitoring
   - verification
3. Semi-formal methods
   - UML diagrams
   - OCL
   - meta modeling
4. Testing