Verification & Testing

Roderick Bloem
IAIK

Green & blue seats
No masks necessary when seated

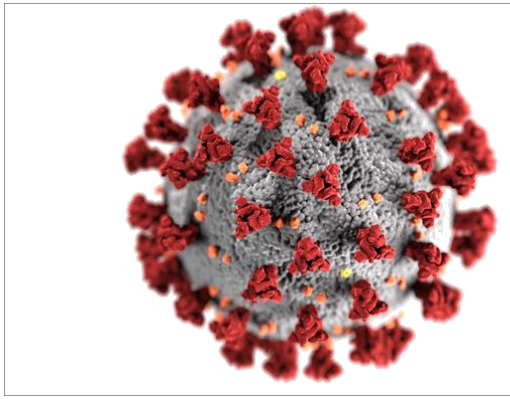
50% attendance

Corona

Register in Teachcenter, first come first serve

Videos

online: last year's & this year's videos
Watch this year's videos for details on exercises etc



Today

1. Administrative
2. Motivation

Administrative

Material & Communications

- **Webpage:** https://www.iaik.tugraz.at/vt
- **Question Hours:** Mondays before deadlines.
- **Discord:** https://discord.gg/7ScBn2u6 channel VT (activate with check mark)
- **Email:** benedikt.maderbacher@iaik.tugraz.at
  erwin.peterlin@student.tugraz.at

How to get a grade?

Lecture:

Take the exam (main exam date: 31 Jan 2022)

Exercises:

- 4 assignments
- At least one submission → you'll get a grade

Plan

DATE	TOPIC
14 Oct (BM)	Eraser & Locktree
21 Oct	Memory Debuggers
28 Oct (BM)	Symbolic Methods
04 Nov	Hoare Logic
18 Nov, i11 (BM)	Static Analysis
25 Nov (BM)	Deductive Program Verification
26.11.2020	Java Path Finder
2 Dec, 9 Dec, 16 Dec	SLAM
~~23 Dec, 30 Dec, 6Jan~~	— Christmas Holidays —
13 Jan	Java Pathfinder
20 Jan	Current Research Topics
27 Jan	Question Hour
31 Jan	EXAM

Exercises

Assignment	UE Handout	UE Question Hour	UE Deadline
A1 Locktree	14 Oct	25 Oct	28 Oct
A2 Hoare	4 Nov	15 Nov	18 Nov
A3 Dafny	25 Nov	13 Dec	16 Dec
A4 SLAM	16 Dec	17 Jan	20 Jan

Grading Scale (Exercise):

```
if (points(a1) >= 10 && points(a2) >= 10 &&
    points(a3) >= 10 && points(a4) >= 10)
{
    sum = points(a1) + points(a2) + points(a3) + points(a4)
    if (sum / 3.0 >= 87.5)
        return 1;
    if (sum / 3.0 >= 75)
        return 2;
    if (sum / 3.0 >= 62.5)
        return 3;
    if (sum / 3.0 >= 50)
       return 4;
}
return 5;
```

The Sorry State of Testing

```
Apple SSL/TSL v55741, Feb. 2014
SSLVerifySignedServerKeyExchange:
. . .
hashOut.data = hashes + SSL_MD5_DIGEST_LEN;
hashOut.length = SSL_SHA1_DIGEST_LEN;
if ((err = SSLFreeBuffer(&hashCtx)) != 0)
    goto fail;
if ((err = ReadyHash(&SSLHashSHA1, &hashCtx)) != 0)
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &clientRandom)) != 0)
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
    goto fail;
    goto fail;  /* MISTAKE! THIS LINE SHOULD NOT BE HERE. err==0 */
if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
    goto fail;

err = sslRawVerify(...);
. . .
```


http://nakedsecurity.sophos.com/2014/02/24/anatomy-of-a-goto-fail-apples-ssl-bug-explained-plus-an-unofficial-patch/

Microsoft EULA

Except for the Limited Warranty and to the maximum extent permitted by applicable law, [we] provide the Software and support services (if any) AS IS AND WITH ALL FAULTS, and hereby disclaim all other warranties and conditions, whether express, implied or statutory, including, but not limited to, any (if any) implied warranties, duties or conditions of merchantability, of fitness for a particular purpose, of reliability or availability, of accuracy or completeness of responses, of results, of workmanlike effort, of lack of viruses, and of lack of negligence, all with regard to the Software, and the provision of or failure to provide support or other services, information, software, and related content through the Software or otherwise arising out of the use of the Software.

this is an old EULA. Newer software comes with a 90-day limited warranty

Damage due to Bugs (US alone)

$20-$60 billion annually

Size of software industry: $120billion

Things Go Very Wrong

Things Go Very Wrong

Ariane 5 flight 501, 4 June 1996

Reuse of module written for Ariane 4, which is slower.
Accelleration values do not fit the 16 bit integer.

1. Out-of-range value leads to an unhandled exception in active and backup system
2. Software transmit diagnostic data to main computer.
3. Main computer interprets diagnostic input as navigation data
4. Rockets starts tearing apart, triggers self destruct system

Failed system was not even needed on Ariane 5.

Cost: $400m

Report: Software bug led to death in Uber's self-driving crash

Sensors detected Elaine Herzberg, but software reportedly decided to ignore her.

TIMOTHY B. LEE - 5/8/2018, 12:12 AM

More?

1993 – Intel Pentium floating point divide

2000 – National Cancer Institute, Panama City.

2003 – Northeast blackout

Faulty software may always be a part of the electric grid's DNA – Tom Kropp, manager, enterprise information security program, Electric Power Research Institute

Toronto, 14 August 2003 evening (Wikipedia)

What about Other Disciplines?

Si-o-se Pol bridge, 1600, Isfahan

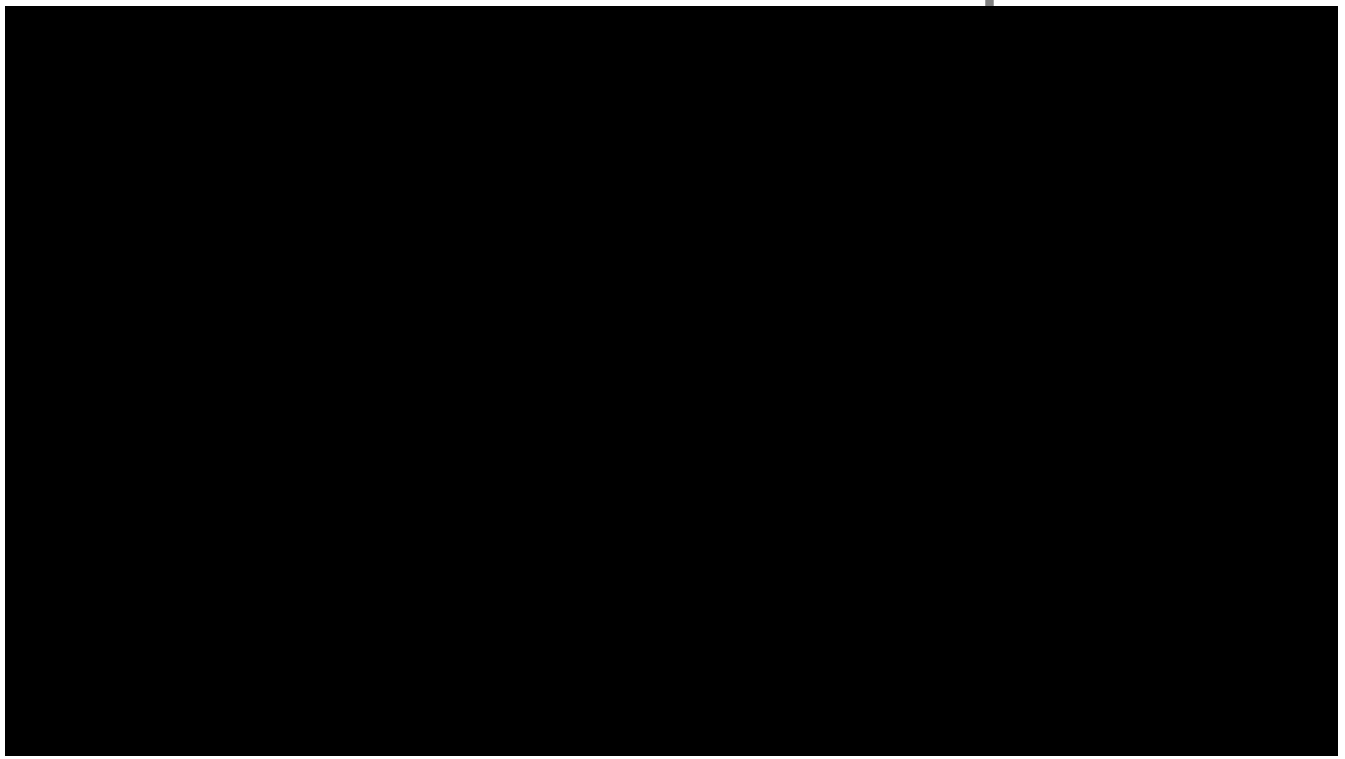
What about Other Disciplines?

"Engineering is the discipline, art, and profession that applies scientific theory to design, develop, and analyze technological solutions."

Civil engineering is an engineering discipline. Computer science is not.

Why not?

What about Other Disciplines?



Tacoma Narrows Bridge. Washington, 1940

Fragile suspension bridge (new type of design)

Aerodynamics!

What about Other Disciplines?

Erasmus Bridge

Rotterdam, Netherlands, 1997

Aerodynamical problem

Solved by adding extra wires

What about Other Disciplines?

Millenium Bridge

London, 2000. Cost: £18M.

`Suspension bridge´

Resonance problem

Added shock absorbers (Cost: £5M)

What about Other Disciplines?

Common theme in failures: **new design**

In computer science, every design is new!

Two contributions

1. **Mathematical rigor**: Verify, don't test!
2. **Correctness first**: Establish correctness while programming

Verification & Testing

Testing: Try out the software for many different scenarios

Verification: prove the correctness of software

Testing: some payoff for any size system

Verification: scaling is hard

MAIN CHALLENGE

State of the Art

Verification is standard

- In VLSI design
- In MS Windows development
- At Facebook
- At Amazon
- ...

Improving Testing

Dynamic: Get more from testing

- Concurrency: Find suspicious access patterns or locking patterns
- Memory access: be stricter
- Symbolic execution

Static: Make sure no bugs exist

- Manual Hoare proofs
- Model checking
- Abstraction techniques

Plan

Dynamic Algorithms

- Deadlocks: Eraser & Locktree
- Memory use: Valgrind & Purify

Static Algorithms

- Symbolic Execution
- Java Path Finder
- Static Analysis
- Hoare Logic
- Abstraction and refinement: Microsoft's SLAM