Software Verification and Testing

Azadeh Farzan
CS410 - Fall 2019
My Info

Send me email: azadeh@cs.toronto.edu

Stop by my office: BA 3252

More on: www.cs.toronto.edu/~azadeh
How are you graded?

- Initial Quiz: 5%
- A few problem solving assignments and a few mini-projects (automatically graded) -> 65%
- 3 Exams: 10% each
  - No final exam at the end.
Motivation

- **Software Validation**: one of the toughest open problems in Computer Science.
- Verification has always been derived by academia
  - very rich theoretical basis
  - logics, algorithms, calculi, ...
  - a lot of room for pragmatism
  - theoretically-motivated heuristics
A List of Known Software Bugs

- Northeast blackout
- Data race error
- Ariane V Crash (1996)
- 64 bit to 16 bit conversion
- Pentium FDIV bug (1997)
- Lookup table had mistakes
- Mars Orbiter
- Feet-per-second vs. Newtons-per-second
Therac-25

- radiation therapy over-radiated patients

Windows crashed during Gate’s presentation in 2006

- windows is used to control highly sensitive army carriers (including those that carry thermo-nuclear intercontinental ballistic missiles).
Newer Bugs

- The Heartbleed bug
- Random generator error
- Loads of airline outages
- British Airways (the most recent)
- Loads of news about security breeches
- Spectre: most famous
What kind of certification do we get for software these days?
11. EXCLUSION OF INCIDENTAL, CONSEQUENTIAL AND CERTAIN OTHER DAMAGES. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL MICROSOFT OR ITS SUPPLIERS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS OR CONFIDENTIAL OR OTHER INFORMATION, FOR BUSINESS INTERRUPTION, FOR PERSONAL INJURY, FOR LOSS OF PRIVACY, FOR FAILURE TO MEET ANY DUTY INCLUDING OF GOOD FAITH OR OF REASONABLE CARE, FOR NEGLIGENCE, AND FOR ANY OTHER PECUNIARY OR OTHER LOSS WHATSOEVER) ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF OR INABILITY TO USE THE SOFTWARE PRODUCT, THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT SERVICES, OR OTHERWISE UNDER OR IN CONNECTION WITH ANY PROVISION OF THIS EULA, EVEN IN THE EVENT OF THE FAULT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, BREACH OF CONTRACT OR BREACH OF WARRANTY OF MICROSOFT OR ANY SUPPLIER, AND EVEN IF MICROSOFT OR ANY SUPPLIER HAS BEEN ADVISED OF THE POSSIBILITY OF
The GPL

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
My favourite part of “The Good Omens”
... along with the standard computer warranty agreement which said that if the machine 1) didn't work, 2) didn't do what the expensive advertisements said, 3) electrocuted the immediate neighborhood, 4) and in fact failed entirely to be inside the expensive box when you opened it.
... this was expressly, absolutely, implicitly and in no event the fault or responsibility of the manufacturer, that the purchaser should consider himself lucky to be allowed to give his money to the manufacturer, and that any attempt to treat what had just been paid for as the purchaser's own property would result in the attentions of serious men with menacing briefcases and very thin watches.
Opinions?
Our Holy Grail

- Make software (more) reliable

- Software is a product!
  
  - needs industry standards.

- A notion of certification for Software

- Meanwhile ... make it more reliable
  
  - partial validation, intelligent testing, ...

- Next generation languages with better validation support.
What is Verification Anyway?

- **Proving** (in a **formal** way) that program satisfies a specification written in a logical language.

- **Formal models** for programs.

- **Logics** for specifications.

- **Algorithms** for checking the model against the specification.
Extended Example:
Greatest Common Divisor in Dafny
What is the point?

Watch this talk!

And, this one if your interest was piqued.