This talk is about…

Stability

Well-being

Trust

Why Zika Is This Year's Scary Virus

It is "spreading explosively" in the Americas and may be the next public health emergency.

Volkswagen: The scandal explained

By Russell Hotten
Business reporter, BBC News

10 December 2015 | Business

FEB 13, 2013 @ 09:37 AM   135,574 VIEWS

Microsoft's Excel Might Be Th
Dangerous Software On The P

Tim Worstall, CONTRIBUTOR

I have opinions about economics, finance and public policy. FULL

Opinions expressed by Forbes Contributors are their own.

No, really, it's possible that Microsoft's Excel is the mos
dangerous software on the planet. Yes, more dangerou
rogue code running a nuclear power plant, than the
that was deliberately sent off to sabotage Iran's nuclear
program, worse, even, than whatever rent in the fabric of space
time led to the invention of Lolcats. Really, that serious.

http://www.bbc.com/news/business-3432477

http://onforb.es/1RRZPhg

Microsoft

Zorn, PLDI 2016

RiSE – Research in Software Engineering

What's New in Computer Science?

Deep Learning

Where are the Programming Languages?

Presenting **DeepPLDI**:
The First PLDI paper written by an RNN

- Data: 7 years of PLDI 2007-2015, 304 files, 25Mb of text

- HW: Intel i7, Nvidia GeForce GTX Titan GPU

- RNN Software: Torch7 (http://torch.ch/) with CUDA, fork
  https://github.com/billzorn/torch-rnn/tree/dev

- RNN: 3-layer LSTM, 512 cells/layer, 40k training batches

- Thanks to Bill Zorn, U. Washington

- Also see "The Unreasonable Effectiveness of Recurrent Neural Networks"
  http://karpathy.github.io/2015/05/21/rnn-effectiveness/

Microsoft

Presenting **DeepPLDI**:
The First PLDI paper written by an RNN

Excerpt: "This work are not a solution to separation logic since the system requires only symbolic execution to erroridy details of dynamically nested query hardware. **We present a convenient alias analysis that attains a number of queries in a typedef style**, the design of the stand-representation is the case that symmetric constructs can be applied and how to matter. For example, inductive properties to support table loads and analysis, a keyword assumption to the signature for ΓF across a dynamically computed list. Our language's defects by computing these points are synthesized ing a synthesis of the sizes and mutations fence in Section 3.2.1."
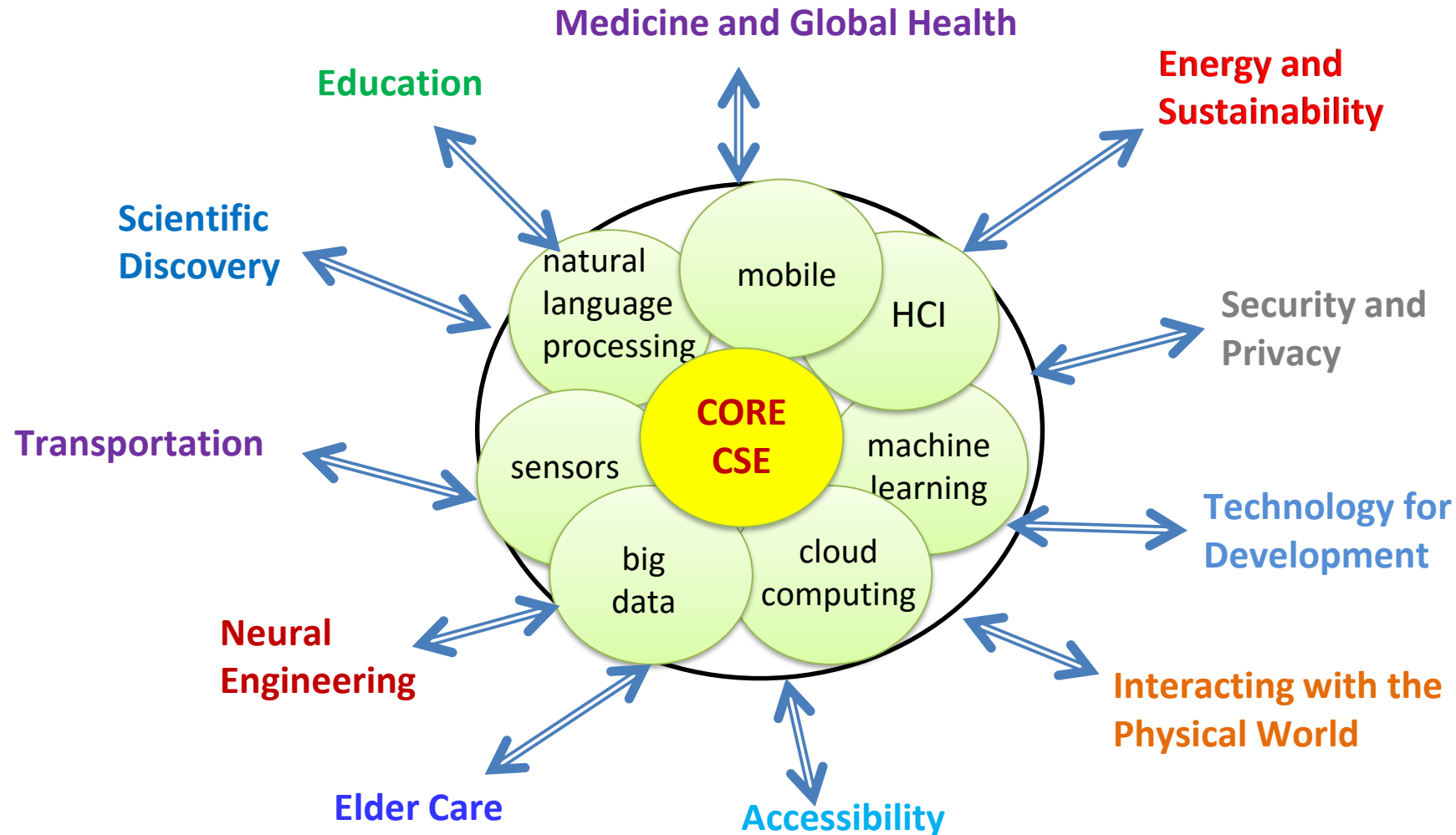
- **DeepPLDI**, 2016

Microsoft

Languages are Central to Disruption

- VisiCalc, 1979
- Visual Basic, 1991
- Java, 1991
- JavaScript, 1996
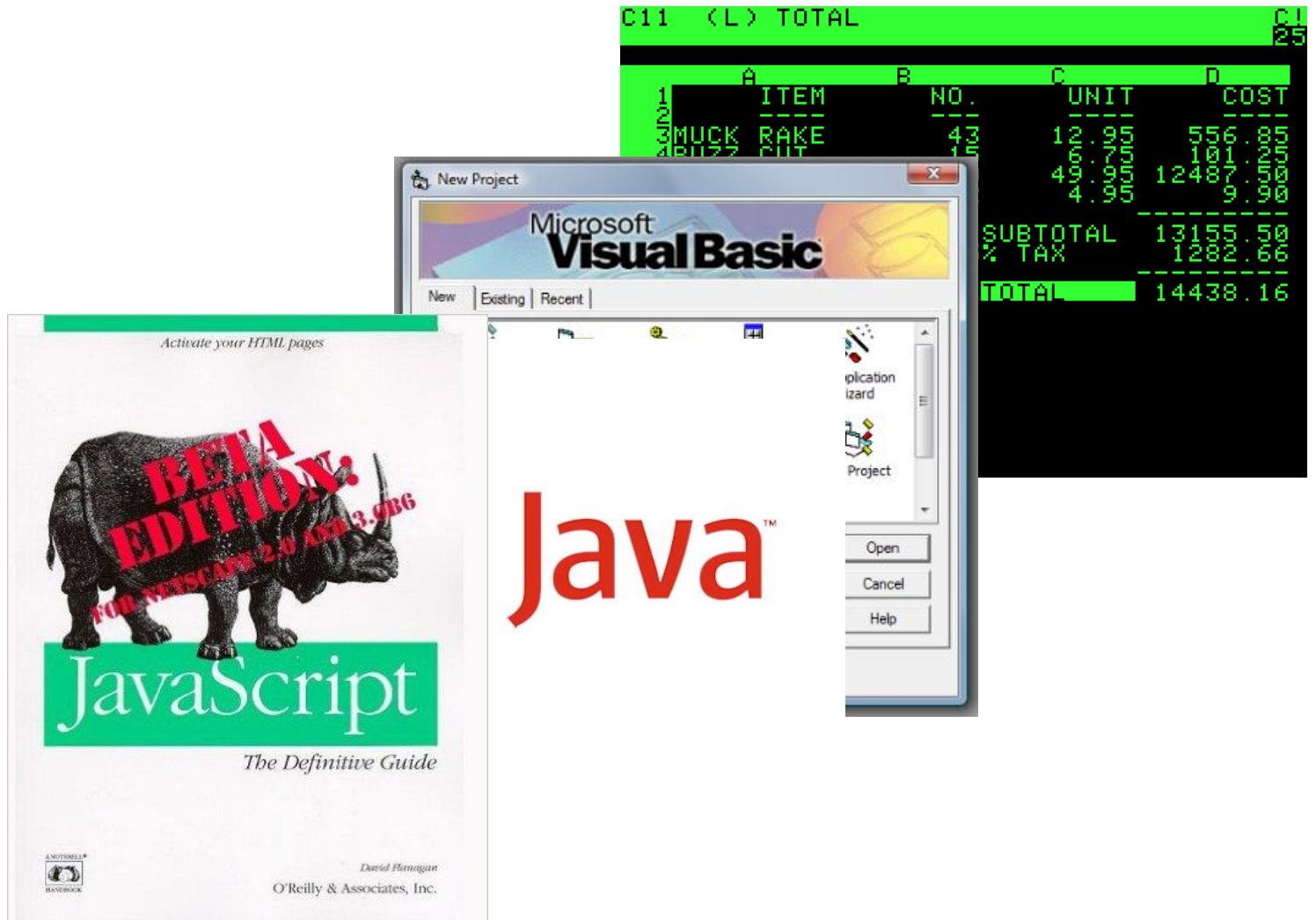
And Computing is Central to Everything…

The Rapidly Expanding World of Computing

Graphic: Lazowska

Zorn, PLDI 2016

Three Examples

Public Health
Financial Stability
Cybersecurity

Public Health

Active Zika Transmission (CDC) http://www.cdc.gov/zika/geo/active-countries.html   Zorn, PLDI 2016

Detour: Is Code Really Dead?

In the sciences the authority of deep learning output is not worth as much as one result from an SMT solver

In the sciences the authority of thousands of opinions is not worth as much as one tiny spark of reason

In the sciences the authority of thousands of opinions is not worth as much as one tiny spark of reason

la che l'autorità dell'opinione di mille nelle scienze non val per un solo, sì perché le presenti osservazioni spogliano d'autorità decreti de' passati scrittori, i quali se veduto le avessero, avrebbono diversamente determinato.

Galileo Galilei (trans. 1957)

Galileo Galilei (trans. 2016)

Galileo Galilei (Original)

Third letter on sunspots (December 1612)

Soon, we won't program computers.
We'll train them. BY JASON TANZ

WIRED

/* the end of code */

What that means for us. BY CADE METZ

Zorn, PLDI 2016

Honoring Automated Reasoning at Scale

Pioneering achievements

Changing math & science

Awards / recognition

The 2005 Software System Award
Presented to
J Strother Moore
Robert S. Boyer
Matt Kaufmann
for the

Formal Proof—The Four-Color Theorem

Georges Gonthier

Automation of Mathematical Induction
as part of the History of Logic

J Strother Moore
Dept. Computer Sci., Gates Dell C., 2317 Speedway,
The University of Texas at Austin, Austin, TX 78701
moore@cs.utexas.edu

Claus-Peter Wirth
FB AI, Hochschule Harz, D–38855 Wernigerode, Germany
wirth@logic.at

SEKI Report SR–2013–02

Nqthm

AWARDS
ACM Software System Award
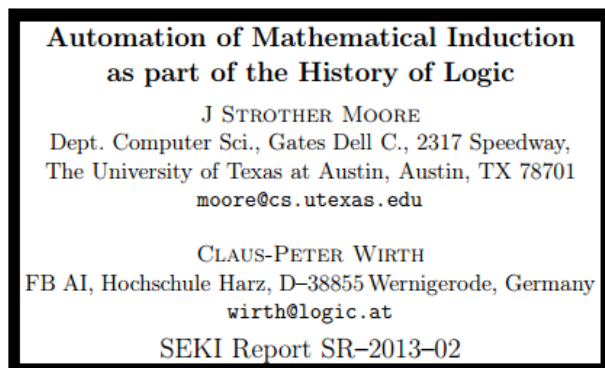
Z3

Z3 wins 2015 ACM SIGPLAN Award

Microsoft

Zorn, PLDI 2016

Example: the Z3 SMT Solver
Leonardo de Moura and Nikolaj Bjørner, MSR

Many important problems can be expressed as a system of constraints in some logic

Solution/Model

$$x^2 + y^2 < 1 \; and \; xy > 0.1$$ ➡ sat, $x = \frac{1}{8}, y = \frac{7}{8}$

$$x^2 + y^2 < 1 \; and \; xy > 1$$ ➡ unsat, Proof

Is execution path P feasible?   Is assertion X violated?

Path Exploration   **Program Verification**

Z3 is a platform that many build on:
- 30,000 downloads
- 2800+ citations

Is Formula F Satisfiable?

Microsoft

SMT Solvers are already superhuman

((Fuel (ZFuel) (SFuel (prec Fuel)))))(declare-fun MaxIFuel () Fuel)(declare-fun MaxFuel () Fuel)(declare-fun PreType (Term) Term)(declare-fun Valid (Term) Bool)(declare-fun HasTypeFuel (Fuel Term Term) Bool)(define-fun HasTypeZ ((x Term) (t Term)) Bool(HasTypeFuel ZFuel x t))(define-fun HasType ((x Term) (t Term)) Bool(HasTypeFuel MaxIFuel x t));;fuel irrelevance(assert (forall ((f Fuel) (x Term) (t Term))(! (= (HasTypeFuel (SFuel f) x t)(HasTypeZ x t)):pattern ((HasTypeFuel (SFuel f) x t)))))(define-fun IsTyped ((x Term)) Bool(exists ((t Term)) (HasTypeZ x t)))(declare-fun ApplyTF (Term Fuel) Term)(declare-fun ApplyTT (Term Term) Term)(declare-fun Rank (Term) Int)(declare-fun Closure (Term) Term)(declare-fun ConsTerm (Term Term) Term)(declare-fun ConsFuel (Fuel Term) Term)(declare-fun Precedes (Term Term) Term)(assert (forall ((t Term))(! (implies (exists ((e Term)) (HasType e t))(Valid t)):pattern ((Valid t)))))(assert (forall ((t1 Term) (t2 Term))(! (iff (Valid (Precedes t1 t2)) (< (Rank t1) (Rank t2))):pattern ((Precedes t1 t2)))))(define-fun Prims.precedes ((a Term) (b Term) (t1 Term) (t2 Term)) Term(Precedes t1 t2))(declare-fun Range_const () Term); <start constructor String_const>;;;;;;;;;;;;;;;;Constructor(declare-fun String_const (Int) String);;;;;;;;;;;;;;;;Constructor distinct(assert (forall ((@u0 Int)) (! (= 0(String_constr_id (String_const @u0))) :pattern ((String_const @u0)))));;;;;;;;;;;;;;;;Projector(declare-fun String_const_proj_0 (String) Int);;;;;;;;;;;;;;;;Projection inverse(assert (forall ((@u0 Int)) (! (= (String_const_proj_0 (String_const @u0))@u0) :pattern ((String_const @u0)))));;;;;;;;;;;;;;;;Discriminator definition(define-fun is-String_const ((@u0 String)) …

Part of a **4-megabyte** Z3 input generated in the proof of a verified TLS implementation (courtesy of Nikhil Swamy)

What does all this have to do with **Public Health**?

Public Health meets Formal Methods

What does this…

Zika outbreak fuelled by mosquito control failure, says WHO boss

23 May 2016 | Health

AP

…have to do with this?

Microsoft

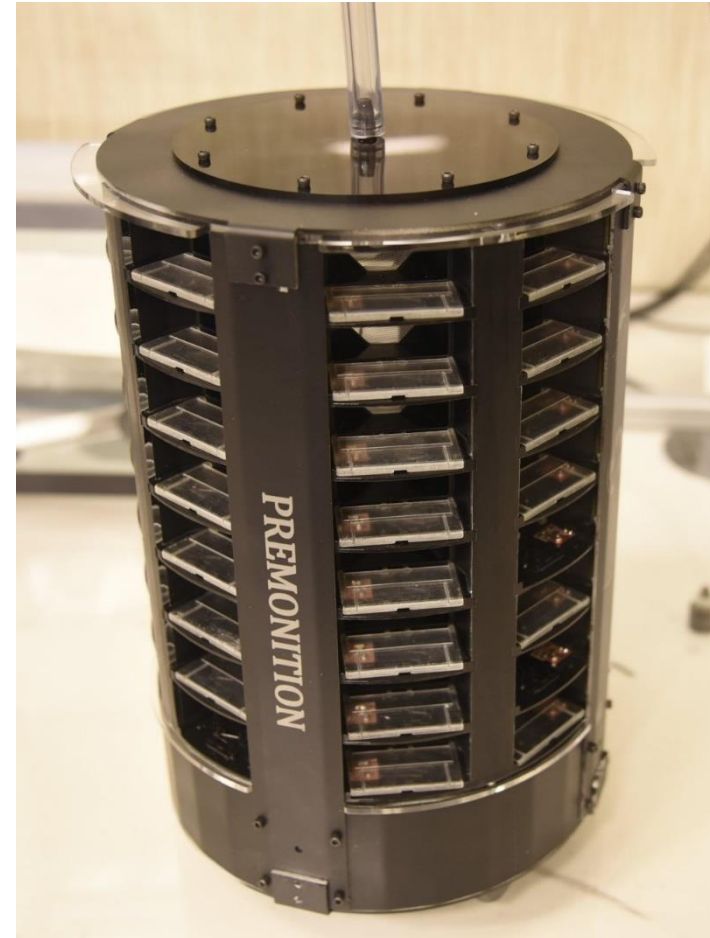Zorn, PLDI 2016

It starts with a question…

What if you could use mosquitos as sensors to detect the presence of infectious disease around the globe?

Building a Better Mosquito Trap

Catch
Uses .... ecies
Light
12-14
Reus

C02-baited CDC UV trap, circa 2015

PREMONITION

Premonition trap, 2016

Images courtesy of Ethan Jackson

Zorn, PLDI 2016

Internet of (Field Biology) Things: Premonition

Repeat

Drone identifies placement sites

Analysis identifies Infectious diseases

DNA samples sent to cloud
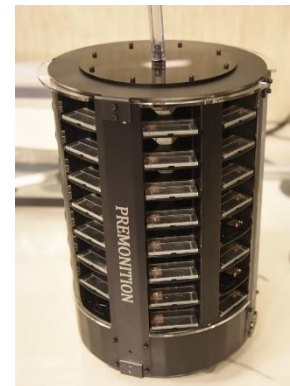
Mosquito trap located in likely spots

Microsoft Research
Safe Cyber-Physical Systems Expedition

High-level Planning

Correct Control

Robust Sensing

Secure OS
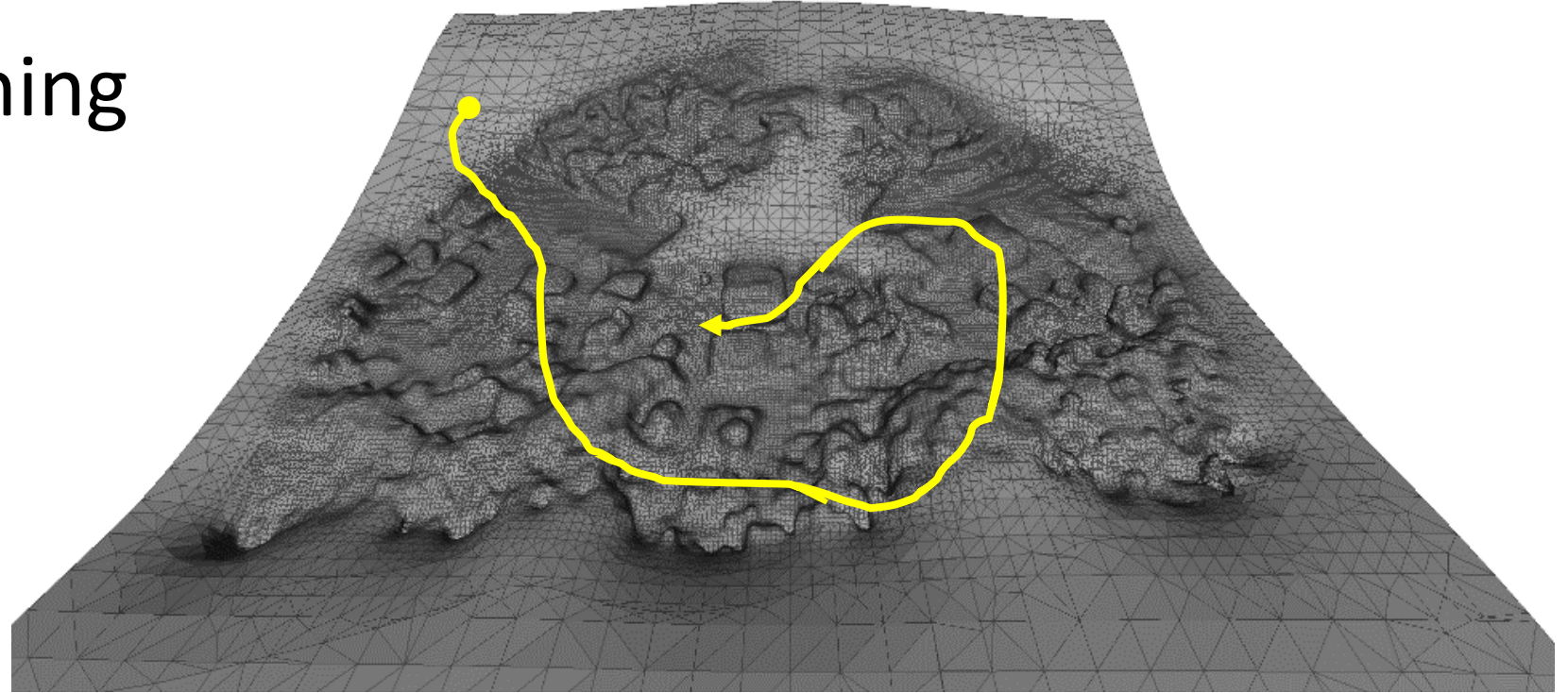
Safe despite limited power, external disturbances, sensor noise and complex missions

Automated Reasoning at Scale is Transformative

Enabling rapid advances in sciences based on:

Exponential improvements in sensing + devices

Cloud computing

Statistical and logical reasoning at scale

The future looks bright!

Financial Stability

Increasingly, society depends on correct and efficient analysis of data

It all started with spreadsheets...
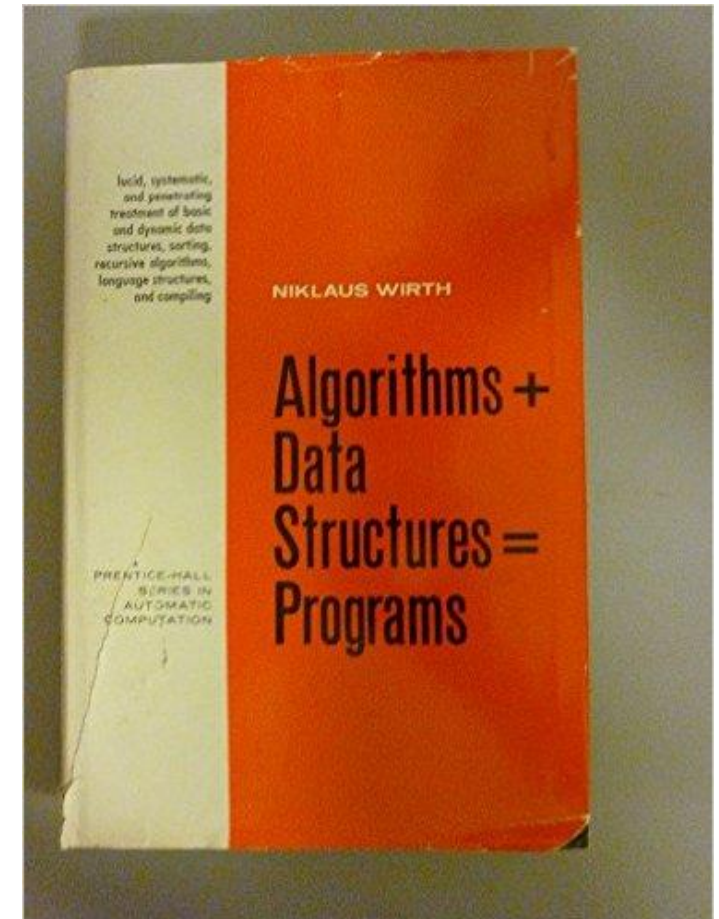
Aside: Code, Data, and Noise

- Programming languages people like to think about code
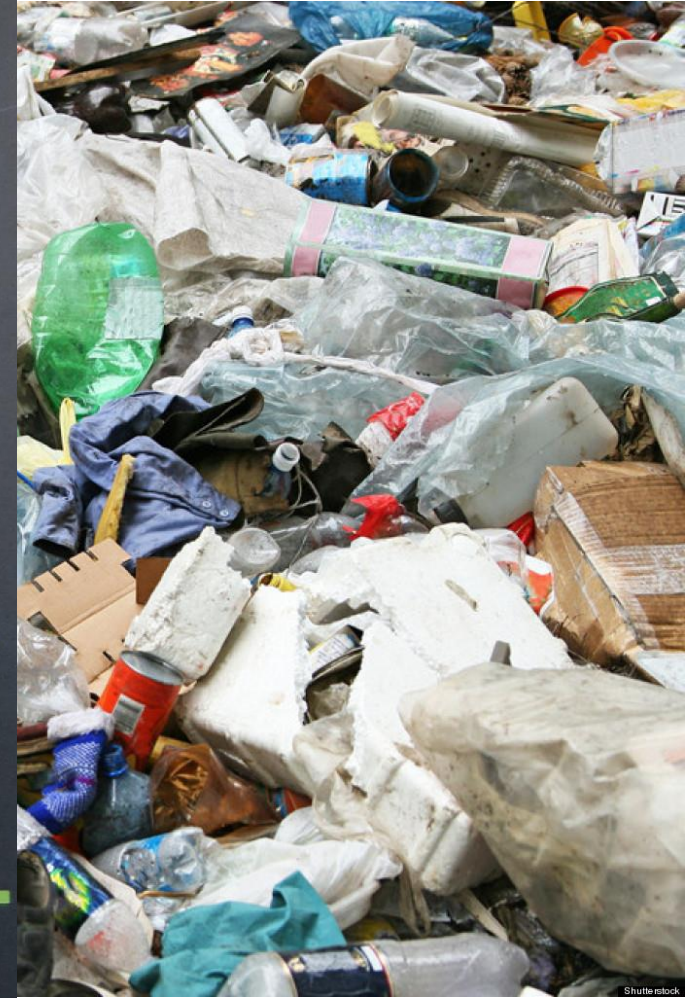- Consider Niklaus Wirth:
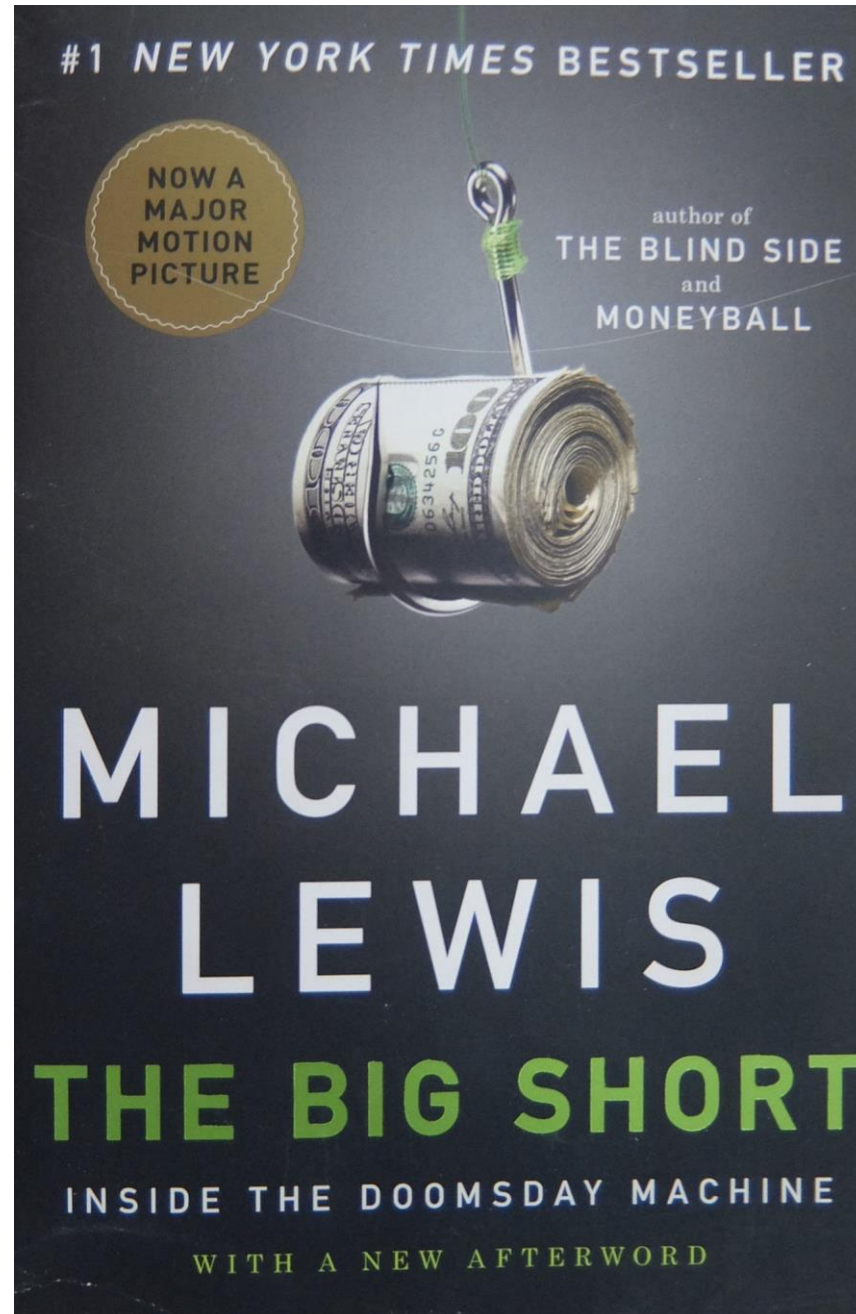
Algorithms + Data Structures = Programs

Wrong!

Programs = Algorithms + Data Structures + **Data**

Garbage in, garbage out is not the complete story

More reasoning required

Zorn, PLDI 2016

Code and Data Always Coexist…

- Question (too easy): consider this regular expression

  ([a-z0-9][-a-z0-9_\+\.]*[a-z0-9])@([a-z0-9][-a-z0-9\.]*[a-z0-9]\.
  (arpa|root|aero|biz|cat|com|coop|edu|gov|info|int|jobs|mi
  l|mobi|museum|name|net|org|pro|tel|travel|ac|…)
  |([0-9]{1,3}\.{3}[0-9]{1,3}))

- What does it do?
- Here's a hint: benzorn@acm.org

Microsoft

Programming by example combines (implicit) code and data directly

In the PowerShell ConvertFrom-String commandlet:

{username*:benzorn}@{domain*:acm.org}

generates a program that generalizes to extract the user and domain name from every row of an input file

See: *"Spreadsheet Data Manipulation using Examples"*, CACM 2012, Research Highlights Paper,
Sumit Gulwani, William Harris, Rishabh Singh
and
https://blogs.msdn.microsoft.com/powershell/2014/10/31/convertfrom-string-example-basedtext-parsing/

Microsoft

Spreadsheets combine data and code in novel and innovative ways

From: Fisher, Marc, and Gregg Rothermel. "The EUSES spreadsheet corpus…"
ACM SIGSOFT Software Engineering Notes. Vol. 30. No. 4. ACM, 2005.

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	**Annex 5.1**	**Final table: Historical trends in forest resources**											
2													
3	Forest area (1000 ha)												
4													
5		value	year	value	year	value	year	value	year	value	year	value	year
6													
7	Albania	1,000	1950	930	1981	910	1990	902	1995				
8	Austria	3,139	1951	3,177	1955	3,166	1960	3,230	1967	3,165	1977	3,330	1989
9	Belgium	541	1947	601	1950	588	1962	600	1970	620	1980	639	1997
10	Bulgaria	2,964	1947	3,259	1958	3,200	1970	3,300	1980	3,222	1990	3,124	1995
11	Czech Republic	2,416	1950	2503	1960	2,410	1970	2505	1980	2,552	1990	2486	2000
12	Denmark	348	1947	436	1950	374	1960	373	1965	466	1979	400	1981
13	Finland	20,700	1938	21,874	1952	21,057	1959	22,500	1968	23,225	1979	23,373	1986
14	France	10,954	1947	11,307	1953	11,500	1958	11,000	1959	13,090	1970	13,340	1981
15	Germany	7,548	1947	9,558	1952	9,996	1958	9,616	1963	9,428	1968	9,800	1970
16	Greece	500	1947	2,000	1953	1,976	1958	1,992	1963	2,289	1964	2,300	1970
17	Hungary	1,107	1947	1,253	1950	1,232	1958	1,214	1963	1,466	1970	1,563	1981
18	Ireland	89	1947	124	1951	145	1958	171	1962	268	1970	347	1980
19	Italy	5,900	1940	5,625	1950	5,826	1960	6,162	1970	6,363	1980	6,760	1990

Spreadsheets Have Bugs, Often About Money

Is This Spreadsheet a Tax Evader ?
How H. M. Customs & Excise Test Spreadsheet Applications

Raymond J Butler, CISA :
H. M. Customs and Excise, Ralli Quays, 3 Stanley Street, Salford, M60 9LA UK
rbutler.c&e.cau@gtnet.gov.uk / ray.butler@hmce.gov.uk
©Crown Copyright reserved, published by permission of the Commissioners of H M Customs & Excise

Findings:

- 7 files, 21 worksheets examined

- Average 713 formulas/file

- Total taxes: 12M pounds

- Total error: 1.37M pounds = 11% of total

Zorn, PLDI 2016

Sometimes the Errors are Significant

Bloomberg   Markets   Tech   Pursuits   Politics   Opinion

JPMorgan Pays $920 Million to Settle London Whale Probes

2012 trading activities of a
single individual
at JP Morgan resulted in
a total loss estimated at

$6.2 billion

The actual problem in the Whale's spreadsheet:
"After subtracting the old rate from the new rate, the spreadsheet **divided by their sum instead of their average**, as the modeler had intended. This error likely had the effect of muting volatility by a factor of two and of lowering the VaR . . ."

Microsoft

Important Policies Are Based on Incorrect Computation

ROOSEVELT INSTITUTE
REIMAGINE THE RULES

events   blog   about   FDR library   c

PROJECTS   INSIGHTS   ROOSEVELTER

NEXT NEW DEAL: THE BLOG OF THE ROOSEVELT INSTITUTE

ECONOMY AND GROWTH, RORTYBOMB

Researchers Finally Replicated Reinhart-Rogoff, and There Are Serious Problems.

By Mike Konczal | 04.16.13

Used by economists to justify austerity policy

Based on faulty calculations in the spreadsheet

http://rooseveltinstitute.org/researchers-finally-replicated-reinhart-rogoff-and-there-are-serious-problems/

Microsoft

Zorn, PLDI 2016

Inside Reinhart-Rogoff

				Debt/GDP				Real GDP growth Debt/GDP		
Country	Coverage	Total	30 or less	30 to 60	60 to 90	90 or above	30 or less	30 to 60	60 to 90	90 or a
US	1791-2009		129	59	23	5	4.02099797756343	3.42285727458613	3.26406756046117	-1.8151
UK	1830-2009		3	68	27	82	2.53381807093758	2.21396433936988	2.07237886235964	1.8046!
Sweden	1880-2009		79	40	11	0	2.91802819692192	2.86025681953054	2.66582383238736	
Spain	1850-2009		26	53	47	30	1.5933244354603	3.18706387741504	1.29386323254985	2.8046!
Portugal	1880-2009		='C:\Users'	='C:\Users'	='C:\Users\z	='C:\Users\zor	='C:\Users\zorn\SkyL	='C:\Users\zorn\SkyL	='C:\Users\zorn\SkyL	='C:\Us
Norway	1880-2009		='C:\Users'	='C:\Users'	='C:\Users\z	='C:\Users\zor	='C:\Users\zorn\SkyL	='C:\Users\zorn\SkyL	='C:\Users\zorn\SkyL	='C:\Us
New Zealand	1932-2009		9	33	17	19	2.46555555555556	2.88957165083001	3.883683368704	3.6134!
Netherlands	1880-2009		17	50	32	8	4.08261358545019	2.8319405911495	2.35009357783615	2.0094
Japan	1885-2009		47	42	11	11	4.94889741153636	3.7178925579162	3.88479257818286	0.6872!
Italy	1880-2009		26	12	39	49	5.35263165338344	4.93890175331293	1.86680970618687	0.6857
Ireland	1949-2009		8	14	32	7	4.40161993155657	4.45716687321354	3.95082638923823	2.4427
						55	4.00128154768729	0.3402	4.8201448495605	2.4701!
						0	3.5920823547989	0.875803377525033	n.a.	
						37	4.93808903234011	2.67222210756024	2.8182086124344	2.3364!
						3	3.23397006139386	3.01414632266669	4.2566217835184	1.9133(
Denmark	1880-2009		='C:\Users'	='C:\Users'	='C:\Users\z	='C:\Users\zor	='C:\Users\zorn\SkyL	='C:\Users\zorn\SkyL	='C:\Users\zorn\SkyL	='C:\Us
Canada	1925-2009		3	52	23	7	1.933	4.49840539324629	2.9878650913178	2.2079!
Belgium	1835-2009		37	60	32	31	2.95628925515421	2.59200241233773	2.0976137405758	3.2621!
Austria	1880-2009		43	32	35	0	4.30558940335994	2.99136331961633	2.3410234597052	
Australia	1902-2009		38	33	23	8	3.14160853067272	4.13710606493654	2.2914666819559	4.5965(
			=SUM(E2(	=SUM(E5:	=SUM(F5:	=SUM(G5:G	=SUM(H5:H2	=AVERAGE(I5:I19)	=AVERAGE(J5:J19)	=AVERAGE(K5:K1!	=AVE!
Minimum								=MIN(I5:I19)	=MIN(J5:J19)	=MIN(K5:K19)	=MIN(
Maximum								=MAX(I5:I19)	=MAX(J5:J19)	=MAX(K5:K19)	=MAX

Denmark, Canada, Belgium, etc
probably feel that they should be incuded

Microsoft

Formula View

Where are Formulas Expected?

	FY04DueIn	Inv-WRMR	Inv-(WRMR+TR)	Inv+DueIn-(WRMR+TR)
	0	=G2-D2	=G2-(D2+E2)	=G2+H2-(D2+E2)
	102361640	-4253731	-74793920	27567720
	800000	=G4-D4	=G4-(D4+E4)	=G4+H4-(D4+E4)
	0	=G5-D5	=G5-(D5+E5)	=G5+H5-(D5+E5)
	0	=G6-D6	=G6-(D6+E6)	=G6+H6-(D6+E6)
	2100			

Implicit dependence – formula expected

Spreadsheet Tools Still Underinvested in PL

Correctness advances

- Spreadsheet smells [Hermans et al., ICSM 2012]

- Data debugging / CheckCell [Barowy et al., OOPSLA 2014]

- Cell clustering / Custodes [Cheung et al., ICSE 2016]

Productivity advances

- Excel 2013 Flash Fill [Gulwani POPL 2011]

- Table extraction / FlashRelate [Barowy et al., PLDI 2015]

- BlinkFill [Singh VLDB 2016]

Correctness Beyond Spreadsheets

How Investors A...
Social Media to...

Bloomberg Markets Tech Pursuits Politics Opinion

Introducing Binatix: A Deep Learning Trading Firm That's Already Profitable

Recode Sept. 10 2014 http://on.recode.net/1svpE2a

How many financial decisions are now based on technology that we don't understand and is likely to have bugs?

April 25, 2013 – 1:36 PM PDT

Bloomberg April 25, 2013 http://bloom.bg/1Y79MPb

Microsoft

Zorn, PLDI 2016

Reasoning about Code + Data

Combining code with data is powerful:
  Spreadsheets
  HTML + JavaScript + CSS

Reasoning about data is as important as code

Tools for such systems are relatively immature

Much is at stake

Trust and Security

Zorn, PLDI 2016

Recall: Rapidly Expanding World of Computing
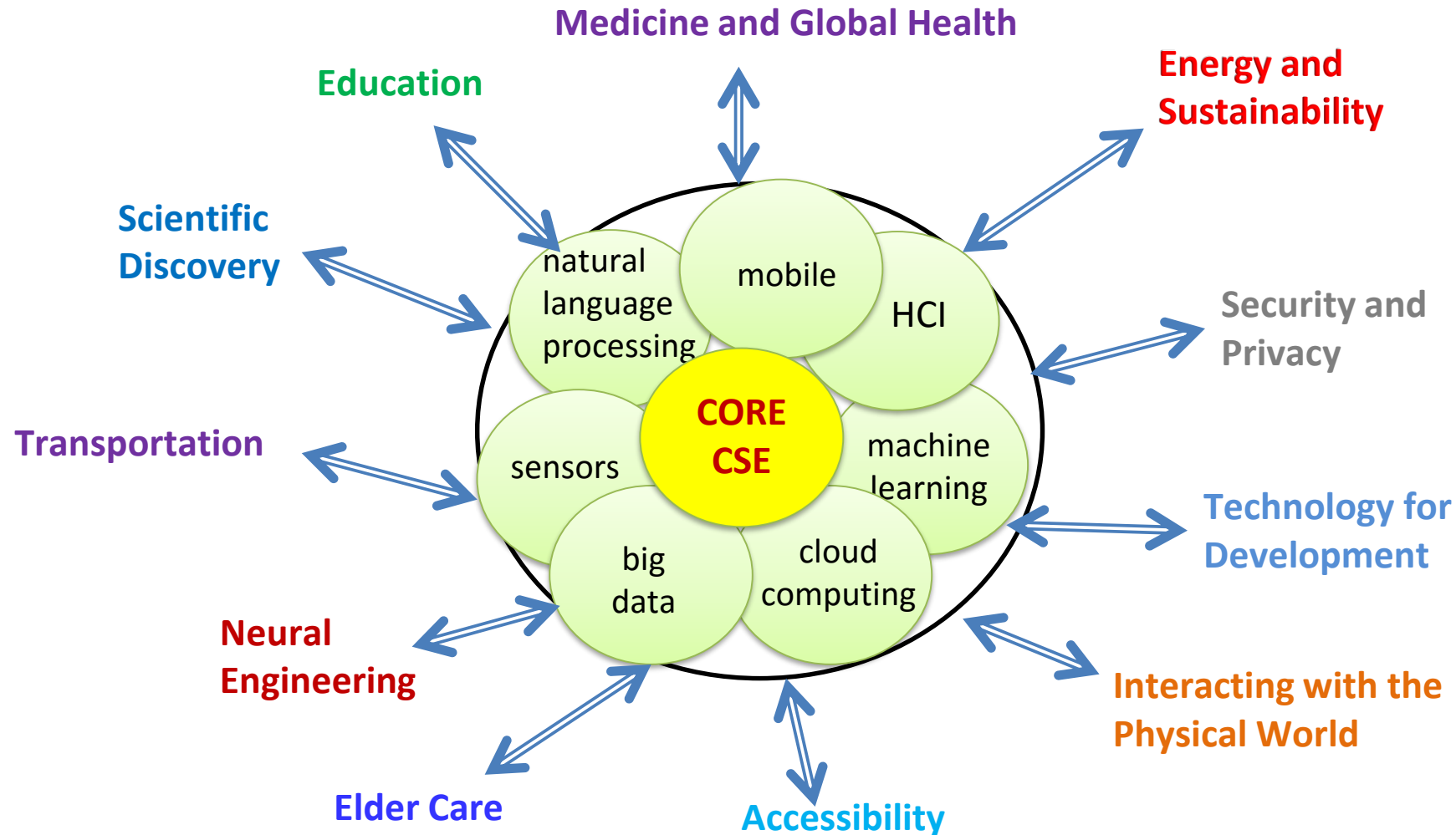
Graphic: Lazowska

Zorn, PLDI 2016

Toyota Hires All-Star Team for Robotics and Artificial Intelli

by Jason Sil

Towards the social media enabled jet engine

September 26, 2012

Posted by Paul
Wallbank at 10:02 am

Add comments

Observation:
Every company is a
software company

"What if my jet engine could talk to me

Mother Jones   POLITICS   ENVIRONMENT   CULTURE   PHOTO ESSAYS

Must Reads: $15 an Hour Isn't the Answer | Why You Shouldn't Bet on Fossil Fuels | Look Who's Running Burma

ENVIRONMENT
→ Climate Change, Climate Desk, Corporations, Food and Ag, Tech, Top Stories

Monsanto Is Using Big Data to Take Over the World

The GMO giant wants to help you beat climate change...with your phone.

—By **Tim McDonnell** | Wed Nov. 19, 2014 6:00 AM EST

Microsoft

Yes, this is a computer too

Every object is a computer

MS Band

Amazon Echo

Ring.com

Nest

Zorn, PLDI 2016

Implications of CS + X

How much does your life depend on correct software?

What's the trend?

Can governments understanding or regulate this trend?

When do you start worrying?

Microsoft

One Trend: Ransomware

Percentage of FireEye NX and EX Appliances Sharing Information with FireEye Dynamic Threat Intelligence Detecting Ransomware
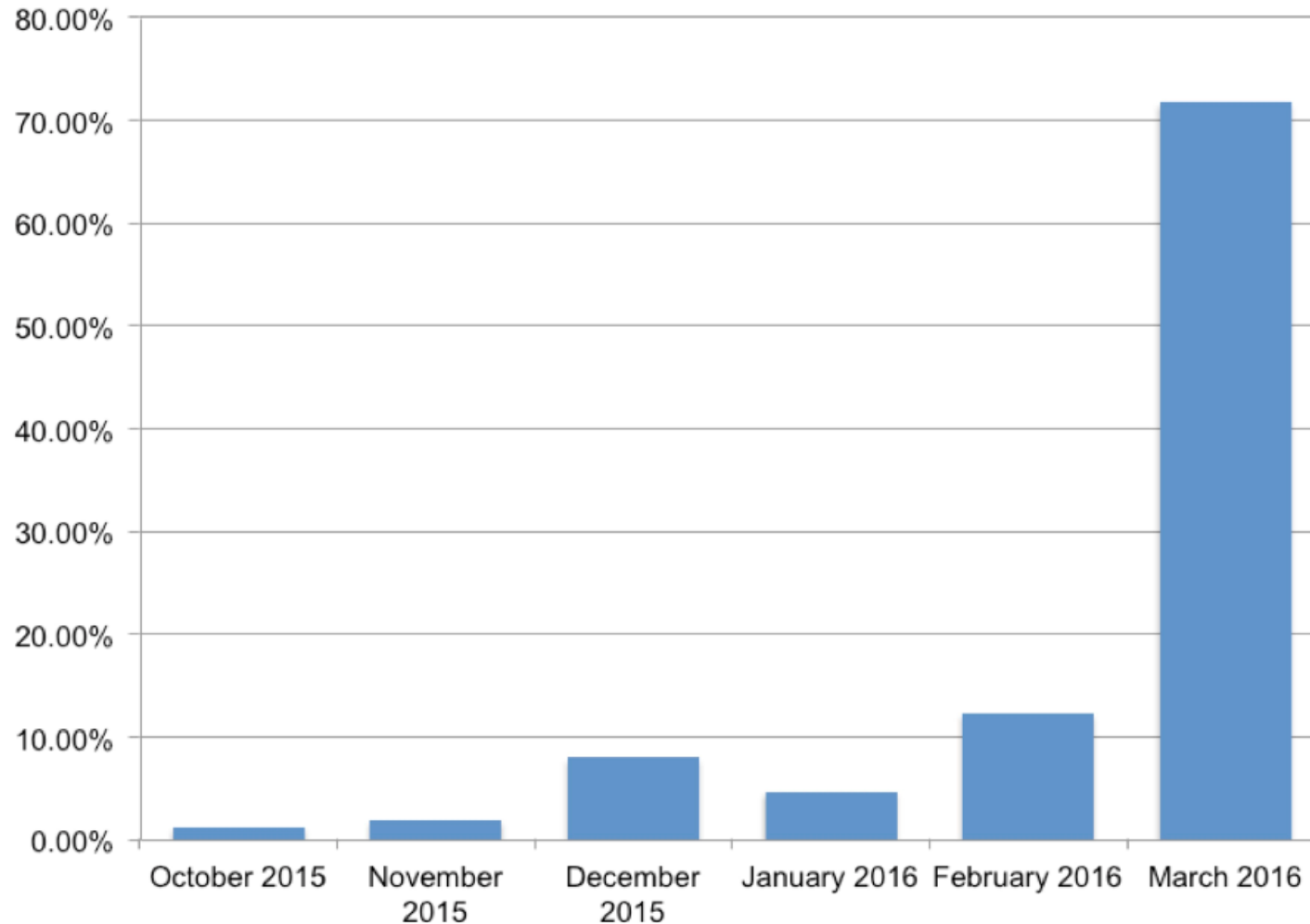
Businesses and individuals increasingly targeted by ransomware

Dramatic increases in 2016

FireEye, "Ransomware Activity Spikes in March", http://bit.ly/1VefZZd

Zorn, PLDI 2016

Smart Everything Increases the Attack Surface

I BOUGHT SOME AWFUL LIGHT BULBS SO YOU DON'T HAVE TO

FEB. 24TH, 2016 04:37 PM

MJG59

I maintain an application for bridging various non-Hue lighting
enough like a Hue that an Amazon Echo will still control them
was colour support, so I picked up some cheap bulbs and a bri
iRainbow001, and it's terrible.

Mathew Garrett Blog, Feb. 2016
https://mjg59.dreamwidth.org/40397.html

Findings:
Trivial credentials
No encryption
Easy to crash
No longer supported

Zorn, PLDI 2016

Did I Mention Companies Cheat?

Exp **MIT Technology Review**

gen's Emissions Scandal

Volkswage used to chea

RUSSELL and DEREK WATKINS UPDATED June 1, 2016

CLE

A View from **David Zax**

Many Cars Have a Hundred Million Lines of Code

Who gets to write it?

December 3, 2012

You can hide a lot
in 100M lines of code

MIT Technology Review, Dec. 3, 2012 http://bit.ly/24xwGiH

Microsoft

Sounds really hard…

Required: Adversarial Thinking for All Engineers

Sokwoo Rhee (AD CPS, NIST): "How would you have prevented StuxNet?"

- Computer scientist: "Reduce attack surface, limit access, …"
- Mechanical eng.: "Install a limit switch on the centrifuges."

Microsoft
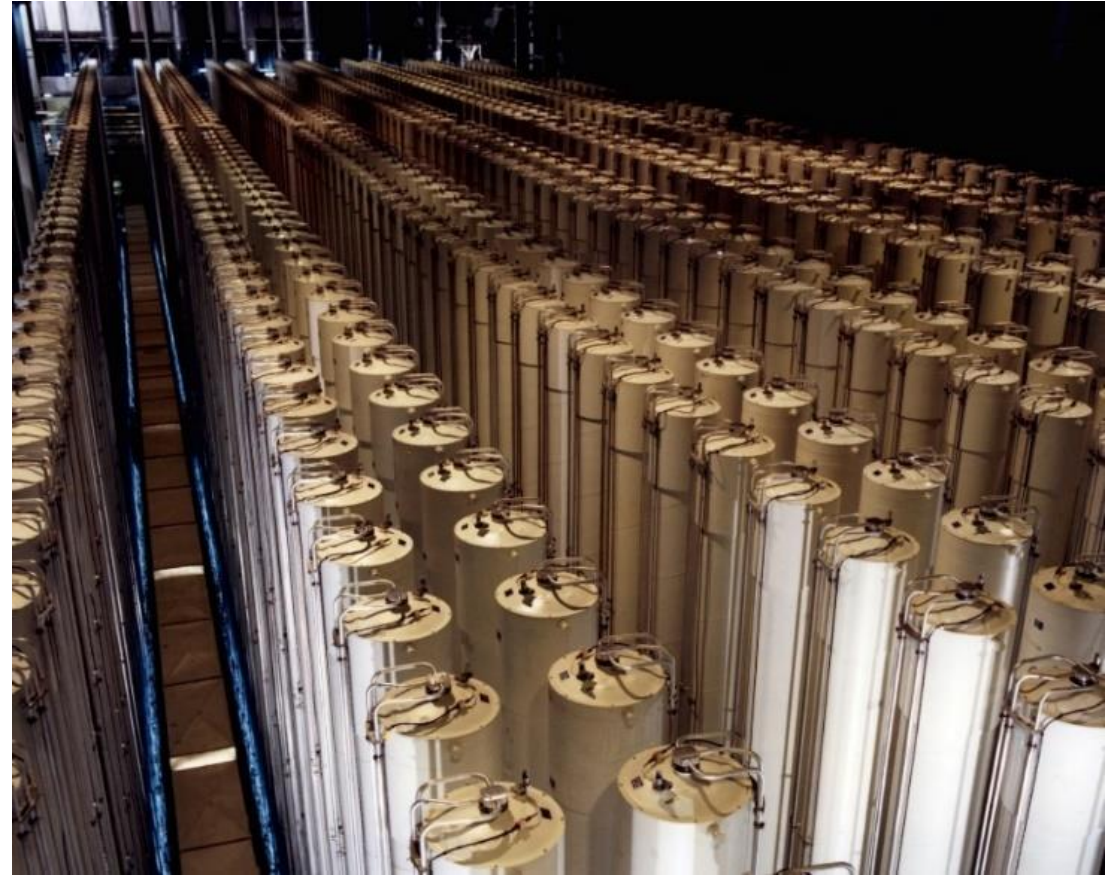
Trust, but Verify

UL Launches Cybersecurity Assurance Program

New UL 2900 Series of Standards Offer Testable Cybersecurity Criteria for Network-Connectable Products & Systems

http://www.ul.com/cybersecurity

Emphasis on up-to-date patches, testing methods, code analysis, crypto

Do we really know how to provide "cybersecurity assurance"?
How assured are you?

Microsoft

Can we really verify?
Two Expeditions: DeepSpec and Everest

Scalable reasoning meets software verification at scale

deep spec | the science of deep specification

About | **Research ▾** | Education | People | Industry | Students | Jobs | Visitors | Events

DeepSpec is an Expedition in Computing funded by the National Science Foundation.

We focus on the **specification and verification of full functional correctness** of software and hardware.

http://deepspec.org/ $10M NSF Expedition in Computing Awarded 2016

Microsoft

Everest Expedition: Microsoft Research

Goal: drop-in verified HTTPS replacement

Challenges:
- scalability of verification
- performance
- usable tool chain

Slide courtesy of Cedric Fournet
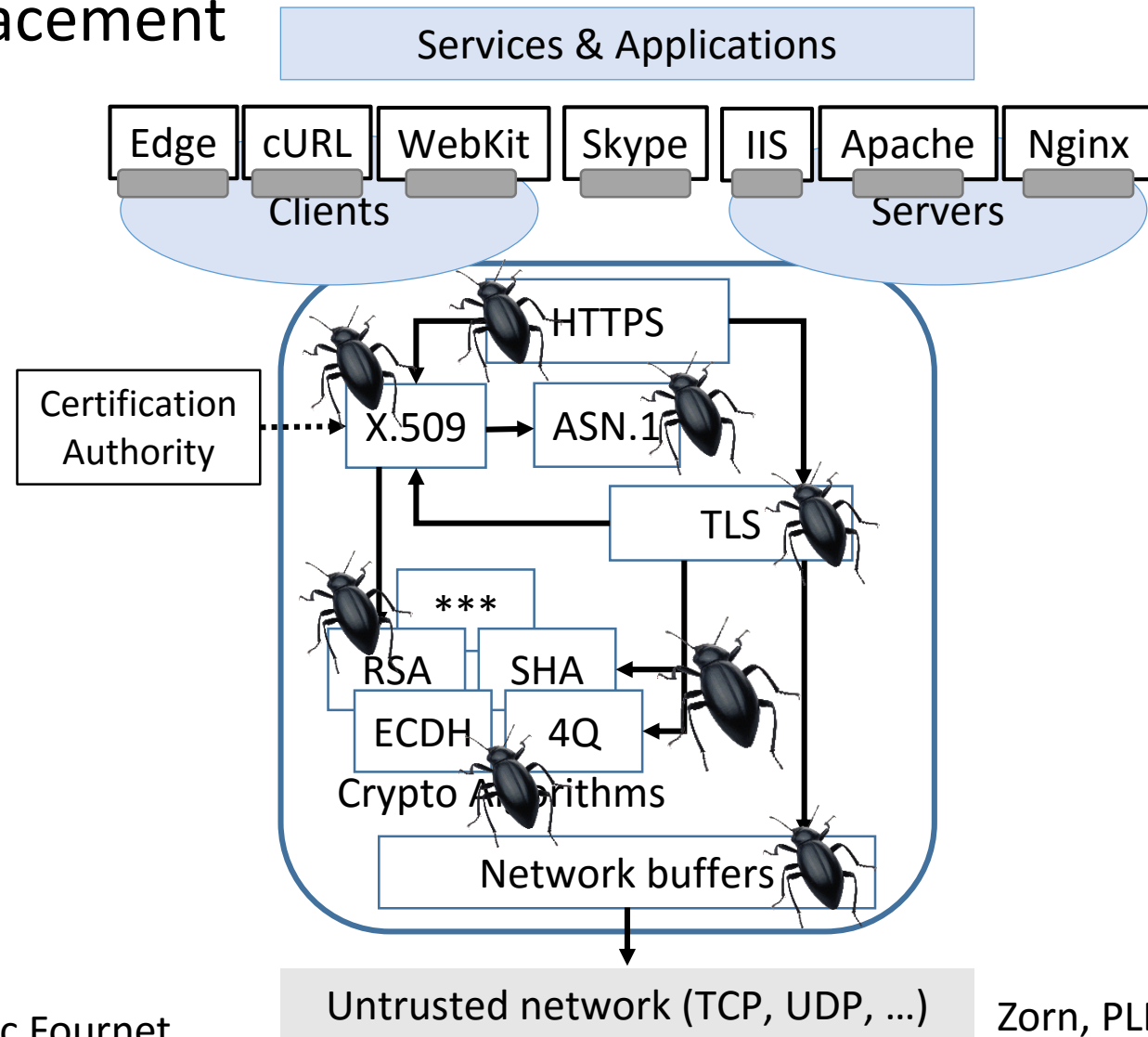
Zorn, PLDI 2016

Is Software the
Hero or the Villain?

Disruptions are Happening

- ## Smart objects will replace dumb objects

- The software embedded in this objects
  ## will be written in the next 5 years, but
  ## will have implications for the next 50 years

- Our ## lives will depend on these objects...

- We need ## languages, tools, and processes to make these objects safe

The Cathedral and the Skyscraper

Heroic effort, amazing engineering, one of a kind...

Stronger materials, reusable components, mathematical analysis...

Microsoft

Zorn, PLDI 2016

Building the Skyscraper: Key Elements

Reasoning at scale

Understanding code and data
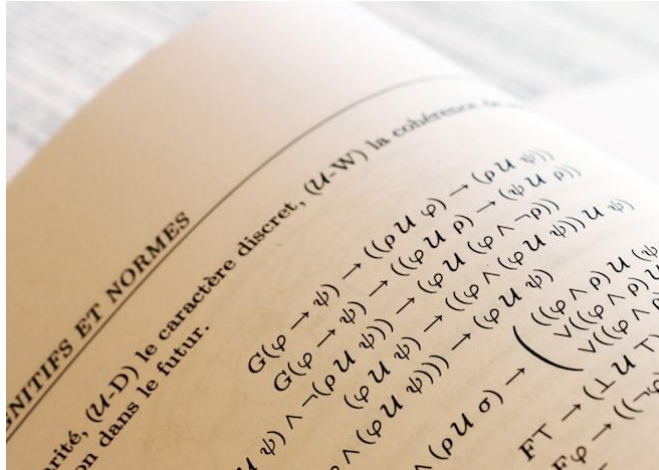
Assuming cyber-physical systems

Requiring verified components

Thank you!

Follow me: @benzorn https://twitter.com/benzorn

DeepPLDI: In order to guarantee termination of pairs defined via conversion and verification constraint from the valid-register files to termination and refinement types…
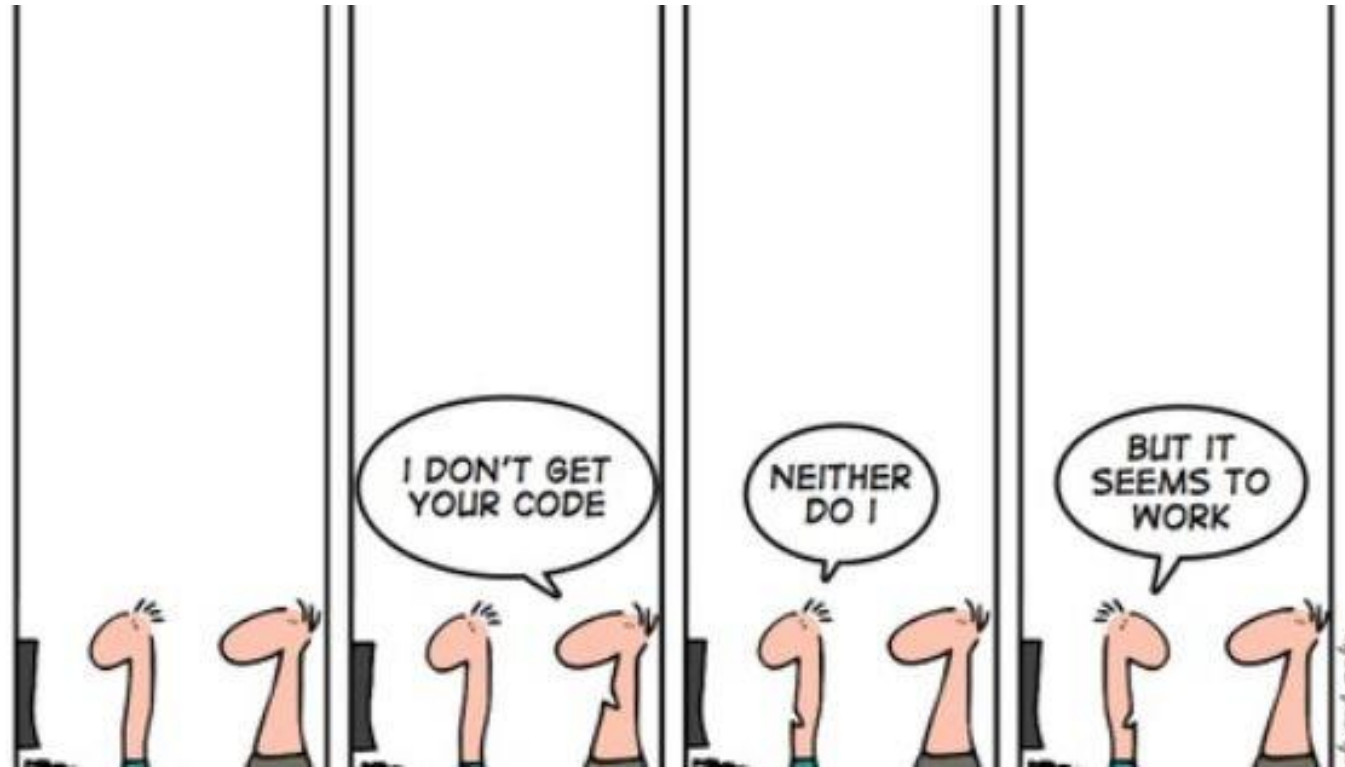
The Existential Threat of AI

Stephen Hawking, Elon Musk, and Bill Gates Warn About Artificial Intelligence

The Observer, 8/19/2015 http://bit.ly/1Pcjf1s
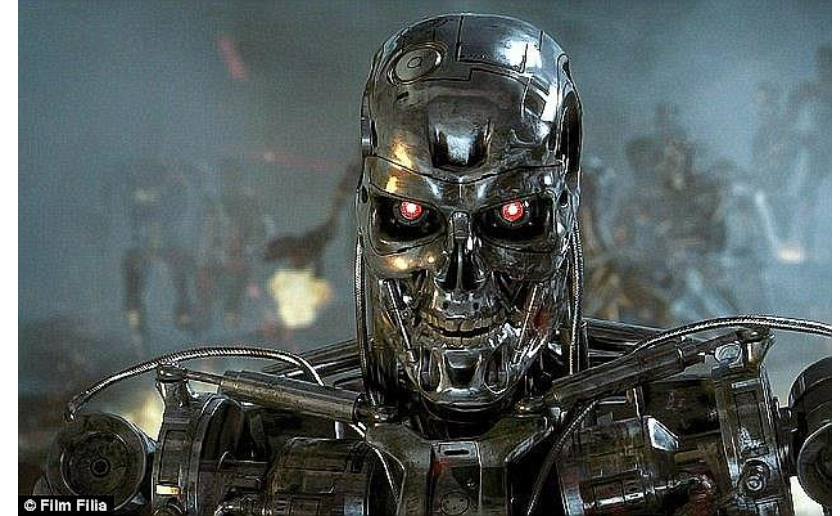
Rapid rise of AI in robotics, vision, etc. raises concerns

Microsoft

The Existential Threat of ~~AI~~ Bad Software

From: http://blog.castsoftware.com/when-good-software-goes-bad/

The Existential Threat of ~~AI~~ Bad Software

- AI is always part of a complete SW system
- Real risk is not knowing what SW can or will do…but:

- Assuming an adversary is first step (bad actors)
- Testing is the traditional approach
- Testing might fail when input/output behaviors are sufficiently complex – <u>this is a PL challenge</u>

Thank you!

Acknowledgements

Follow me: @benzorn https://twitter.com/benzorn

DeepPLDI: In order to guarantee termination of pairs defined via conversion and verification constraint from the valid-register files to termination and refinement types…