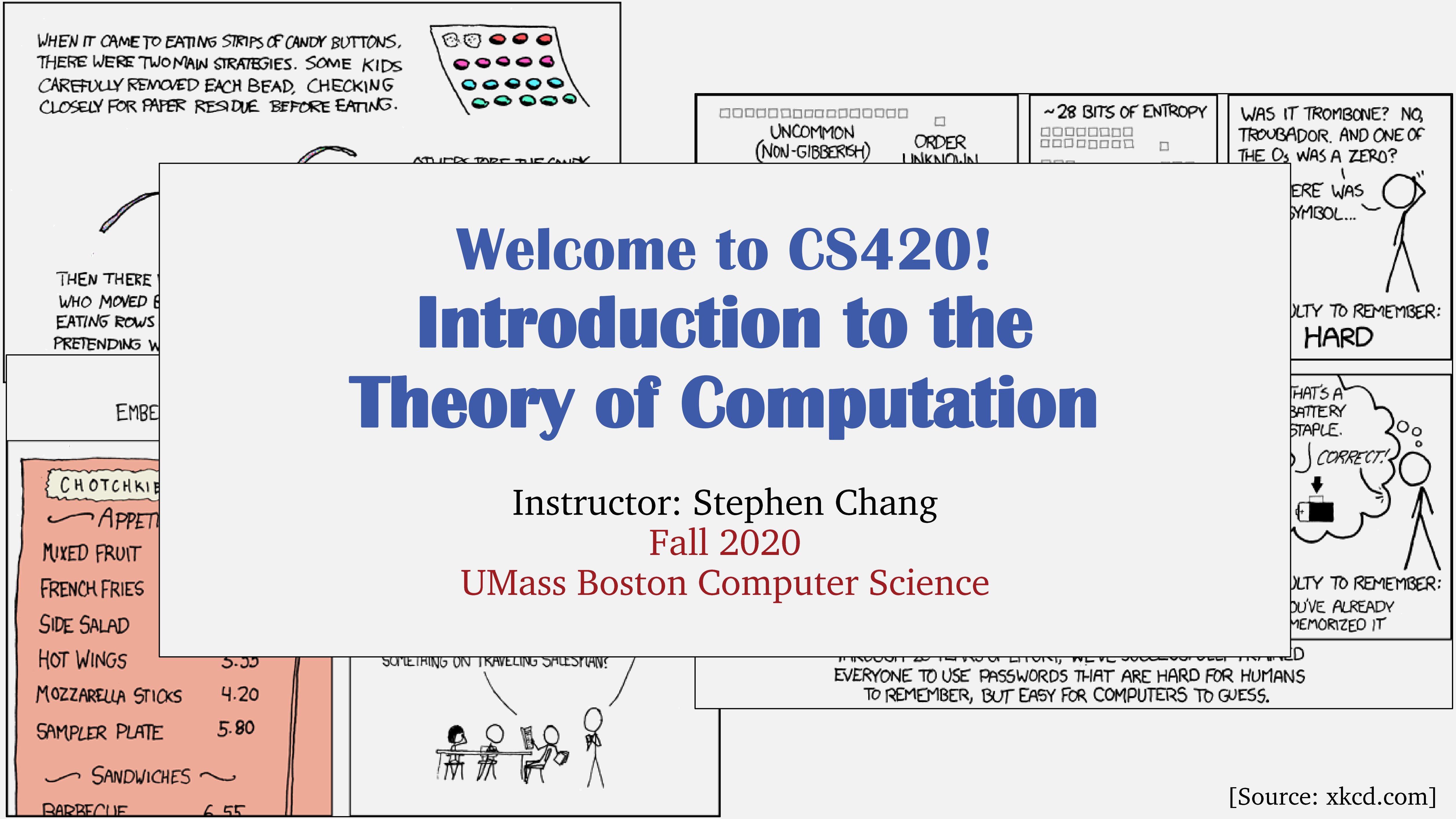

WHEN IT CAME TO EATING STRIPS OF CANDY BUTTONS, THERE WERE TWO MAIN STRATEGIES. SOME KIDS CAREFULLY REMOVED EACH BEAD, CHECKING CLOSELY FOR PAPER RESIDUE BEFORE EATING.
THEN THERE
WHO MOVED
EATING ROWS
PRETENDING W
EMBE
CHOTCHKIE
APPETI
MIXED FRUIT
FRENCH FRIES
SIDE SALAD
HOT WINGS
MOZZARELLA STICKS 4.20
SAMPLER PLATE 5.80
SANDWICHES
BARBECUE 6.55
SOMETHING ON TRAVELING SALESMAN?
UNCOMMON (NON-GIBBERISH)
ORDER UNKNOWN
~28 BITS OF ENTROPY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
ERE WAS
YMBOL...
LTY TO REMEMBER:
HARD
THAT'S A BATTERY STAPLE.
CORRECT!
LTY TO REMEMBER:
OU'VE ALREADY MEMORIZED IT
EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Welcome to CS420!

Introduction to the Theory of Computation

Instructor: Stephen Chang

Fall 2020

UMass Boston Computer Science

[Source: xkcd.com]

Test Poll

Lecture Logistics

- Lectures will be recorded
  - (Recordings will not be posted, due to privacy concerns)
- Keep audio and video off normally
- I may call on students randomly
  - This helps me to get to know each of you individually
  - Turn on audio and video at this time
  - Please be presentable
- Type questions into Zoom’s chat
  - Don’t use the hand raise feature
  - Please be patient since I may only monitor occasionally

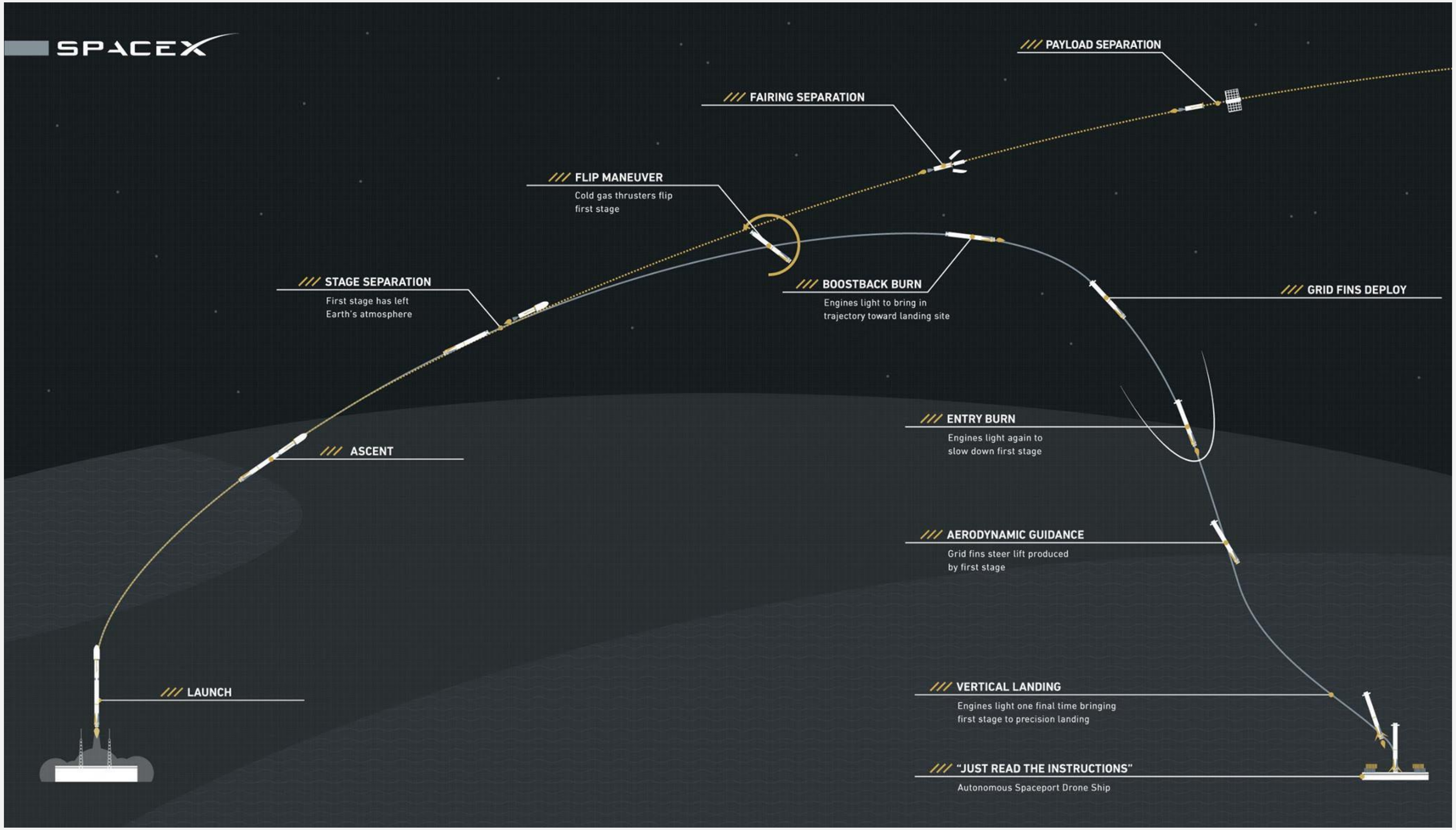
The theory of computation is about …

- Mathematical models of computers

- What is a computer?
  - Many different kinds, with varying “power”

- What is a model?
  - compare with Physics:
  - Has models **to predict behavior** of:
    - Atoms
    - flying baseballs
    - planets, etc.

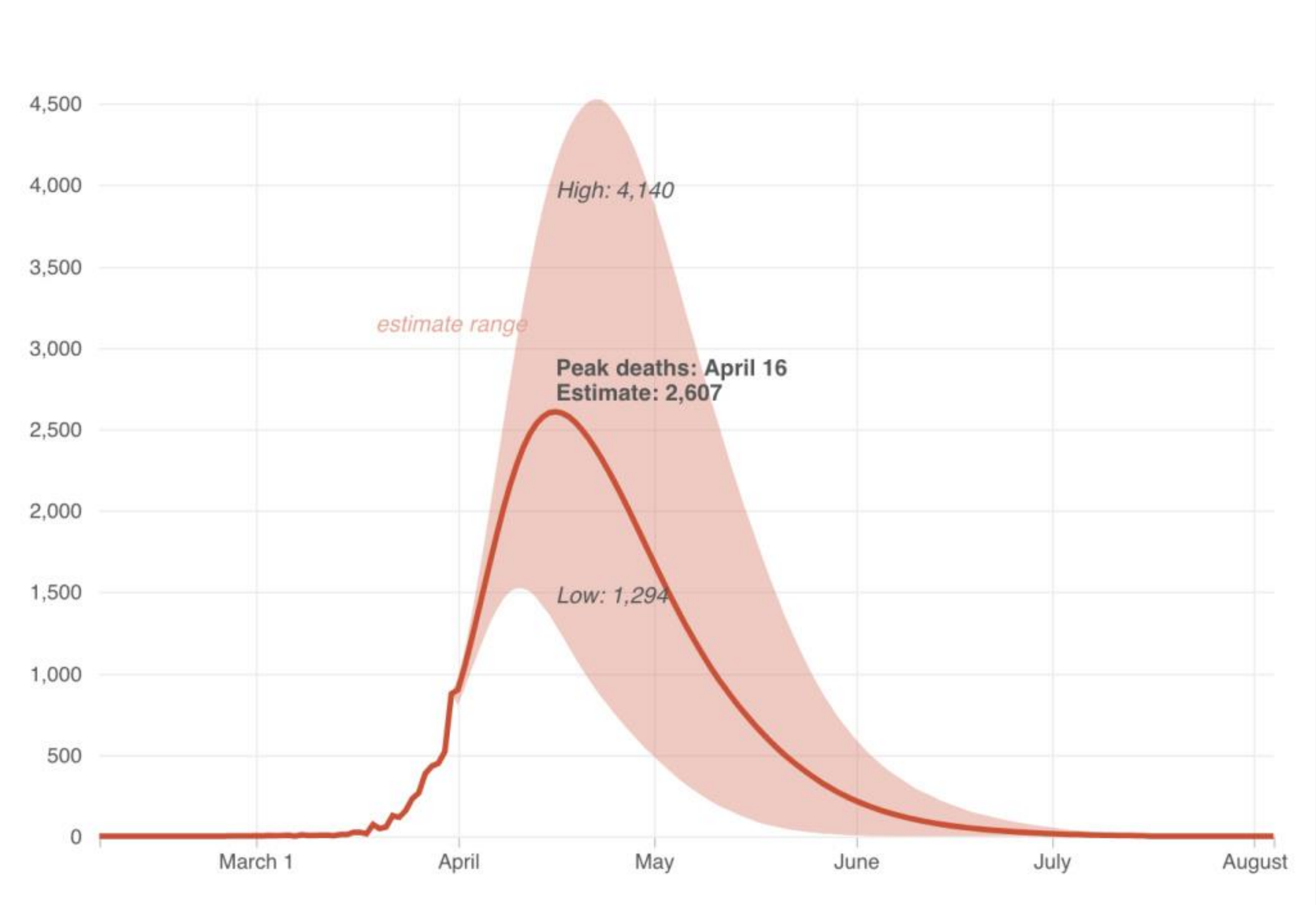
In physics, models can predict …


SPACEX
/// PAYLOAD SEPARATION
/// FAIRING SEPARATION
/// FLIP MANEUVER
Cold gas thrusters flip first stage
/// STAGE SEPARATION
First stage has left Earth's atmosphere
/// BOOSTBACK BURN
Engines light to bring in trajectory toward landing site
/// GRID FINS DEPLOY
/// ENTRY BURN
Engines light again to slow down first stage
/// ASCENT
/// AERODYNAMIC GUIDANCE
Grid fins steer lift produced by first stage
/// LAUNCH
/// VERTICAL LANDING
Engines light one final time bringing first stage to precision landing
/// "JUST READ THE INSTRUCTIONS"
Autonomous Spaceport Drone Ship

Models predict … with varying accuracy

WELCOME TO FLORIDA
MS
2 PM Sat
2 PM Fri
2 AM Fri
2 PM Mon
Cuba
2 PM Thu
5 PM Wed
Mexico
THE CONE OF UNCERTAINTY STATE
Jamaica
Belize
Guatemala
Honduras
makeameme.org

Models predict … with varying accuracy



Some models are worthless

> “We were seeing things that were
> 25-standard deviation moves
> [a 25 std dev event happens once every 100,000 **years**],
> several days in a row.

David Viniar, Goldman Sachs CFO,
August 2007 financial crisis

Math: The “Language” of Models

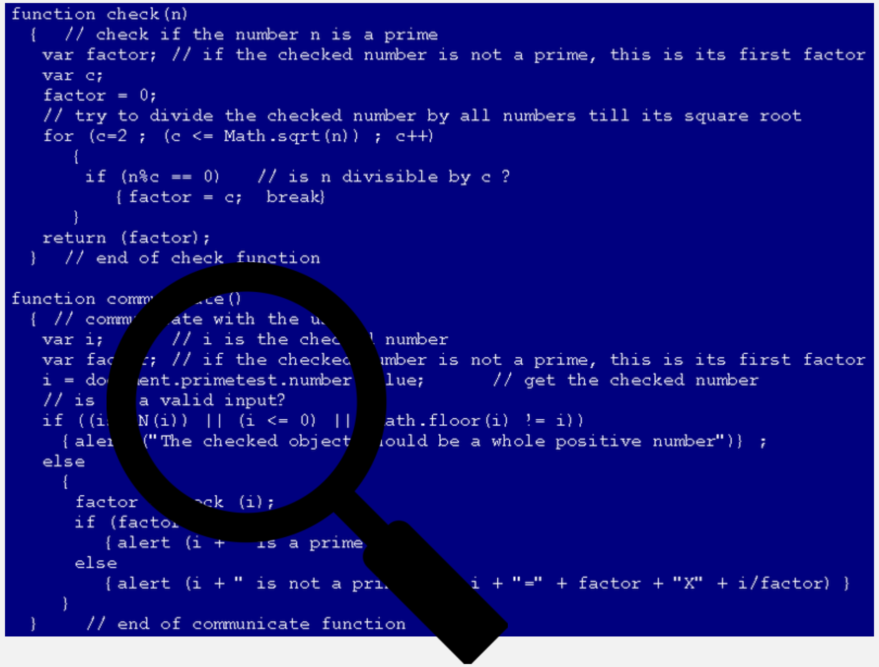
- Physics: algebra, calculus, differential eqs

- Biology: probability

- Computer Science: discrete math, set theory, logic
    - See Chapter 0 in the textbook:
    - *Intro to the Theory of Computation*, 3rd ed, by Michael Sipser

This is mostly a math course!

Why make predictions about computers?



```
function check(n)
  {   // check if the number n is a prime
    var factor; // if the checked number is not a prime, this is its first factor
    var c;
    factor = 0;
    // try to divide the checked number by all numbers till its square root
    for (c=2 ; (c <= Math.sqrt(n)) ; c++)
       {
        if (n%c == 0)    // is n divisible by c ?
           { factor = c;   break}
       }
    return (factor);
  }   // end of check function

function comm      te()
  {  // comm     ate with the u
    var i;         // i is the chec   d number
    var fac   r; // if the checked   umber is not a prime, this is its first factor
    i = doc   ent.primetest.number   lue;       // get the checked number
    // is      a valid input?
    if ((i    N(i)) || (i <= 0) ||    ath.floor(i) != i))
      { aler   ("The checked object   ould be a whole positive number")} ;
    else
      {
       factor       ck (i);
       if (facto
          { alert (i +    is a prime
       else
          { alert (i + " is not a pri          i + "=" + factor + "X" + i/factor) }
      }
  }     // end of communicate function
```

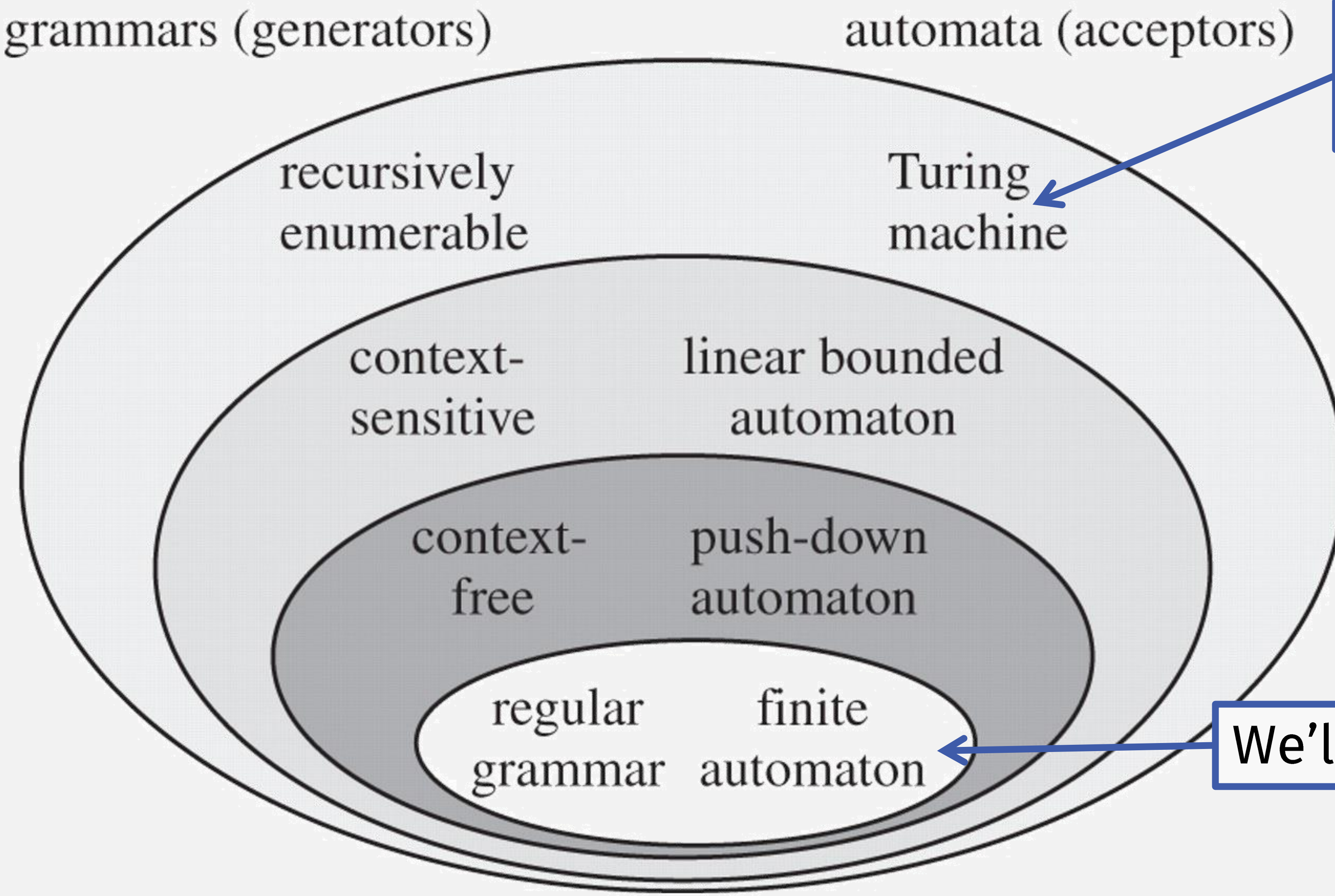
Can we make predictions about computers?

- The **Halting Lemma** says:

- **Rice's Theorem** says:
  - "all non-trivial, semantic properties of programs are undecidable"

- Actually:
  - it depends on the computation model!

Many levels of computational power



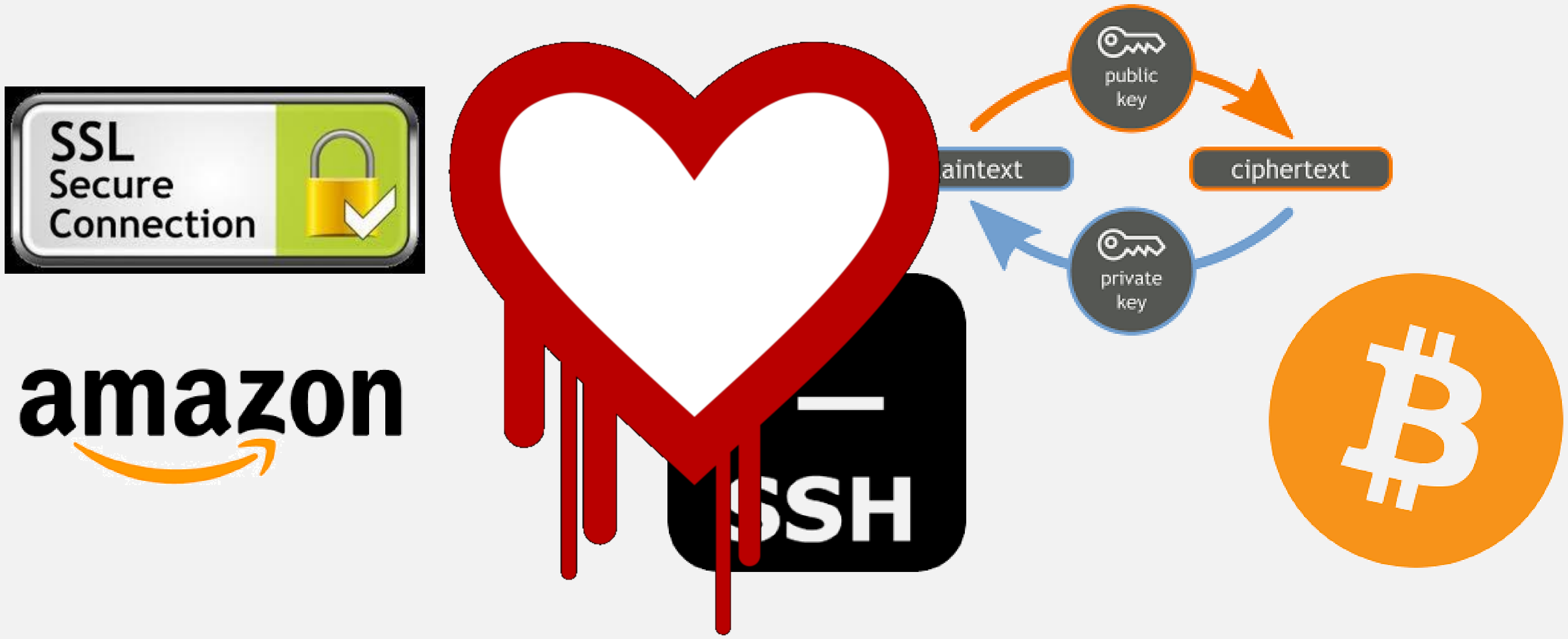
Halting Lemma, Rice's Theorem

- more complex
- more powerful
- less restricted

We'll start here

Knowing a Computer’s Limit is Still Useful!

- In Cryptography:
  - Perfect secrecy: impossible in practice
  - Slightly imperfect secrecy (i.e., computationally bounded adversary):

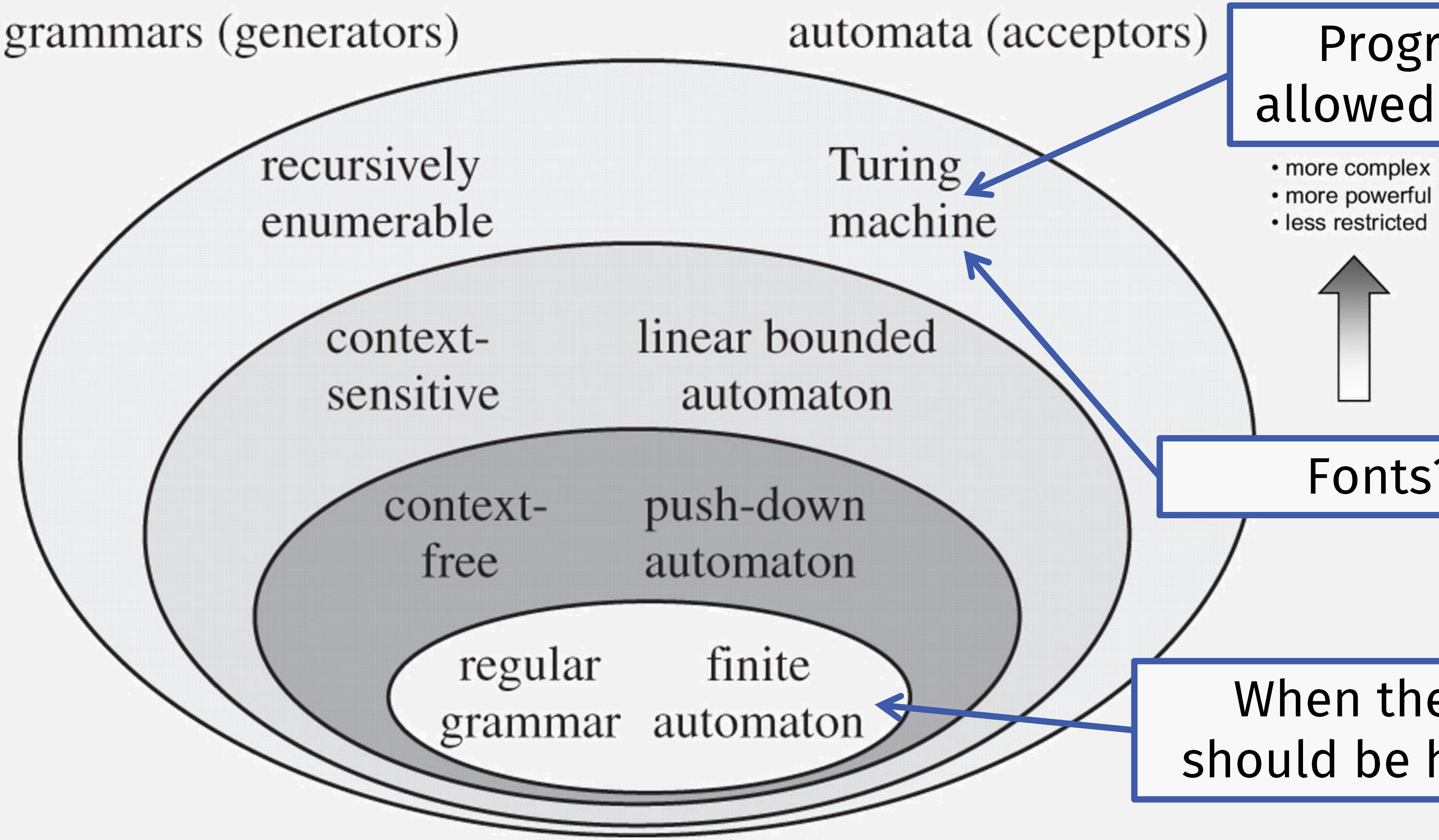


LANGSEC: Language-theoretic Security

> “LANGSEC is an area of research that regards
> the Internet insecurity epidemic
> as a consequence of not paying attention to
> the computational power given to inputs

langsec.org

LANGSEC: Language-theoretic Security

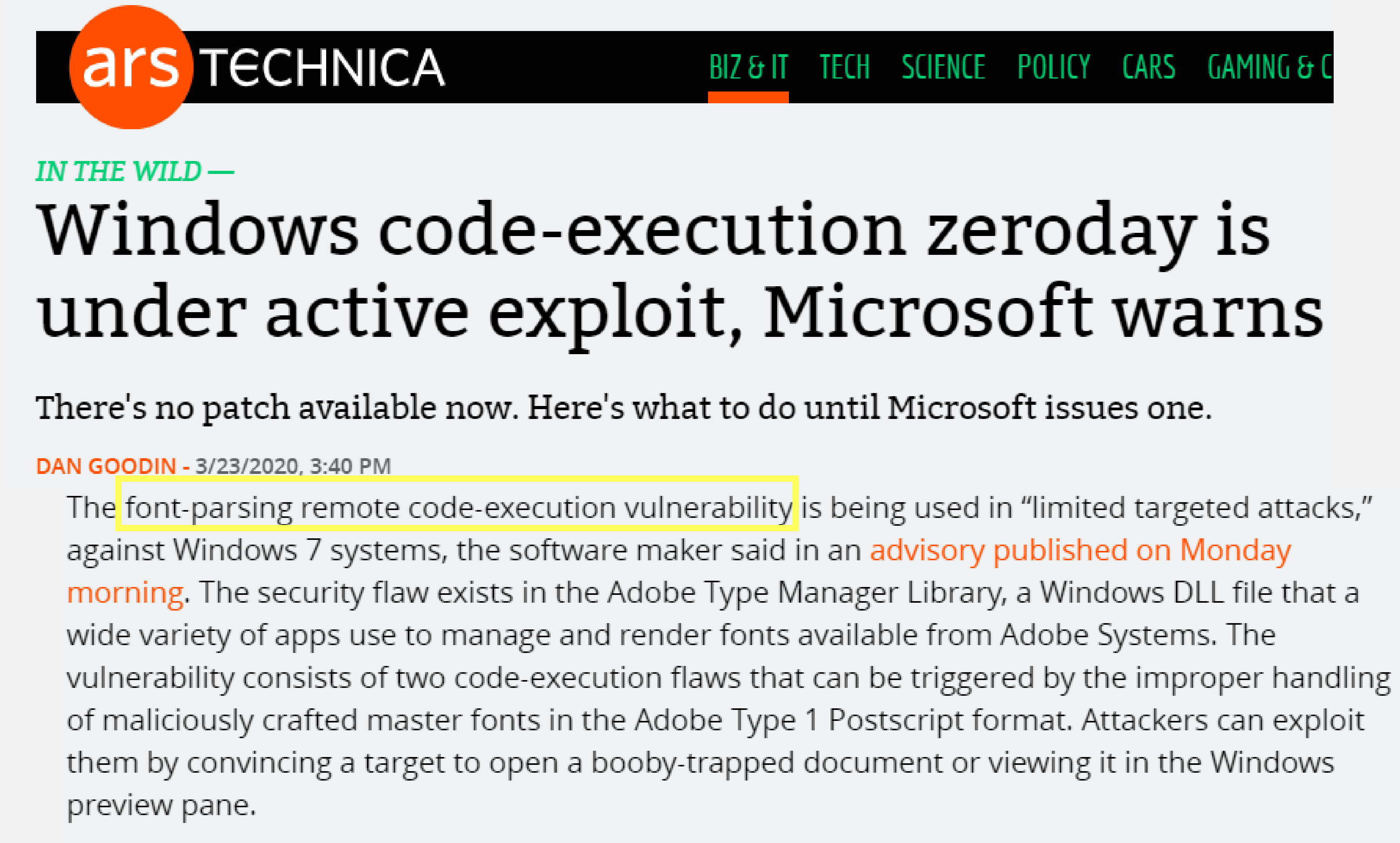


Programs are allowed to be here

Fonts?

When they should be here

What computing power should fonts have?



IN THE WILD —

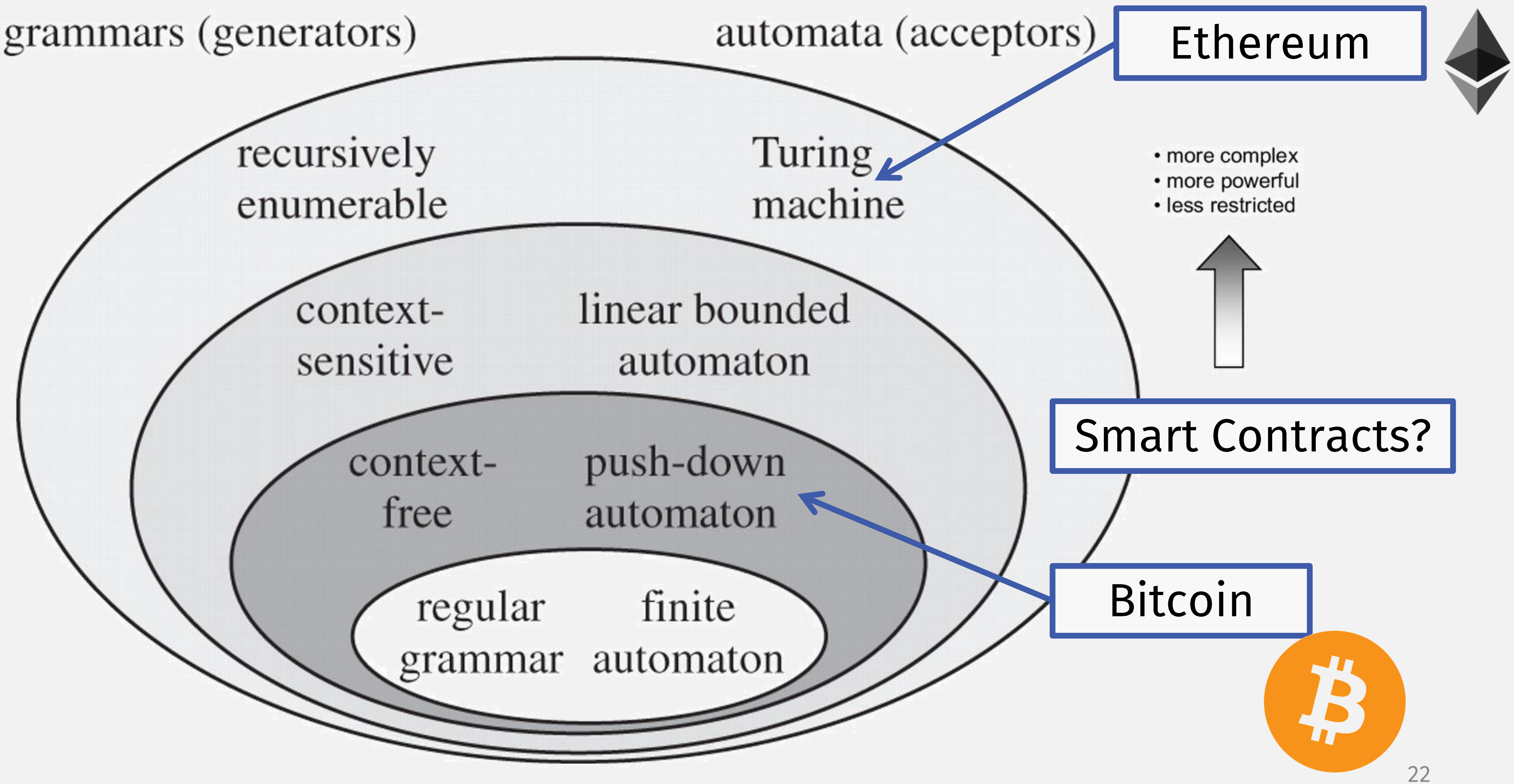
Windows code-execution zeroday is under active exploit, Microsoft warns

There's no patch available now. Here's what to do until Microsoft issues one.

DAN GOODIN - 3/23/2020, 3:40 PM

The font-parsing remote code-execution vulnerability is being used in "limited targeted attacks," against Windows 7 systems, the software maker said in an advisory published on Monday morning. The security flaw exists in the Adobe Type Manager Library, a Windows DLL file that a wide variety of apps use to manage and render fonts available from Adobe Systems. The vulnerability consists of two code-execution flaws that can be triggered by the improper handling of maliciously crafted master fonts in the Adobe Type 1 Postscript format. Attackers can exploit them by convincing a target to open a booby-trapped document or viewing it in the Windows preview pane.

LANGSEC: Language-theoretic Security



grammars (generators)

automata (acceptors)

recursively enumerable

Turing machine

context-sensitive

linear bounded automaton

context-free

push-down automaton

regular grammar

finite automaton

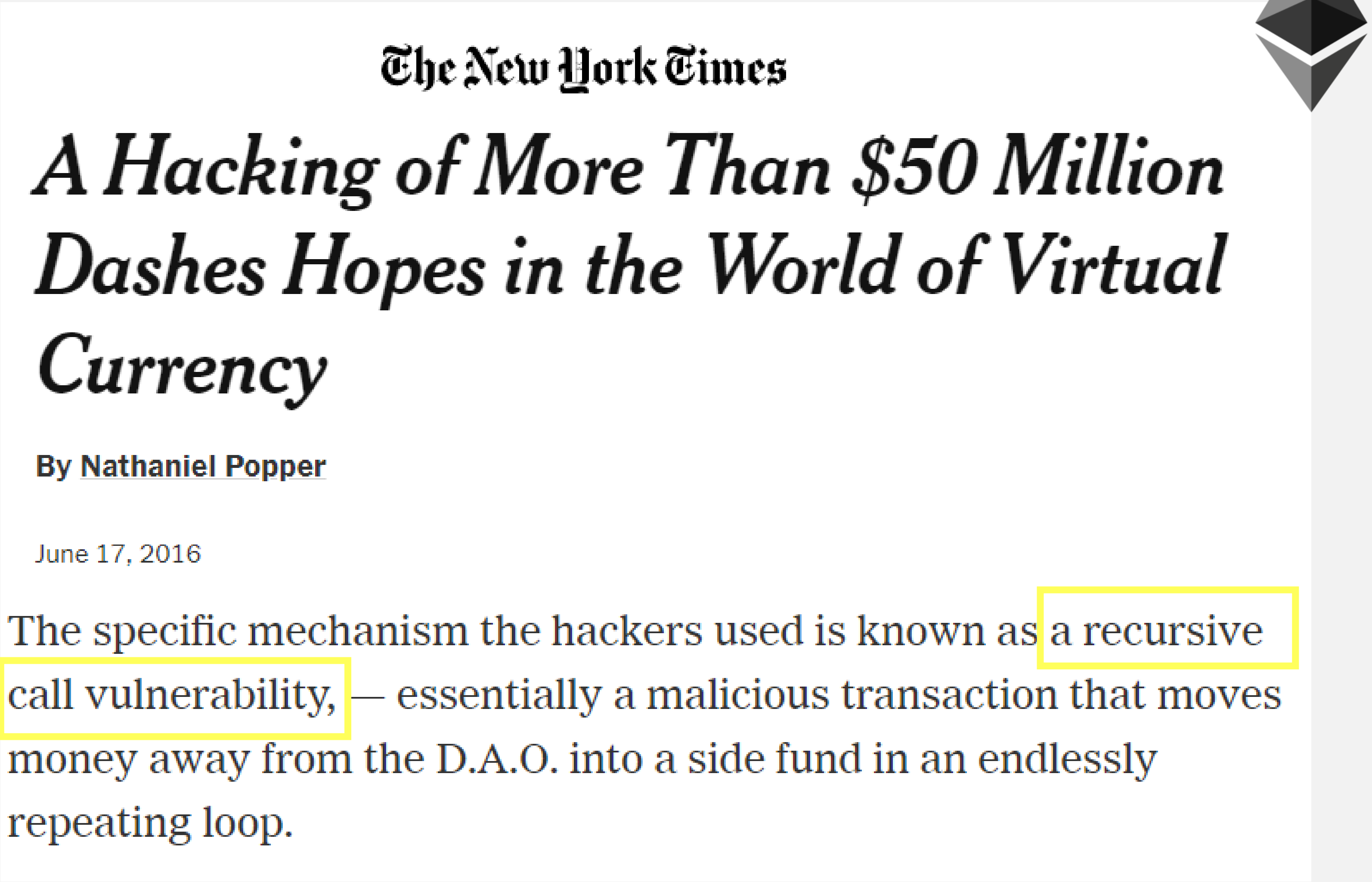
- more complex
- more powerful
- less restricted

Ethereum

Smart Contracts?

Bitcoin

What power should smart contracts have?



The New York Times

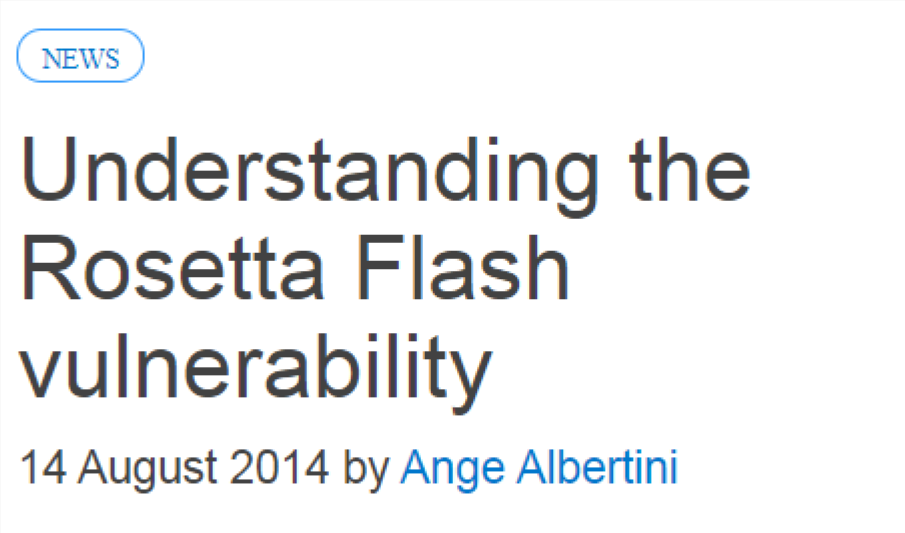
A Hacking of More Than $50 Million Dashes Hopes in the World of Virtual Currency

By Nathaniel Popper

June 17, 2016

The specific mechanism the hackers used is known as a recursive call vulnerability, — essentially a malicious transaction that moves money away from the D.A.O. into a side fund in an endlessly repeating loop.

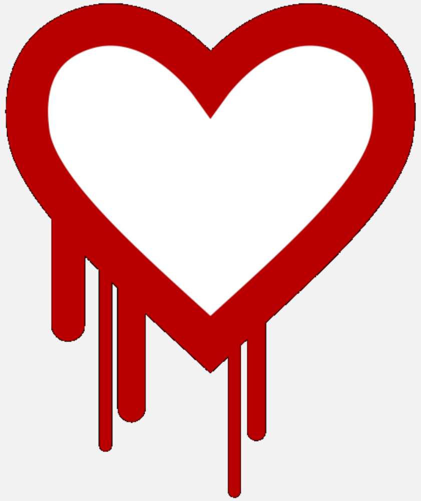
What computing power should ??? have?

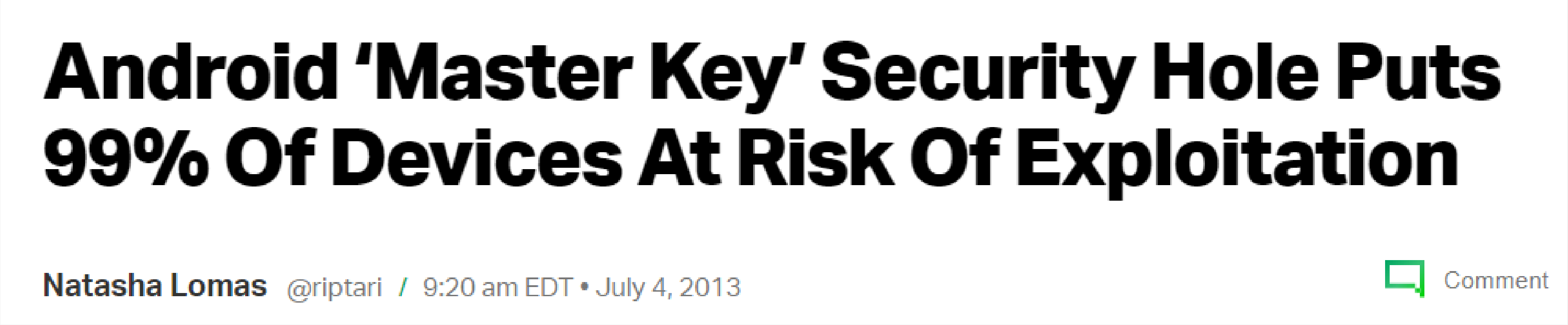


NEWS

Understanding the Rosetta Flash vulnerability

14 August 2014 by Ange Albertini





Android 'Master Key' Security Hole Puts 99% Of Devices At Risk Of Exploitation

Natasha Lomas @riptari / 9:20 am EDT • July 4, 2013

Check-In Quiz 0

Course Logistics

Course website:

https://www.cs.umb.edu/~stchang/cs420/f20/