Lecture 24: Computer Security

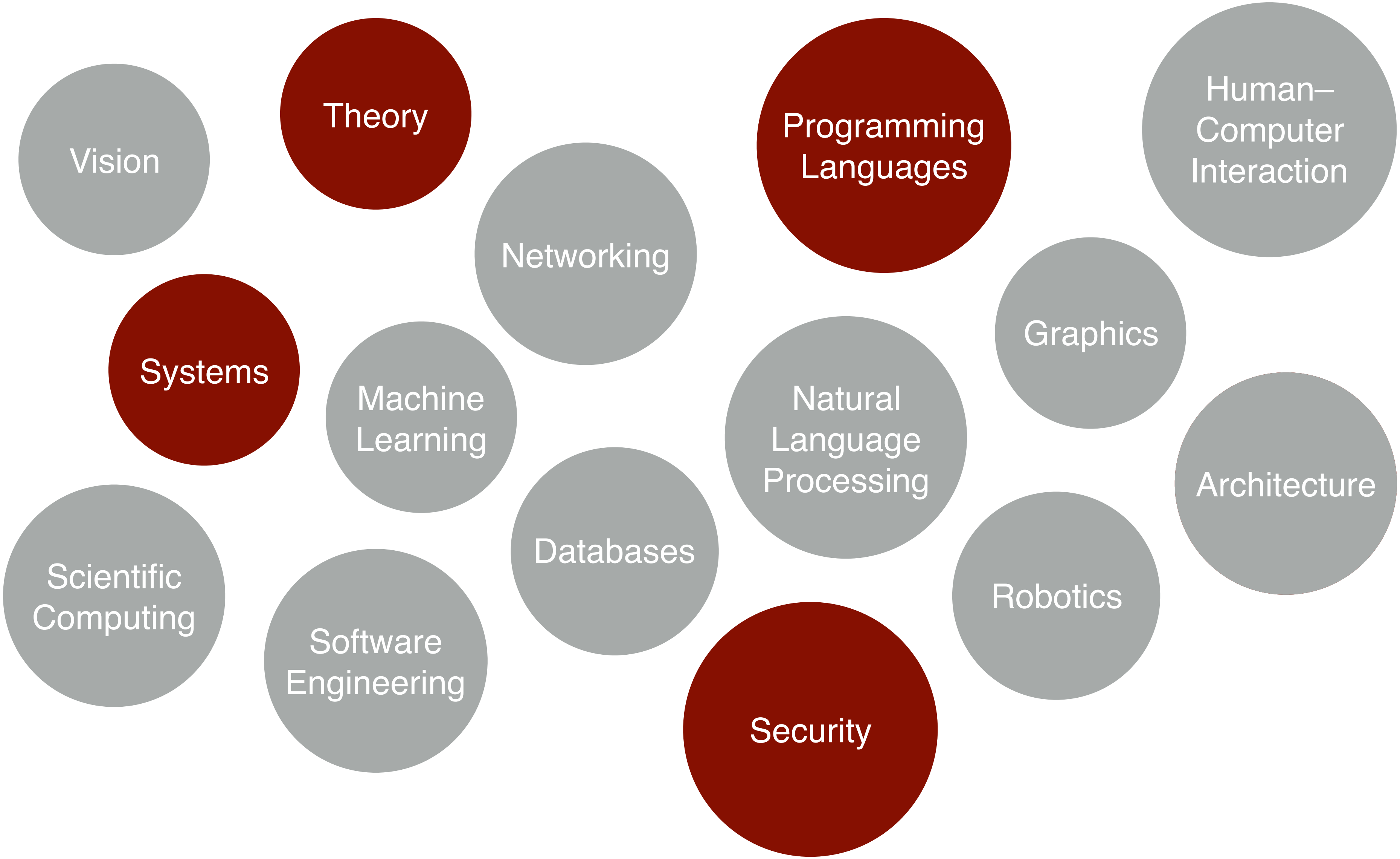
CS 51P

December 7, 2022

Computer Science

- Vision
- Theory
- Networking
- Programming Languages
- Human–Computer Interaction
- Graphics
- Systems
- Machine Learning
- Natural Language Processing
- Architecture
- Databases
- Scientific Computing
- Software Engineering
- Robotics
- Security

Computer Security



Vision

Theory

Networking

Programming Languages

Human–Computer Interaction

Systems

Machine Learning

Graphics

Natural Language Processing

Architecture

Scientific Computing

Software Engineering

Databases

Robotics

Security

Computer Security

- Security is about making sure that computers behave correctly
- A **secure system** should:
  1) Do what it is supposed to do
  2) Not do anything else

What might go wrong

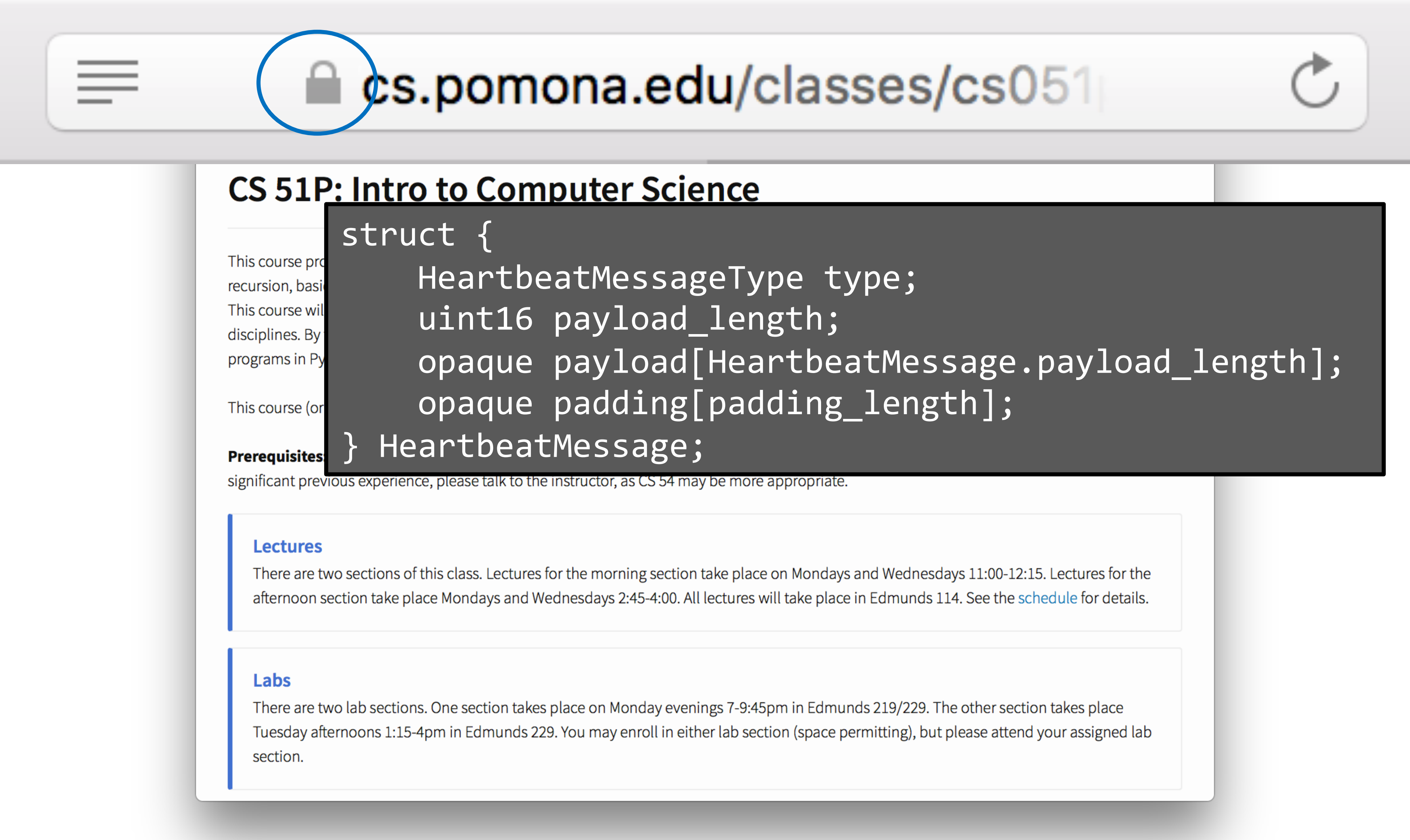
```
class ObjectStore:

    def __init__(self, len):
        self.objects = [None]*len

    def read(self, i):
        return self.objects[i]

    def store(self, i, o):
        self.objects[i]= o
```

OpenSSL



cs.pomona.edu/classes/cs051

CS 51P: Intro to Computer Science

This course pro

recursion, basi

This course wil

disciplines. By

programs in Py

This course (or

Prerequisites:

significant previous experience, please talk to the instructor, as CS 54 may be more appropriate.

Lectures

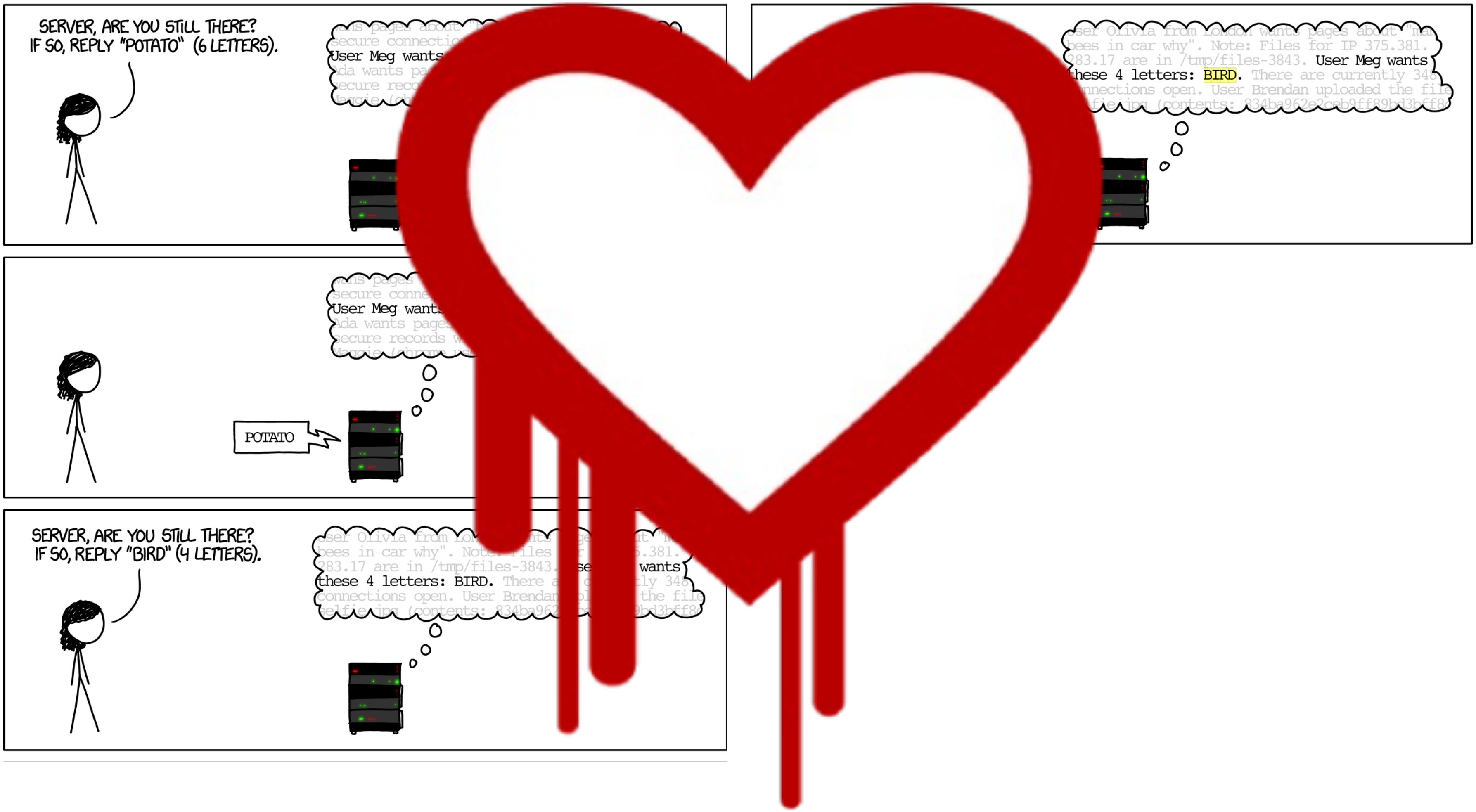
There are two sections of this class. Lectures for the morning section take place on Mondays and Wednesdays 11:00-12:15. Lectures for the afternoon section take place Mondays and Wednesdays 2:45-4:00. All lectures will take place in Edmunds 114. See the schedule for details.

Labs

There are two lab sections. One section takes place on Monday evenings 7-9:45pm in Edmunds 219/229. The other section takes place Tuesday afternoons 1:15-4pm in Edmunds 229. You may enroll in either lab section (space permitting), but please attend your assigned lab section.

```
struct {
    HeartbeatMessageType type;
    uint16 payload_length;
    opaque payload[HeartbeatMessage.payload_length];
    opaque padding[padding_length];
} HeartbeatMessage;
```

Heartbleed


SERVER, ARE YOU STILL THERE? IF SO, REPLY "POTATO" (6 LETTERS).
User Meg wants
POTATO
SERVER, ARE YOU STILL THERE? IF SO, REPLY "BIRD" (4 LETTERS).
User Olivia from London wants pages about "bees in car why". Note: Files for IP 375.381.283.17 are in /tmp/files-3843. User Meg wants these 4 letters: BIRD. There are currently 346 connections open. User Brendan uploaded the file selfie.jpg (contents: 834ba962e2ceb9ff89bd3bff8

What might go wrong

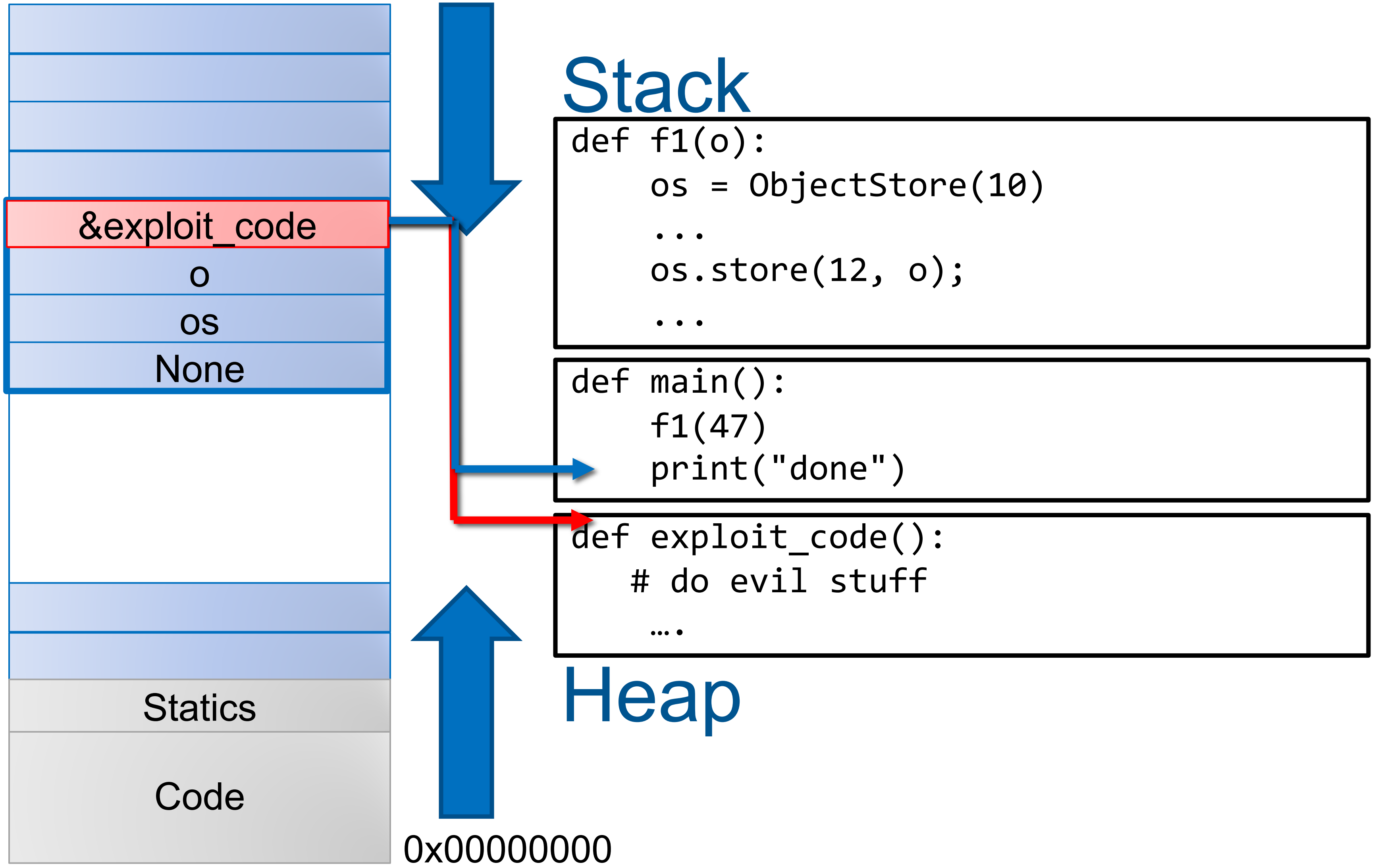
```
class ObjectStore:

      def __init__(self, len):
            self.objects = [None]*len


      def read(self, i):
           return self.objects[i]


      def store(self, i, o):
           self.objects[i]= o
```

Memory

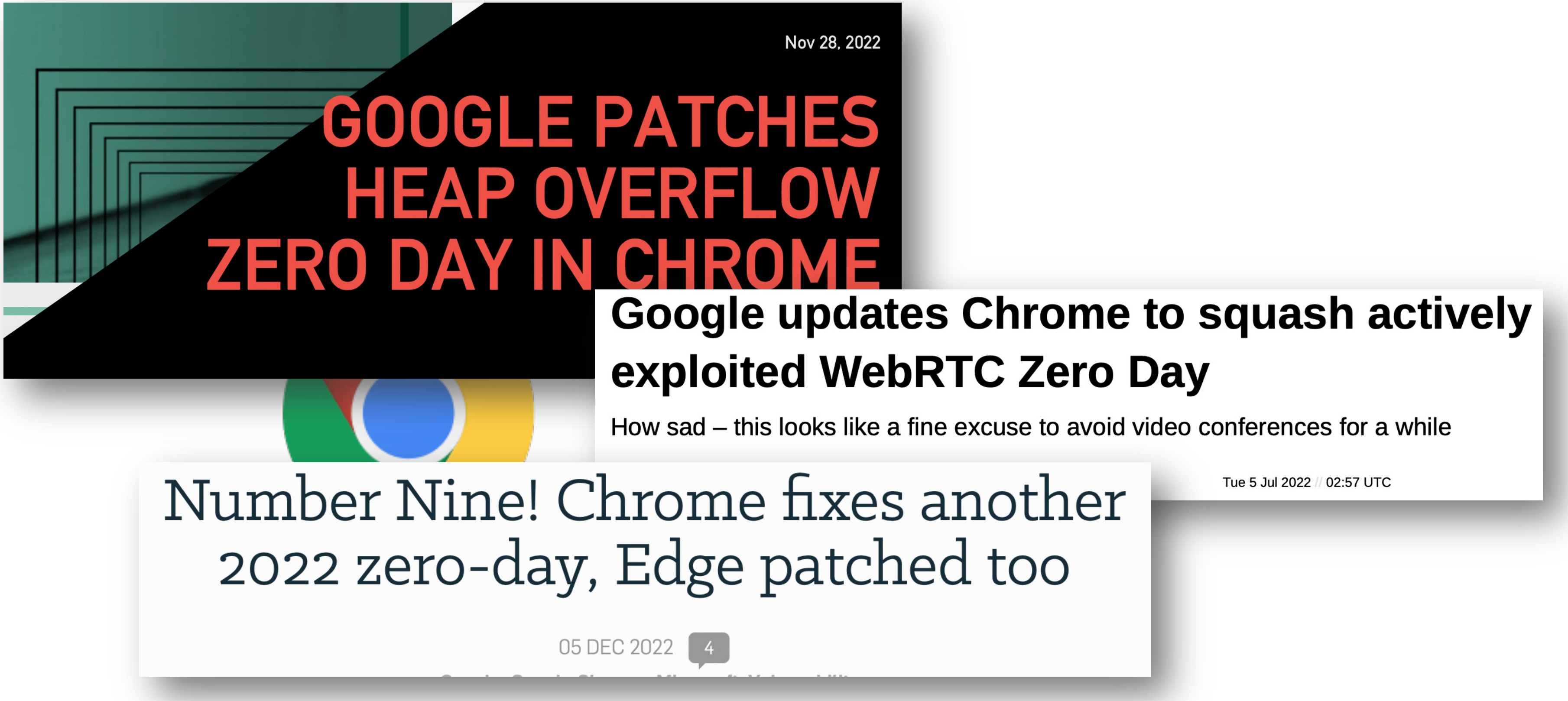


```
def f1(o):
    os = ObjectStore(10)
    ...
    os.store(12, o);
    ...
```

```
def main():
    f1(47)
    print("done")
```

```
def exploit_code():
   # do evil stuff
    ….
```

Chrome Vulnerability



Nov 28, 2022

GOOGLE PATCHES HEAP OVERFLOW ZERO DAY IN CHROME

Google updates Chrome to squash actively exploited WebRTC Zero Day

How sad – this looks like a fine excuse to avoid video conferences for a while

Tue 5 Jul 2022 // 02:57 UTC

Number Nine! Chrome fixes another 2022 zero-day, Edge patched too

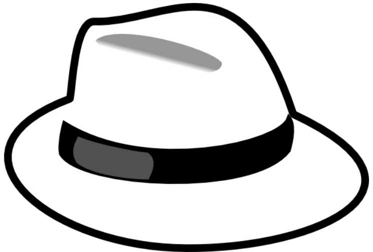
05 DEC 2022 4

So how do we fix this?

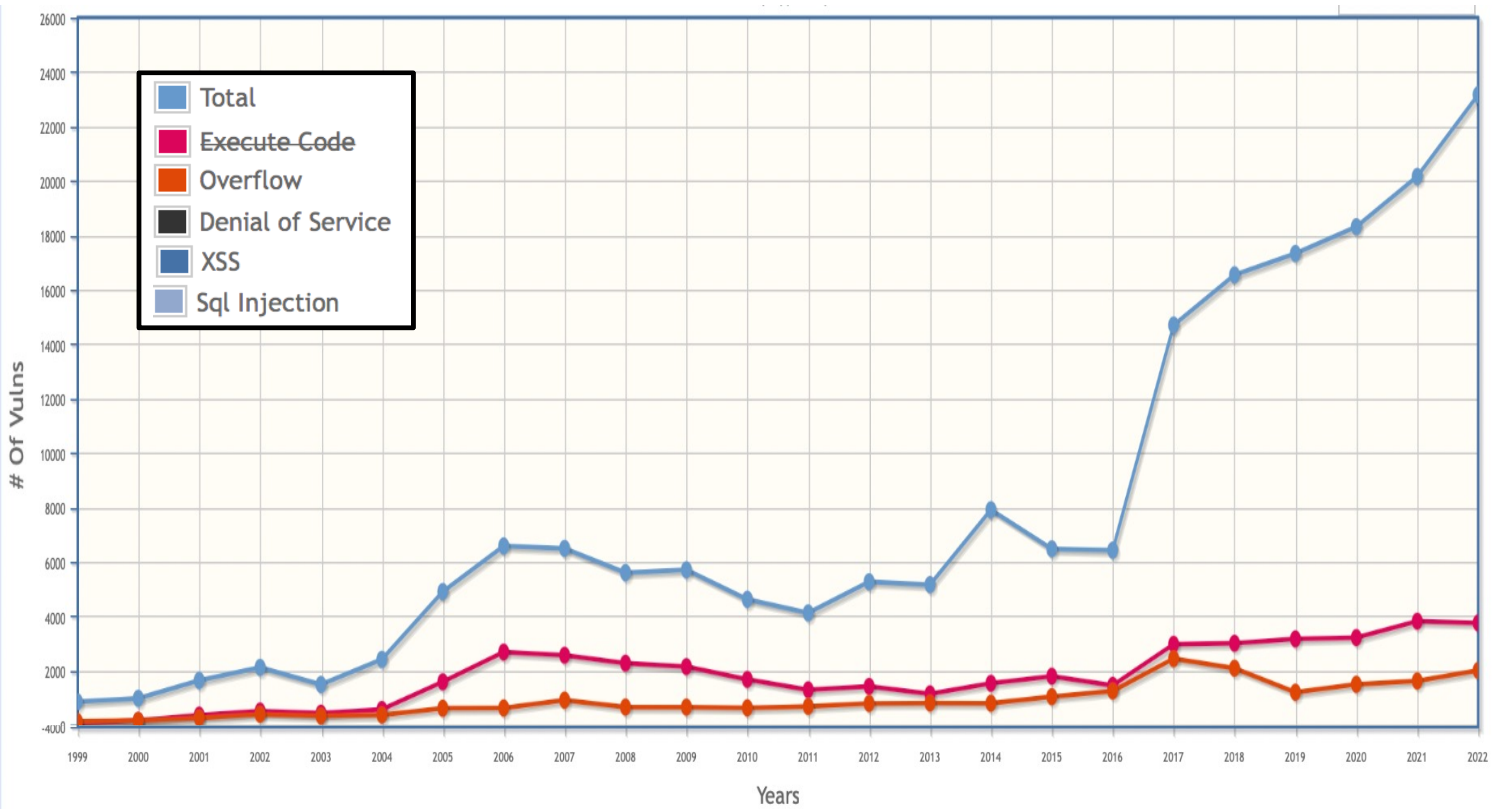
- Testing
- Bug finding tools

FindBugs™

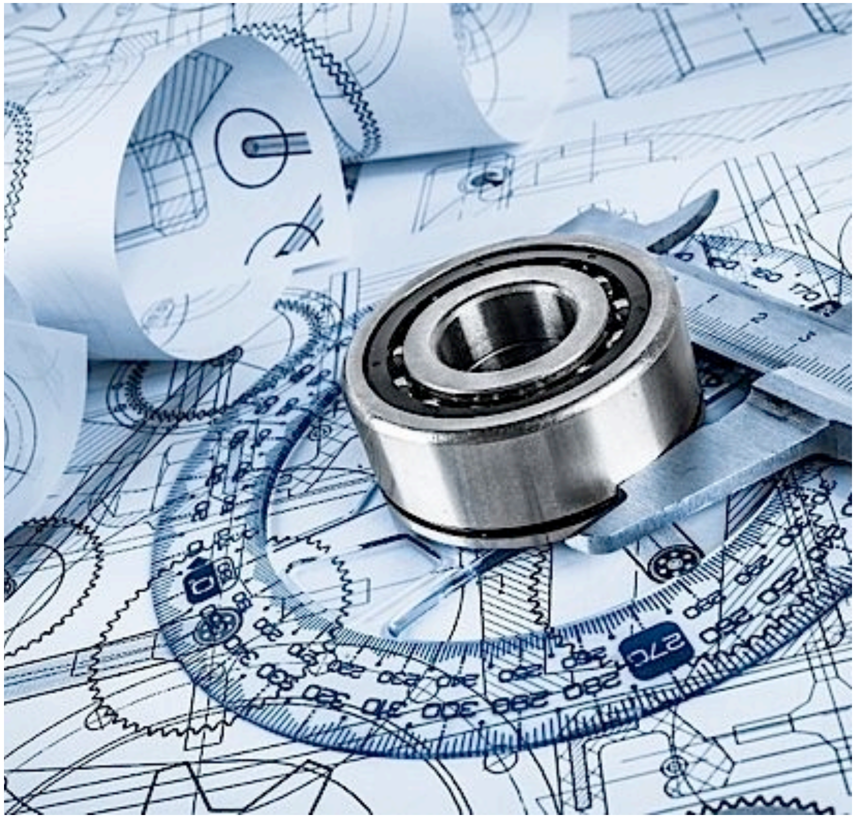
- Provably correct code
- White-hat hacking



Vulnerabilities by Year



So how do we fix this?



Security by Design

- Build secure, trustworthy computer systems/applications/etc.
- Define what the system is supposed to do
- Make sure it does that (and only that)

Engineering Security

Attacks
are perpetrated by
threats
that cause
incorrect behavior
by exploiting
vulnerabilities
which are controlled by
countermeasures.

Classes of Countermeasures

Authentication: mechanisms that bind principals to actions

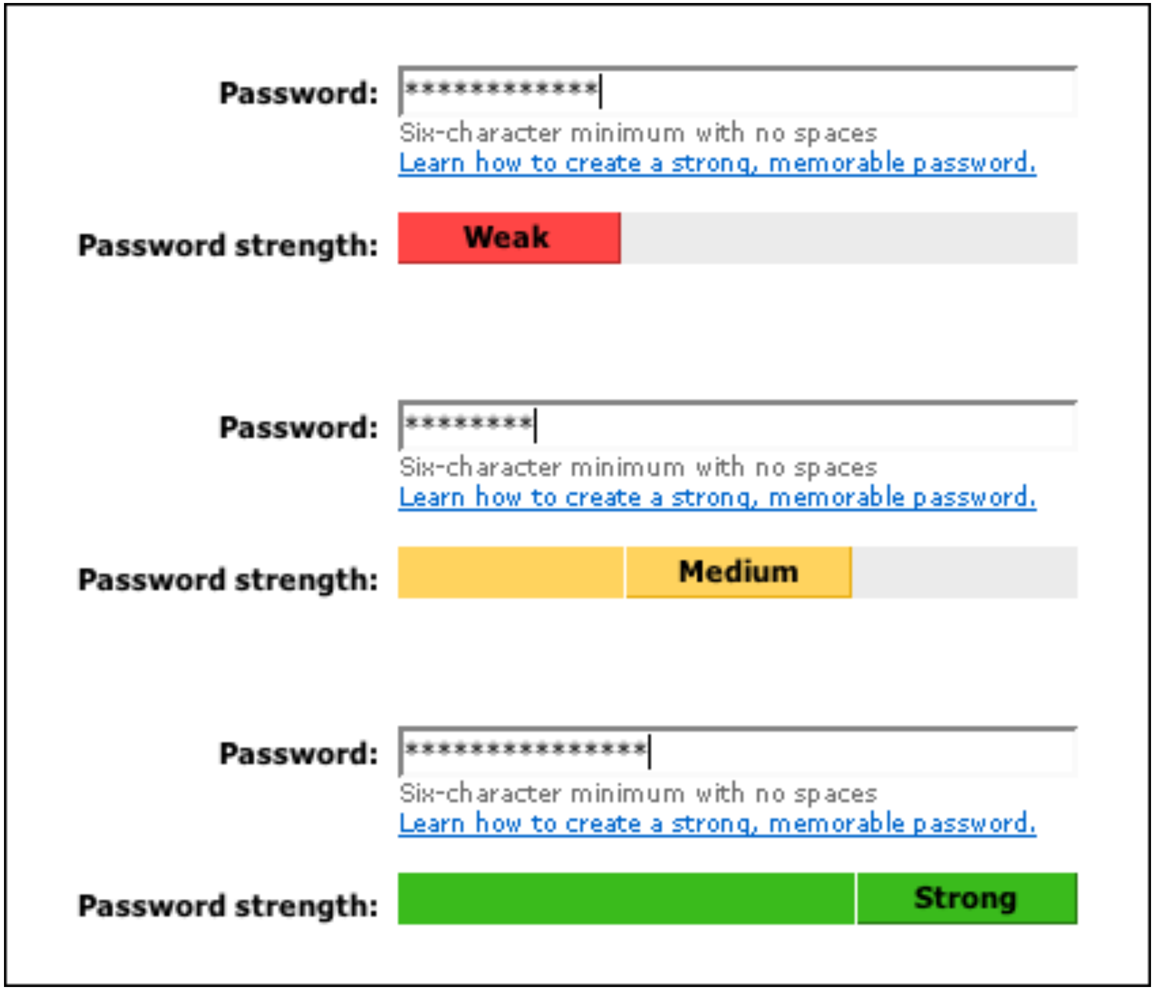
Authorization: mechanisms that govern whether actions are permitted

Audit: mechanisms that record and review actions

Assumptions

Most Common Passwords (2022)

1.
2.
3.
4.
5.



Password: ************

Six-character minimum with no spaces

Learn how to create a strong, memorable password.

Password strength: Weak

Password: ********

Six-character minimum with no spaces

Learn how to create a strong, memorable password.

Password strength: Medium

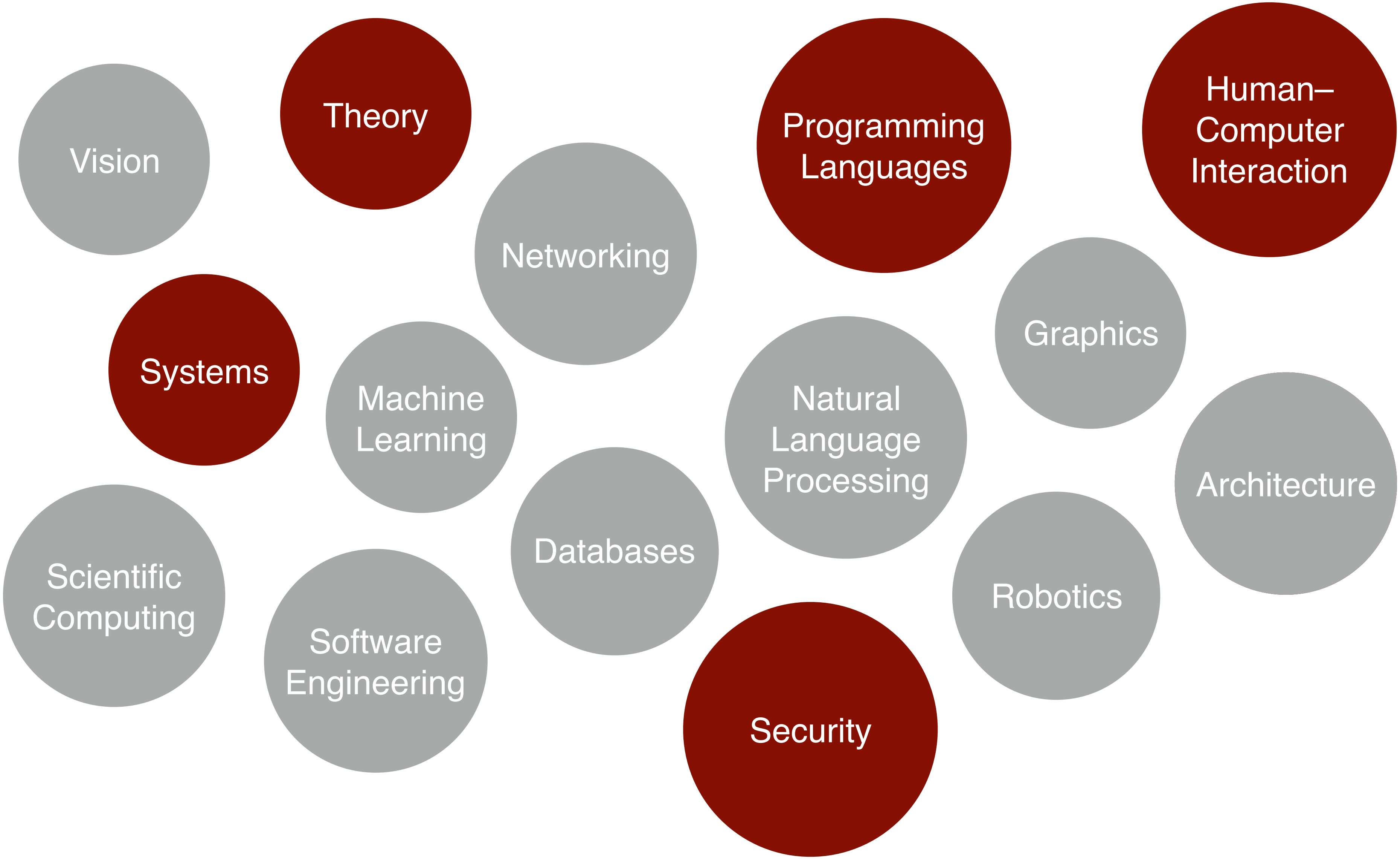
Password: ***************

Six-character minimum with no spaces

Learn how to create a strong, memorable password.

Password strength: Strong

Usable Security



Vision

Theory

Networking

Programming Languages

Human–Computer Interaction

Systems

Machine Learning

Graphics

Natural Language Processing

Architecture

Scientific Computing

Software Engineering

Databases

Robotics

Security

Prospect Theory

- Reference-dependence
- Isolation
- Pseudocertainty

- Loss Aversion
- Certainty
- Source-dependence

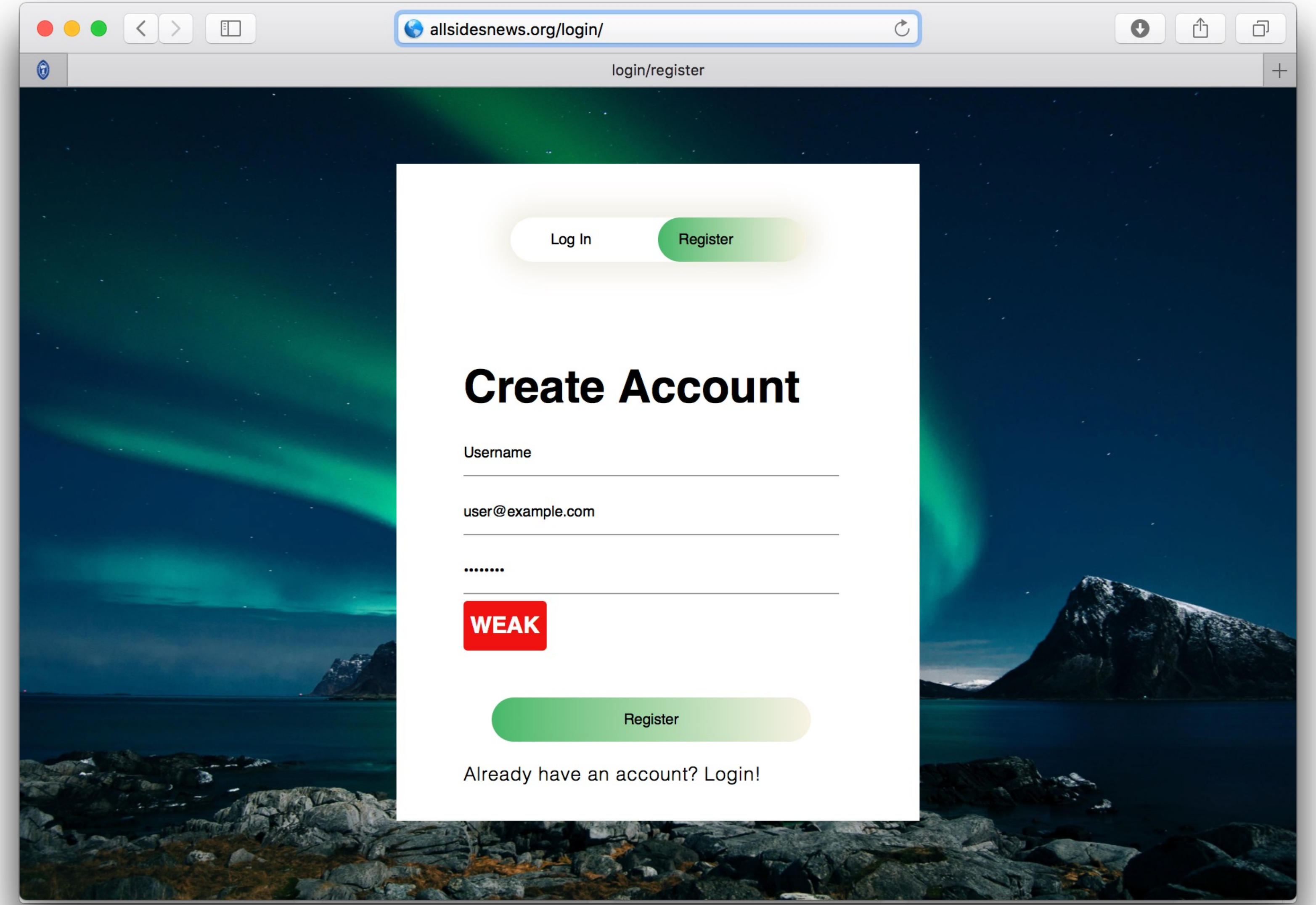
Prospect Theory as Descriptive Model

- **Finance:** which stocks investors sell [Shefrin & Statman, 1985]
- **Insurance:** predicting over-insurance[Sydnor, 2010]
- **Savings:** patterns in spending [Koszegi & Rabin, 2009]
- **Security:** adoption of 2FA [Qu et al., 2019]
- **Privacy:** disclosure of personal information [Adjerid et al., 2013]

Prescriptive Applications of Prospect Theory

- Nudge employees to increase their retirement contributions [Thaler & Benartzi, 2004]
- Nudge teams in high-tech factories to increase productivity [Hossain & List, 2012]
- Nudge teachers to improve student outcomes [Levitt et al., 2016]

Password Selection



allsidesnews.org/login/

login/register

Create Account

Username

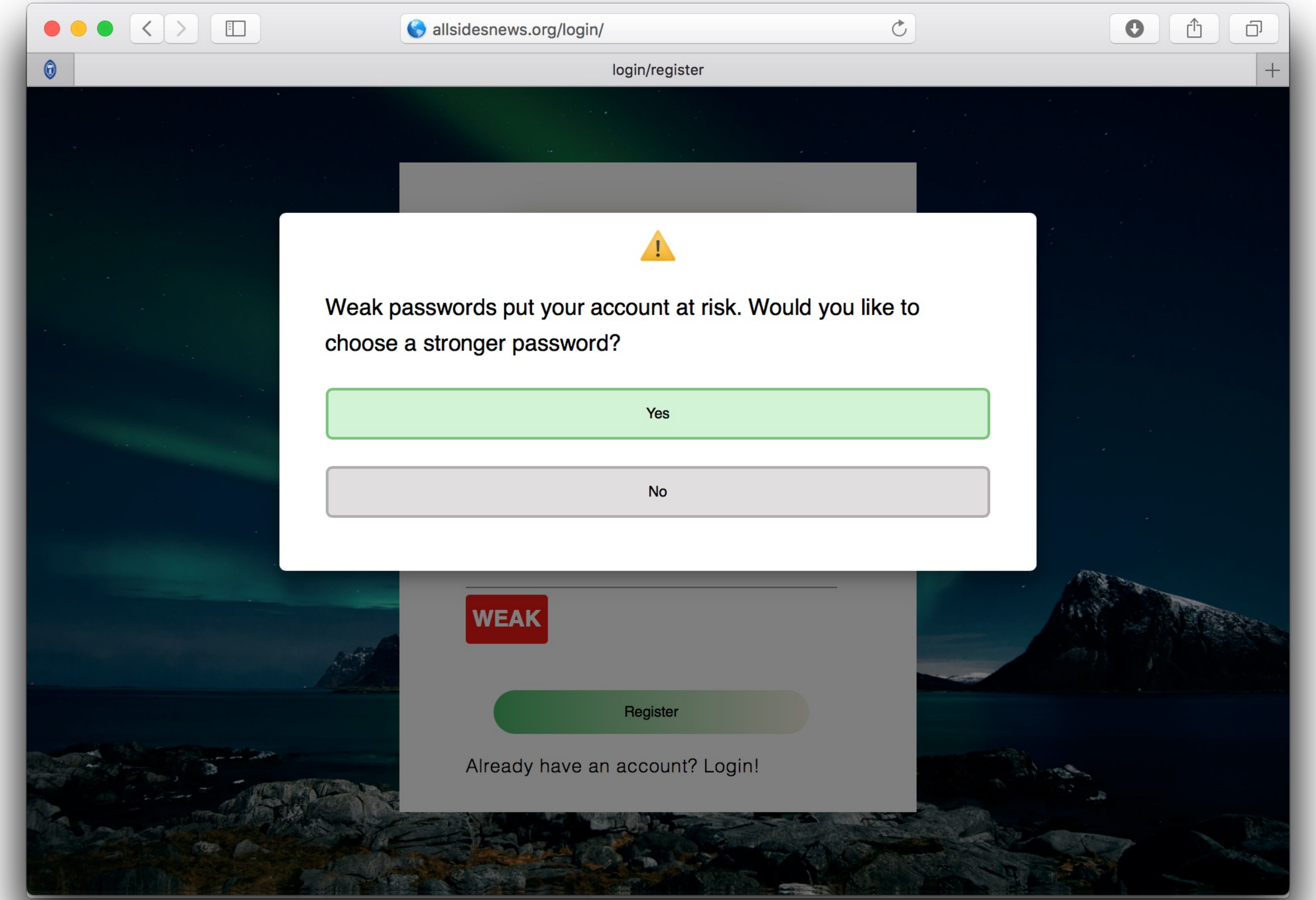
user@example.com

••••••••

WEAK

Already have an account? Login!

Framing Password Selection



Weak passwords put your account at risk. Would you like to choose a stronger password?

Framing Password Selection

- Positive Framing

  Go Back: Choose a stronger password to reduce the risks of financial loss and identity theft

  Continue: Create account with current password

- Neutral Framing

  Go Back: Yes

  Continue: No

- Negative Framing

  Go Back: Choose a stronger password

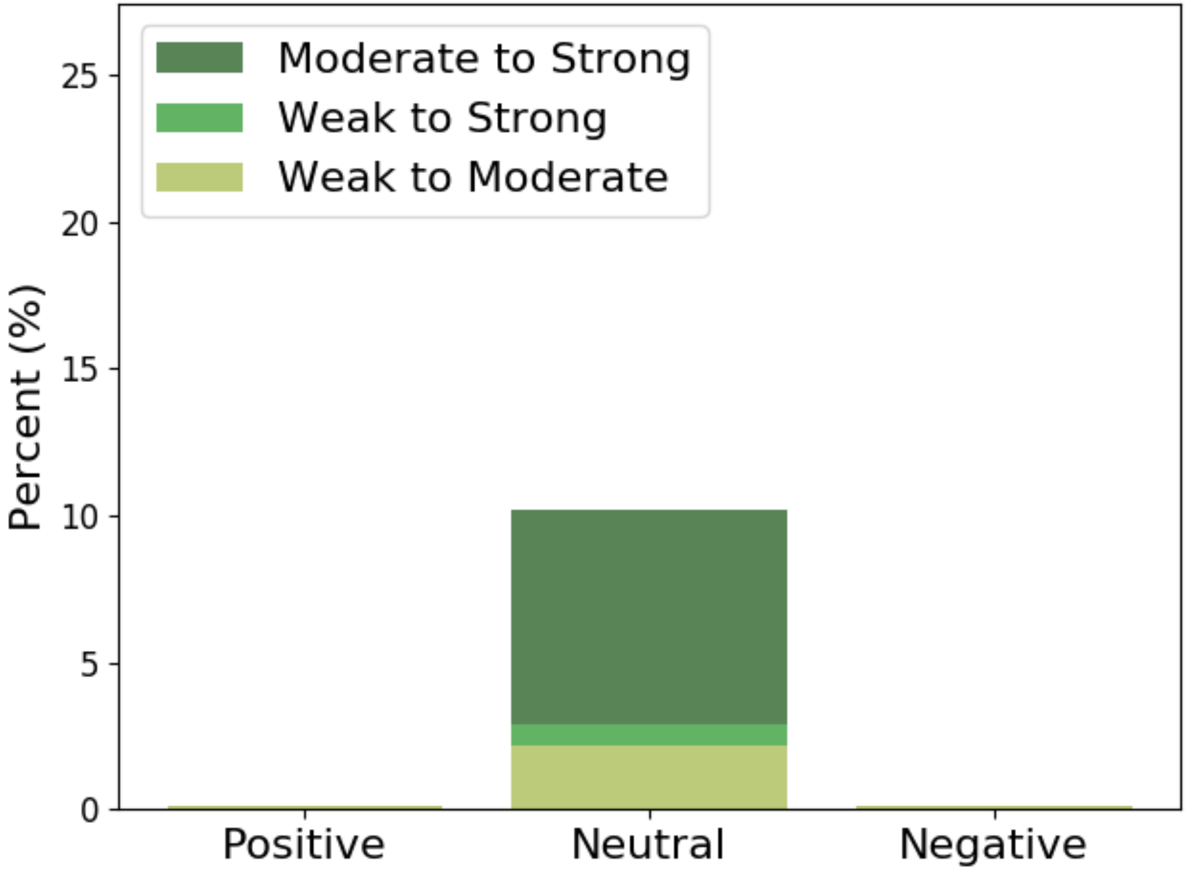
  Continue: Ignore potential risks of financial loss and identity theft and create account with current password

User Study: Password Selection

- 762 U.S. residents recruited on Amazon Mechanical Turk

- Task: Beta Test Aggregated News Website
- Participants were given test username and email, asked to use a password of their choice

Framing Password Selection



Security Decision Theory

GDPR CCPA

LD946 PIPA

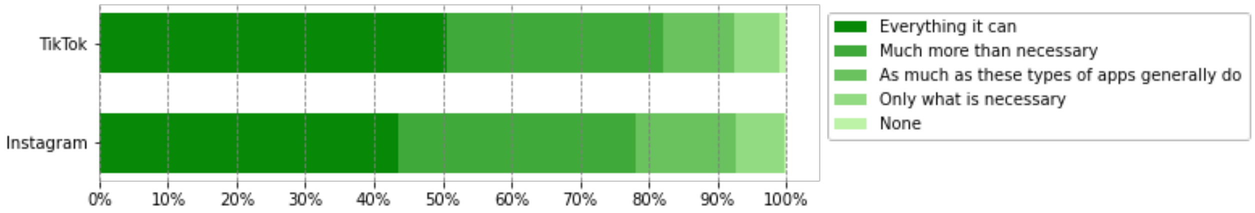
APPI **Legal Privacy**

SB220

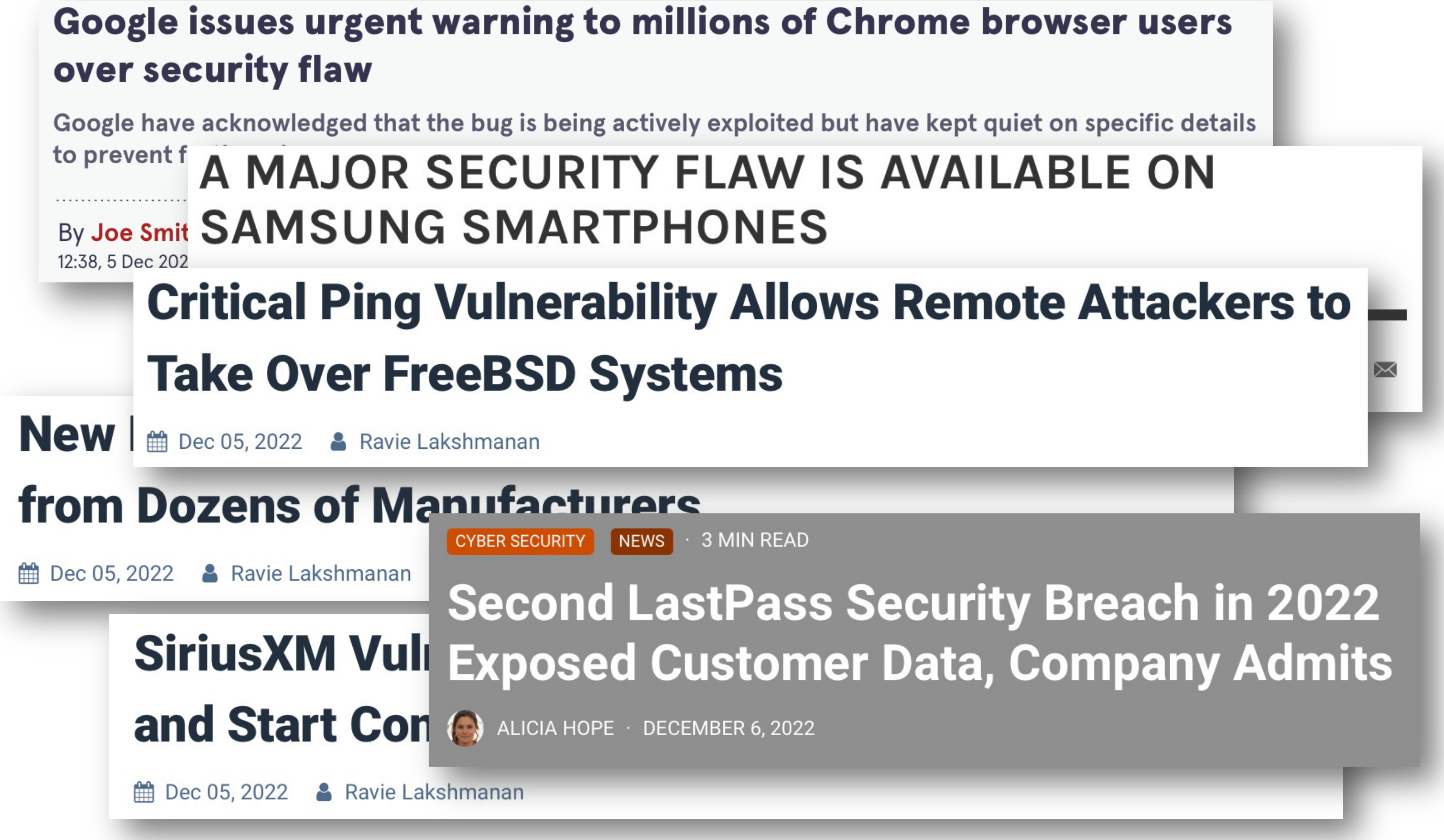
PDPA LGPD CDPA

SB260 POPIA CPRA

Privacy Threats



Today



Google issues urgent warning to millions of Chrome browser users over security flaw

Google have acknowledged that the bug is being actively exploited but have kept quiet on specific details to prevent f

By Joe Smit

12:38, 5 Dec 202

A MAJOR SECURITY FLAW IS AVAILABLE ON SAMSUNG SMARTPHONES

Critical Ping Vulnerability Allows Remote Attackers to Take Over FreeBSD Systems

Dec 05, 2022 Ravie Lakshmanan

New

from Dozens of Manufacturers

Dec 05, 2022 Ravie Lakshmanan

CYBER SECURITY NEWS · 3 MIN READ

Second LastPass Security Breach in 2022 Exposed Customer Data, Company Admits

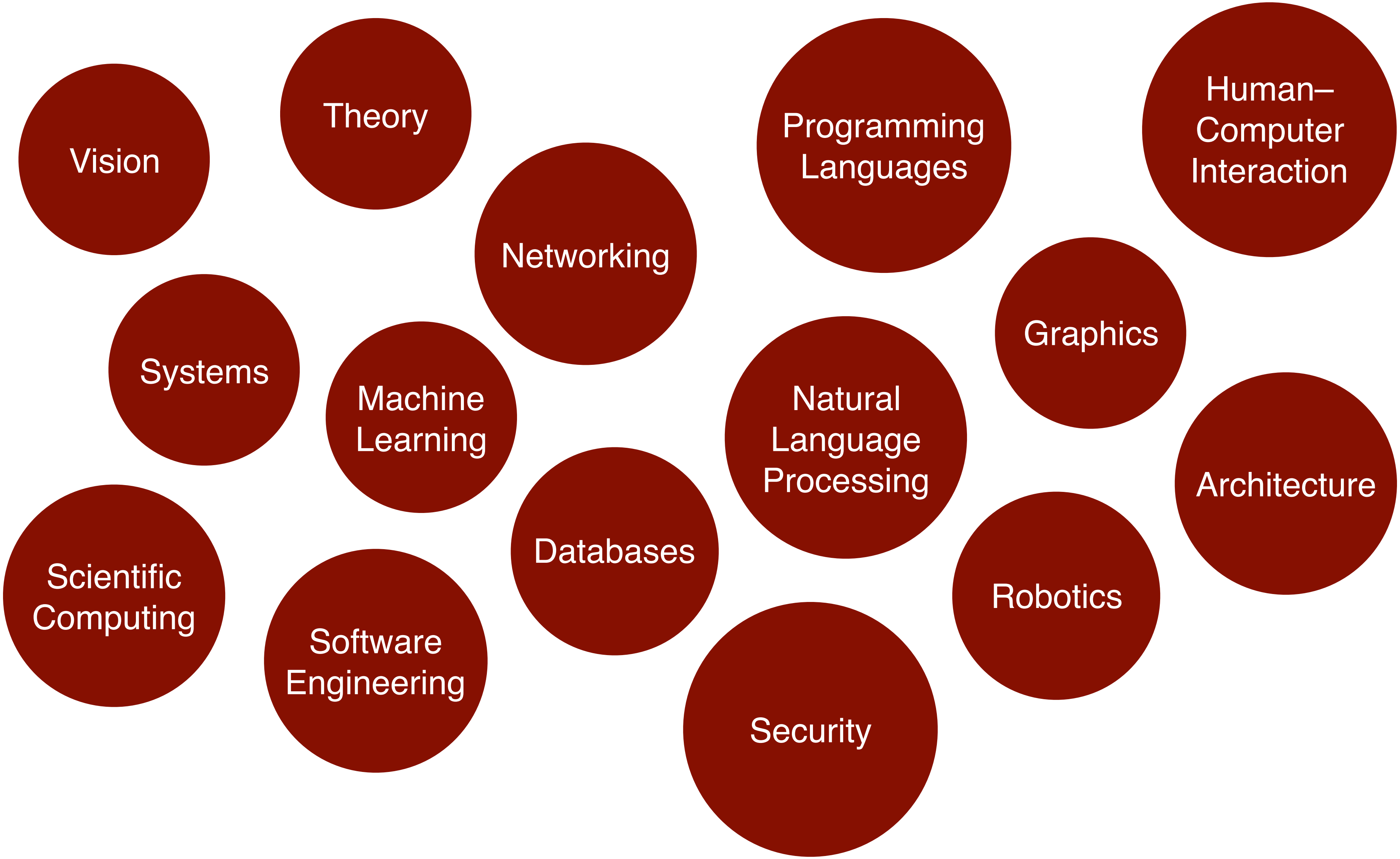
ALICIA HOPE · DECEMBER 6, 2022

SiriusXM Vul

and Start Con

Dec 05, 2022 Ravie Lakshmanan

Introduction to Computer Science



Vision

Theory

Networking

Programming Languages

Human–Computer Interaction

Systems

Machine Learning

Graphics

Natural Language Processing

Architecture

Scientific Computing

Software Engineering

Databases

Robotics

Security