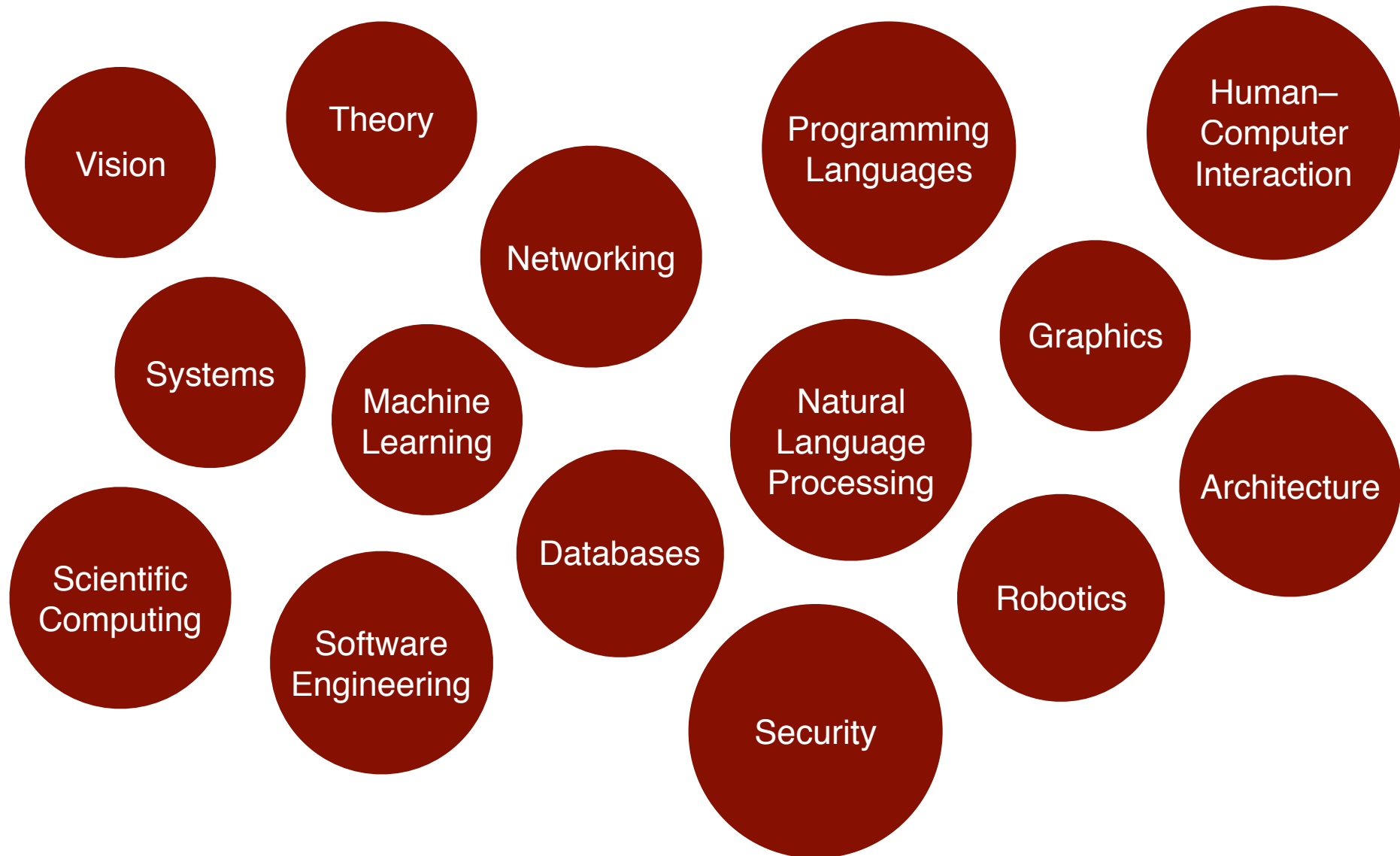


Lecture 24: Security and Privacy

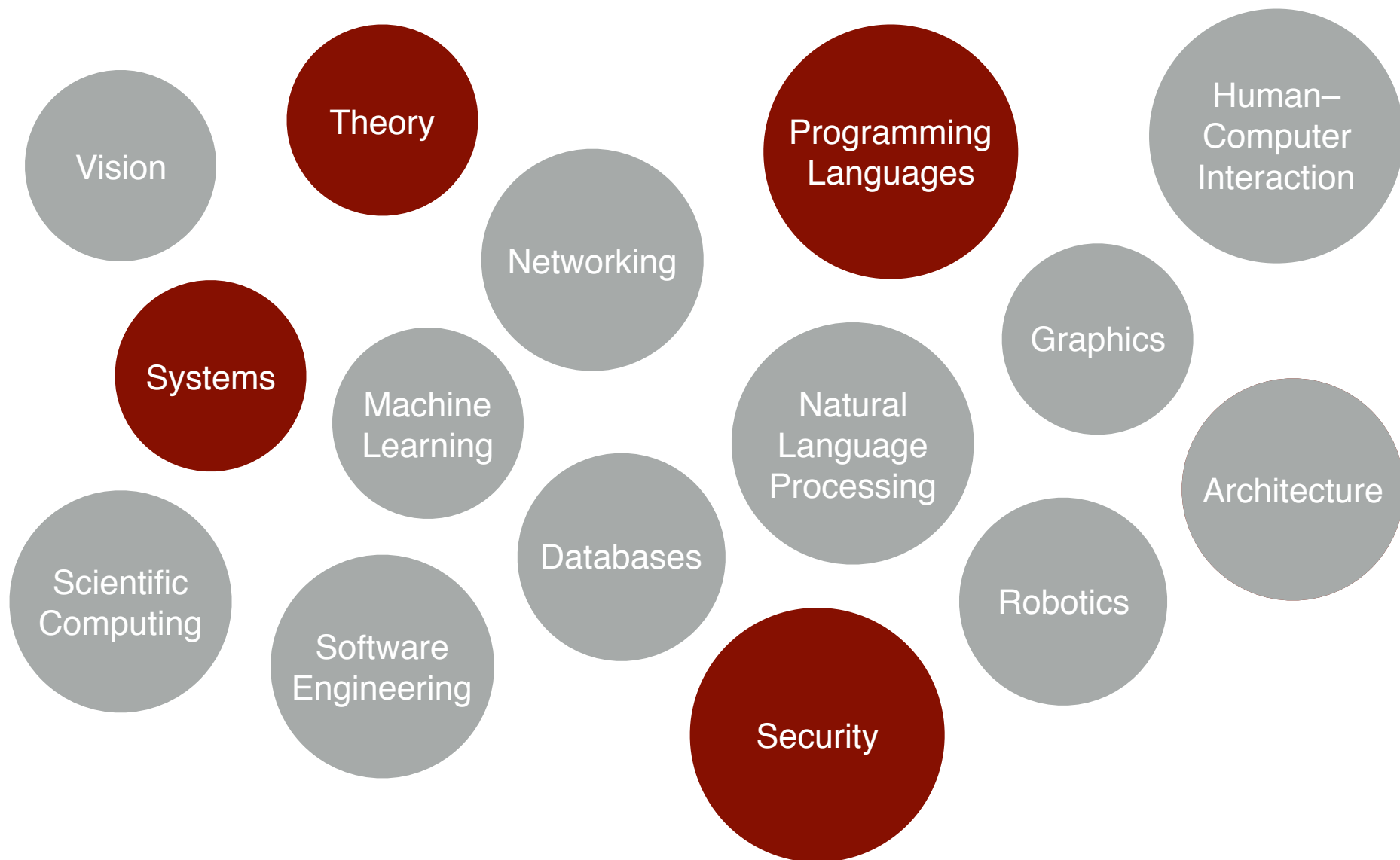
CS 51P

December 9, 2019

Computer Science



Computer 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(i):  
        return self.objects[i]
```

```
    def store(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.

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

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 Edmonds 114. See the [schedule](#) for details.

Labs

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

What might go wrong

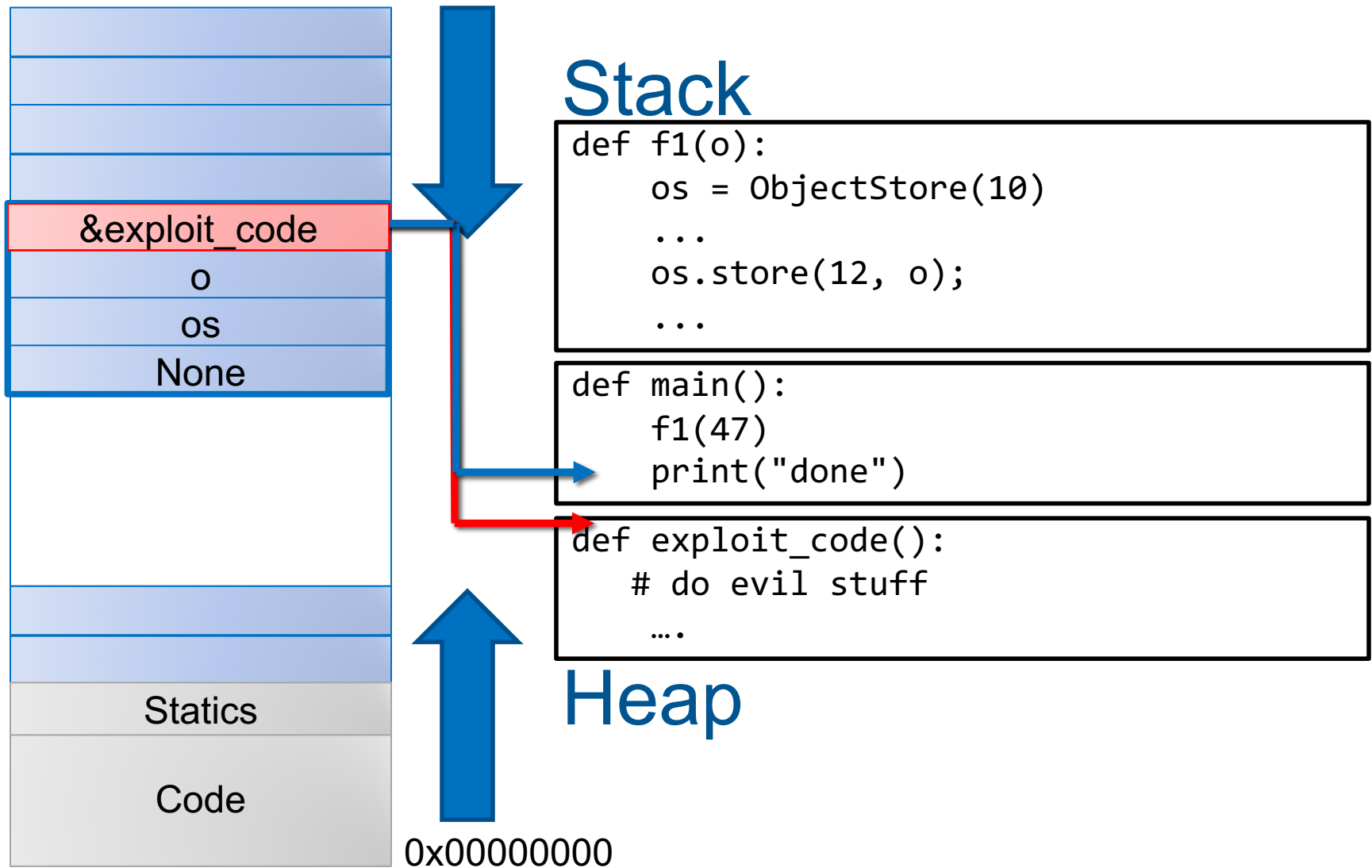
```
class ObjectStore:
```

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

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

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


Memory



WhatsApp Vulnerability



It's 2019 and a WhatsApp call can hack a phone: Zero-day exploit infects mobes with spyware

Rap for snoopware chaps in chat app voice yap
trap flap – now everyone patch

By [Iain Thomson](#) in [San Francisco](#) 14 May 2019 at 01:18 164 [SHARE](#) ▼

So how do we fix this?

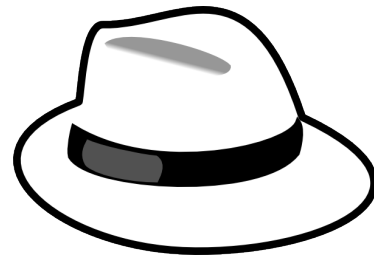


- Testing
- Bug finding tools

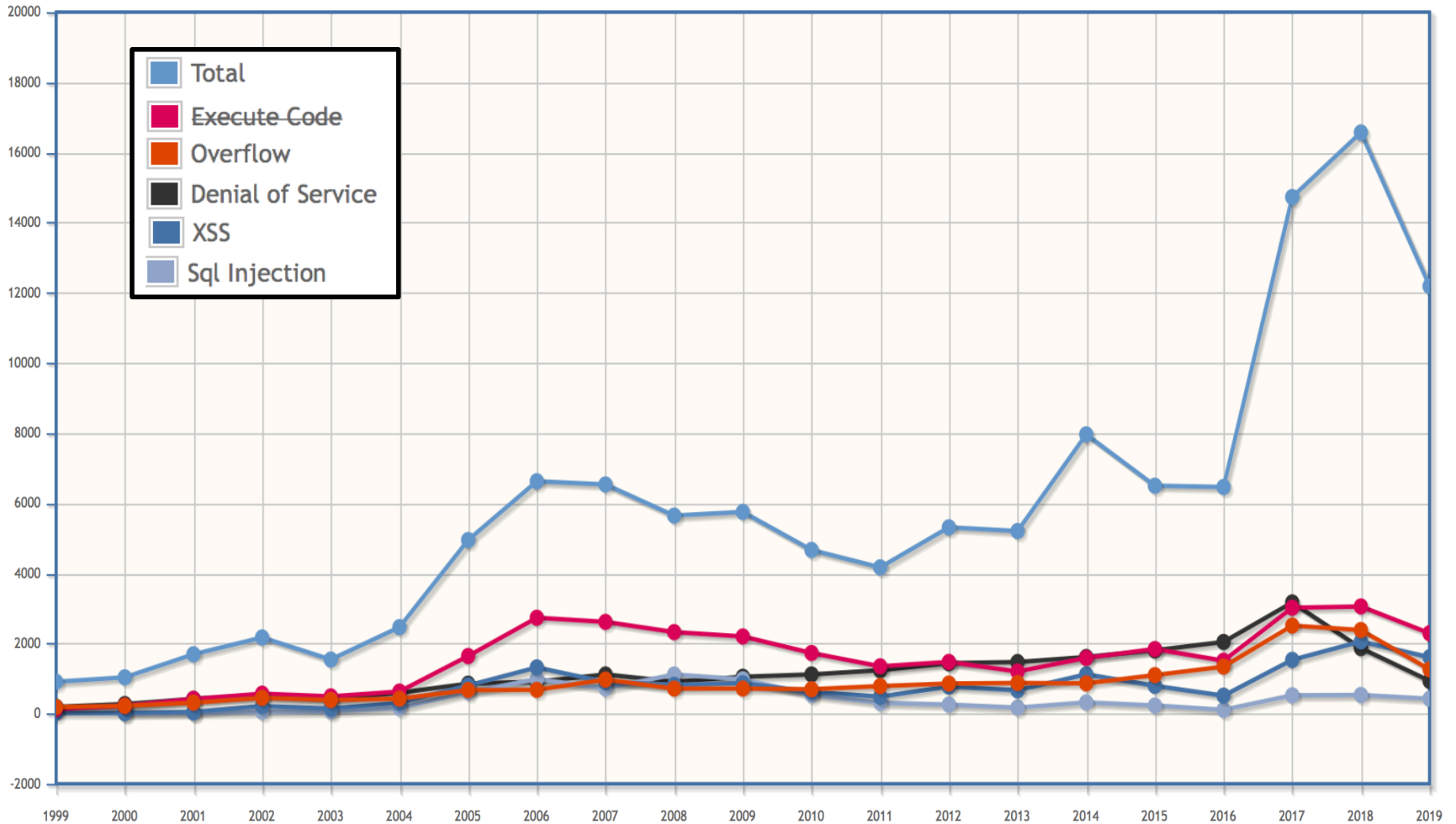


FindBugs

- Provably correct code
- White-hat hacking

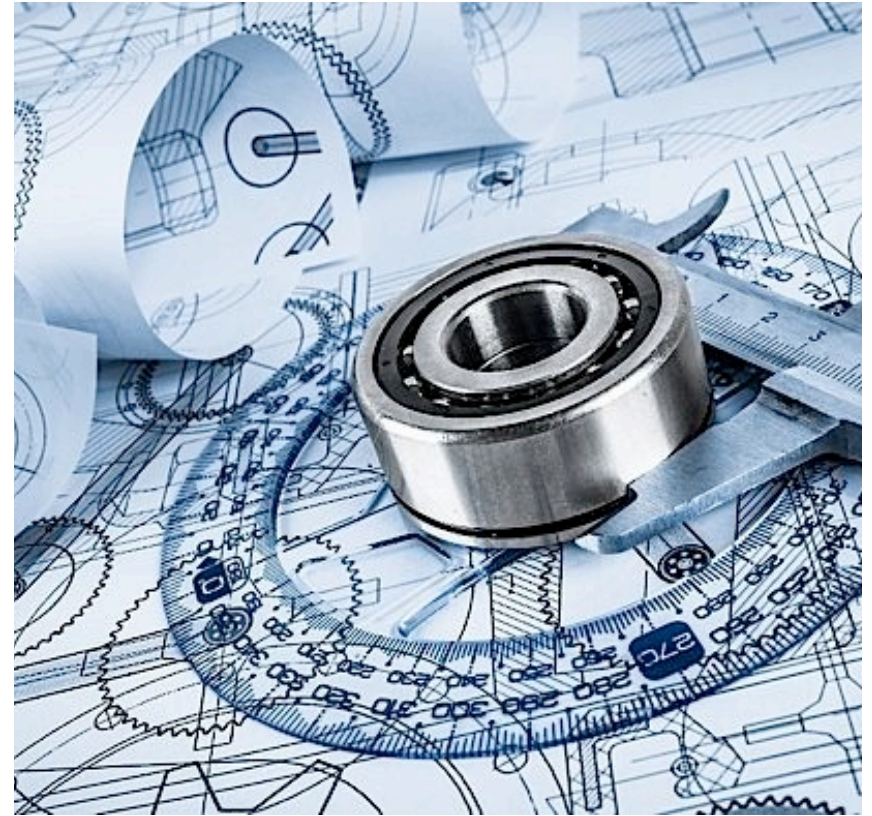


Vulnerabilities by Year





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

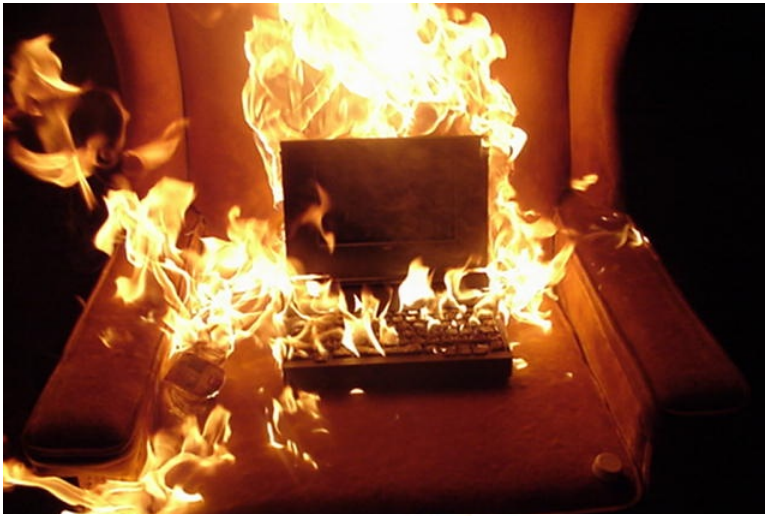
vulnerabilities

which are controlled by

countermeasures.

What are the threats?

Threat Models



Capabilities, Resources, Motivation

Threat Models

A CRYPTO NERD'S
IMAGINATION:

HIS LAPTOP'S ENCRYPTED.
LET'S BUILD A MILLION-DOLLAR
CLUSTER TO CRACK IT.

NO GOOD! IT'S
4096-BIT RSA!

BLAST! OUR
EVIL PLAN
IS FOILED!



WHAT WOULD
ACTUALLY HAPPEN:

HIS LAPTOP'S ENCRYPTED.
DRUG HIM AND HIT HIM WITH
THIS \$5 WRENCH UNTIL
HE TELLS US THE PASSWORD.

GOT IT.



Engineering Security

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

Security Goals

- "The system shall prevent/detect *action* on/to/with *asset*."
 - e.g., "The system shall prevent theft of money"
 - e.g., "The system shall prevent erasure of account balances"

Security goals should specify **what** not **how**

- Poor goals:
 - "the system shall use encryption to prevent reading of messages"
 - "the system shall use authentication to verify user identities"
 - "the system shall resist attacks"

CIA

Confidentiality
Integrity
Availability

Confidentiality Goals

Protection of assets from unauthorized disclosure
i.e., which principals are allowed to learn what

Examples:

- Keep contents of a file from being read (*access control*: more later)
- Keep information secret (*information flow*: more later)
 - value of variable secret
 - behavior of system
 - information about individual

Integrity Goals

Protection of assets from unauthorized modification
i.e., what changes are allowed to system and its
environment, including inputs and outputs

Examples:

- Output is correct according to (mathematical) specification
- No exceptions thrown
- Only certain principals may write to a file (access control)
- Data are not corrupted or tainted by downloaded programs (information flow)

Availability Goals

Protection of assets from loss of use
i.e., what has to happen when/where

Examples:

- Operating system must accept inputs periodically
- Program must produce output by specified time
- Requests must be processed fairly (order, priority, etc.)

Denial of service (DoS) attacks compromise availability

Aspects of security

- **Confidentiality:** protection of assets from unauthorized disclosure
- **Integrity:** protection of assets from unauthorized modification
- **Availability:** protection of assets from loss of use

Exercise

- **Attack:** John copies Mary's homework
- What is a **security goal** this attack would violate?
- Which **aspect** of security does that policy address?

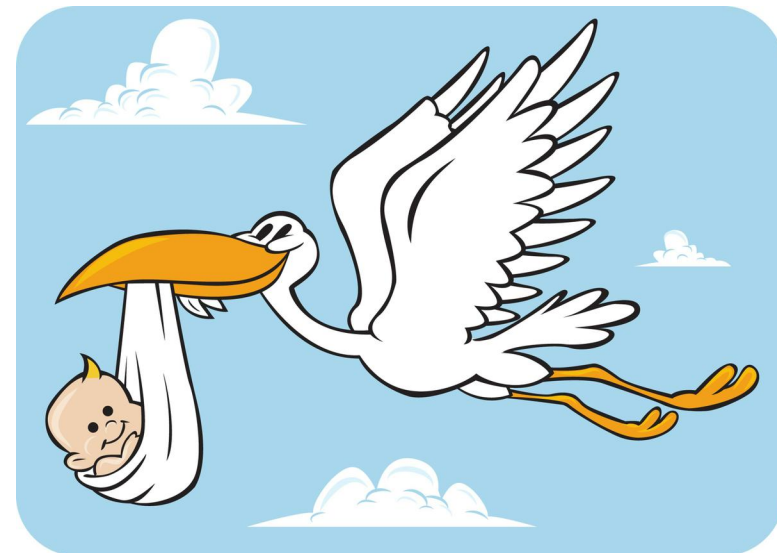
Exercise

- **Attack:** Paul causes Linda's system to freeze
- **Goal?**
- **Aspect?**

Exercise: Stork Baby Delivery




The *stork baby delivery system* allows an autonomous aircraft (a *stork*) to deliver a payload (a *baby*) to a geographic location prespecified by some higher authority (*providence*). Prior to take-off, providence programs a stork with the geographic location describing where the baby should be delivered. Throughout the mission, the stork transmits back to providence a video of the landscape (labeled with geographic location coordinates) that the stork flies over. While a stork is in flight, providence may issue commands to that stork and change the location for the delivery, alter the path being followed to that location, or abort the mission.

Threat model: The adversary desires to prevent baby deliveries. The adversary has access to radio equipment that transmits and receives on the same frequencies that providence uses for communication with a stork. The adversary also controls weapons systems that can destroy a stork in flight.



How do we design countermeasures

Classes of Countermeasures

- | | | |
|------------------------------------|---|---|
| 79 Au Gold 196.967 | Authentication: mechanisms that bind principals to actions |  |
| 79 Au Gold 196.967 | Authorization: mechanisms that govern whether actions are permitted |  |
| 79 Au Gold 196.967 | Audit: mechanisms that record and review actions |  |

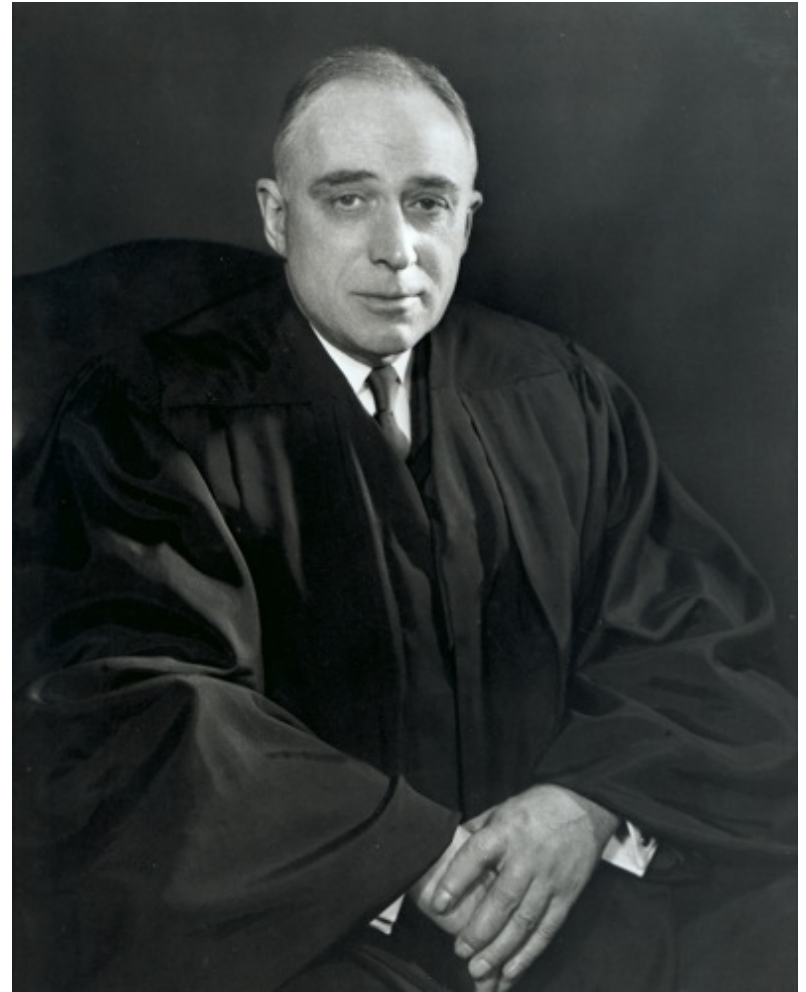
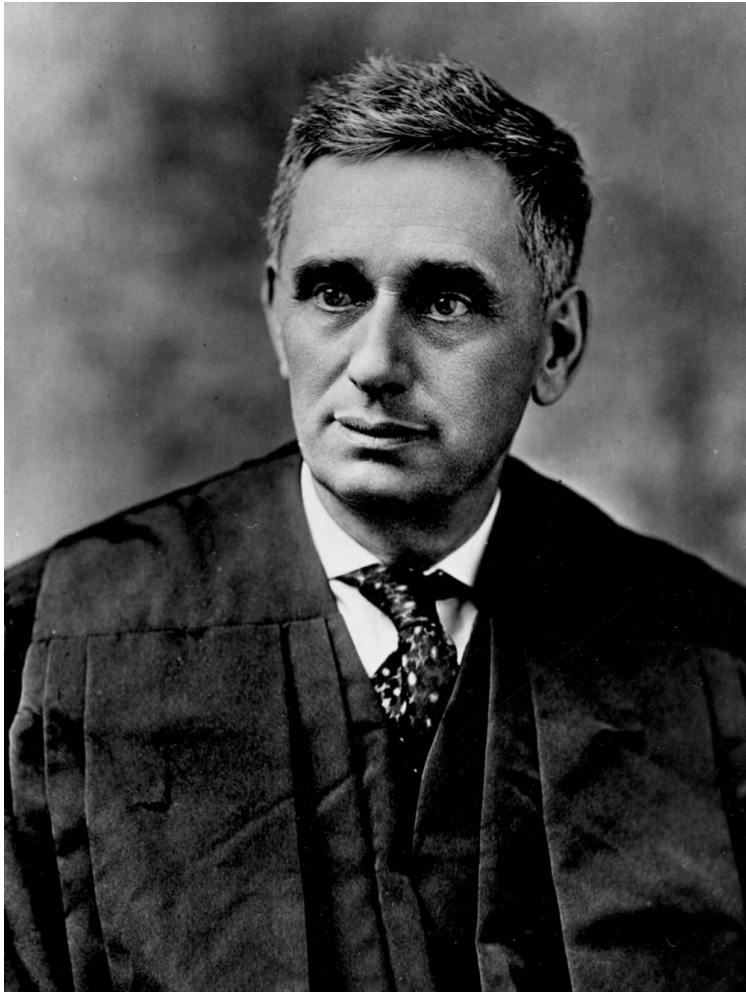
What is Privacy?



What is a privacy violation?

- Police read papers stored in your home
- Police read papers you threw in the trash
- Police read your medical records
- Your parents read your medical records
- Pomona uses your medical records in a research study
- Police read your texts/Facebook messages
- Police read your Facebook posts
- Police read your emails
- Google employee reads your emails
- Google uses your emails to target personalized ads
- Someone tracks your location for months (using phone)

Privacy in American Law



EDITOR'S PICK | 6,794 views | Dec 3, 2019, 08:59am

New Google Android Threat: Dangerous Security Flaw Puts Most Apps At Risk

Today

Incident Of The Week: Mixcloud Data Breach Puts 20 Million Users at Risk

Data Privacy Exposure Could Lead To Millions

Zoom Opens Video Device Security

A second Zoom operating system workaround, this time a security hack.

Tags: Incident Of Access Data Breach

By Brent Kelly
December 03, 2019



12/06/2019

Latest Android vulnerabilities can brick your phone, control the camera, steal your cash, and more

by Alan Friedman / Dec 08, 2019, 12:04 PM

Corvus Insurance Announces Alerts for BlueKeep Cybersecurity Vulnerability

PRWeb | FOLLOW+

December 09, 2019 1:20pm | Comments

Rancho Cucamonga-based w

New Linux Vulnerability Lets Attackers Hijack VPN Connections

EDITOR'S PICK | 194,427 views | Dec 7, 2019, 05:03am

By EIPUBL

By Sergiu Gatlan

Google Confirms Critical Android 8.0 And 10 'Permanent' Denial Of

Windows Hello for Business Affected by Serious Vulnerability; Microsoft Issues Advisory

by Silviu STAHIE on December 9, 2019