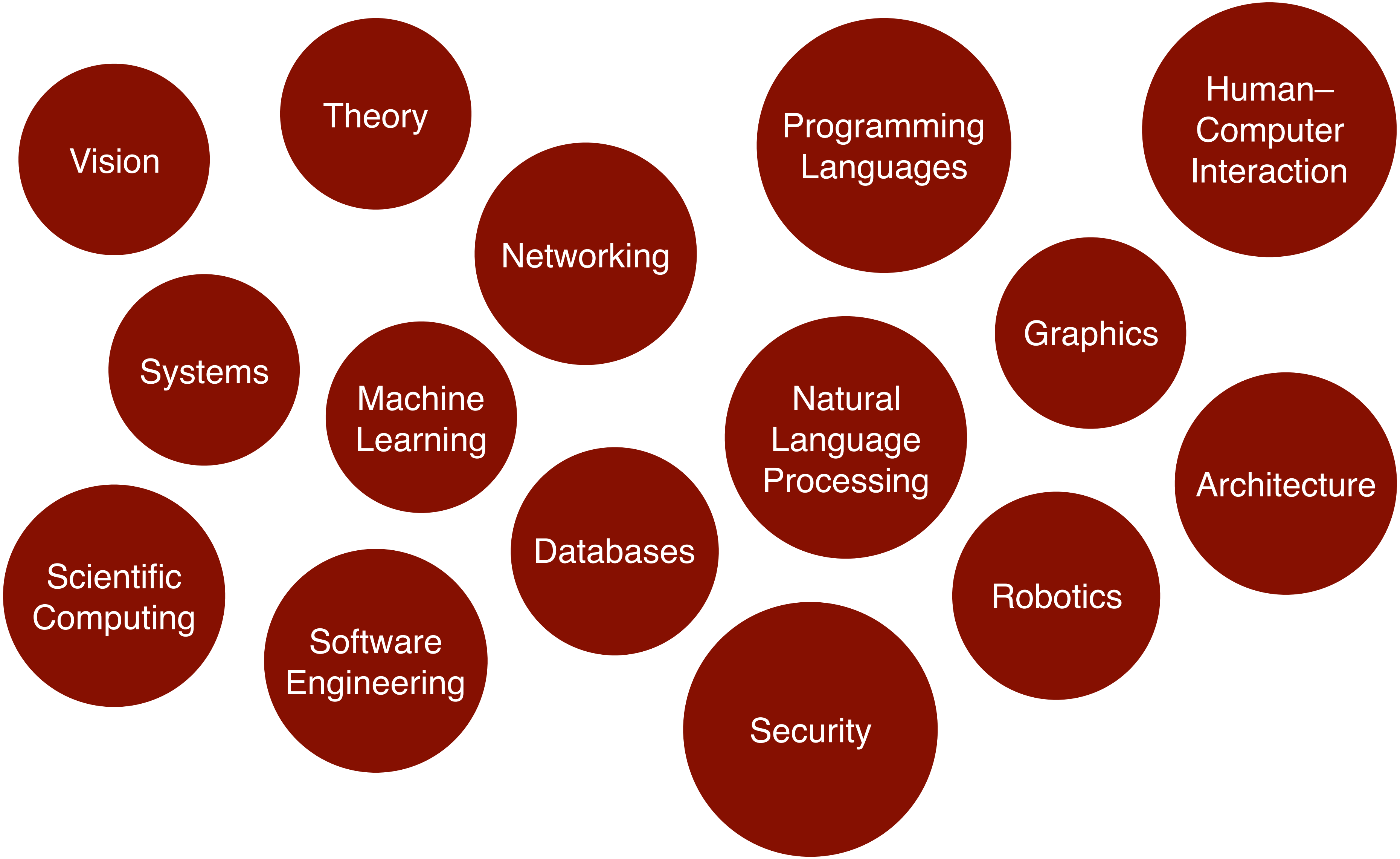
Computer Security

CS 2110

3 May, 2018

Computer Science



Vision

Theory

Networking

Programming Languages

Human–Computer Interaction

Systems

Machine Learning

Graphics

Natural Language Processing

Architecture

Scientific Computing

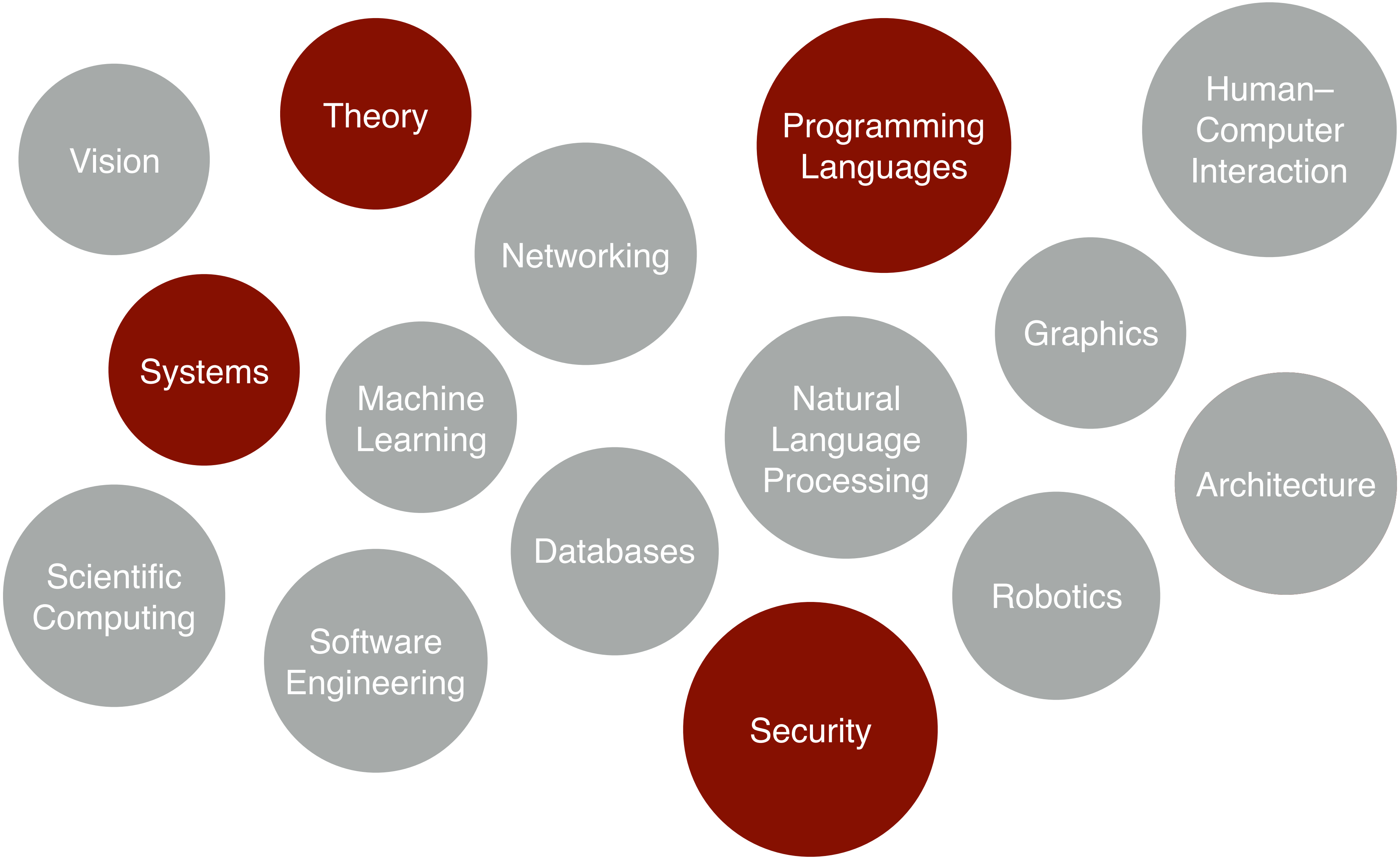
Software Engineering

Databases

Robotics

Security

Computer Security



Vision

Theory

Networking

Programming Languages

Human–Computer Interaction

Graphics

Systems

Machine Learning

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

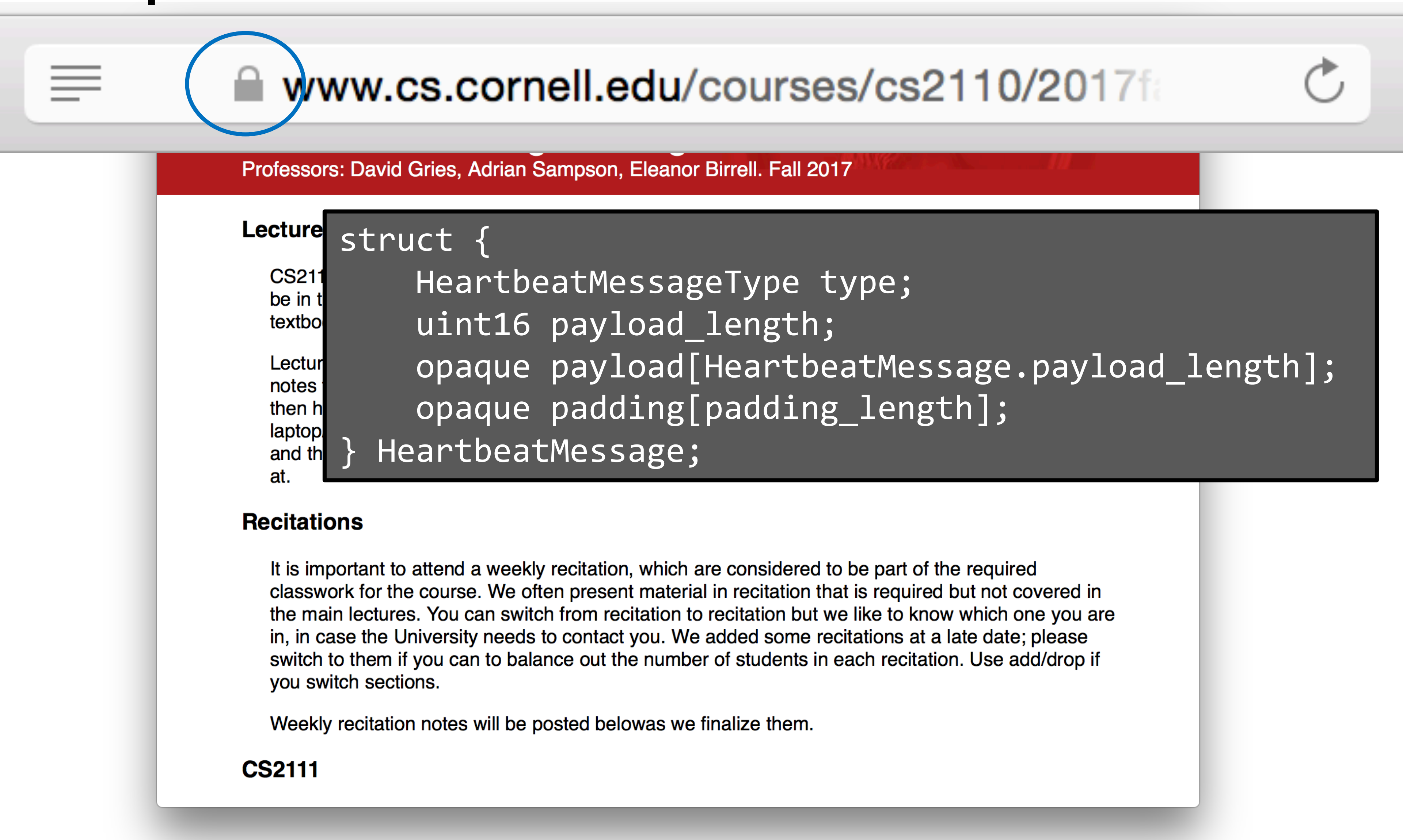
```
public class ObjectStore {
      private Object[] objects;

      public ObjectStore(int len){
            objects = new Object[len];
      }

      public Object read(int i){
            return objects[i];
      }

      public void store(int i, Object o){
            objects[i]= o;
      }
}
```

OpenSSL



www.cs.cornell.edu/courses/cs2110/2017f

Professors: David Gries, Adrian Sampson, Eleanor Birrell. Fall 2017

Lecture

CS211
be in t
textbo

Lectur
notes
then h
laptop
and th
at.

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

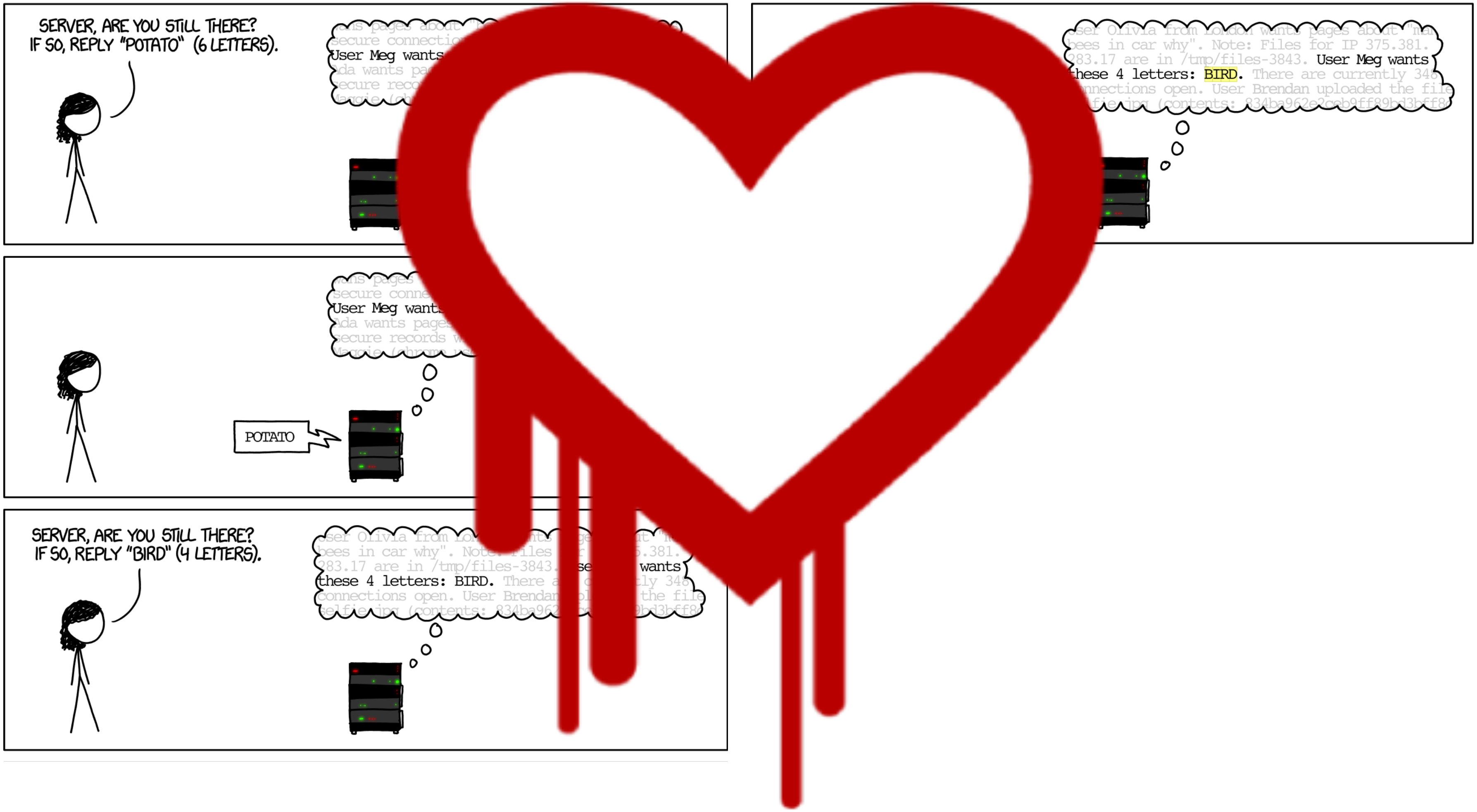
Recitations

It is important to attend a weekly recitation, which are considered to be part of the required classwork for the course. We often present material in recitation that is required but not covered in the main lectures. You can switch from recitation to recitation but we like to know which one you are in, in case the University needs to contact you. We added some recitations at a late date; please switch to them if you can to balance out the number of students in each recitation. Use add/drop if you switch sections.

Weekly recitation notes will be posted belowas we finalize them.

CS2111

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 "ma 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

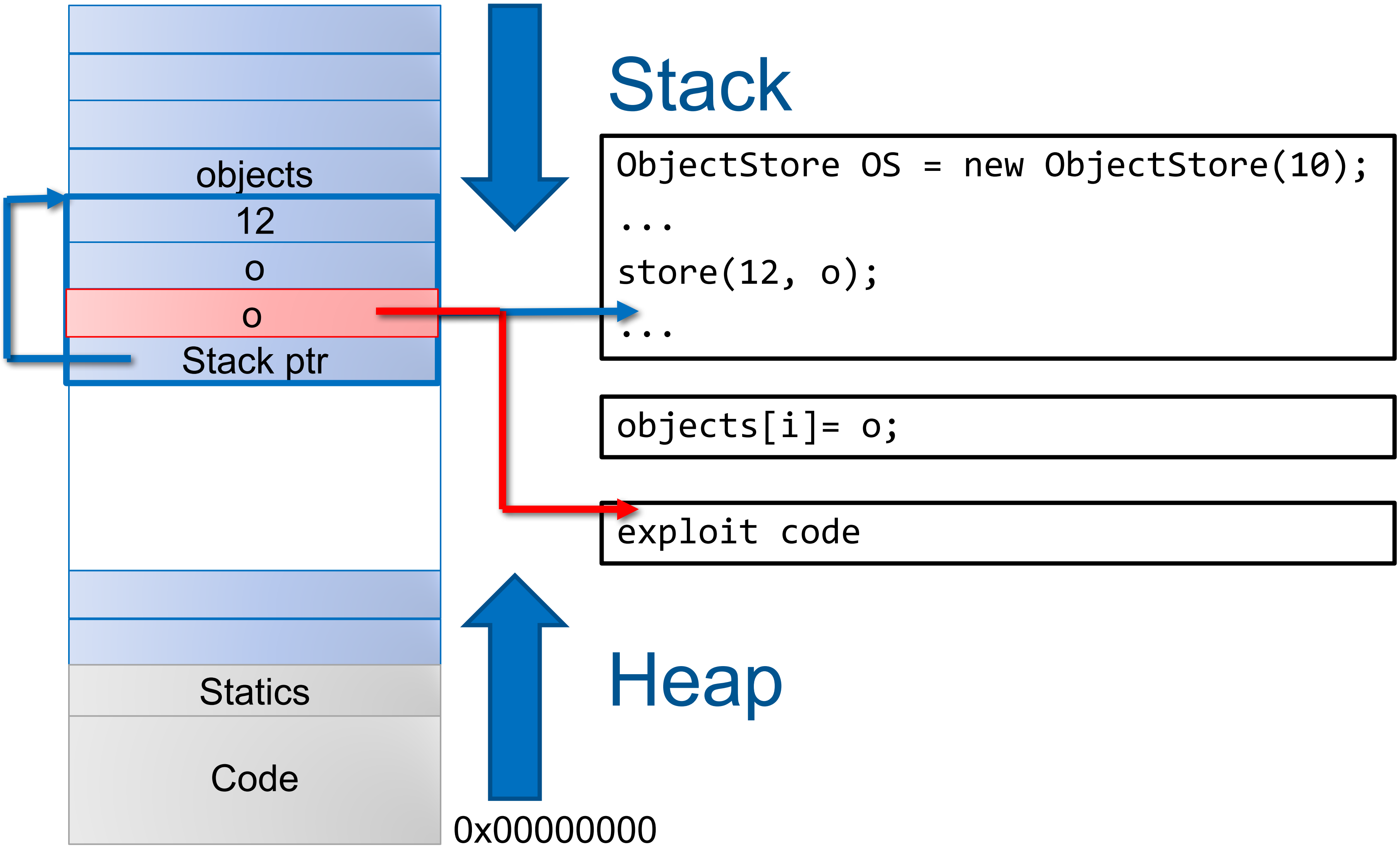
```
public class ObjectStore {
	private Object[] objects;

	public ObjectStore(int len){
		objects = new Object[len];
	}

	public Object read(int i){
		return objects[i];
	}

	public void store(int i, Object o){
		objects[i]= o;
	}
}
```

Memory

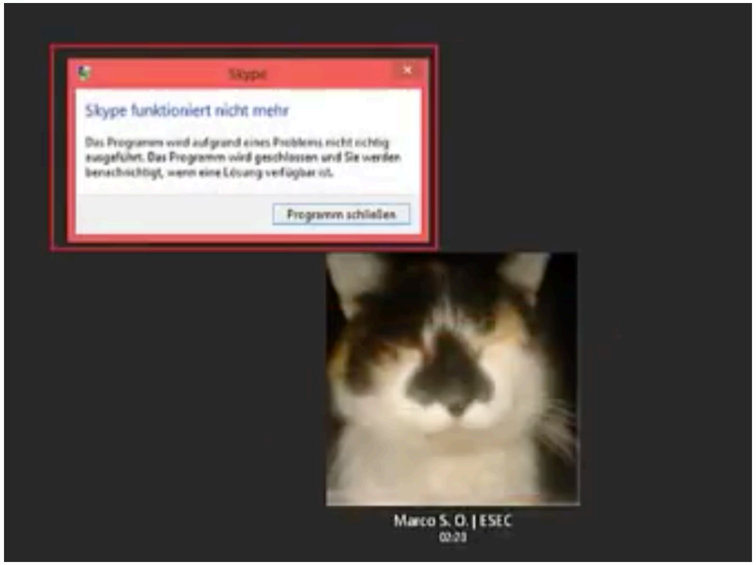


```
ObjectStore OS = new ObjectStore(10);
...
store(12, o);
...
```

```
objects[i]= o;
```

```
exploit code
```

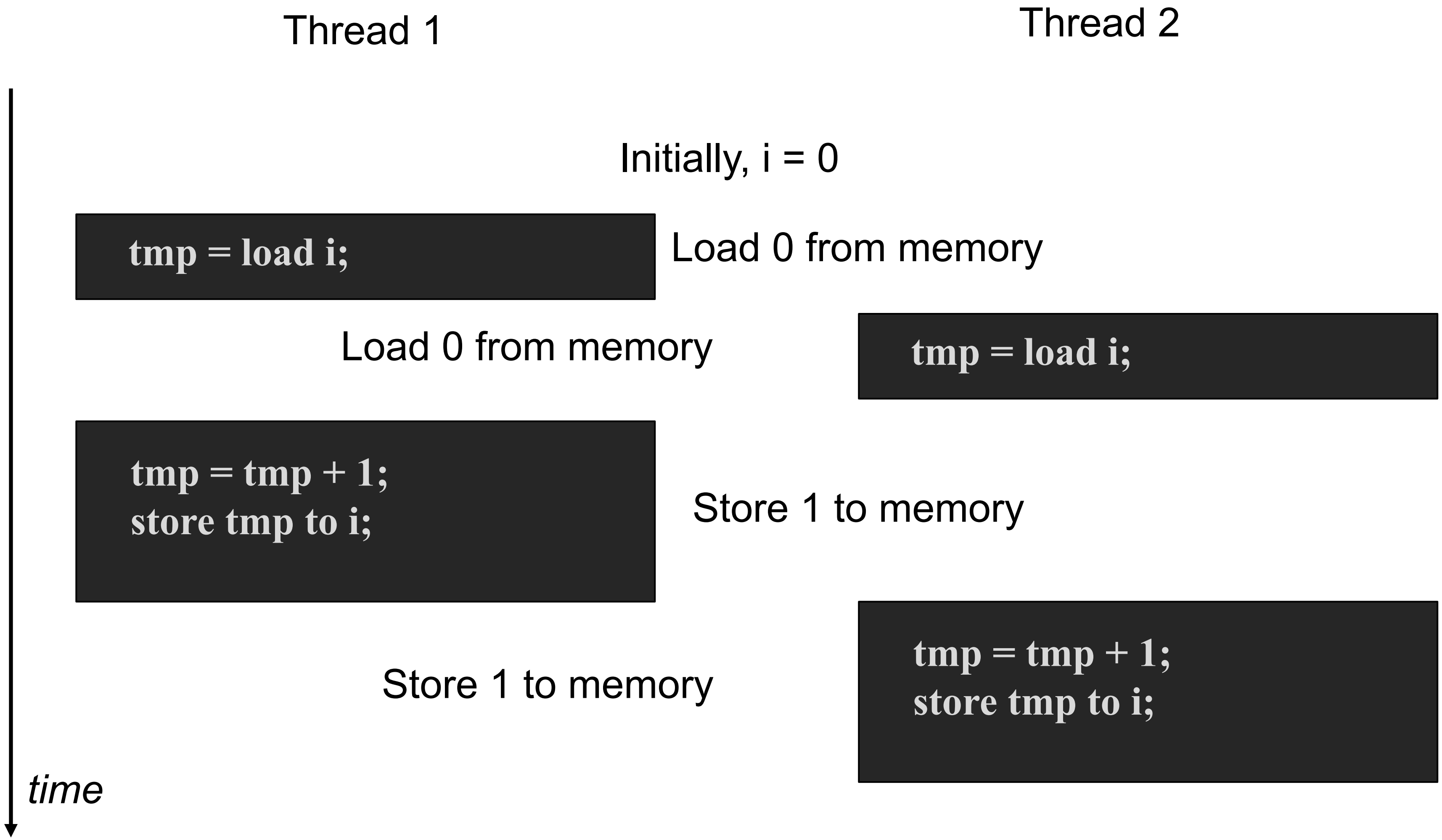
Skype Vulnerability



Skype funktioniert nicht mehr

Das Programm wird aufgrund eines Problems nicht richtig ausgeführt. Das Programm wird geschlossen und Sie werden benachrichtigt, wenn eine Lösung verfügbar ist.

What might go wrong



Thread 1

Thread 2

Initially, i = 0

```
tmp = load i;
```

Load 0 from memory

Load 0 from memory

```
tmp = load i;
```

```
tmp = tmp + 1;
store tmp to i;
```

Store 1 to memory

Store 1 to memory

```
tmp = tmp + 1;
store tmp to i;
```

Copy-on-write (COW)

- Common resource optimization
- When someone copies a file, it doesn't really get copied
- If/when someone modifies the "copy" the original file gets copied and modified

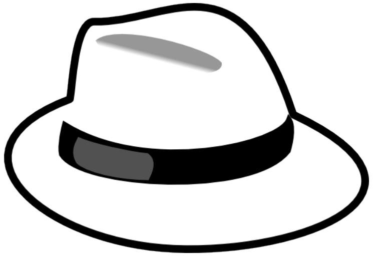
Privilege Escalation

So how do we fix this?

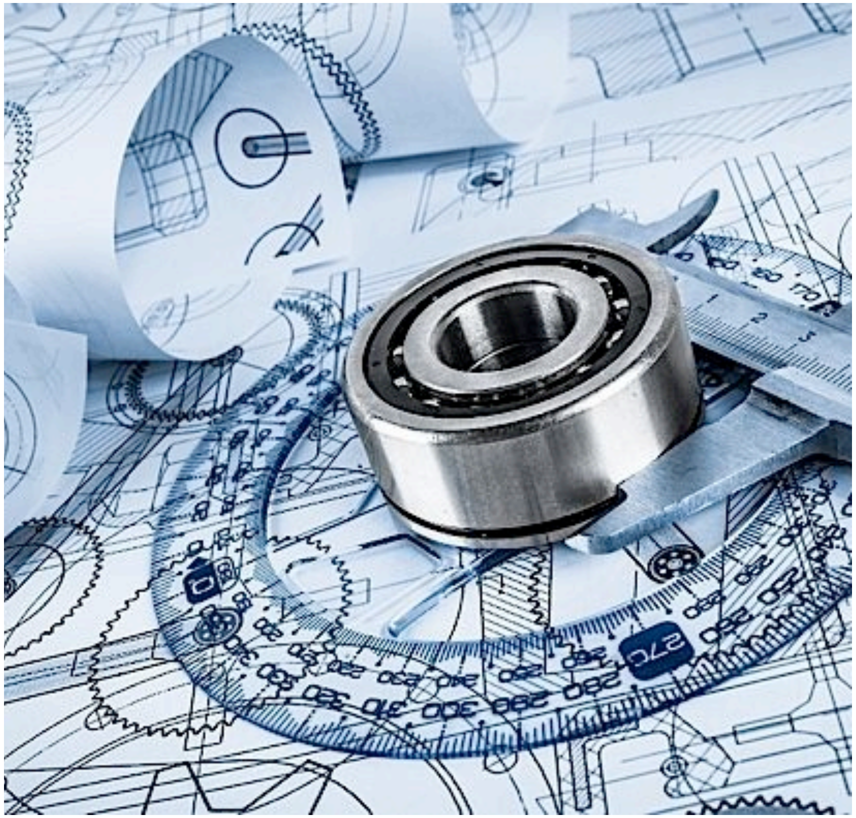
- Testing
- Bug finding tools

TM
FindBugs

- White-hat hacking



So how do we fix this?



Security by Design

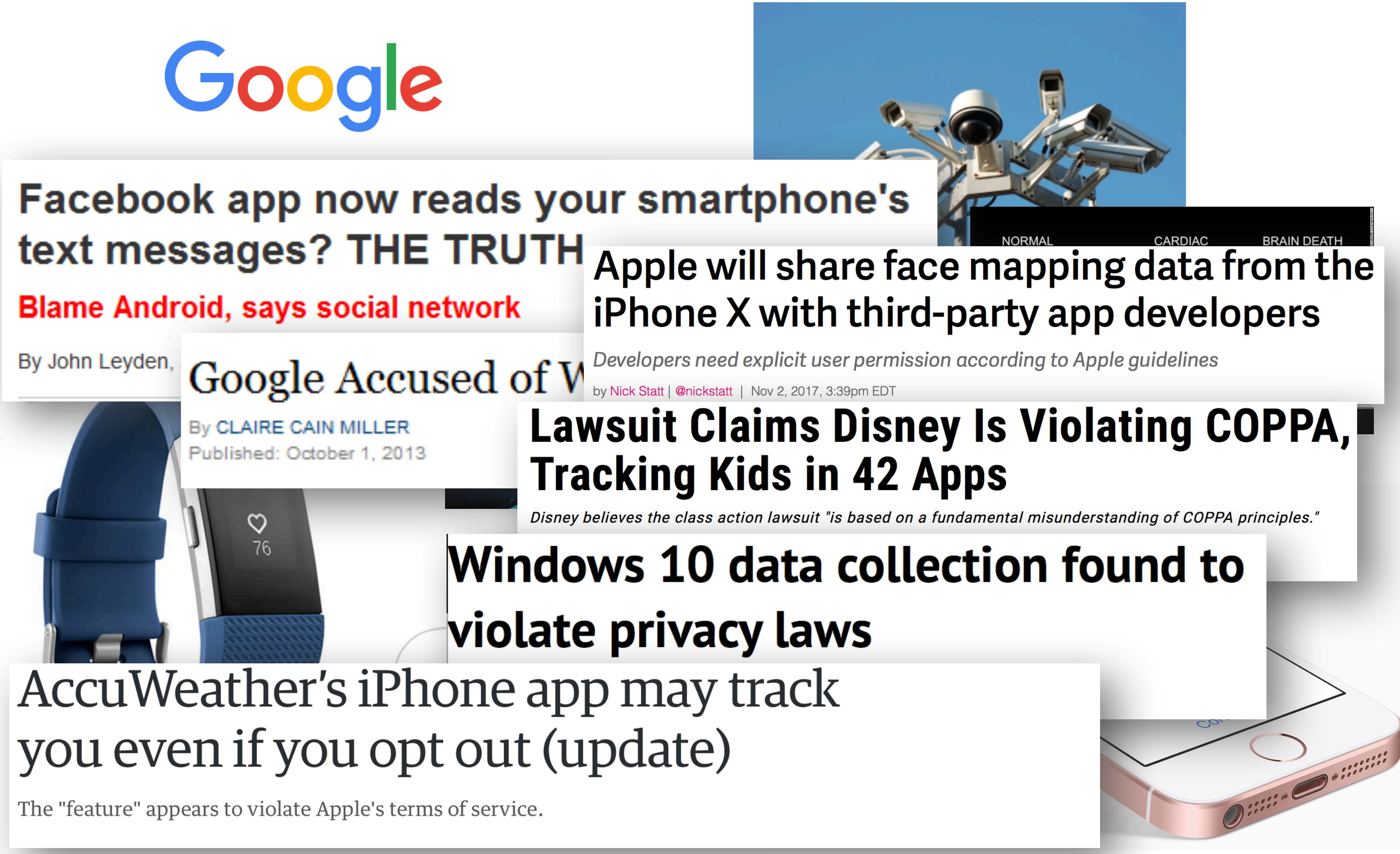
- Build secure, trustworthy computer systems/applications/etc.
- Define what the system is supposed to do
- Make sure it does that (and only that)

Engineering Security

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

How do we specify what systems are and are not supposed to do?

Example: Data Privacy



Facebook app now reads your smartphone's text messages? THE TRUTH

Blame Android, says social network

By John Leyden,

Google Accused of W

By CLAIRE CAIN MILLER
Published: October 1, 2013

Apple will share face mapping data from the iPhone X with third-party app developers

Developers need explicit user permission according to Apple guidelines

by Nick Statt | @nickstatt | Nov 2, 2017, 3:39pm EDT

Lawsuit Claims Disney Is Violating COPPA, Tracking Kids in 42 Apps

Disney believes the class action lawsuit "is based on a fundamental misunderstanding of COPPA principles."

Windows 10 data collection found to violate privacy laws

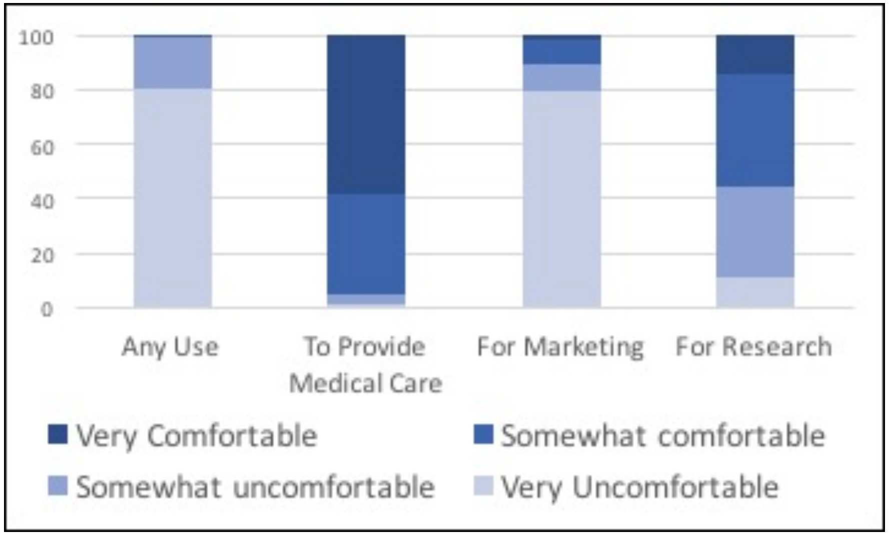
AccuWeather's iPhone app may track you even if you opt out (update)

The "feature" appears to violate Apple's terms of service.

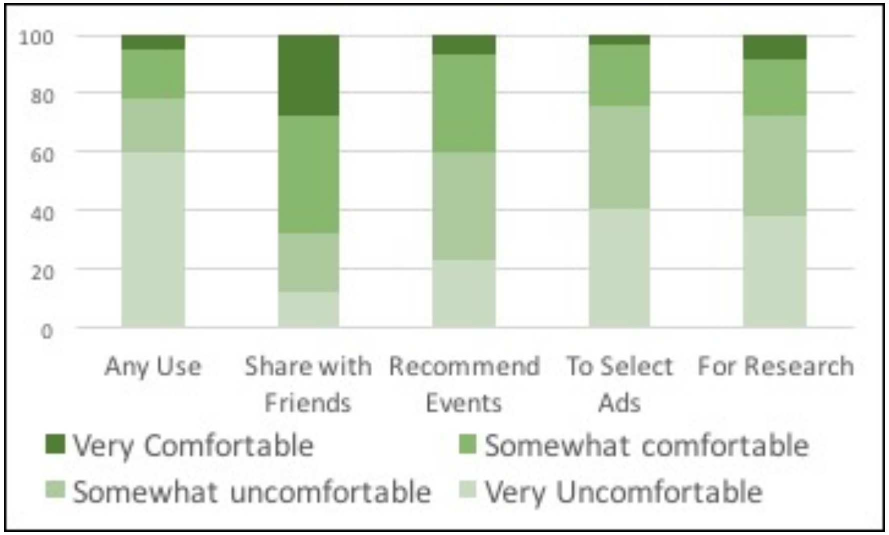
What is Privacy?

Use-Based Privacy

- Privacy viewed as **restrictions on uses** [Cate02]
- Captures modern privacy goals
  - express restrictions in presence of necessary sharing

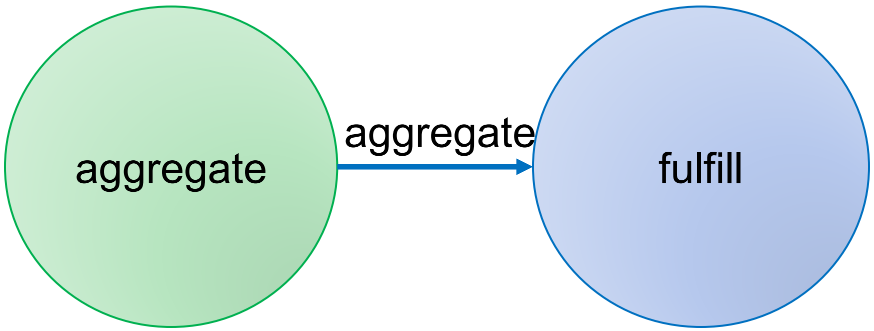


Medical Data



Social Network Data

Policy Language



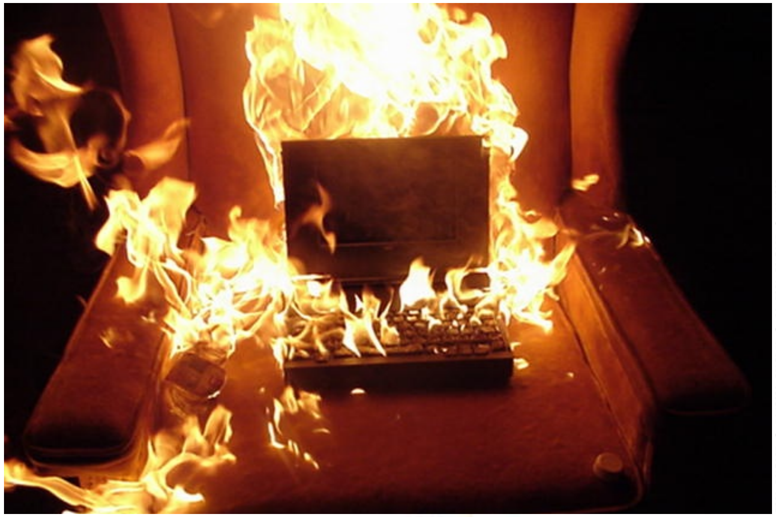
```
[{"curr":"1",
"states":{"1":{"name":"s1-1",
"permissions":{"aggregate":true},
"transitions":{"aggregate":"s2-1"},
"defaultPermission":false},
"2":{"name":"s2-1",
"permissions":{"fulfill":true},
"transitions":{},
"defaultPermission":true}}},
{"curr":"2",
"states":{"1":{"name":"s1-2",
"permissions":{"aggregate":true},
"transitions":{"aggregate":"s2-2"},
"defaultPermission":false},
"2":{"name":"s2-2",
"permissions":{"fulfill":true},
"transitions":{},
"defaultPermission":true}}}]
```

Engineering Security

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

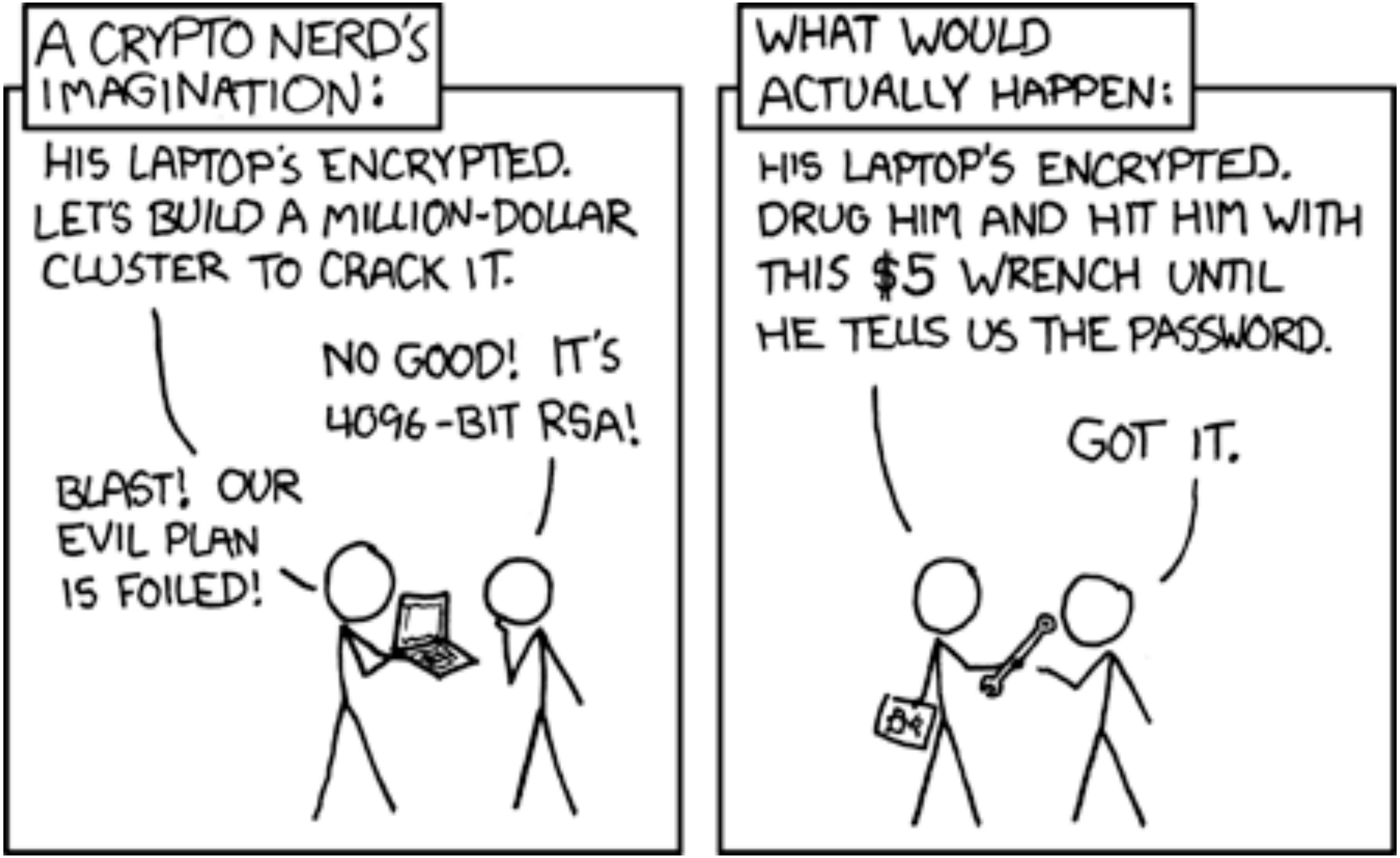
What are the threats?

Threat Models

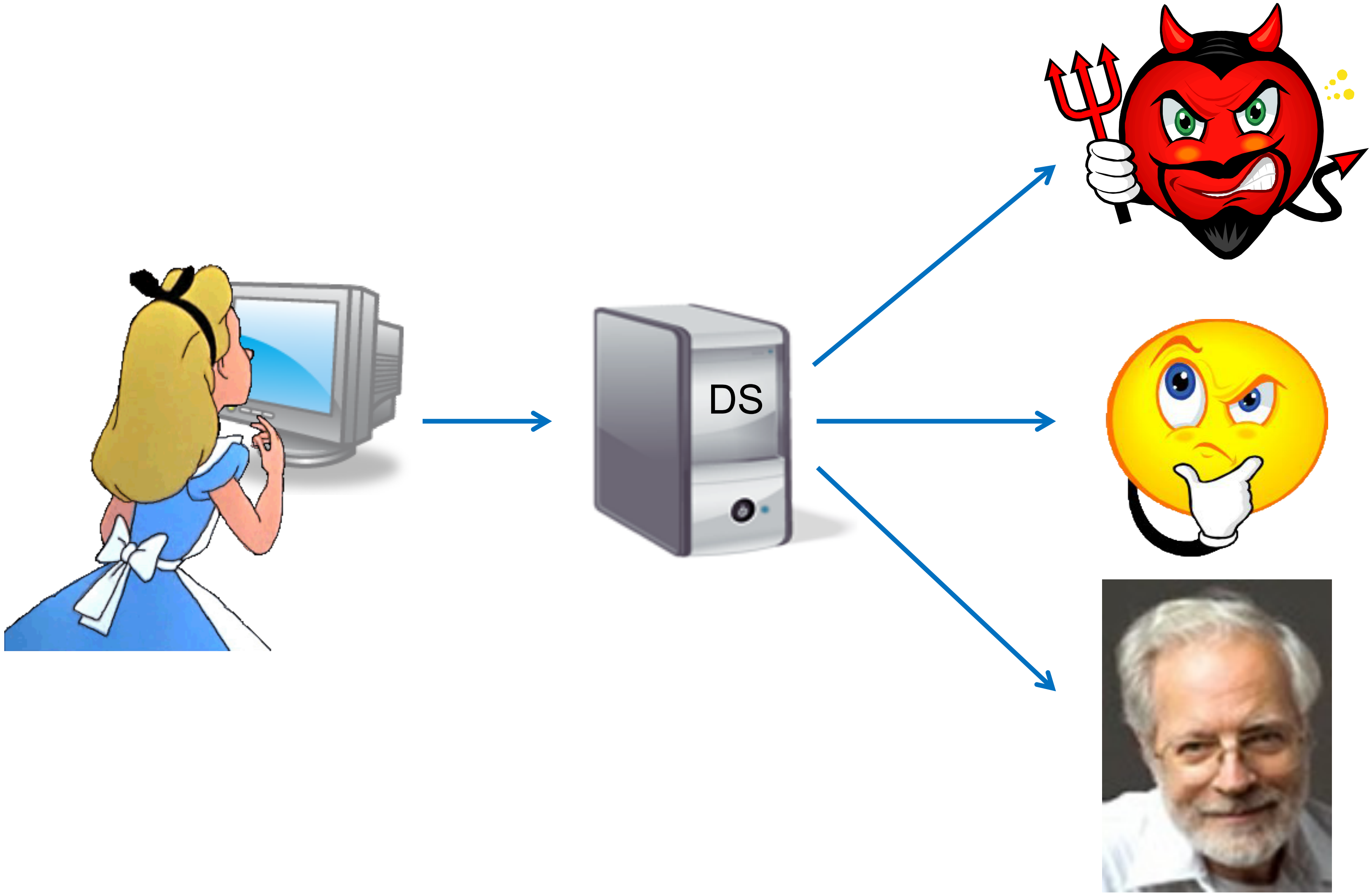


Capabilities, Resources, Motivation

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.

Example: Threat Model for Data Privacy



Engineering Security

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

How do we design countermeasures

Classes of Countermeaures

Authentication: mechanisms that bind principals to actions

Authorization: mechanisms that govern whether actions are permitted

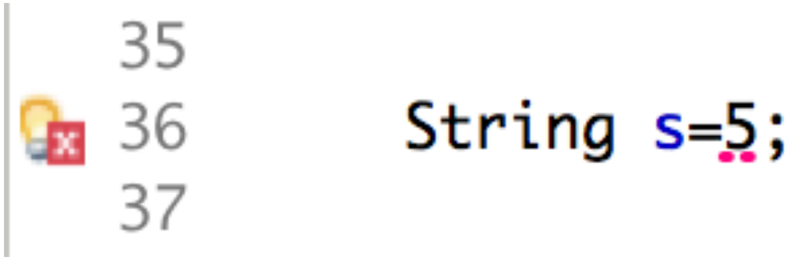
Audit: mechanisms that record and review actions

Approaches to security

- Axiomatic security
  - You trust someone else to get it right

Approaches to security

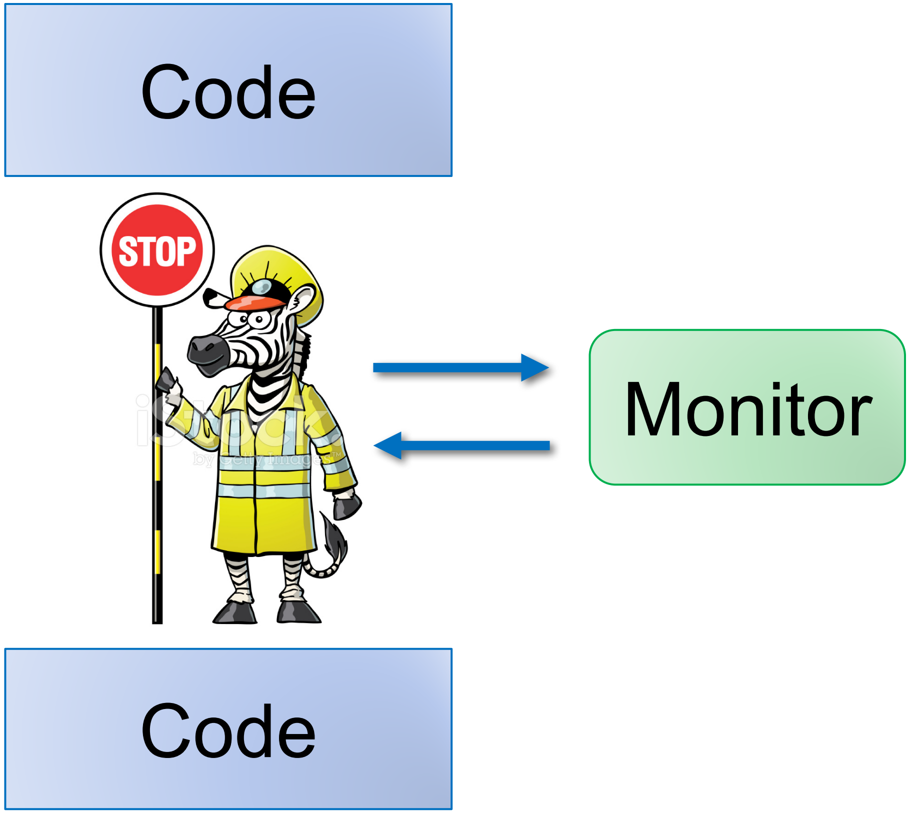
- Axiomatic security
  - You trust someone else to get it right
- Constructive security
  - E.g., compiler checks, automated proofs



```
String s=5;
```

Approaches to security

- Axiomatic security
  - You trust someone else to get it right
- Constructive security
  - E.g., compiler checks, automated proofs
- Synthetic security
  - Modify the code to add checks (e.g., monitoring)



Code

Monitor

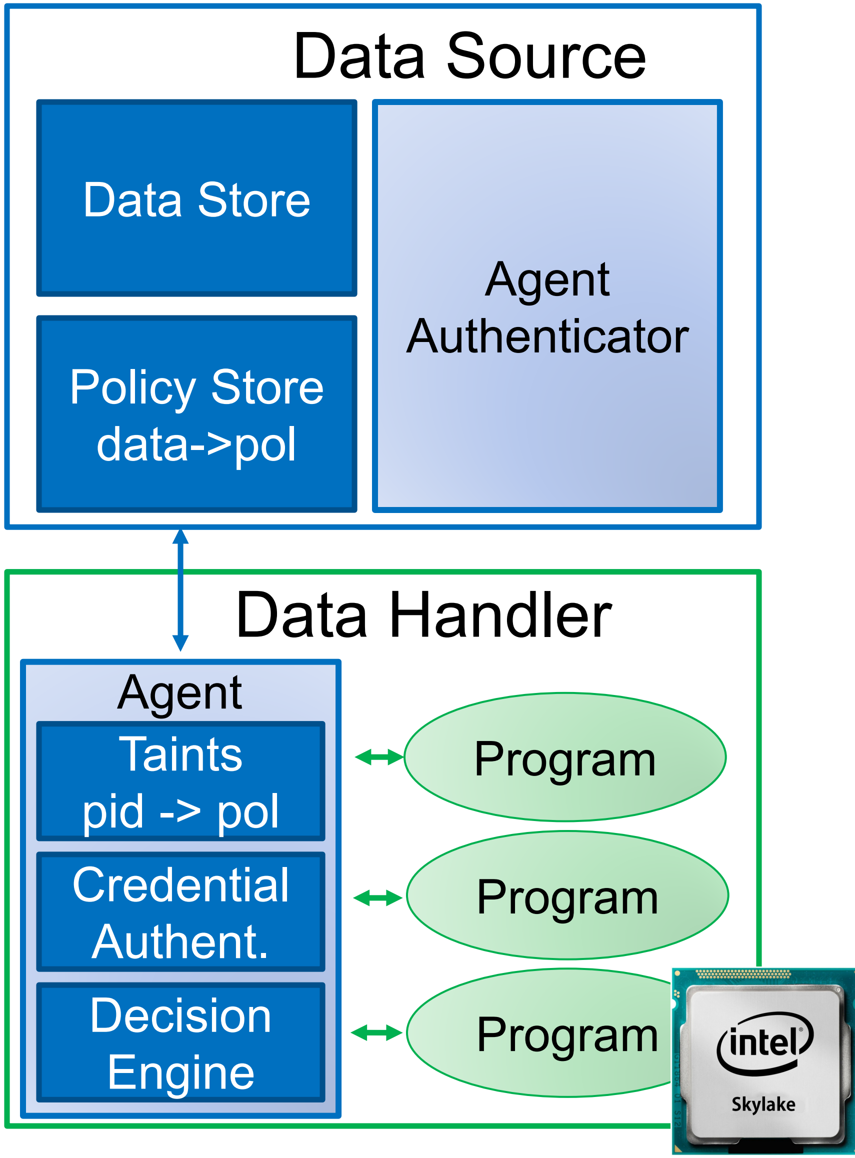
Code

Approaches to security

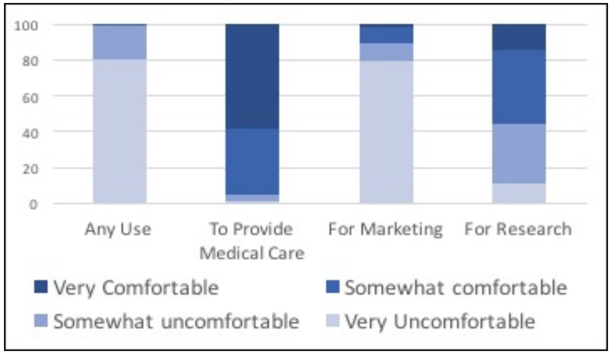
- Axiomatic security
  - You trust someone else to get it right
- Constructive security
  - E.g., compiler checks, automated proofs
- Synthetic security
  - Modify the code to add checks (e.g., monitoring)
- Deterrence through accountability
  - Make sure you'll notice if something goes wrong

Example: Data Privacy from SGX

- Policy enforcement implemented by external monitor that runs on DHs
  - monitor can send/receive values from DS
  - monitor shares values with authorized programs co-located at DH
    - auth decisions based on credentials
  - unauthorized values are cryptographically sealed with associated policy to prevent authorized use
  - monitor maintains taint for each program, automatically derives policies for derived values



Security



```
[{"curr":"1",
"states":{"1":{"name":"s1-1",
"permissions":{"aggregate":true},
"transitions":{"aggregate":"s2-1"},
"defaultPermission":false},
"2":{"name":"s2-1",
"permissions":{"fulfill":true},
"tr
"de                  n":true}}}]
```