Computer Security

CS 2110

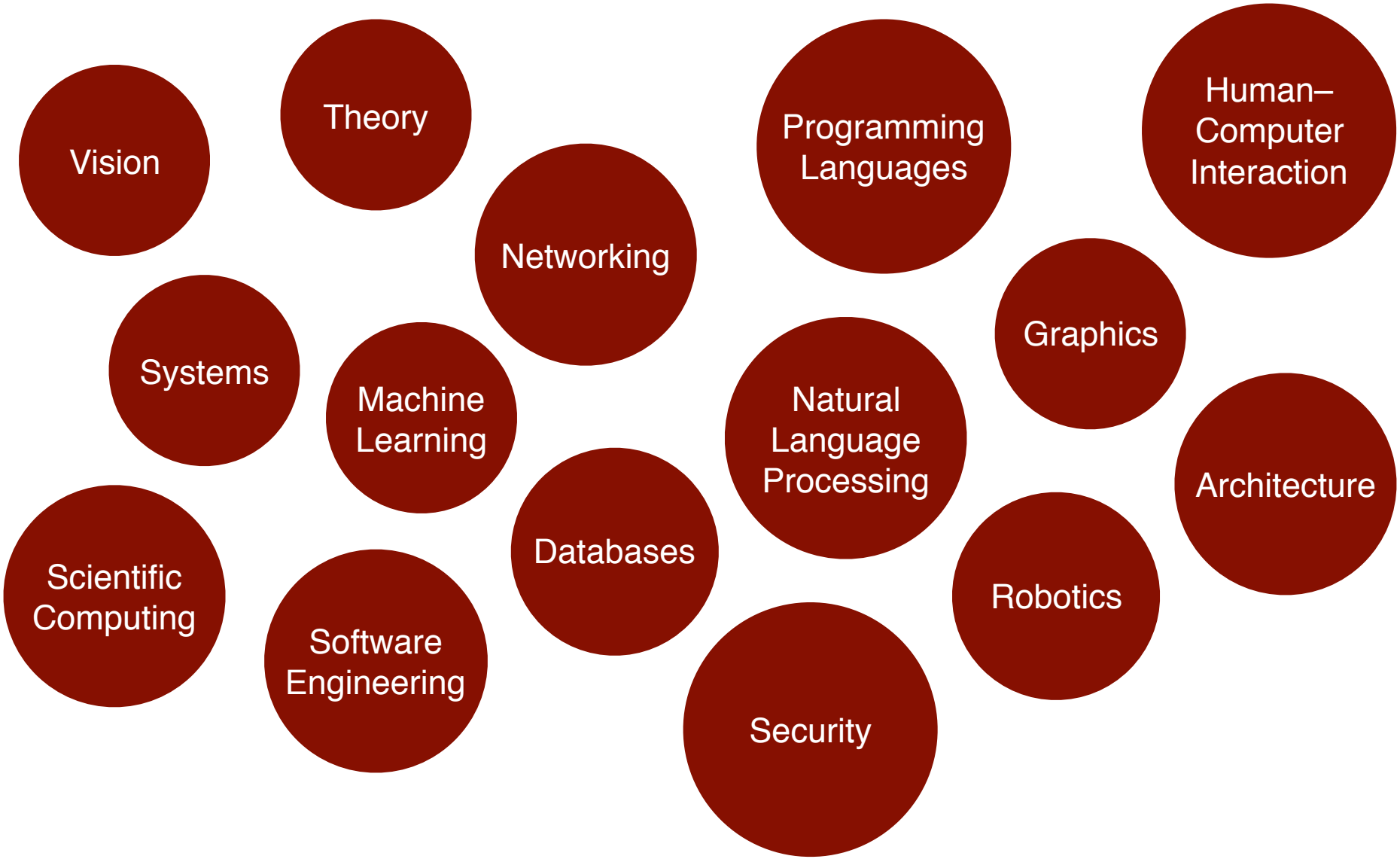
28 November, 2017

Announcements

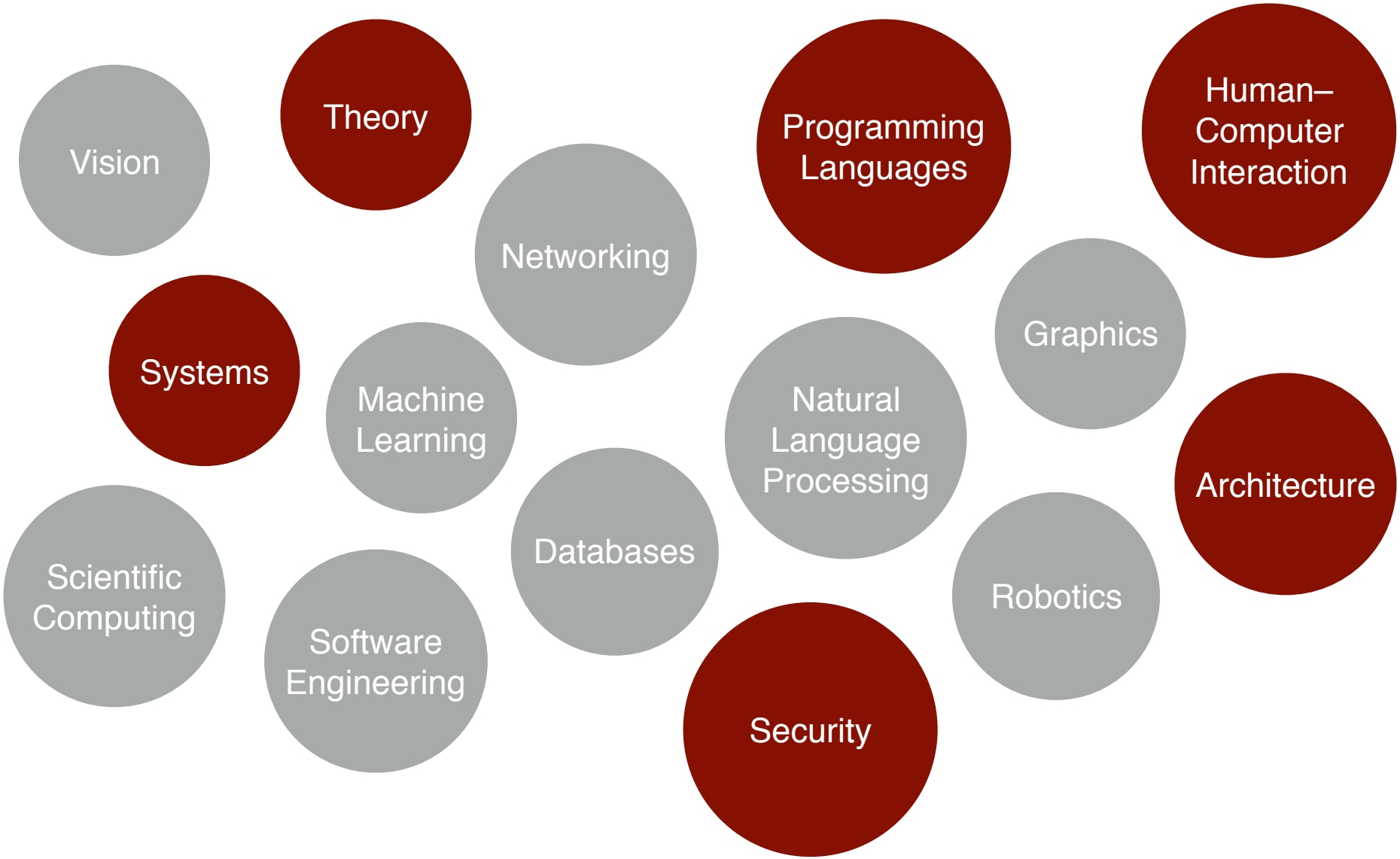
- Course evals are available. Fill them in by 3pm tomorrow to receive an extra 1% towards your final grade.
- Recitations this week will be on a variety of topics, you can attend whichever one you want:

Tu 12:20	Bard 140	Regular Expressions	We 12:20	Bard 140	Debugging
Tu 12:20	Hollister 368	Kooky Data Structures	We 12:20	Olin 218	Dynamic Program.
Tu 12:20	Olin 216	Sound	We 1:25	Bard 140	Version Control
Tu 12:20	Upson 216	Coding Interviews	We 1:25	Upson 216	Optionals
Tu 1:25	Hollister 206	Java 9	We 2:30	Bard 140	TBA
Tu 1:25	Hollister 312	Dynamic Programming	We 2:30	Phillips 407	Coding Interviews
Tu 2:30	Hollister 110	TBA	We 7:30	Upson 142	Coding Interviews
Tu 2:30	Olin 165	Collections			
Tu 3:35	Bard 140	Distributed Computing			

Computer Science



Computer Security



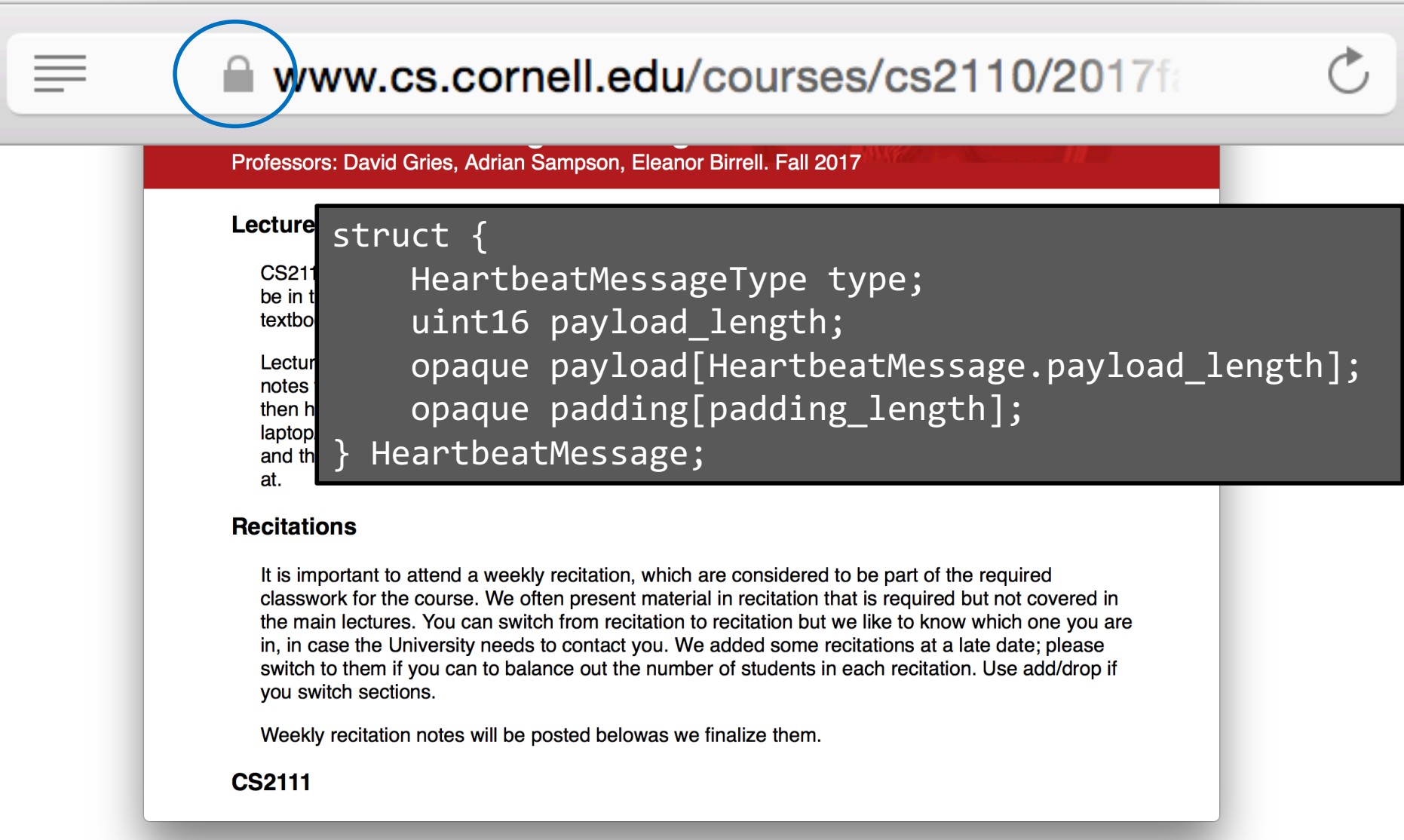
Computer Security

- 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

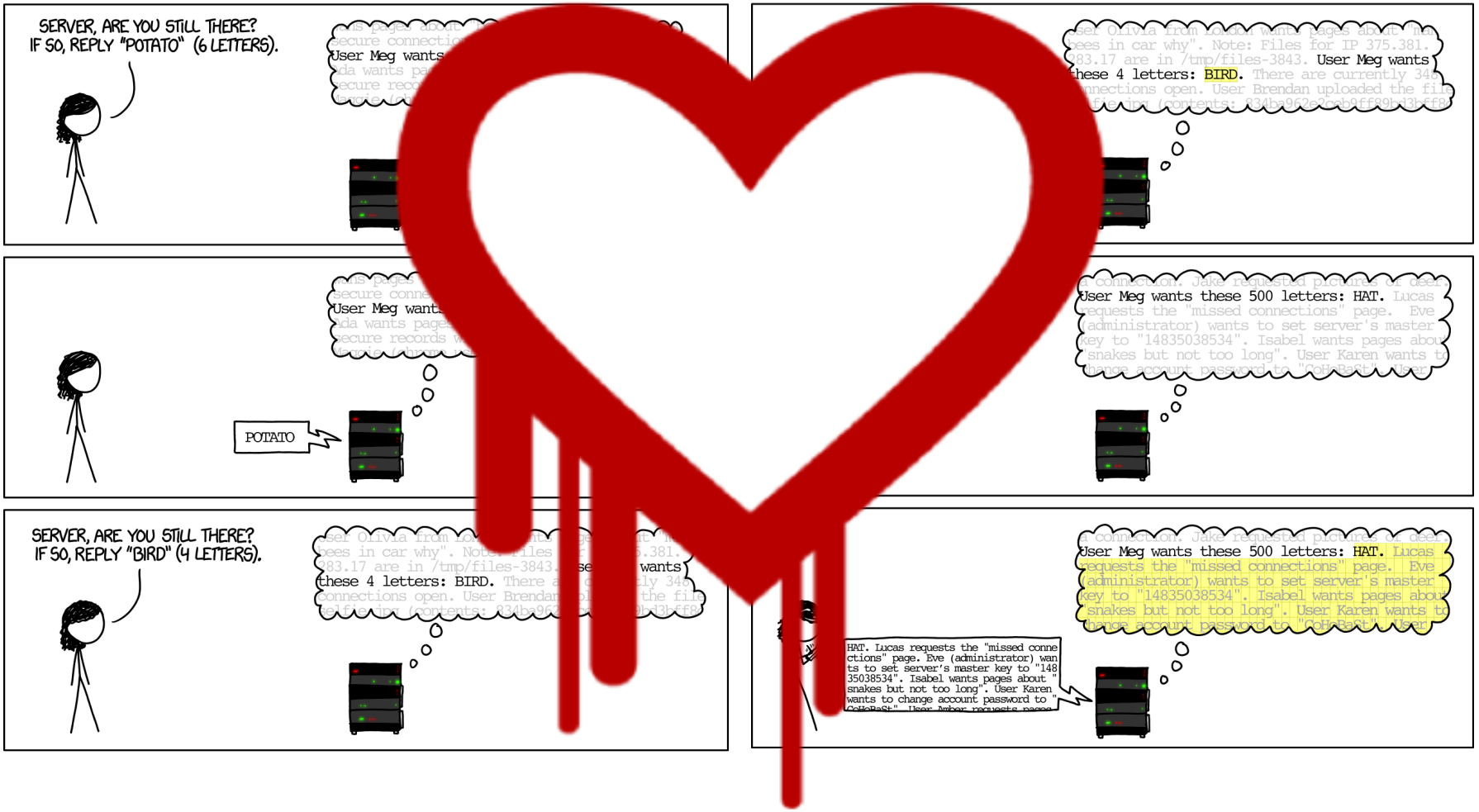
What might go wrong

```
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

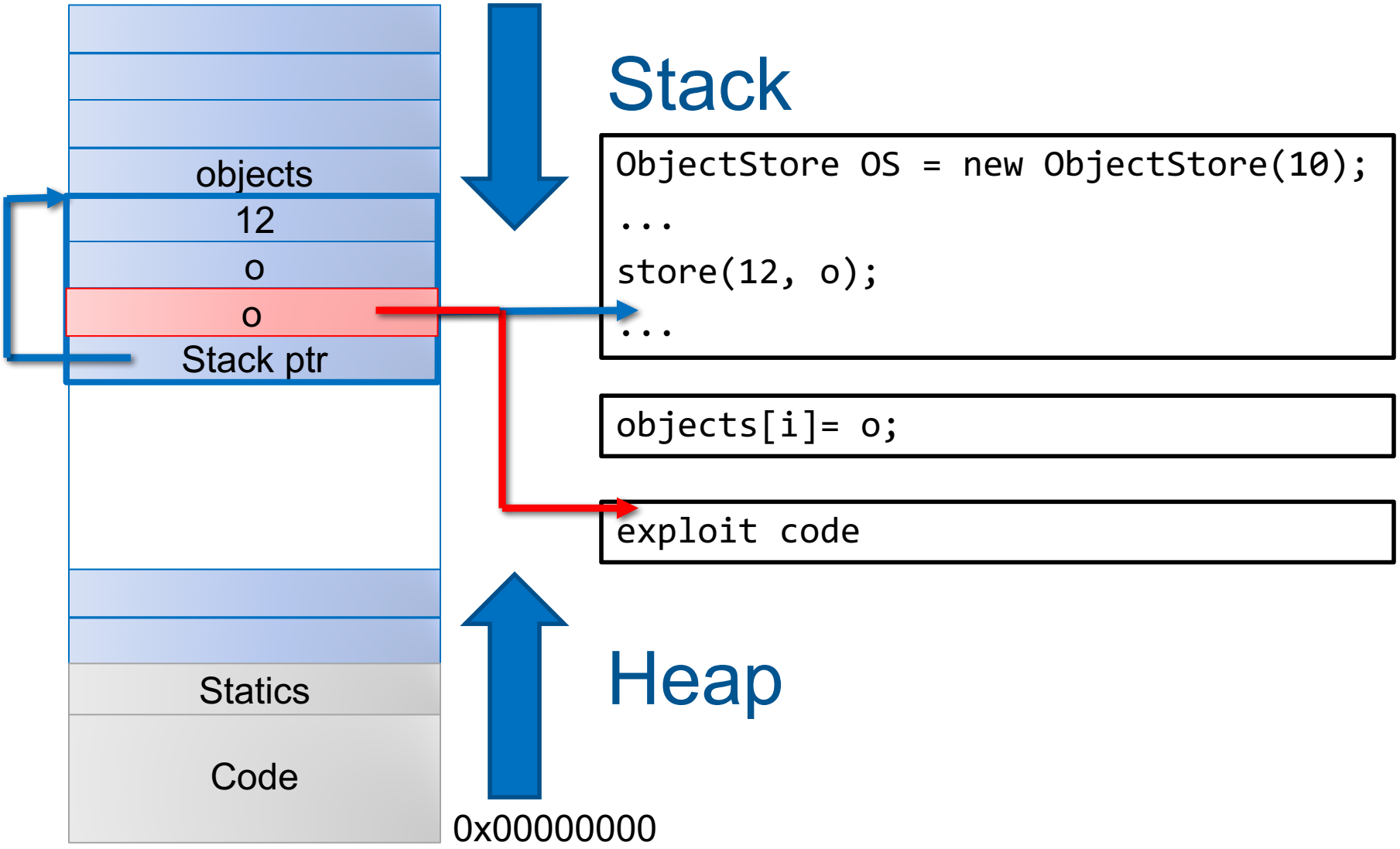
Heartbleed


SERVER, ARE YOU STILL THERE? IF SO, REPLY "POTATO" (6 LETTERS).
POTATO
SERVER, ARE YOU STILL THERE? IF SO, REPLY "BIRD" (4 LETTERS).
these 4 letters: BIRD.
User Meg wants these 500 letters: HAT.
HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about "snakes but not too long". User Karen wants to change account password to

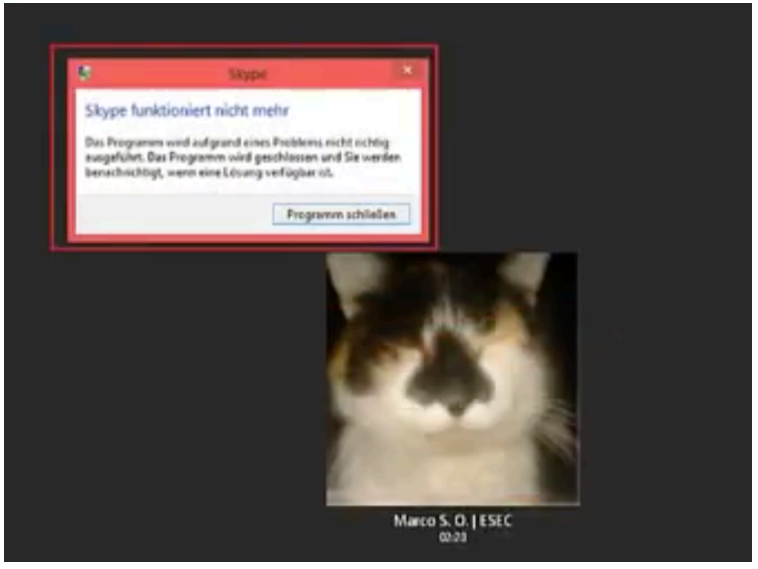
What might go wrong

```
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;
	}
}
```

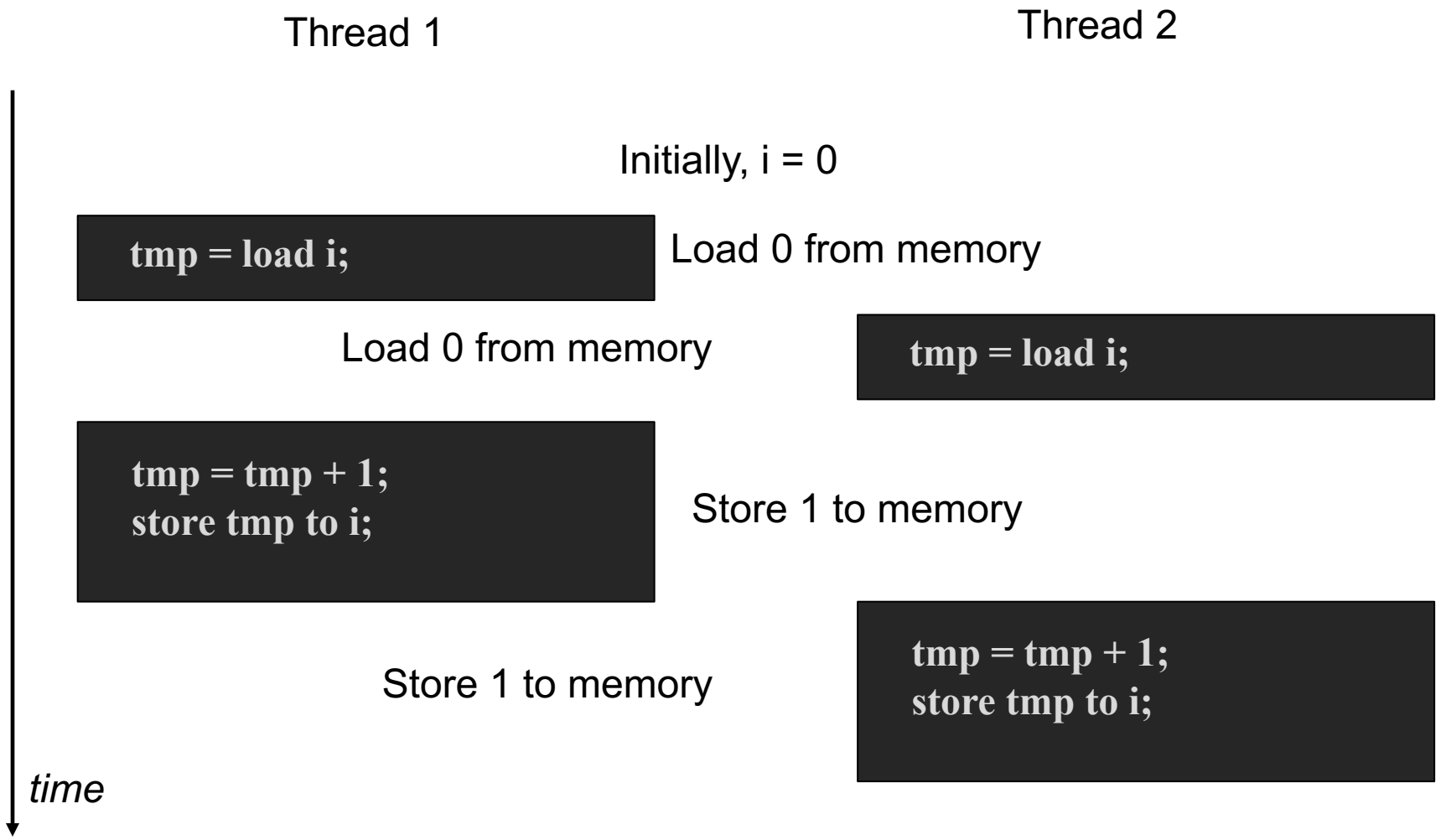
Memory


objects
12
o
o
Stack ptr
Statics
Code
0x00000000
Stack
ObjectStore OS = new ObjectStore(10);
...
store(12, o);
...
objects[i]= o;
exploit code
Heap

Skype Vulnerability



What might go wrong



Copy-on-write (COW)

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

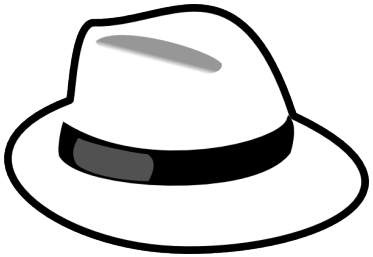
Privilege Escalation

So how do we fix this?

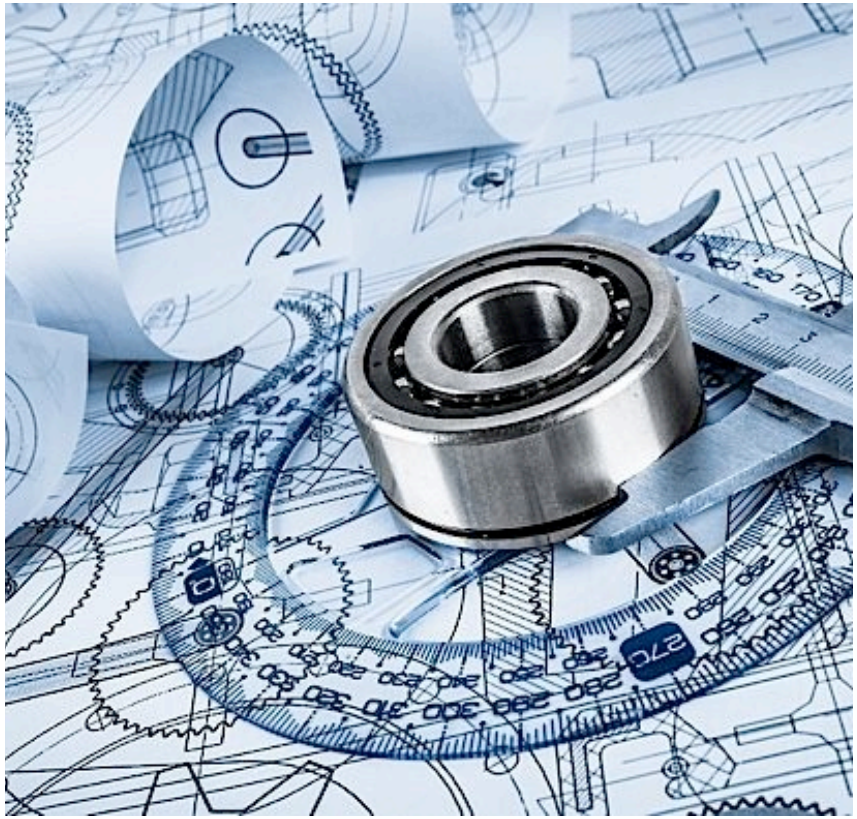
- Testing
- Bug finding tools

FindBugs™

- White-hat hacking



So how do we fix this?



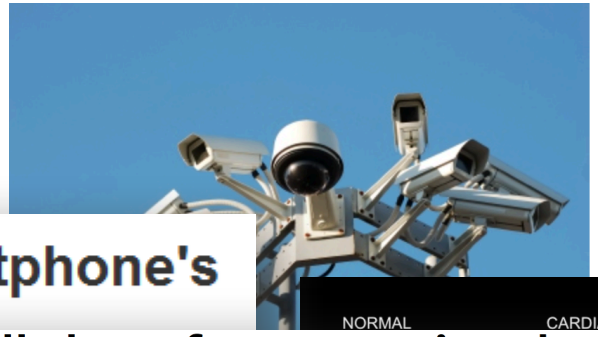
Security by Design

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

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

Example: Data Privacy

Google



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

Blame Android, says social network

By John Leyden,

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

Google Accused of W

By CLAIRE CAIN MILLER

Published: October 1, 2013

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

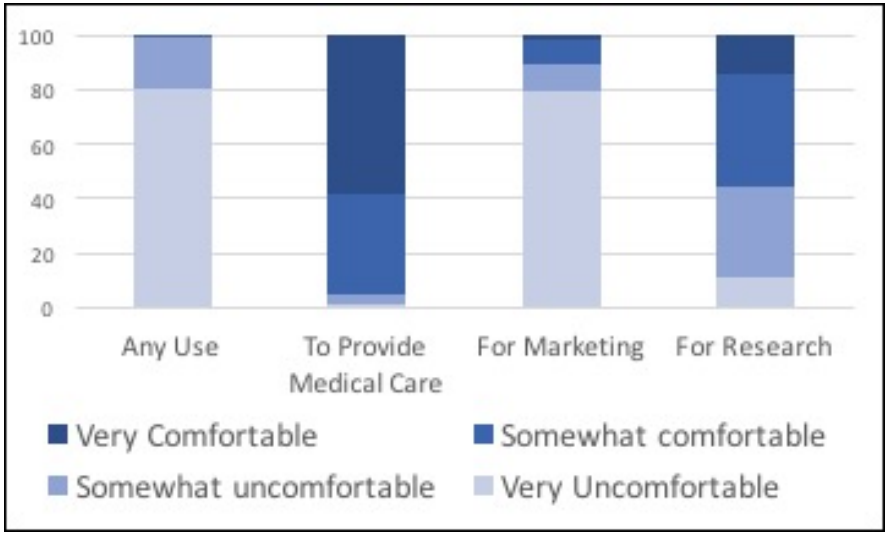
AccuWeather's iPhone app may track you even if you opt out (update)

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

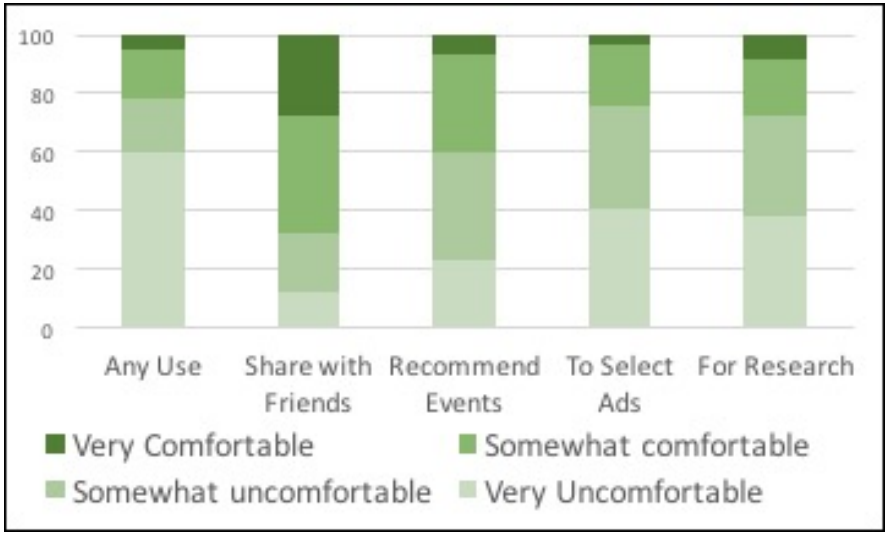
What is Privacy?

Use-Based Privacy

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

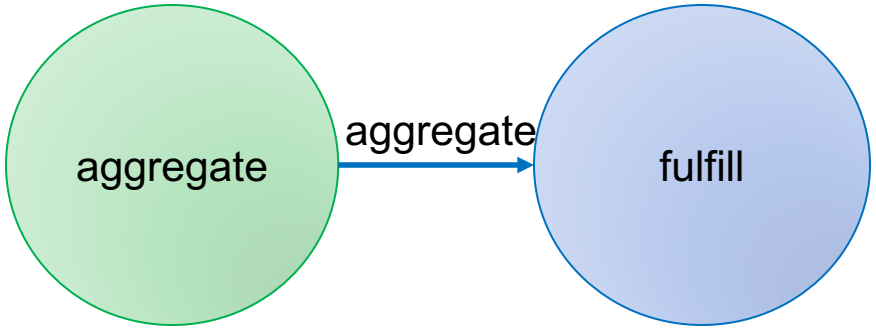


Medical Data



Social Network Data

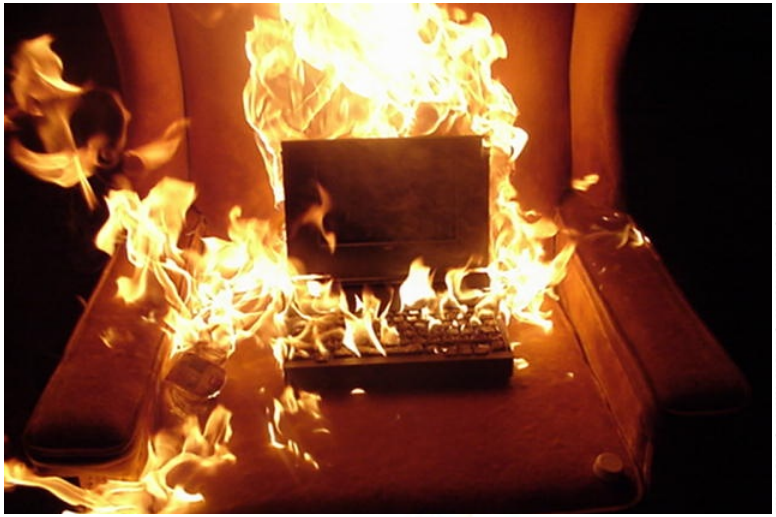
Policy Language



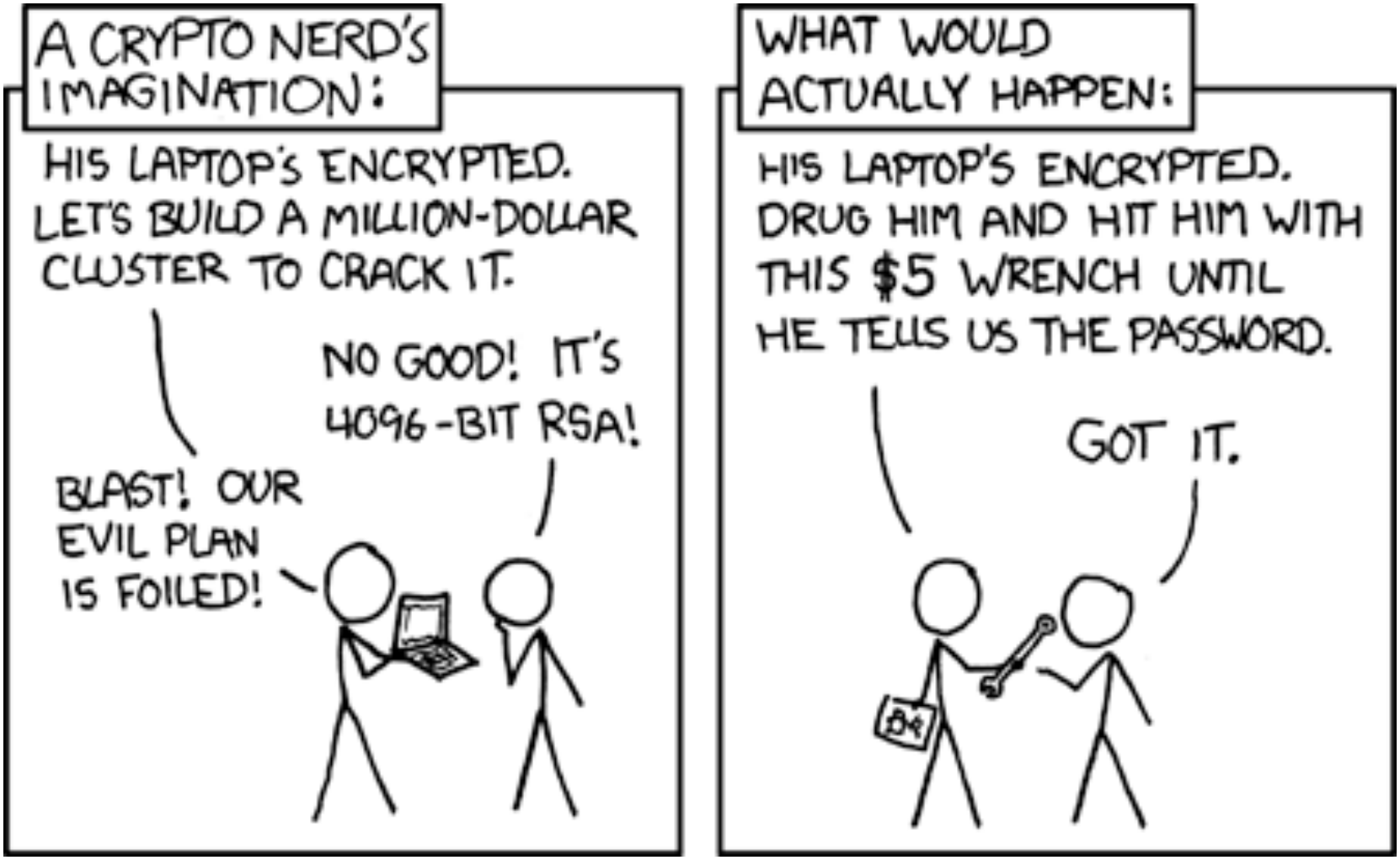

```
[{"curr":"1",
"states":{"1":{"name":"s1-1",
"permissions":{"aggregate":true},
"transitions":{"aggregate":"s2-1"},
"defaultPermission":false},
"2":{"name":"s2-1",
"permissions":{"fulfill":true},
"transitions":{},
"defaultPermission":true}}},
{"curr":"2",
"states":{"1":{"name":"s1-2",
"permissions":{"aggregate":true},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

How do we make systems secure?

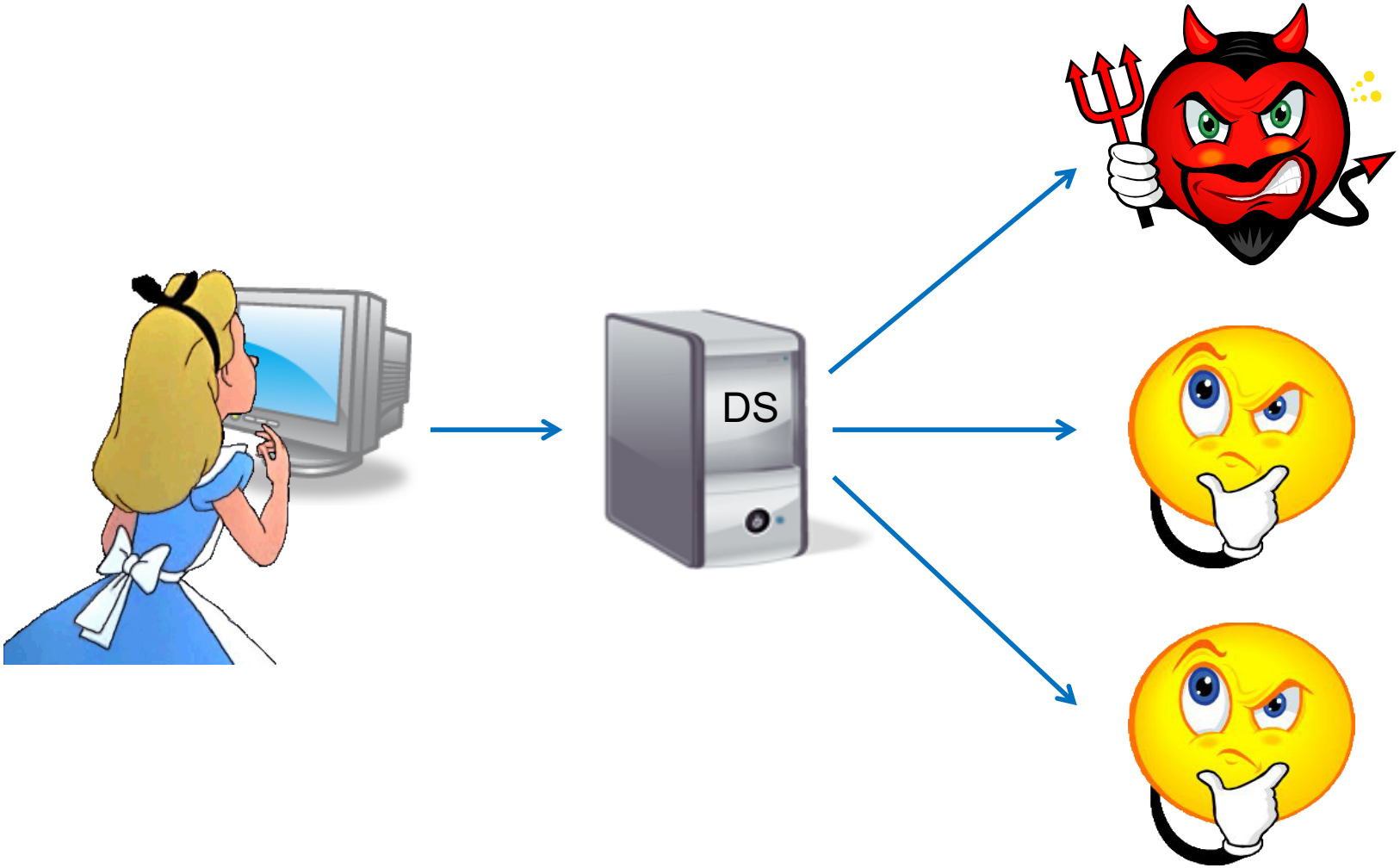
Threat Models



Threat Models



Example: Threat Model for Data Privacy

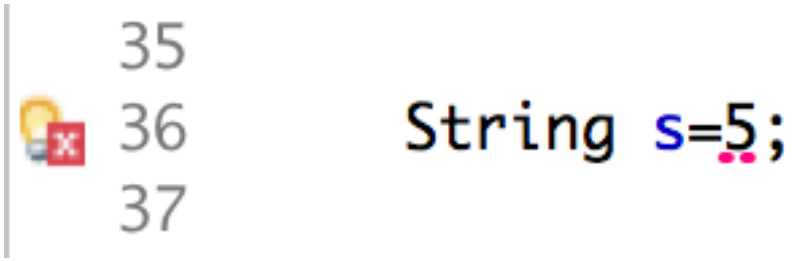


Approaches to security

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

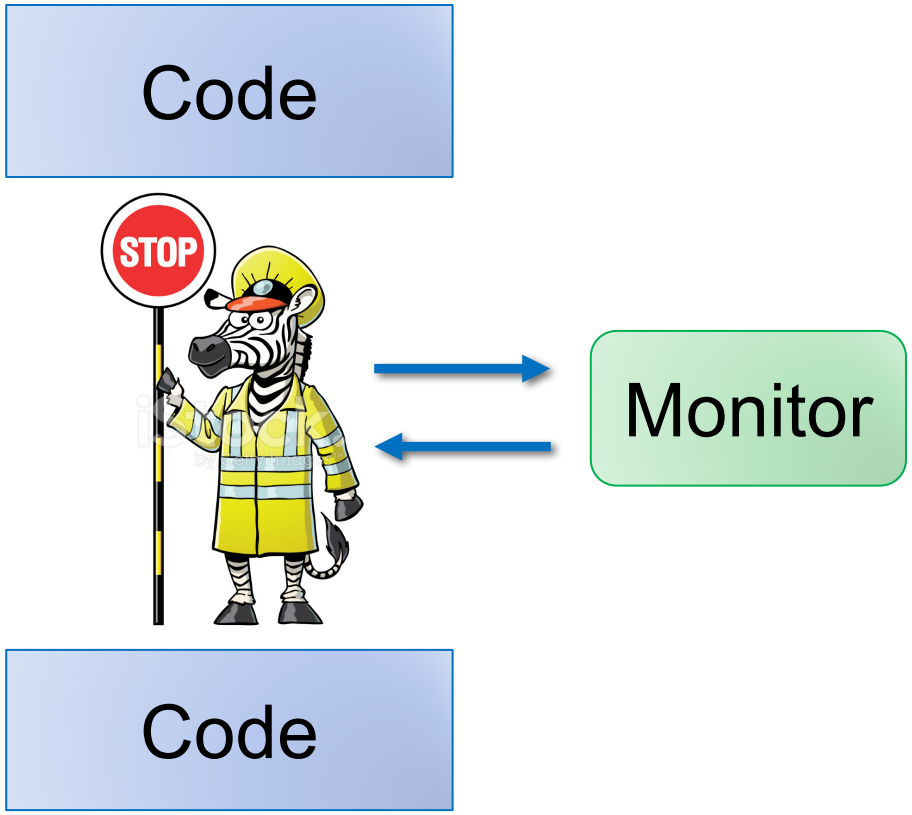
Approaches to security

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



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)

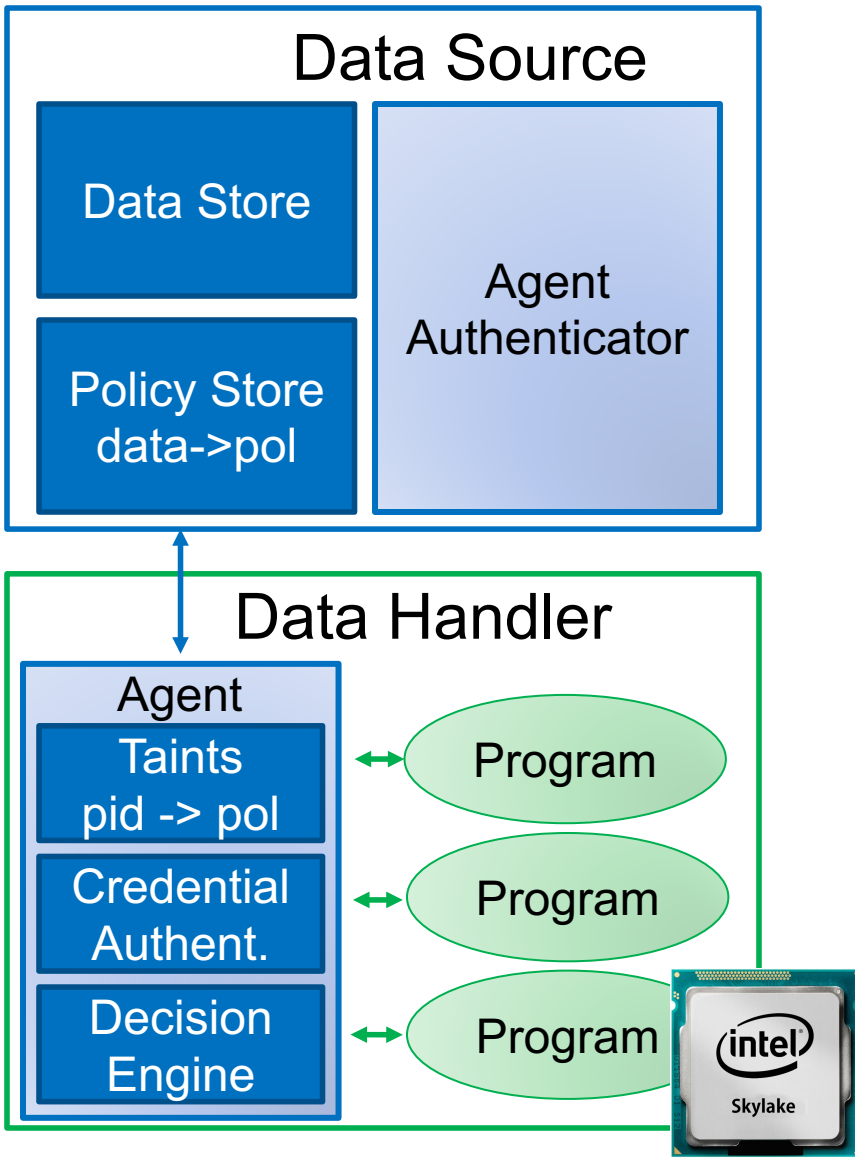


Approaches to security

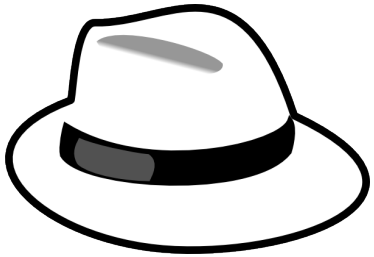
- Axiomatic security
  - You trust someone else to get it right
- Constructive security
  - E.g., compiler checks, automated proofs
- Synthetic security
  - Modify the code to add checks (e.g., monitoring)
- Deterrence through accountability
  - Make sure you'll notice if something goes wrong

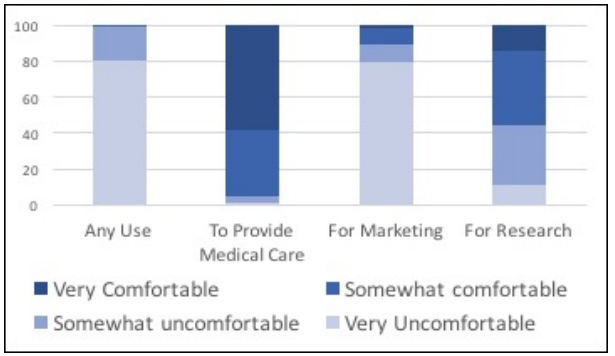
Example: Data Privacy from SGX

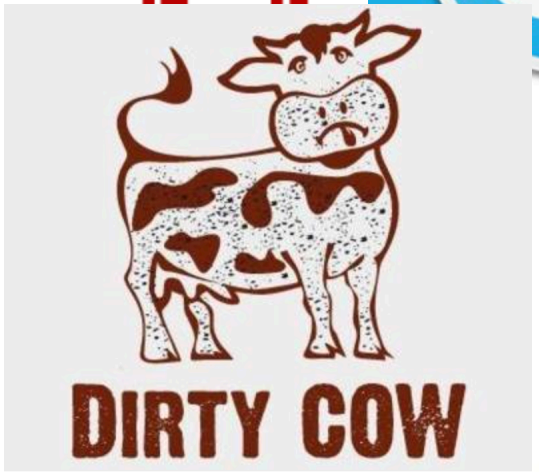
- Policy enforcement implemented by external monitor that runs on DHs
  - monitor can send/receive values from DS
  - monitor shares values with authorized programs co-located at DH
    - auth decisions based on credentials
  - unauthorized values are cryptographically sealed with associated policy to 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":tru
"transitions":{"aggregate":"s2
"defaultPermission":false},
"2":{"name":"s2-1",
"permissions":{"fulfill":true}
                ':{},
               ission":true}}}]
```