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:

<table>
<thead>
<tr>
<th>Day</th>
<th>Time</th>
<th>Location</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tu</td>
<td>12:20</td>
<td>Bard 140</td>
<td>Regular Expressions</td>
</tr>
<tr>
<td>Tu</td>
<td>12:20</td>
<td>Hollister 368</td>
<td>Kooky Data Structures</td>
</tr>
<tr>
<td>Tu</td>
<td>12:20</td>
<td>Olin 216</td>
<td>Sound</td>
</tr>
<tr>
<td>Tu</td>
<td>12:20</td>
<td>Upson 216</td>
<td>Coding Interviews</td>
</tr>
<tr>
<td>Tu</td>
<td>1:25</td>
<td>Hollister 206</td>
<td>Java 9</td>
</tr>
<tr>
<td>Tu</td>
<td>1:25</td>
<td>Hollister 312</td>
<td>Dynamic Programming</td>
</tr>
<tr>
<td>Tu</td>
<td>2:30</td>
<td>Hollister 110</td>
<td>TBA</td>
</tr>
<tr>
<td>Tu</td>
<td>2:30</td>
<td>Olin 165</td>
<td>Collections</td>
</tr>
<tr>
<td>Tu</td>
<td>3:35</td>
<td>Bard 140</td>
<td>Distributed Computing</td>
</tr>
<tr>
<td>We</td>
<td>12:20</td>
<td>Bard 140</td>
<td>Debugging</td>
</tr>
<tr>
<td>We</td>
<td>12:20</td>
<td>Olin 218</td>
<td>Dynamic Program.</td>
</tr>
<tr>
<td>We</td>
<td>1:25</td>
<td>Bard 140</td>
<td>Version Control</td>
</tr>
<tr>
<td>We</td>
<td>1:25</td>
<td>Upson 216</td>
<td>Optionals</td>
</tr>
<tr>
<td>Tu</td>
<td>2:30</td>
<td>Bard 140</td>
<td>TBA</td>
</tr>
<tr>
<td>Tu</td>
<td>2:30</td>
<td>Phillips 407</td>
<td>Coding Interviews</td>
</tr>
<tr>
<td>Tu</td>
<td>7:30</td>
<td>Upson 142</td>
<td>Coding Interviews</td>
</tr>
<tr>
<td>Tu</td>
<td>3:35</td>
<td>Bard 140</td>
<td>Distributed Computing</td>
</tr>
</tbody>
</table>
Computer Science
Computer Security

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

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 these 4 letters: BIRD.

User Meg wants these 500 letters: HAT. Lucas requests the "misused 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 "Heartbleed_Never_Expire".
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

Stack

Heap

0x00000000
Skype Vulnerability
What might go wrong

Initially, $i = 0$

Thread 1

```c
tmp = load i;
```

Load 0 from memory

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

Store 1 to memory

Thread 2

```c
tmp = load i;
```

Load 0 from memory

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

Store 1 to memory
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
• White-hat hacking
So how do we fix this?

AT LEAST
YOU TRIED
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

Google Accused of Violating COPPA, Tracking Kids in 42 Apps
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](chart1.png)

![Social Network Data](chart2.png)
Policy Language

```json
[{
    "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

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
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":true
},
"transitions":{
"aggregate":"s2-1",
"defaultPermission":false
},
"2":{
"name":"s2-1",
"permissions":{
"fulfill":true
}
},
"3":{
"name":"s3-1",
"permissions":{
"fulfill":false
}
}
}
}]}