Syllabus for CS3923 / 6813: Computer Security
New York University
Fall 2017
Professor Cappos
Thursdays 6PM-8:30PM; Dibner Auditorium

To contact professor: jcappos@nyu.edu
2 MetroTech, room 10.082
Phone: 646-997-3116
Office hours: Tu 4:30PM-5:30PM or by appointment

Graduate teaching assistants:
Mohammed Ashraf Ali, ashrafali@nyu.edu
Office hours: Mo 11AM-noon
Office hour location: 2 MetroTech, cubicle area 10.098

Srinivas Piskala Ganesh Babu, spg349@nyu.edu
Office hours: Fr 1-2PM
Office hour location: 2 MetroTech, cubicle area 10.098

Aakar Deveshkumar Jinwala, aakar.jinwala@nyu.edu
Office hours: Th noon-1PM
Office hour location: 2 MetroTech, cubicle area 10.098

Course Description
This class provides a firm grounding in computer security concepts and basics. Students learn
about threat modeling, principles of secure design, security policies, access control technologies,
and similar topics.

During this course, students will:
1. Understand physical security and online security.
2. Construct of a reference monitor that restricts access to network and disk resources for a
   virtual machine. Analysis of the implementations for security flaws.
3. Analyze flaws in a practical system. Implementation of an extension to fix at least one of
   these issues. An analysis of proposed fixes to understand their security properties.
4. Obtain a deep understanding of virtualization including Type 1 (which we further subdivide by
   those that virtualize hardware versus a set of kernel patches that jail different VMs) and Type 2
   virtualization, their implementation, and the efficiency, security, simplicity, and resource savings
   tradeoffs. Students are tested on their knowledge of virtualization tradeoffs.
5. Learn about database topics related to security including Hashing and Encryption, Database
   access controls (DAC, MAC, RBAC, Clark-Wilson), Information flow between databases/servers
   and applications, and Common DBMS vulnerabilities such as SQL injection.

Course Objectives
Objective 1: Learn to think with a security mindset while remaining ethical
Objective 2: Learn the core concepts of access control, reference monitors, and security policies that are commonly used in modern OSes.
Objective 3: Learn the basics of building and analyzing secure systems.
Objective 4: Understand virtualization, including different virtualization techniques and how they impact security and efficiency

Course Structure
This class has weekly lectures that cover the topics at a high level. Almost every week there is also an assignment due the following week that reinforces the covered topics. Assignments are a major focus of the class and are weighed heavily in assessment. Please be sure to keep up with the assignments as they are key to doing well in the class.

Readings
There is no textbook for this class. The lectures will often include online materials that need to be read.

Grading etc:
Quizzes: 5% (cannot be made up if missed)
Exam 1: 7% (exam 1)
Exam 2: 8% (exam 2)
Exam 3: 10% (final)
Projects: 70% (three assignments each with 3 sub parts)
Late assignments will not be accepted

Extra credit
You can attend specific talks and provide a write-up about them for a small amount of extra credit. Information about these talks will be posted on the classes site ahead of time. The first extra credit will add 1 point on your final grade, the second will add 1/2 a point, the third will add 1/3 of a point, etc.

Course schedule
<table>
<thead>
<tr>
<th>Date</th>
<th>Topic</th>
<th>Assignments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sept 7</td>
<td>Introduction</td>
<td>A1.1 (Python)</td>
</tr>
<tr>
<td>Sept 14</td>
<td>Security Design Principles</td>
<td>A1.2</td>
</tr>
<tr>
<td>Sept 21</td>
<td>Threat Modeling</td>
<td>A1.3</td>
</tr>
<tr>
<td>Sept 28</td>
<td>Security Policies</td>
<td>A1.3 (due)</td>
</tr>
<tr>
<td>Oct 5</td>
<td>Exam 1</td>
<td>(Repy)</td>
</tr>
<tr>
<td>Oct 12</td>
<td>Access Control (1): OSes, phones</td>
<td>A2.1</td>
</tr>
<tr>
<td>Date</td>
<td>Topic</td>
<td>Section</td>
</tr>
<tr>
<td>--------</td>
<td>----------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Oct 19</td>
<td>Access Control (2): IFC, O-Cap</td>
<td>A2.2</td>
</tr>
<tr>
<td>Oct 26</td>
<td>Containerization: VMs, SFI, DoS</td>
<td>A2.3</td>
</tr>
<tr>
<td>Nov 2</td>
<td>Exam 2</td>
<td>A2.3 (due)</td>
</tr>
<tr>
<td>Nov 9</td>
<td>Crypto primitives / PIR (<strong>CSAW</strong>)</td>
<td>A3.1</td>
</tr>
<tr>
<td>Nov 16</td>
<td>Privacy and key management</td>
<td>A3.2</td>
</tr>
<tr>
<td>Nov 23</td>
<td><strong>NO CLASS</strong></td>
<td></td>
</tr>
<tr>
<td>Nov 30</td>
<td>Software validity and rights</td>
<td></td>
</tr>
<tr>
<td>Dec 7</td>
<td>Injection attacks and defenses</td>
<td>A3.3</td>
</tr>
<tr>
<td>Dec 14</td>
<td>Cryptocurrency and IoT security</td>
<td>A3.3 (due)</td>
</tr>
<tr>
<td>Dec 21</td>
<td><strong>Final</strong></td>
<td></td>
</tr>
</tbody>
</table>

**Academic Dishonesty:**
Students must follow the collaboration guidelines for the projects. All tests and quizzes are individual. Students must behave ethically at all times. **Academic dishonesty will be severely punished and will extend beyond failing the class.** For more details, see the Code of Conduct: [http://engineering.nyu.edu/academics/code-of-conduct/academic-misconduct](http://engineering.nyu.edu/academics/code-of-conduct/academic-misconduct)

**Moses Center Statement of Disability**

If you are student with a disability who is requesting accommodations, please contact New York University's Moses Center for Students with Disabilities at 212-998-4980 or mosescsd@nyu.edu. You must be registered with CSD to receive accommodations. Information about the Moses Center can be found at [www.nyu.edu/csd](http://www.nyu.edu/csd). The Moses Center is located at 726 Broadway on the 2nd floor.