Cloud Computing Security

Syllabus - Fall 2020

# Class Information

|  |  |
| --- | --- |
| Instructor | Chris Monson <[monson@jhu.edu](mailto:monson@jhu.edu)>  Office hours: [Slack is my office](https://jhu-cloudsec-2020.slack.com) :-) - [Join here](https://join.slack.com/t/jhu-cloudsec-2020/shared_invite/zt-h0uy4ssy-V8OY_Zkg60Iu50mbLC5Atg)  CA: |
| Time and Room | Asynchronous and online, due to Covid-19. New lectures, labs, assignments, etc. will be posted by the Friday before any relevant due dates. This course has no exams. It does have presentations, which are tentatively scheduled for the last two Fridays of the semester. We should work together to determine whether those dates and times work for everyone. |

# Course Description

This course is designed to introduce students to cloud technology fundamentals with a particular emphasis on security considerations. This includes containers and orchestration, authentication and authorization, delegation of trust, protecting sensitive data and code, and guarding against malicious processes. While security is an emphasis in this course, general concepts will form a large part of the curriculum.

# Prerequisites and Required Materials

You will need to be

* Comfortable with Python or another AppEngine-Standard-supported language.
* Comfortable with or willing to self-start on minimal HTML and JavaScript.

You will need to have or obtain

* A free tier AppEngine project.
* Access to a suitable machine or VM (a Mac laptop is fine, for example) capable of
  + Building and running **Docker** containers,
  + Running either **minikube** or full **Kubernetes**, and
  + Running the **AppEngine SDK** using your compatible language of choice.

# Introduction and Policies

Welcome to the Cloud Computing Security class! We will be covering topics about cloud computing in general, gaining experience with foundational security questions and techniques, and studying relevant literature, both past and present. While the course is going to have an emphasis on security in the cloud, there will be a substantial emphasis on more general cloud issues, as well. You can expect that we will cover topics in cloud, security, *and* cloud security.

During this class, you will be engaging in several activities designed to help you learn useful skills and thought processes, and of course to earn a grade. Among them are labs, papers, class participation, presentations, and a final project.

Labs and projects will be graded on how well the *end result* matches the lab requirements. Your code will be submitted for inspection, and your working systems will be presented to me or an assistant to assess whether they meet the necessary criteria. Code will be expected to be well formatted, well documented, well organized, correct, and original work.

Papers and presentations will be graded on how well the requirements are met, and whether the arguments are well supported (when there are arguments). We will discuss strategies for writing good papers in class during the first week, and advice will be posted in the class forum. Good writing, particularly when describing security issues, is an important skill to refine, so there will be an emphasis on that in this course.

Participation will be fairly subjectively graded, based on perceived engagement with topics and discussion. As not everyone is equally comfortable with in-class discussion, participation can also be awarded based on willingness to participate in *online* discussion, giving aid and adding insights. The grade breakdown for these is listed below.

# Assignments

Grades will be assigned based on assignments, participation, and a final project. For assignments, there will be both labs and written documents. The basic breakdown is as follows:

|  |  |
| --- | --- |
| Labs and Written Assignments | 85% |
| Final Project | 15% |

# Grades

Grades are on the standard schedule with plusses and minuses at instructor discretion:

**A**: 90-100, **B**: 80-89, **C**: 70-79

# Students are Human (and so are Professors)

## Ethics and Integrity

All assignments are expected to be completely original work. Where appropriate, you may use libraries, but all assignments require some amount of original code, original writing, etc. The rule for group interaction is simple: when producing a work product, be alone with your own thoughts, and your own hands doing the work.

Study groups are encouraged. They are very effective in a learning setting. Just make sure that when fingers are on the keyboard, everything you type is your own work and your own thoughts.

It should go without saying that this means you cannot use code you find online, or anything written by another student. In the case of written assignments, quotes must be given proper attribution, and must not represent the bulk of your work.

If you find that someone is acting without integrity or unethically, please report it immediately. Follow the guidelines of the [Undergraduate Academics Ethics Board](http://e-catalog.jhu.edu/undergrad-students/student-life-policies/#UAEB).

## Student Responsibility

I care about your success as a student. I am also somewhat demanding when it comes to personal responsibility. I expect that

* Assignments will be turned in by the beginning of class on the day they are due,
* Labs will be passed off with myself or an assistant in the same timely manner,
* Students will take responsibility for their own extenuating circumstances, for example,
  + Getting notes from others when they are absent from class,
  + Seeking out help when stuck or struggling, or
  + Seeking advice and permission early when extenuating life circumstances arise.

In other words, don’t wait, don’t stay stuck, and don’t expect help to come to you, rather seek it out when you need it. I want your success to truly be your own, so go out and get it. I am a resource for you and strive to always be available to help when you need it. I just won’t necessarily know that you need it without you asking for it.

It may become necessary as the class progresses to make some changes to assignments, schedule, etc. Be prepared to be flexible: I will make changes when necessary.

## Personal Well Being

If you are sick during a semester when in-person classes are in session, particularly with something likely to be contagious, stay home and notify me by email. Visit the health and wellness center as needed. See also the university [illness policy](http://studentaffairs.jhu.edu/student-life/support-and-assistance/absences-from-class/illness-note-policy).

If you are a student with a disability, please contact me at your earliest convenience *and* obtain an accommodation letter from the [JHU Office for Student Disability Services](http://web.jhu.edu/disabilities/).

If you are struggling with anxiety, stress, depression, or other mental health concerns, please consider visiting the [JHU Counseling Center](http://studentaffairs.jhu.edu/counselingcenter). Encourage struggling friends to do the same. The struggle is real; don’t delay getting help if you need it.

# Topic Schedule

We will cover the following topics (loosely - things can get shuffled a bit based on surprises or the discovery of class needs) through the semester. Note that there are associated write-ups for several of the reading assignments. Reading is always assigned **after** the corresponding lecture. Note also that some of these may change as the semester wears on. Treat the accuracy of this list as “descending over time”, watch your email/slack, and you’ll be just fine.

|  |  |  |
| --- | --- | --- |
| **Date** | **Topic** |  |
| 2020-09-04 | [Syllabus, Cloud Intro](https://drive.google.com/open?id=1cUDDiZQ-hW4NqwUFJOt8iK2v9fl0IaL-SF6pKmmYnh4)  ([Slides](https://docs.google.com/presentation/d/1dMar3Sia1wYkP7Ly8L8AWjSB3-IZYAU2ClJuBxYUOD8/edit?usp=sharing)) | Due next week:   * Lab 0: [Cloud “Hello, World!”](https://docs.google.com/document/d/1f0pc34rsR2kGF6P_EJTIcFNmPLpKJpGMjGvqAA81fWg)   Reading for next week:   * [Writing Types and Tips](https://docs.google.com/document/d/17XqIxtWuKuV-B3xalmkori9dkFEWGdthnZmPahtyA0U) * [What is Cloud Computing](https://www.infoworld.com/article/2683784/cloud-computing/what-is-cloud-computing.amp.html) * [A View of Cloud Computing](https://dl.acm.org/citation.cfm?id=1721672) * [The NIST Definition of Cloud Computing](https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf) |
| 2020-09-11 | [Authentication](https://docs.google.com/document/d/1ky6Kd8sN3PMpvnTR2xMvF9YslrPBRgkE8I5qkPq6Xuo/edit?usp=sharing)  ([Slides](https://drive.google.com/open?id=14XwUhaYYHp_OnFEH9QckshHaXGoT67x5VN6a9vXLi_s)) | Due today:   * Lab 0: [Cloud “Hello, World!”](https://docs.google.com/document/d/1f0pc34rsR2kGF6P_EJTIcFNmPLpKJpGMjGvqAA81fWg)   Due next week:   * Lab 1: [AppEngine Standard App](https://docs.google.com/document/d/14McjsEuwRoesPJTFusc8IQ80xGZ2m8J53mRj-S-ZADw) * Paper 1: [Authentication Recommendation](https://docs.google.com/document/d/1L49VN548qrViE0e_0sntY4yZoPRySMg8VvIiUazvX1k/edit#heading=h.q8avhr4uqoab)   Reading for discussion next week:   * [Authentication Cheat Sheet](https://www.owasp.org/index.php/Authentication_Cheat_Sheet) * [Understanding SSH Auth](https://www.digitalocean.com/community/tutorials/understanding-the-ssh-encryption-and-connection-process) * [Session Auth Best Practices](https://stackoverflow.com/questions/20963273/spa-best-practices-for-authentication-and-session-management) |
| 2020-09-18 | [PaaS and IaaS Design](https://docs.google.com/document/d/1Z-Pg9Xue0RfZ8BU0y90fVx7ehGWvXMVei6AV_ciXCWk/edit?usp=sharing) | Due today:   * Paper 1: [Authentication Recommendation](https://docs.google.com/document/d/1L49VN548qrViE0e_0sntY4yZoPRySMg8VvIiUazvX1k/edit#heading=h.q8avhr4uqoab) * Lab 1: [AppEngine Standard App](https://docs.google.com/document/d/14McjsEuwRoesPJTFusc8IQ80xGZ2m8J53mRj-S-ZADw)   Due next week:   * Lab 2: [Password-Based Authentication](https://docs.google.com/document/d/1AWV38YFirD9_cIfl-nDZfG29hTq6CfqKbMsDxR4rp1M)   Reading for next week:   * [SRE Book: Production Environment](https://landing.google.com/sre/book/chapters/production-environment.html) * [SRE Book: Simplicity](https://landing.google.com/sre/book/chapters/simplicity.html) * [Cluster Design Principles](https://docs.google.com/document/d/1izEMvDNjJUMNijh2ZJsjfYHV4qxLBySOZn9ayLaiH80/edit?usp=sharing) |
| 2020-09-25 | [Authorization and Delegation](https://docs.google.com/document/d/1nWf1J2LCOKO_W6gd99ZPsbAilmQ1irek0wOGkLs9QVM/edit?usp=sharing)  ([Slides](https://docs.google.com/presentation/d/1nhv2ksV7SMYjMQhrt6FDANozVomRr0GM-RuuftOxxaE/edit?usp=sharing)) | Due today:   * Lab 2: [Password-Based Authentication](https://docs.google.com/document/d/1AWV38YFirD9_cIfl-nDZfG29hTq6CfqKbMsDxR4rp1M)   Due next week:   * Lab 3: [OpenID Connect Implementation](https://docs.google.com/document/d/1gAnZN0WtjqetMCFRuU7g5Flslv2ODa9ErHk5xlJgXck/edit#)   Reading for next week:   * [OAuth 2.0 RFC](https://tools.ietf.org/html/rfc6749) |
| 2020-10-02 | [VMs and Mostly Containers](https://docs.google.com/document/d/1yyxSe7jFO3FsxJ89iS8RfDyCC90-rjPgVrmATkH3i7o) | Due today:   * Lab 3: [OpenID Connect Implementation](https://docs.google.com/document/d/1gAnZN0WtjqetMCFRuU7g5Flslv2ODa9ErHk5xlJgXck/edit#)   Due next week:   * Lab 4: [Docker Introduction](https://docs.google.com/document/d/1W_YQwv023a2dsJYrOdD1b7re0vb7eNOO1xkp8mXOMYU)   Reading for next week:   * [Introduction to Linux Containers](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux_atomic_host/7/html/overview_of_containers_in_red_hat_systems/introduction_to_linux_containers) * [Linux Container Article - Part I](https://www.linuxjournal.com/content/everything-you-need-know-about-linux-containers-part-i-linux-control-groups-and-process) * [Linux Container Article - Part II](https://www.linuxjournal.com/content/everything-you-need-know-about-linux-containers-part-ii-working-linux-containers-lxc) * [Docker Overview](https://docs.docker.com/engine/docker-overview/) * [Singularity Containers](https://www.nextplatform.com/2017/04/10/singularity-containers-hpc-reproducibility-mobility/) |
| 2020-10-09 | [What Containers Really Are](https://docs.google.com/document/d/1VMoj5r03f3TMXiQyojSERA5qL0Reszzkg5doDgXZyxo/edit?usp=sharing)  <https://youtu.be/sK5i-N34im8> | Due today:   * Lab 4: [Docker Introduction](https://docs.google.com/document/d/1W_YQwv023a2dsJYrOdD1b7re0vb7eNOO1xkp8mXOMYU)   Due next week:   * Paper 2: [Container Hardening](https://docs.google.com/document/d/1ypUsb8cfHgQdyG7bsP-lOo2bTAPEXqr0xxkGyt1gX_0/edit?usp=sharing) * [Final Project Topic](https://docs.google.com/document/d/1xOA-Yug5CJUESVC_UqZvdaz7IF-Okj-jhoiANoc67qs)   Reading for next week:   * [Escaping Docker Using waitid()](https://www.twistlock.com/2017/12/27/escaping-docker-container-using-waitid-cve-2017-5123/) * [Abusing ... Linux Containers](https://www.nccgroup.trust/uk/our-research/abusing-privileged-and-unprivileged-linux-containers/) * [Docker Security Myths/Legends Video](https://www.youtube.com/watch?v=uQigvjSXMLw) * [Understanding/Hardening Containers](https://www.nccgroup.trust/globalassets/our-research/us/whitepapers/2016/april/ncc_group_understanding_hardening_linux_containers-1-1.pdf) |
| 2020-10-16 | [Attack Vectors](https://docs.google.com/document/d/1JkuSJkBfl0E41UwXXT2Ivmli1Ao7NF6TgnOmOS837jA/)  ([Slides](https://docs.google.com/presentation/d/1O0IqcwDqFm3KGjDeCQEJze_dq5Ehd76yd6-BmQ90AA0)) | Due today:   * Paper 2: [Container Hardening](https://docs.google.com/document/d/1ypUsb8cfHgQdyG7bsP-lOo2bTAPEXqr0xxkGyt1gX_0/edit?usp=sharing) * [Final Project Topic](https://docs.google.com/document/d/1xOA-Yug5CJUESVC_UqZvdaz7IF-Okj-jhoiANoc67qs/edit?usp=sharing)   Due next week:   * Lab 5: [Escape](https://docs.google.com/document/d/1NWUoT83OzRxju4WB2-4hZBGEaqZsmM-UJka6nCNuBoc/edit?usp=sharing)   Reading for next week:   * [Most Common Attacks](https://blog.sucuri.net/2014/11/most-common-attacks-affecting-todays-websites.html) * [The 10 Most Common … Attacks](https://securityintelligence.com/the-10-most-common-application-attacks-in-action/) * [Dirty Dozen](https://www.csoonline.com/article/3043030/security/12-top-cloud-security-threats-for-2018.html) |
| 2020-10-23 | [Container Orchestration](https://docs.google.com/document/d/1is0uzDNfrp57EUKZxmzLb2WIfhRx148cluY8jEeks9Q/edit?usp=sharing) | Due today:   * Lab 5: [Escape](https://docs.google.com/document/d/1NWUoT83OzRxju4WB2-4hZBGEaqZsmM-UJka6nCNuBoc/edit?usp=sharing)   Due next week:   * Lab 6: [Multi-Container System](https://docs.google.com/document/d/1IlxIYEHBwQy1QSM8QEwtyNidJK_Ixt8gfsyC9v6dd4c/edit#heading=h.xbsi5rv6ptj6)   Reading for next week:   * [Container Orchestration w/Kubernetes](https://medium.com/onfido-tech/container-orchestration-with-kubernetes-an-overview-da1d39ff2f91) * [What is Kubernetes...?](https://www.infoworld.com/article/3268073/kubernetes/what-is-kubernetes-container-orchestration-explained.html) * [How to Choose Orchestration](https://medium.freecodecamp.org/how-to-choose-the-right-container-orchestration-and-how-to-deploy-it-41844021c241) * [Comparing Container Orchestrators](https://www.weave.works/blog/comparing-container-orchestration/) |
| 2020-10-30 | [Distributed Foundations](https://docs.google.com/document/d/1QG6LvVTaisePafPp8eH1a0vf_qtQCvjU9xyrKdkQ26I)  ([Slides](https://docs.google.com/presentation/d/1yqs-n_eigoMLa8wNyAIi3ahKjlT71Ma4j3sGEzecDfY)) | Due today:   * Lab 6: [Multi-Container System](https://docs.google.com/document/d/1IlxIYEHBwQy1QSM8QEwtyNidJK_Ixt8gfsyC9v6dd4c/edit#heading=h.xbsi5rv6ptj6)   Due next week:   * Lab 7: Orchestration and Namespaces   Reading for next week:   * [Comparison of Dist. File Systems](https://en.wikipedia.org/wiki/Comparison_of_distributed_file_systems) * [Testing of Several Dist File Systems](http://iopscience.iop.org/article/10.1088/1742-6596/513/4/042014/pdf) * Pick an S3-compatible one to study |
| 2020-11-06 | PKI, TLS, and Bitcoin  ([Slides](https://docs.google.com/presentation/d/1e5h6FE6zJC_YwUbsIhgzfdKB7LEiANr4EhXOY1o7m8c/edit?usp=sharing)) | Due today:   * Lab 7   Reading for next week:   * [Prometheus](https://prometheus.io/) * [TICK](https://www.influxdata.com/time-series-platform/) * Do a comparative analysis |
| 2020-11-13 | Encryption at Rest | Due next week:   * [Final Project Report](https://docs.google.com/document/d/1xOA-Yug5CJUESVC_UqZvdaz7IF-Okj-jhoiANoc67qs/edit?usp=sharing)   Reading for next week:   * [Public Key Infrastructure](https://en.wikipedia.org/wiki/Public_key_infrastructure) * [PKI - OpenStack](https://wiki.openstack.org/wiki/PKI) * [Beginner Guide to PKI](https://www.techrepublic.com/article/a-beginners-guide-to-public-key-infrastructure/) |
| 2019-11-20 | Class Presentations | Due today:   * [Final Project Report](https://docs.google.com/document/d/1xOA-Yug5CJUESVC_UqZvdaz7IF-Okj-jhoiANoc67qs/edit?usp=sharing) |
| 2019-12-04 | Class Presentations |  |