HACS 102

Foundations of Cybersecurity II

Spring 2014

Time and room TBA

3 credits

Course Syllabus

Course Description: HACS102 will build upon skills learned in HACS100 towards the completion of a collaborative design project. The group project in this course will combine technical, analytical, and communication skills, further engaging students in the practice of cybersecurity. Students will learn about design concepts and data analysis as they engage in a team project designing, deploying, and collecting and analyzing data from a honeypot. The hands-on nature of the course will give students experiential insight about how and why attackers attack and how to engage in protective measures to prevent attacks.

Instructors: Dr. Michel Cukier
Office: 0151E Martin Hall

Email: mcukier@umd.edu

Office hours: Tuesdays: 2:00pm-3:00pm or by appointment

Dr. Jandelyn Plane
Office: 1113 AV Williams

Email: jplane@cs.umd.edu

Office hours: Wednesdays: 1:30-3:30 or by appointment

Bertrand Sobesto

Office: 4400 Computer and Space Sciences Building

Email: bsobesto@umd.edu

Office hours: TBD

General Education:

Scholarship in Practice (SIP).

Readings:

On-line material – references provided during the semester.

Class Web Site:

Communication between instructor and students outside the classroom will take place primarily through CANVAS (http://elms.umd.edu/). Please visit the site regularly for assignments and announcements.

Backgrounds:

ACES students will enter HACS102 with the foundational knowledge learned in HACS100. ACES students come from a variety of majors and have a range of unique skill sets. The diversity of backgrounds among ACES students will be vital to forming interdisciplinary teams that draw from each student's strengths.

Schedule:

The class schedule is posted online. It is subject to updates as the semester proceeds. When the schedule is changed, an announcement will be posted.

Learning Outcomes:

- Students will demonstrate cybersecurity skills and knowledge through a hands-on project;
- Students will demonstrate their ability to work closely with peers and mentors who have different backgrounds and skill sets;
- Students will demonstrate their understanding of the design process;
- Students will demonstrate their ability to use data collection and analyzing tools for cybersecurity research;
- Students will demonstrate their understanding of the multi-disciplinary aspect involved in computer attacks and defense.

Assessment:

The course grade will be calculated as follows:

- Active engagement and collaboration: 15%
- Weekly status reports: 10%
- Design presentation: 10%
- Design proposal: 20%
- Final presentation: 10%
- Final report: 25%
- Service-based learning: 10%

Project

In cybersecurity, a honeypot is a computer or a site intended as a "trap" for attackers. The honeypot appears as an attractive target, yet it is not truly part of a network and can be used as a monitoring tool to collect data about attacks. In teams of four or five, students will work to design, develop, and deploy their own research honeypot. These teams will be selected by the instructors, and are intended to be interdisciplinary, as the project will require a combination of skills in analyzing data, writing, programming, and presenting. Each team will write and present a design proposal with their strategies for deploying the honeypot, without giving away their plans to their peers. Use of open-source tools is permitted and encouraged. As the projects are under construction, teams will meet with instructors weekly to report on their status and any project issues that arise. When the

development process is complete, teams will run their honeypots live on the Internet so that data can be collected. After deployment, teams will compete to break into one another's framework while collecting and analyzing data from their own honeypot. Each team will write and present a final report evaluating their own project, analyzing the data collected, and discussing their strategies for attacking other teams' honeypots.

Weekly Status Reports

After the design proposal has been submitted, teams are expected to meet weekly with instructors during class time to give a brief a status report regarding project progression. Questions and concerns about technical issues, team dynamics, or other problems should be brought up to instructors at this time. In order to engage in meaningful status reports, students are expected to document project decisions and progress throughout the semester.

Academic Integrity

The University of Maryland, College Park has a nationally recognized code of Academic Integrity, administered by the Student Honor Council. This Code sets standards for academic integrity at Maryland for all undergraduates and graduate students. As a student you are responsible for upholding these standards for this course. It is very important for you to be aware of the consequences of cheating, fabrication, facilitation, and plagiarism. For more information, please visit http://www.shc.umd.edu/.

Academic integrity is a foundation for learning. The University has approved a Code of Academic Integrity available on the web at http://www.testudo.umd.edu/soc/dishonesty.html. The Code prohibits students from cheating on exams, plagiarizing papers, forging signatures, etc. The Code is administered by a Student Honor Council, which strives to promote a community of trust on the College Park campus. Allegations of academic dishonesty can be reported directly to the Honor Council (314-8206) by any member of the campus community.

The University Senate requires that students sign this statement if it is included on an exam or assignment:

> *"I pledge on my honor that I have not given or received any unauthorized assistance on this examination (or assignment)."*

Students with Disabilities

If a student is eligible for and requesting academic accommodations due to a disability, the student is requested to provide to the instructor a letter of accommodation, prepared by the Office of Disability Support Services (DSS), before the end of the add/drop period of the semester. Visit http://www.counseling.umd.edu/DSS/ for more information on disability support.

Attendance

Students are expected to attend all classes throughout the semester. Missing class will result in a loss of Active Engagement points. In special cases of medical emergencies and illnesses, religious observances, or University-approved participation in a University event, absences may be excused with no penalty.

Students who miss a single class for a medical reason must make a reasonable effort to contact their instructor in advance. If a prolonged absence of two or more weeks is expected due to an illness or medical emergency, the student must provide the instructor with medical documentation of the situation.

Students will not be penalized for participation in religious observances, and students will be allowed to make up academic assignments that are missed due to this type of absence. Students are responsible for notifying the instructor within the first two weeks of the semester, by email or in person during office hours, of projected absences during the semester.

For more information on UMD's attendance policies, refer to the Undergraduate Catalogue section on attendance.

Preliminary Course Calendar

WEEK 1

Class 1

- Course intro, review syllabus
- Team assignments

Class 2

- Team exercises

WEEK 2

Class 1

- Fundamentals of computer networks
- Open Systems Interconnection model
- TCP/IP, routing principles

Class 2

- Introduction to honeypots
- Definitions and motivations
- Challenges to running honeypots

WEEK 3

Class 1

- Design concepts and tools: what to include in your proposal?
- Design exercises

Class 2

- Introduction to data collection with honeypots
- Data storage and organization
- Sensors in computer networks

WEEK 4

Class 1

- What should be included in the design presentation

Class 2

- Design exercises

WEEK 5

Class 1

- *Proposals due*
- Design presentations (separate; to instructors)

Class 2

- Design presentations (separate; to instructors)

WEEK 6

Class 1

- Status reports: 5 minutes per group
- Project work

Class 2

- Lecture on common project issues
- Attack strategies

WEEK 7

Class 1

- Status reports: 5 minutes per group
- Project work

Class 2

- Lecture on common project issues

---SPRING BREAK---

WEEK 8

Class 1

- Status reports: 5 minutes per group
- Project work

Class 2

- Lecture on common project issues

WEEK 9

Class 1

- Status reports: 5 minutes per group
- Project work

Class 2

- Lecture on common project issues

WEEK 10

Class 1

- Deploy honeypots
- Data collection and analysis tips

Class 2

- Status reports on attack strategies

WEEK 11

Class 1

- Status reports on data collection and attack strategies
- Project time

Class 2

- Lecture on common project issues
- Attack strategies and data analysis tips

WEEK 12

Class 1

- Status reports on data collection and attack strategies
- Project time

Class 2

- Lecture on common project issues

- Attack strategies and data analysis tips

WEEK 13

Class 1

- Status reports on data collection and attack strategies
- Project time

Class 2

- Lecture on common project issues
- Attack strategies and data analysis tips

WEEK 14

Class 1

- *Final reports due*
- Project presentations

Class 2

- Project presentations

WEEK 15

Class 1

- Project presentations

Class 2

- Project feedback