Program Analysis for Software and Web Security

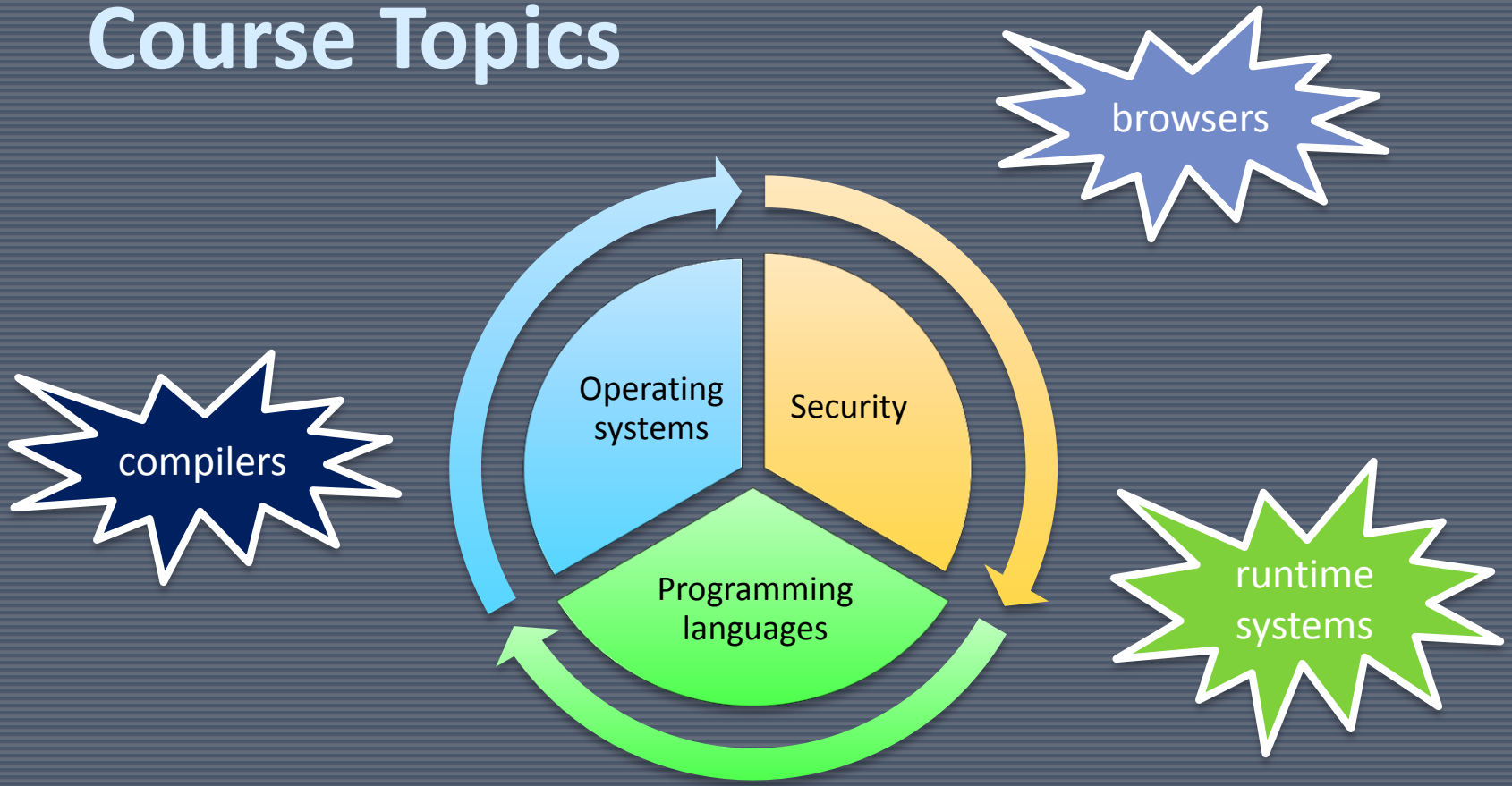
CSE 504

Ben Livshits
Microsoft Research and UW

Course Summary

- Target audience:
  - Ph.D. and Master's students
  - Advanced undergrads are welcome
  - If you are an *undergrad* considering this course, please consult the instructor prior to enrolment
- Primarily a paper reading course
- Will have external presentations by research and industry leaders
- Students are expected to read, discuss, and present research papers
- Designed to familiarize students with research in program analysis for security in the past 10 years

Course Topics



Which Techniques Will I See?

Memory safety				
4/14	Buffer overruns	Static Overrun Detection Comprehensive Protection		
4/19	Language solutions	CCured: Type-Safe Retrofitting of Legacy Code Detecting Format-String Vulnerabilities with Type Qualifiers	Dynamic Overrun Detection	
4/21	Worms	Vigilante: End-to-End Containment of Internet Worms		Marcus Peinado
4/26	Heap spraying	Nozzle Another heap ing paper	Randomness (TBD)	
4/28	Symbolic execution	EXE: Automatically Gen	Testing	

Type systems and static analysis

Runtime analysis

Symbolic execution

Which Techniques Will I See? (2)

Web security				
5/3	SQL Injection/XSS	Finding Securi…erabilities i… Analysis	…tacks	
5/5		Spectator: Detection and Containment of JavaScript Worms	Static Detection of Security Vulnerabilities in Scripting	
5/10	Mash-ups	BrowserShield: Vulnerability-D…	…actions for Client	
5/12	Browser security	BEEP	…Vulnerabilities	Nikhil Swamy
5/17		ConScript		
5/19	Malware on the Web	The Ghost In The …wser Analysis	…us Content Using Monkey-Spider Honeyclient	
5/24	Static analysis on the Web	Gatekeeper: Mostly Static Enforce… …rity a… Reliability Policies for JavaScript Code Staged Information Flow for JavaScript		
5/26	Languages	SWIFT		

Points-to analysis

Browser hacking

Aspect languages

Expected Workload

- Students are responsible for
  - Reading one paper per class and writing a very short summary
  - Be actively involved in in-class discussions
  - Leading 2- 3 presentations done in pairs, if enough people register
  - These typically involve more preparation and discussions with the instructor

- Paper response template: to be submitted individually before class
  - Contributions (3-5 points, no more than 1 line each)
  - Cons/weaknesses (3-5 points, no more than 1 line each)
  - Follow-up work /mini-projects (3-5 points, no more than 1 line each)

- Do come to class prepared:
  - Carefully read the paper and get as much as you can out of it on your own
  - There will almost always be parts you don’t fully understand
  - This is to be expected, this is what class discussions are for

Presentations

- One of the goals of the course is for you to develop strong presentations skills
  - Don't expect to get it right the first time around
  - Expect to benefit from these skills for years to come
  - It's okay to look at other people's presentations of these papers, it's not okay to copy them verbatim
  - Expect to iterate over your slides

- Expectations:
  - A good presentation involves a lot of work
  - Presentations are to be done in teams
  - Expect to spend several hours preparing
  - Figure out how your want to subdivide the work
  - You will need to read more (optional papers) and address them in your presentation

- Office hours
  - After class
  - Have your presentation ready for a dry run one class meeting before

Presenting Technical Papers in CS

- **Presentation Zen** by Garr Reynolds

- **Presentation advice:**
  - Giving a talk by Mike Ernst
  - Advice on giving talks by Tessa Lau
  - Tips for a Good Conference Talk by Jennifer Widom
  - Hints on making presentations by Jeff Offutt
  - Some Advice on giving a Talk, by Olivier Danvy. Issues in making an oral presentation
  - Presentation advice by Armando Fox
  - Conference talk advice from Mark Hill.

from http://people.engr.ncsu.edu/txie/advice.htm

Grading

- Grading
  - Presentations
  - Paper reports
  - Class participation
  - Project (to be decided)

- Exact breakdown is TBD

Industry Perspective

- One of the features of the course will the a focus on how many of the techniques are used in the industry
- Will have several external speakers from MSR and Microsoft

Questions?

- Check out the course home page:

  http://www.cs.washington.edu/education/courses/cse504/10sp/

- Email the instructor
  - Ben Livshits
  - livshits@microsoft.com