Cybersecurity Research Seminar
Fall 2015

Patrick Tague

#1: Course Introduction

Class #1

- Very brief overview of the course
- Logistics
- Course information
- Talk about projects

Research in Cybersecurity

- In this course, we will:
  - Learn how to do research in cybersecurity, including how to
    - ...read (many) research papers
    - ...review a research paper
    - ...write a research paper
    - ...give a tech presentation
    - ...etc.
  - Take part in a government-proposed and -mentored research project

Project Topics

- A list of project topics has already been prepared by several Technical Directors from various gov't orgs
  - Problem list will be available on Blackboard shortly
  - Tech Directors are presenting their problems during the Friday class meetings (some presented last week, but were recorded and will be made available)

Goals of the Course

- Understand how research works, especially tailored to cybersecurity fields
- Learn about the state of the art in a chosen sub-field within cybersecurity
- Hands-on research experience on a project with real-world interest (w/ gov't stakeholders)
- Maybe a publication or open-source release

Multi-University Course

- This course is run collaboratively at 8 universities
  - One day per week will be “CMU Only”, and one will be a WebEx session with all participants
  - Student groups at other universities may be working on the same / similar projects
  - Students, staff, and faculty at other universities will get access to your project deliverables

Course Websites

http://mews.sv.cmu.edu/teaching/14850/f15/

https://purr.purdue.edu

Prereqs

- This course has official prereqs
  - **Information Security** (e.g., 14-741, 18-730)
  - **Applied Information Security** (14-761)
  - **Network Security** course (14-731)

- If you haven't taken all of these courses:
  - Come talk to me.
  - There's still a good chance you can take the course and do very well.

Registration

- This course has 2 concurrent sections
  - **It's important that you register for the right one**
  - **If you're in Pittsburgh, please register for section A**
  - **If you're in SV, please register for section SV**

Waitlists

- If you're currently on the waitlist:
  - Send me an email or come talk to me. Let me know which of the prereqs you have, why you want to take this course, etc.

Deliverables

- Bid
- Literature review
- Statement of Work & presentation
- Weekly dashboards
- Progress report & presentation
- Knowledge and resource sharing plan
- Final report, poster, & presentation

- Some things will be submitted to Blackboard, some to PURR, some to both

Projects

Project Topics

- Project topics can vary:
  - Research mentors from a list of gov't orgs have prepared a list of projects of current interest – these projects are available to all student groups at partner universities as well
  - In some cases, industry mentors may propose additional projects
  - Student groups can propose their own project, but the group must find their own mentor

Project Teams

- Forming teams and choosing topics:
  - These two things are not independent
  - Try to choose team members with common interests, different backgrounds, etc., **not just your friends**
  - Multiple teams at CMU cannot work on the same project, but teams at other schools may overlap
  - Teams can include students from multiple universities, if schedules and interests align

Important Dates

All important dates will be posted on the course website

How to Contact Me

- Instructor: Patrick Tague
  - **Email: tague@cmu.edu**
  - Office: B23 218
  - Phone: 650-335-2827
  - **Skype: ptague**
  - Office hours: Open-door, open-calendar, by appt
    - Public Google calendar: **http://goo.gl/FlVbRK**

Best: find times on my calendar, email to request a meeting (in person, Skype, phone, etc.)

Some Syllabus-type Details

- Class meetings:
  - Wed 11:30am-1:20pm PDT / 2:30-4:20 EDT (broadcast SV ↔ Pgh)
  - Fri 10:30am-12:20pm PDT / 1:30-2:20pm EDT (SV ↔ WebEx, Pgh ↔ WebEx)
  - B23 211 @ SV campus, Henry DEC @ Pgh campus
- Class website
  - Schedule, slides, papers, project details, …
- No textbooks

Reading Research Papers

- *You'll be reading a lot of papers!*
  - Reading research papers is not like reading textbooks, they're much more forgiving and can be read efficiently
  - **We'll have a whole class devoted to how to do this efficiently**

Important Policies

- **Academic Integrity:** all students are expected to adhere to academic integrity policies set forth by CMU, CIT, ECE, INI, etc. See
  - ECE Academic Integrity Policy (and handbook)
  - INI Student Handbook
  - College of Engineering Policies
  - CMU Academic Integrity Policy
- **My Collaboration Policy**: discussion is encouraged, but **assignments must be done individually**
  - Copying is cheating, cheating → failing grade
- **Plagiarism**: no copying, attribute ***all*** content sources
- **My Wiki Policy**: if you cite Wikipedia (or similar) pages directly, you will fail the assignment/deliverable
- **Re-grading**: on a case-by-case basis, contact me

Ethics of S&P Work

- Research, development, and experimentation with sensitive information, attack protocols, misbehavior, etc. should be performed with the utmost care

- You are expected to follow a strict ethical code, especially when dealing with potentially sensitive information

- If anything is unclear, ask before going forward

Questions?

Any questions about the course?

Feel free to contact me later.

PURR Resources

- Project lists and lots of other info will be made available on PURR throughout the semester
  - Everyone will get access to PURR
  - I'll post important things (e.g., project list on BB)
  - Presentations from Technical Directors will be available on PURR (some happened last week).

September 4:
TD Presentations