

# CS 5770: Software Vulnerabilities and Security

Spring 2017

Tamara Bonaci  
[t.bonaci@neu.edu](mailto:t.bonaci@neu.edu)



# CS 5770 – Software Vulnerabilities and Security

- **Time:** Thursdays from 6:00 – 9:00pm at **the Cornish College, LUI 202**
  - Lectures from 6:00 – 8:00pm
  - Lab from 8:00 – 9:00pm
- **Instructor:** Tamara Bonaci (t.bonaci@neu.edu)
  - **Office hours:** By appointment after 5pm
- **TA:** Rahul Mondal
  - **Office hours:** TBD
- **Course website:** lectures and reading material on Piazza
- **Course dropbox for assignment submission:** Logistics TBD
- **Course discussion board:** Piazza
- **Assignment grades:** NEU Blackboard

# What is CS 5770 Spring 2017?

- Foundational graduate security course, providing an introduction to tools, concepts and ideas of modern security research
- **Course goals:**
  - Examine major vulnerability classes that can be introduced in various software domains and levels of the software stack
  - Understand effective techniques for defending against exploitation in situ
  - Understand approaches for detecting the presence of vulnerabilities during development and deployment
  - Gain hands-on experience in attacking and defending vulnerable software

# CS 5770 Spring 2017 - Prerequisites

- Foundational graduate security course, providing an introduction to tools, concepts and ideas of modern security research
- **Expectation:** maturity in mathematics of computer science and in computer engineering:
  - A solid understanding of data structures and algorithms,
  - Ability to write programs from scratch,
  - Familiarity with command-line Unix development environment
- But eagerness to learn is the most important (and expected 😊)

# (Expected) Course Progression

- Week 1:** Course overview. Introduction to security, its goals and objectives.
- Week 2:** Cryptography – Introduction and symmetric encryption.
- Week 3:** Cryptography – Block ciphers. Public key cryptosystems.
- Week 4:** Cryptography – Hash functions and message authentication codes.
- Week 5:** Cryptography. Digital signatures. Key management.
- Week 6:** System security – Users and privileges.
- Week 7:** System security – Shells, races and sandboxing. **Midterm.**
- Week 8:** Software security – Introduction and memory corruption.
- Week 9:** Software security – Memory corruption.
- Week 10:** Software security – Vulnerability and malware analysis.
- Week 11:** Network security – Link, network and transport layer attacks.
- Week 12:** Web security – SSL/TLS. Basic Web security model.
- Week 13:** Web security – Web application security (XSS, SQL injection, session management).
- Week 14:** Privacy and anonymity.
- Week 15:** Final project presentations.

# Course Logistic

- **Course will be graded based upon:**
  - Midterm – 15% of the grade
  - In-class activities – 10% of the grade
  - Homework – 25% of the grade
  - Lab: 20% of the grade
  - Project – 30% of the grade

# Course Logistic - Midterm

- Midterm – 15% of the grade
- In the seventh week of the semester (Feb 23)  
from 6-7pm
- Covering material related to cryptography

# Course Logistic – Homework

- **Five HWs** related to cryptography material
- A mix of written questions and coding/simulation problems
- You are welcome to code/simulate using any software tool you prefer (e.g., Matlab, Mathematica, Python), but please **submit all your code and simulation models**

# Course Logistic – In-class Activities

- Activities done in class
- Graded on a scale 0-2, where:
  - 0 - missed or irrelevant in-class activity,
  - 1 - relevant answers submitted, and
  - 2 - good and interesting answers submitted, and/or interesting discussion in class
- There could possibly be an in-class activity every week, but we will take your **seven best scores** into account

# Course Logistics - Labs

- **Five labs** through the quarter
- At least two lab sessions to work on every lab assignment
- Encouraged to work in groups of two people, ***but you can work alone***
- Each lab will be graded based upon deliverables, which will be defined in each individual lab assignment
- **First lab – in the third week, January 26**

# Course Logistics - Project

- You will choose a topic related to any area of security and privacy (including those not directly covered in this course)
- Individual or team work (up to 3 members)
  - Group project should reflect a multi-person effort
- **Several milestones:**
  - Project proposal (in the 5<sup>th</sup> week)
  - Progress report (in the 11<sup>th</sup> week)
  - Final report (in the 15<sup>th</sup> week)
  - Project presentation (in the finals week)

# Course Logistics - Final Exam

- **Good news** – no final exam
- Instead - project presentations during finals week

# Course Material

- **No textbook**
- **Good additional material:**
  - N. Daswani, C. Kern, and A. Kesavan, *Foundations of Security, What Every Programmer Needs to Know*, Apress, 2007
  - C. Kaufman, R. Perlman, and M. Speciner, *Network Security: Private Communication in a Public World*, Prentice Hall, 2002
  - D. Stinson, *Cryptography Theory and Practice, Third Edition*, CRC Press, 2006
  - W. Stallings, *Cryptography and Network Security, Principles and Practice, 5th Edition*, Prentice Hall, 2006
  - B. Schneier, *Applied Cryptography, Protocols, Algorithms and Source Code in C*, Wiley, 1996
  - Menezes, P. Van Oorschot, S. Vanstone, *Handbook of Applied Cryptography* (available online)

# Course Material

- **If you can, try to attend lectures because:**
  - Lectures will likely cover more than provided in lecture notes, and the provided references
  - Lectures will focus on “big-picture” principles and ideas
  - Your colleagues will likely start interesting discussions during lectures
  - In-class activities and discussions they will start

# Late Turn in Policy

- All assignments are due **by 11:59pm on the assigned date**
- Late assignments will (generally) be dropped 20% per calendar day, and no submissions will be accepted after 5 days
- If you have a meaningful reason for delay (e.g., illness) – ***come and talk to us***
- **Exception to the late turn in policy:** final project presentation have to be turned in on time

# Your Questions

