About this course

This course will provide students with an understanding of the theories, tools, and techniques to identify, exploit, and mitigate software security vulnerabilities in the network, binary, and web levels. Students will study, in-depth, vulnerability classes to understand how to protect software and how to secure software.

We will also cover the history of software security, and ethical considerations. This course will focus on a hands-on approach: In addition to understanding vulnerability classes, students will be required to identify and exploit vulnerabilities.

Specific topics covered include:

- History of Software Security
- Software Security Ethics
- Network Security
- Application Security
- Web Security

Technologies covered include:

- C
- x86-64 Assembly
- HTTP
- HTML
- JavaScript
- SQL
- Scripting languages

Required prior knowledge and skills

- This course will be very challenging, and students are expected to learn the necessary technologies on their own time.
- C/C++ Programming
- Scripting language programming (Something similar to Python, Ruby, or PHP)
- Computer Networking
  - Specifically Ethernet, ARP, Routing, IP Addresses, Fragmentation, ICMP, UDP, and TCP
- Compilers
  - Linkers
  - ELF
- Operating Systems
- Computer Architecture
  - Specifically x86-64 assembly
  - System calls
Learning Outcomes

Learners completing this course will be able to:

- Explain the history of security vulnerabilities.
- Differentiate between ethical and unethical behavior in regards to identifying and exploiting security vulnerabilities.
- Demonstrate local network-level security attacks.
- Evaluate a local networking situation to determine appropriate attacks and the corresponding defenses.
- Analyze a binary application, describe its behavior, identify security vulnerabilities, and develop an exploit.
- Analyze a web application, understand its behavior, identify security vulnerabilities, and develop an exploit.

Estimated Workload/Time Commitment Per Week

15 - 20 hours per week

Technology Requirements

Hardware - Computer

Software and Other (programs, platforms, services, etc.)

- Linux Operating System
  - Possibly running in Virtual Machine
- SSH Client (Putty for Windows)

Creator

Adam Doupé, Ph.D.

Dr. Adam Doupé is an Assistant Professor in the School of Computing, Informatics, and Decision Systems Engineering at Arizona State University and is the Associate Director of the Center for Cybersecurity and Digital Forensics in the Global Security Initiate at Arizona State University. Dr. Doupé was awarded the Top 5% Faculty Teaching Award for the Fulton Schools of Engineering at ASU for 2016, the Fulton Schools of Engineering Best Teacher Award in 2017 and 2018, the Fulton Schools of Engineering Outstanding Assistant Professor Award in 2017, and the NSF CAREER award in 2017. Dr. Doupé has co-authored over 30 peer-reviewed scholarly publications and served on program committees of well-known international security conferences. As a founding member of the Order of the Overflow, Dr. Doupé has organized the DEF CON Capture The Flag competition since 2018.