Advanced Computer Security Program

The program consists of 6 courses. These 6 courses will be covered in 6 months. 3 courses will have project work.
Every course will be ending with a final assessment. This document will guide you through the modules and sub topics covered in each course.

Course 1:

Foundations for Information Security:

Motivation
- Introduction to Motivation

Security Goals
- Holistic Security
- Authentication
- Authorization
- Confidentiality and Data Integrity
- Accountability and Availability
- Non-Repudiation

Attacks
- Common Attacks Pt. 1
- Common Attacks Pt. 2

Attacker Life Cycle
- Introduction
- Explainer Video
- Life Cycle Pt 1,2,3

Mega Breaches
- Introduction
- 2018 - Aadhar, Exactis, Under Armour
- 2017 - Dun and Bradstreet, River City Media, WannaCry, Equifax
- 2016 - Yahoo
- 2013-14 - JPMorganChase, Target
- Defense in Depth
- Predicting Breaches

Security Design Principles
- Simple Web Server(SWS)
- Principle of Least Privilege
- Defense-in-Depth
- Securing the Weakest Link
- Fail-Safe Stance
- Secure by Default

- Simplicity and Usability

Secure System Design

- Threat Modeling
- Designing-In Security
- Convenience vs Security
- Secure SDLC Pt. 1,2
- Security by Obscurity
- Open vs Closed Source
- A Game of Economics

Client State Manipulation

- CSM Example Attacks Pt. 1,2
- POST vs GET
- Cookies
- Javascript
- Ajax
- Forceful Browsing
- Redirects
- File Upload Security

Command Injection

- Explainer Video
- CI Example Attacks Pt. 1,2
- Blacklisting
- Whitelisting
- Escaping
- Second-Order Attacks
- Prepared Statements and Bind Variables
- Impact Mitigation
- Other Command Injection

Buffer Overflows

- Anatomy of Buffer Overflow Attack Pt. 1,2
- Explainer Video
- Safe String Libraries
- StackGuard

Course 2:

Exploiting and Protecting Web Applications:

Injection & Cross-Domain Attacks

- Command Injection
- Mitigation of SQL Injection
- Advanced Injection Commands
- XSS

- More XSS and Mitigation
- XSRF
- XSSI
- HTML 5 Security Issues

Web Security: HTTPS and the lock icon

- Introduction to Web Security
- HTTPS in the browser
- Problems with HTTPS and the lock icon

Web Security: Session Management

- Introduction
- Cookie Protocol Problems
- Session Management
- Session Hijacking

Web Background and Browser Security Model

- Introduction
- HTTP
- Rendering Content
- Isolation
- Navigation
- Communication
- Client State
- ClickJacking
- Frame Busting

Course 3:

Using Cryptography Correctly:

Introduction to Cryptography

Symmetric Encryption

- Brief Overview
- Stream Ciphers
- Block Ciphers
- Using Block Ciphers
- Message Integrity
- Authenticated Encryption

Public Key Cryptography

- Concepts
- Digital Signatures
- Certificates
- Key Exchange: TLS
- Diffie Helman

Identification Protocols

- Authenticating against Users
- Security against Direct Attacks
- Security against Eavesdropping Attacks
- Security against Active Attacks
- Authentication Session - Industry Expert

Advance Primitives

- Brief Overview
- Protocols
- Privacy
- Broadcast Encryption
- Quantum Computing

Course 4:

Network Security

Internet Protocols

- Internet Infrastructure & Protocols
- Routing Security
- Domain Name System

Defenses & Tools

- Protecting Network Connections
- Standard Defenses for Local Networks
- Network Infrastructure Protocols

Denial of Service Attacks

- Handling Unwanted Traffic
- DOS Mitigation

Course 5:

Writing Secure Code:

Control Hijacking Attacks

- Module Overview
- Basic Control Hijacking
- Heap Overflows
- More Control Hijacking
- Format String Bugs
- Use After Free
- Mixing Data & Control
- Platform Defences
- Hardening the Executable
- CFI and CFG

Static & Dynamic Analysis, Fuzzing

- Introduction
- Comparison - Static & Dynamic Analysis
- Static Analysis Principles
- Static Analysis for Security
- Dynamic and Black Box - Tools
- Fuzzing Methods & Examples

Language-Based Security

- Managed Code
- Rust Language

Isolation

- The Confinement Principle
- System Call Interposition
- Isolation via Virtual Machines
- SubVerting VM Isolation
- Software Fault Isolation

Course 6:

Emerging Threats & Defences:

Dealing with a Data Breach

- Why Worry about Data Breaches?
- How to reduce the possibility of a Breach?
- What is considered a Breach?
- Breach Response Planning
- During and After a Breach

Attacks and Defenses

- Attacks and Techniques
- Compression Attacks
- Password Breaches
- Certificates on the Web
- Intel SGX
- Abusing Mobile Sensors
- New Age Security Risk

Cloud Security

- Cloud Architecture, Service Levels, Trust, and Threats
- Software as a Service
- Computing on Encrypted Data
- Trusted Computing

Privacy Concerns

- Privacy and Anonymity
- Network Traffic Analysis
- Web Tracking and Defenses

**This curriculum is not final and is subject to change at any point of time*