CYBERSECURITY FOR TECHNICAL LEADERS SCHEDULE

Getting Started

40 min

Start your learning journey by completing an entrance survey and become familiar with the platform and module design.

- **Entrance survey**
- **Review the Course Guide**
- **Meet the Course Team**
- **Discussion Forum: Introduce Yourself**
- **Review of Software Requirements and Accessibility**

WEEK 1 The Modern Cybersecurity Landscape

4-6 hrs

In week one, you will be introduced to the modern cybersecurity landscape. You will also investigate four security stories and their implications along with software security. You will assess different types of cybersecurity attacks and different took and approaches to ensure system security.

- **Cyber Attacks**
- **What Makes Security Hard?**
- **Modern Cybersecurity Challenge: Security Philosophy**
- **Four Software Security Stories and Their Lessons**
- **Two-Factor Authentication**
- **Log4Shell**
- **Binance Hack**
- **Software Security and Dangerous Security Vulnerabilities**
- **Features of Memory Error**
- **SQL Injection Attack**
- **Cross-Site Scripting Attack**
- **Preventing the Next Vulnerability**
- **Undefined Behavior of Systems**

OPTIONAL TECHNICAL CONCENTRATION - FORMAL METHODS

- **Formal Methods for Security**
- **What Is a Specification?**
- **Formal Specifications**
- **More Examples of Kinds of Module Verified**
- **Formal Verification Techniques**
- **Tools to Lift the Limitations**
- **Symbolic Model Checking**
- **Hoare Logic-Style Verifiers**
- **Interactive Proof Assistants**
- **Styles of Formal Verification**
- **How to Improve Security System**
- **Lessons from Formal Methods for Security**
- **Case Study: Fiat Cryptography**

WEEK 2 | Hardware Security | 4-6 hrs

In week two, you will be introduced to hardware security and discuss how physical system design can prevent exploitation of system vulnerabilities. You will also investigate how hardware and software systems work together to mitigate cybersecurity attacks strengthening the overall security of a system.

- **Differences between Software TCB and Hardware TCB**
- **Hardware Trust**
- **Security Goals**
- **Confidentiality**
- **Integrity and Identification**
- **Different Hardware Attack Threat Models**
- **Power Analysis Attack**
- **Timing Side-channel Attacks and Defenses**
- **RowHammer**
- **Hardware-based Trusted Execution Environment**
- **Intel SGX Security Mechanisms**
- **Case Study: Spectre and Meltdown**
- **Speculative Execution Attack**

OPTIONAL TECHNICAL CONCENTRATION - HARDWARE SECURITY DEEP DIVE

- Introduction to Hardware Security
- What Can Hardware Do For Security?
- Advanced Encryption Standard
- Cryptography Algorithms: Examples
- Accelerating Cryptography: Fully Homomorphic Encryption
- Example Application: Private Inference in the Cloud
- Secure Computing Accelerator
- Encryption and Data Types
- FHE Operations
- Multiplying Polynomials
- Rough Shape of FHE Programs
- Architectural Characteristics of FHE
- F1 Processor
- Leveled FHE
- Bootstrap vs. Leveled FHE
- CraterLake Architecture
- CraterLake Vector Datapath
- Scaling the Vector Datapath with Transposes
- Verifiable Computation
- Similarities and Differences of VC and FHE Computations
- Using CraterLake for VC
- Structure of a Lattice-based VC Scheme
- Private Information Retrieval
- Private Information Retrieval: Trade-Offs
- What Next: FHE + VC for Privacy + Integrity

WEEK 3 | Mitigating Cybersecurity Attacks & the Fundamentals of Cryptography | 4-6 hrs

In week three, you will delve into the fundamental principles of cryptography and user authentication, essential components of cybersecurity. It begins with an exploration of cryptographic techniques, including private key encryption, public key encryption, and digital signatures, highlighting their importance in secure communication.

- Secure Communication Problem
- Private-Key Encryption
- The One-time Pad Construction
- Key Tool: A Pseudo-Random Function
- Public Key Encryption
- RSA Encryption
- The Problem with Active Adversaries
- Digital Signatures
- Secure Communication in Practice
- User Authentication Using Passwords
- Entropy
- Passwords
- Hashing and Salting
- User Authentication from a Computer
- Network Attackers
- Techniques to Build the Authentication System
- Universal 2nd Factor (U2F)
- Authenticating with Biometrics
- Meta Techniques for Authentication
- Lifecycle of User Accounts

OPTIONAL TECHNICAL CONCENTRATION - CRYPTOGRAPHIC TECHNIQUES FOR SECURE COMPUTATION

- Collaboration is Key
- The Paint Point
- Secret Sharing
- Threshold Secret Sharing
- Secure Collaboration with Secret Sharing: The Big Picture
- Secret Sharing
- Homomorphic Encryption (HE)
- Post-Quantum Security
- How Fast Is Homomorphic Encryption?

WEEK 4 | Cloud Security | 4-6 hrs

In week four, you will be given a comprehensive overview of cloud computing and its implications for cybersecurity. It begins by defining cloud computing and exploring the current landscape, then delves into the cloud system stack, from hardware design to application development, highlighting recent trends in both areas.

- Data Centers
- The Cloud System Stack
- Cluster Managers
- Monitoring Tools
- Datacenter Applications
- Performance Metrics
- Tail Latency
- Performance Variability
- Reducing Variability
- Reliability and Availability
- Hardware and Software Complexity Explosion
- Cloud Accelerators
- Emerging Cloud Applications

OPTIONAL TECHNICAL CONCENTRATION - ISOLATION

- Security Condition for Isolation: Integrity
- Flip Property of Integrity: Confidentiality
- Confidentiality Property: Non-Interference
- Non-Interference Is Hard to Achieve: Example
- Implementation and Challenges of Isolation
- How Isolation Is Implemented on OS/VM
- What Is the Operation Performed?
- Language Runtime Isolation
- How Web Assembly Performed High on Real Hardware?

- Security Vulnerability At The Hardware Layer
- Side-Channel Attack
- Hardware Side-Channel Defenses
- Hardware Accelerator Vulnerabilities
- Scheduling Or Contention-based Attacks
- Defenses for Contention-based Attacks
- Denial Service Attack and Defences

WEEK 5 Machine Learning for Cybersecurity 4-6 hrs

In week five, you will investigate the cybersecurity challenges associated with machine learning, focusing on both supervised and unsupervised learning models. It explores the vulnerabilities of these models to cyberattacks and provides strategies for protecting the data used to train them.

- How Data is Used in Machine Learning?
- Cybersecurity Issues in Machine Learning
- Ensuring Data Can Not Be Stolen for Supervised Learning
- Distillation with Neuro Tangent Kernel
- Neural Network Gaussian Process
- Random Feature Approximation Distillation
- Data Distillation and Privacy
- Ensuring Data Privacy for Unsupervised Learning

WEEK 6 Security Vulnerability and Threat Actors of the Internet 4-6 hrs

The sixth week of the course explores the foundational vulnerabilities of the internet's packet carriage layer, highlighting the systemic issues that affect its security. It delves into key systems such as addressing, routing, naming, and cryptography, explaining their inherent weaknesses and the challenges in mitigating them.

- The Persistent Insecurities of the Internet Infrastructure
- Internet Key Systems and Their Persistent Vulnerabilities
- Border Gateway Protocol (BGP)
- Vulnerability: Misaligned Incentives that Lead to Hijacking
- Detecting False Announcements
- Domain Name System (DNS)

- Certificate Authority System
- Denial of Service Attacks
- Reduction of Vulnerability Harm by Enterprise
- Distributed Touch Points
- Migration from Browser to App
- Case Study: Hijacking Amazon
- Lessons from Amazon Hijacks
- Introduction: Cybersecurity Risk
- I.A. Government Role: Laws
- Dilemma: Ethical Hacking to Uncover Bugs
- Some Other I.A. Government Role: Laws
- Laws: State Data Security and Data Breach
- Enforcing the Law
- Coordination and Threat Sharing
- NIST Cybersecurity Framework
- Community Collaboration
- Enterprise Strategies and Roles : Chief Information
- Security Officer (CISO) and Chief Risk Officer
- Privacy in Cybersecurity
- Modern Privacy Begins in the Mainframe Era
- Sector-specific Privacy Laws
- The Privacy-Security Nexus
- Organizational Roles
- Privacy Challenges and Trade-offs

WEEK 7 | Measuring Cyber Risk with MIT's SCRAM Platform | 4-6 hrs

The seventh week of the course provides a comprehensive overview of measuring cyber risk, emphasizing its importance in the broader context of cybersecurity and data protection. It begins with an introduction to cyber risk measurement and its applications, followed by an exploration of new cryptographic tools that enable secure data aggregation.

- Introduction: Measuring Cyber Risk
- Economy and Society
- Modeling and Addressing Risk
- Transfer the Risk
- Reduce the Risk
- Applying the Lessons to Cyber Risk Calculations
- Why Firms Hesitate to Share Data
- The Solution: SCRAM
- Results: Sophisticated Firms and Municipalities

WEEK 8 | AI and Cybersecurity | 4-6 hrs

The eighth week of the course will center In this week, the focus is on the security of applications built using large language models (LLMs), such as OpenAI's ChatGPT. This innovative approach offers significant potential but also introduces new security challenges.

- **Introduction to Large Language Models?**
- **How Will Large Language Models Impact Cybersecurity?**
- **LLMs: Summary**
- **Security of Applications Build Using LLMs: A Different Way to Build Interfaces**
- **Demo: Pizza Delivery App Through Prompting**
- **Malicious User Adding Unwanted Functionality to an Application: Example**
- **Things to Keep In Mind**

Course Wrap-Up

- **Review of Key Concepts**
- **Course Summary and Next Steps**
- **Final Reflection**