# Advanced Cybersecurity

PROGRAM

Stanford | ONLINE

# Quick Facts

**DELIVERY:** Online, Self-Paced

**HOURS TO COMPLETE:** 6 -12 hours per course I 40 hours to earn the certificate

**TOTAL COURSES:** Complete any 5 courses to earn a certificate

**PRICING:** $2,725 Program All-Access Plan or $545 per course

**FLEXIBLE PAYMENT OPTIONS:** Pay for your All-Access Plan over time with three interest-free payments

**CERTIFICATE EARNED:** Stanford Certificate of Achievement in Advanced Cybersecurity

**LEARNING EXPERIENCE INCLUDES**

- Online, self-paced lectures
- Industry examples and interviews
- Some courses include interactive lab environment
- Knowledge checks and engagement exercises


# Overview

More than 10,000 data breaches have occurred in the past 15 years, with an average of more than one breach per day. While these breaches varied in scope and disruption, most had one thing in common: they were preventable.

This program will equip you with the knowledge and skills to safeguard your organization in an increasingly digital world. Guided by leading Stanford faculty and industry experts from top companies like Google and Symantec, you will be stepping into the forefront of cybersecurity. You'll learn to protect networks and cloud environments, secure electronic assets, and design robust systems to prevent attacks.

Through hands-on exercises, you'll identify vulnerabilities, ensure customer privacy, and uphold regulatory compliance. By mastering these critical skills, you'll be prepared to defend against cyber threats and enhance your organization's reputation and security.

- Design and implement solutions that safeguard data and information from breaches and disruptions.
- Identify security gaps in your organization and build resilient systems using industry-proven cybersecurity strategies.
- Proactively detect, prevent, and defend against cyber threats to keep your data secure.
- Strengthen code security by applying proven secure coding principles designed to uncover and fix first-party and third-party software vulnerabilities.
- Implement robust data protection strategies, including identity and access management, to secure information across all applications, platforms, and cloud environments.
- Develop company policies that ensure regulatory compliance while prioritizing customer data protection.

**LEARN MORE**

# Academic Directors and Teaching Team

**John Mitchell**
*Mary and Gordon Crary Family Professor Computer Science*

**Dan Boneh**
*Professor Computer Science and Electrical Engineering*

**Neil Daswani**
*Cybersecurity Executive, Investor, Author, and Educator*

**Zakir Durumeric**
*Assistant Professor Computer Science*

> "Having recently passed the CISSP, I found the course material and instruction to be comprehensive and in sufficient depth. The instructors are world class, guest speakers are respected and practical, and the delivery is flawless from exam execution to later posting your credentials on LinkedIn. Highly recommended!
>
> **Lisa C.**
> *Consultant*

> "Stanford's Advanced Cybersecurity Program delivers a comprehensive and high-quality learning experience, blending foundational principles with real-world applications. The content is expertly crafted by and industry leaders, making it a valuable investment for professionals seeking to enhance their cybersecurity skills and apply them effectively in today's evolving threat landscape.
>
> **Madhavi V.,**
> *Digital Transformation Leader, General Motors*

# WHY STANFORD'S ADVANCED CYBERSECURITY PROGRAM?

**Learn from some of Stanford University's cybersecurity experts.** Stanford's Advanced Cybersecurity Program offers an unparalleled opportunity to learn from esteemed faculty and industry professionals at the forefront of cybersecurity. With instructors from renowned organizations such as Google, LinkedIn, Symantec, LifeLock, OpenAI, and Anthropic, you'll gain insights grounded in both cutting-edge research and real-world application. This program's specialized instruction ensures a comprehensive understanding of the cybersecurity landscape, equipping you with the knowledge to tackle current and emerging threats.

**Acquire practical cybersecurity skills through hands-on learning.** Our curriculum emphasizes a holistic approach to cybersecurity, blending technical proficiency with strategic and organizational insights. You'll engage in useful exercises designed to develop solutions that protect information, data, and communications from unauthorized access and corruption. Courses cover a range of topics, including identifying organizational vulnerabilities, applying secure coding principles, and implementing effective identity and access management strategies. This style of hands-on learning ensures you're well-prepared to anticipate and mitigate cyber threats across various applications, platforms, and cloud environments.

**Benefit from flexible learning tailored to your schedule.** Recognizing the demands of both professional and personal commitments, our program offers a fully self-paced online learning experience. Each course provides 60 days of access to materials, allowing you to watch lectures, complete exercises, and engage with the content at your convenience. For those seeking a more extensive experience, the All-Access Plan offers 365 days of access to all courses in the program, enabling you to learn at a pace that fits your lifestyle. This flexible format ensures that advancing your cybersecurity expertise can seamlessly integrate into your daily routine.

**Earn a recognized credential from Stanford University.** Upon successfully completing five courses, you'll receive a Stanford Certificate of Achievement in Advanced Cybersecurity. This digital certificate, verified on the blockchain, allows you to showcase your accomplishment on professional platforms like LinkedIn, verify your credentials with employers, and communicate the depth of your expertise in the cybersecurity domain.

# Who Is This Program For?

This program is designed for cybersecurity professionals, IT leaders, and those aspiring to top-tier cybersecurity roles. Our learners are motivated to deepen their understanding of advanced cybersecurity threats, defense strategies, and emerging technologies. They are seeking to develop the skills and knowledge necessary to protect organizations from complex cyberattacks and become leaders in the field of cybersecurity. Our learners include Software Engineers, Security/Privacy Engineers, Analysts, Security Architects, Product/Program Managers, CISOs.

Almost 3,000 people have completed the program, across 74 countries.

**TOP 10 COUNTRIES**

United States

Canada

India

United Kingdom

Australia

Mexico

Singapore

Thailand

Brazil

Germany

**TOP SECURITY SECTORS**

Application Security

Security Architecture

Infrastructure Security

Network Security

Platform Security

Vulnerability Management

Threat Intelligence

Privacy

Incident Response

DevOps Security

**TOP JOB FUNCTIONS**

Software Engineer

Security/Privacy Engineer

Analyst

Security Architect

Consultant

Product/Program Manager

CISO and other cybersecurity leaders

# Foundations of Information Security

In an era marked by a relentless surge in cyberattacks, understanding the intricacies of cybersecurity has never been more critical. This course is designed to provide you with a comprehensive knowledge of core cybersecurity principles and techniques, essential for effectively countering the ever-evolving landscape of cyber threats.

This course takes a comprehensive dive into cybersecurity, covering aspects like the motivations behind cyber threats, the attacker lifecycle, and major breaches. It also covers applying secure design principles and techniques, mastering foundational cryptography, and exploring real-world cryptographic tools.

By course completion, you will be well-versed in essential cybersecurity principles and techniques, which will empower you to design and implement more secure solutions and strengthen your own personal digital environment. Additionally, you will benefit from real-world insights shared by industry experts like Parisa Tabriz (Google) and Mukul Khullar (LinkedIn).

- Understand the motivations behind cyber threats and common attack strategies.
- Learn to apply secure design principles and techniques for architecting secure systems.
- Explore foundational principles of cryptography, including critical concepts such as block ciphers and authenticated encryption.
- Discover cryptography's significance in cybersecurity and make sense of concepts such as public key encryption, digital signatures, transport layer security (TLS), and other modern cryptographic tools.
- Assess compliance standards and initiate and manage an effective information security program within any organization.

**INSTRUCTORS**

**Dan Boneh**
*Professor Computer Science and Electrical Engineering*

**Neil Daswani**
*Cybersecurity Executive, Investor, Author, and Educator*

**ENROLL NOW**

## COURSE OUTLINE

**→ Motivation**
Uncover the motivations driving both attacker and defender teams, and gain invaluable insights into key security goals.

**→ Security Design**
Discover the secrets to core security design principles, including the principles of least privilege, securing the weakest link, and the trade-offs between simplicity and usability.

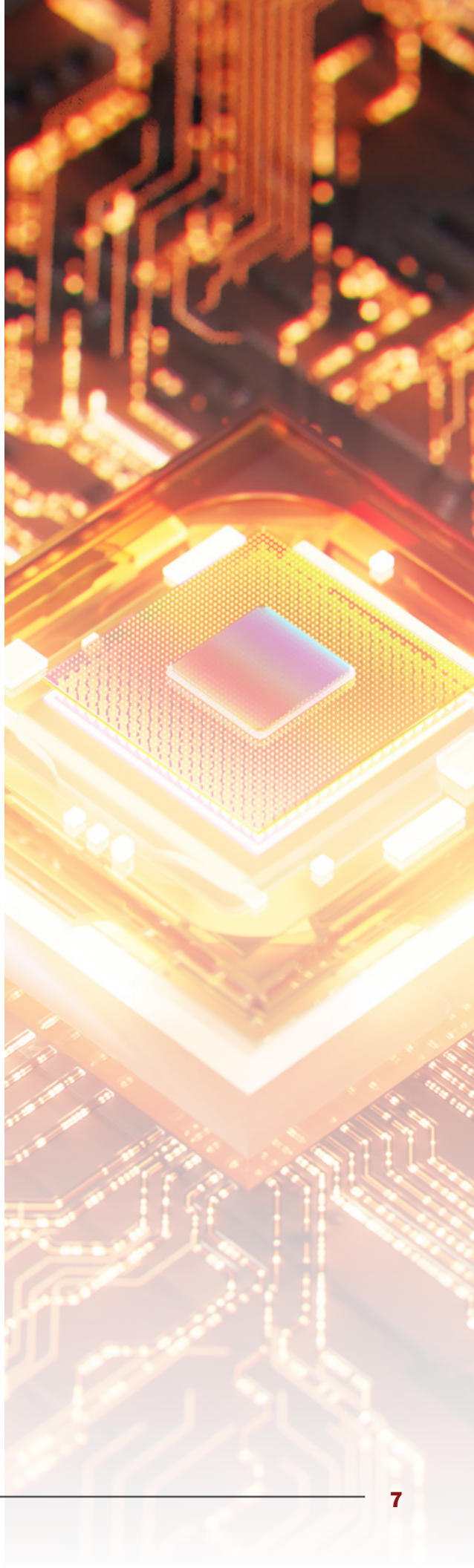
**→ Introduction to Cryptography**
Receive guidance on the principles of cryptography, equipping you with the knowledge to safeguard your computer systems effectively.

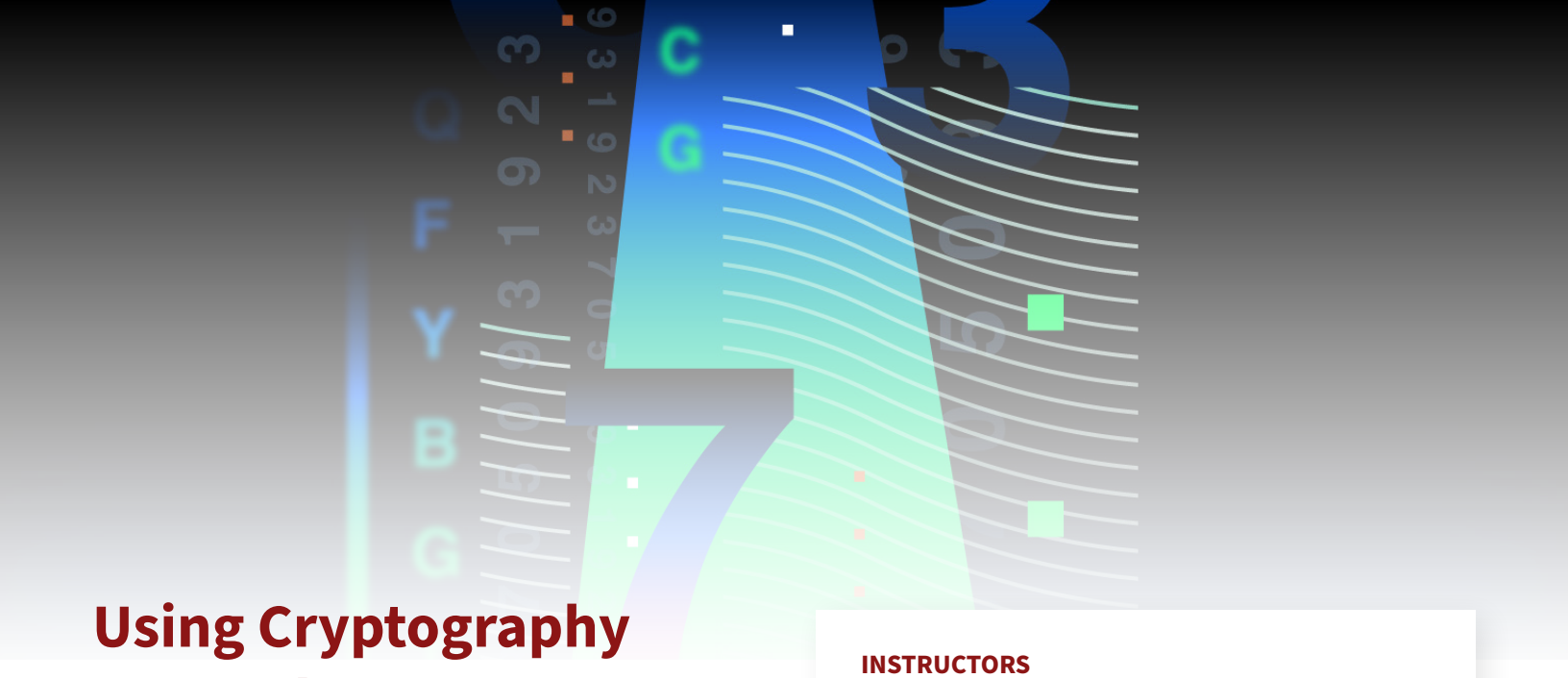
**→ Cryptography in the Field**
Discover the transformative power of cryptography and explore its real-world implementations in digital signatures, TLS session setups, and public key encryption. Learn about cryptography's pivotal role in designing secure systems.

**→ Foundations in Practice**
Learn about common compliance standards and how to integrate this vital knowledge into building and nurturing a successful security program at your organization.

**→ Featured industry experts include:**

- Vint Cerf, Co-Father of the Internet, Google Inc.
- Parisa Tabriz, Engineering Director, Google
- Mike Duff, former Chief Information Security Officer, Stanford University
- Dina Mathers, former Senior Director of Information Security, LifeLock, a Symantec Company
- Mukul Khullar, former Staff Information Security Engineer, LinkedIn





# Using Cryptography Correctly

Cryptographic primitives are effective tools that can help achieve various security goals. However, programs that use cryptography can often be fragile, and simple programming errors can result in large security "holes." Even worse, a company can come away with a false sense of security if their applications use cryptography—due to simple programming errors in how the cryptography is used, their applications could be just as or more vulnerable to attack, but the company may think that it is secure due to the use of cryptography.

This course covers how to use cryptography correctly and teaches programmers how to avoid many common mistakes that result in gaping security holes.

- Understand how to protect your organization's information and communications using symmetric encryption, public keys, and identification protocols.
- Learn to encrypt your data with block ciphers.
- Ensure message confidentiality and integrity with authenticated encryption.
- Authenticate users through appropriate identification protocols and passwords.
- Prevent attacks using challenge-response protocols.

**INSTRUCTORS**

**Dan Boneh**
*Professor Computer Science and Electrical Engineering*

**ENROLL NOW**

## COURSE OUTLINE

- **Symmetric Encryption**
  Master the fundamentals of symmetric encryption. Learn how one-time pad, stream, and block ciphers work, and ensure data security with authenticated encryption.

- **Public-Key Cryptography**
  Uncover the principles of asymmetric encryption, key exchange, and digital signatures. Gain an understanding of how public and private keys work together to secure communications, authenticate users, and protect data integrity.

- **Identification Protocols**
  Learn about secure user authentication and defending against direct, eavesdropping, and active attacks. Explore how to verify identities safely and protect systems from unauthorized access and manipulation.

- **Advanced Primitives**
  Examine cryptographic protocols for secure interactions and privacy-preserving techniques to protect sensitive data.

# Writing Secure Code

A company may have millions of lines of existing code and tens of millions of dollars of investment in its business based on those lines of code. It is not reasonable to expect that the applications that those millions of lines of code support can be redesigned securely from scratch in a cost-effective fashion.

This course covers intermediate and advanced techniques that systems and applications programmers can use to write new code securely, as well as to find and mitigate vulnerabilities in existing code. In addition to covering threats, we will discuss tools and techniques that can be used to secure large amounts of legacy code.

- Differentiate between programming languages and their impacts on code development.
- Find vulnerabilities in your code by performing static and dynamic analysis.
- Eliminate insecure code with practical tools, such as fuzzing.
- Understand, prevent, and mitigate control hijacking attacks.
- Prevent compromise of your entire system by deploying isolation and sandboxing.

## INSTRUCTORS

**Dan Boneh**
*Professor Computer Science and Electrical Engineering*

**John Mitchell**
*Mary and Gordon Crary Family Professor, Computer Science*

ENROLL NOW

## COURSE OUTLINE

- **Control Hijacking Attacks**
  Explore basic control hijacking, heap overflows, format string bugs, and use-after-free exploits, while gaining an understanding of how attackers exploit weaknesses to take control of applications.

- **Static Analysis and Dynamic Analysis, Fuzzing**
  Discover how to uncover vulnerabilities before attackers do. Learn the key differences between static and dynamic analysis, explore static analysis principles for security, and work with dynamic black-box testing tools to identify weaknesses in real time.

- **Language-Based Security**
  Find out how programming languages impact software security. Examine the vulnerabilities of C, the benefits of managed code, and how languages like Rust help prevent common security flaws.

- **Isolation**
  Understanding how to contain threats and limit security breaches is a valuable skill. Gain valuable insight into confinement principles, how to enforce security with system call interpositions, and how virtual machines (VMs) provide isolation.

# Exploiting and Protecting Web Applications

Web applications are vulnerable to many types of attacks that traditional client-server applications are not as susceptible to. These vulnerabilities, over the past several years, have resulted in attacks that have exposed companies to monetary losses and reputational damage.

This course covers these vulnerabilities, how attacks are constructed based on them, and techniques that can be used to mitigate such vulnerabilities. Example web vulnerabilities covered in this course include: client-state manipulation, cookie-based attacks, SQL injection, cross-domain attacks (XSS, XSRF, XSSI), DNS rebinding, timing attacks, user tracking, and HTTP header injection. In addition, this course covers security issues that can arise in Web 2.0 and HTML5 applications that take advantage of heavy use of JavaScript, AJAX, mash-ups, and HTML5 extensions.

- Discover how to prevent attacks on your web applications with input validation, output escaping, signatures, message authentication codes, and frame busting.
- Identify, prevent, and mitigate command injection attacks, such as SQL injections.
- Differentiate between cross-site scripting attacks and cross-site request forgeries, and the appropriate prevention and mitigation methods.
- Protect your websites by eliminating insecure HTML5 inputs.
- Allow users to browse your website safely using correct and secure integrated HTTPS.
- Ward off theft of your clients' data by correctly setting cookies and session tokens.

## INSTRUCTORS

**Dan Boneh**
*Professor Computer Science and Electrical Engineering*

**Neil Daswani**
*Cybersecurity Executive, Investor, Author, and Educator*

**John Mitchell**
*Mary and Gordon Crary Family Professor, Computer Science*

**ENROLL NOW**

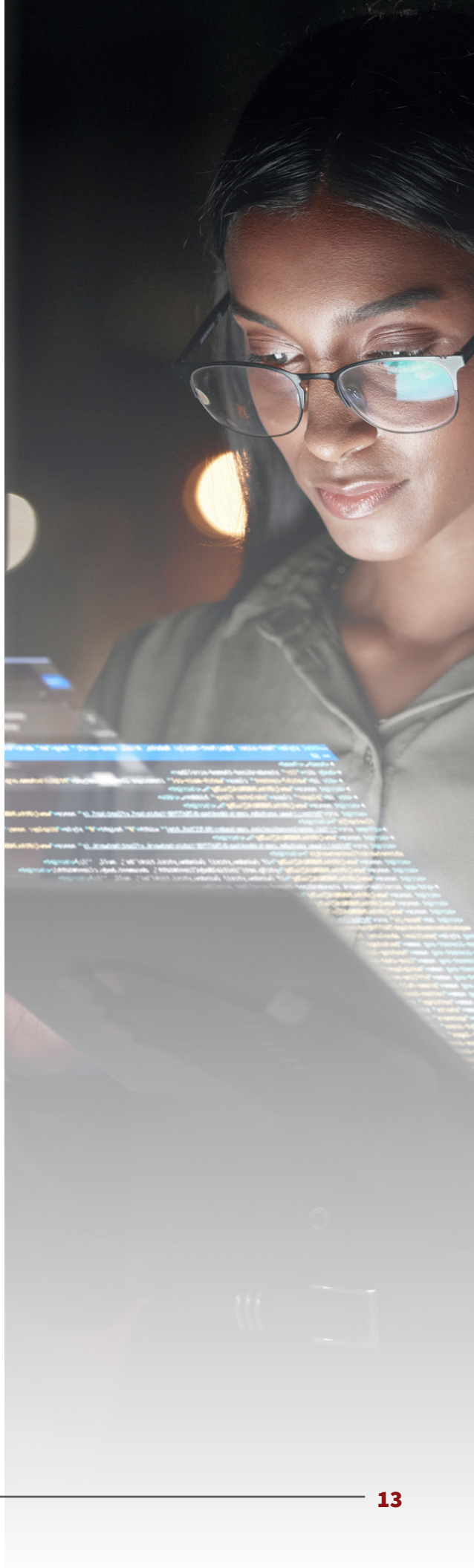
## COURSE OUTLINE

- **Injection and Cross-Domain Attacks**
  Discover command injection techniques, dive into the mitigation of SQL injection, and learn about the best practices for alleviating these vulnerabilities.

- **Web Security: HTTPS and the lock icon**
  Receive a breakdown of how HTTPS integrates with browsers, why it's essential for login pages, and how to properly upgrade from HTTP to HTTPS to maintain security and user trust.

- **Web Security: Session Managements**
  Explore the risks, vulnerabilities, and best practices of user authentication, and learn why weak session management leaves applications open to hijacking and attacks.

- **Web Background and the Browser Security Model**
  Understand how browsers handle web content by exploring the browser security model, including rendering mechanisms, isolation techniques, and secure navigation practices.



# Network Security

In today's interconnected environment, the integrity and security of computer networks are essential. Your organization's data, whether it includes sensitive customer information, financial transactions, or confidential business plans, is a cornerstone of your operations. Ensuring the protection and privacy of this data isn't optional; it's imperative.

Throughout this course, you will develop a comprehensive understanding of network security essentials, ranging from core networking concepts to advanced defense strategies. You will explore critical topics like secure data transmission, Domain Name System (DNS) protection, Denial-of-Service (DoS) attack mitigation, advanced network defenses such as firewalls, and strategies for safeguarding digital privacy. In addition, you will benefit from real-world insights shared by industry experts.

As a bonus, you will have the unique opportunity to experience the teaching of a Stanford graduate course, in a Stanford classroom, by getting access to classroom content that was originally recorded only for Stanford graduate students!

- Receive an explanation of core networking concepts, including how the internet functions, the allocation and utilization of IP addresses, how computers communicate through Address Resolution and routing, and the crucial role of ports in ensuring network security.
- Understand Transmission Control Protocol (TCP) and the intricacies of the TCP three-way handshake and its vital functions in establishing connections.
- Analyze real-world DNS attacks and develop robust defense strategies to protect critical DNS Infrastructure.
- Detect, evaluate, and minimize various DoS attack types.
- Explain and strategize the use of firewalls, network address translation, and application firewalls to reinforce networked systems against potential threats.
- Identify privacy, anonymity, and censorship issues in network security and develop strategies to protect privacy in the digital era.

**INSTRUCTORS**

**Dan Boneh**
*Professor Computer Science and Electrical Engineering*

**Zakir Durumeric**
*Assistant Professor Computer Science*

**ENROLL NOW**

## COURSE OUTLINE

- **Internet Security**
  Receive a breakdown of the inner workings of the internet and a clear understanding of core protocols like ARP, BGP, and TCP. Learn how data flows through networks, why certain protocols are susceptible to attacks, and how to identify and defend against common threats.

- **DNS Security**
  Dive into the vulnerabilities of the Domain Name System (DNS), exploring how attackers manipulate it to redirect traffic, intercept data, and disrupt services.

- **Denial-of-Service**
  Explore the motivations behind Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks, the techniques used to amplify their effects, and the defenses used to mitigate damage.

- **Network Defenses**
  Defending a network requires a multi-layered strategy. Explore the essential tools and techniques to safeguard modern infrastructures.

- **Privacy, Anonymity, and Censorship**
  Discover valuable insights into user anonymity, censorship evasion, and the importance of safeguarding personal data.

- **Other Topics in Network Security**
  The evolution of network security is closely tied to advancements in virtualization and cloud computing. Explore the role of virtual machines (VMs) in modern network security, the challenges of VM isolation, and the importance of hypervisor detection.

# Cloud Security

As organizations increasingly transition to cloud environments, they face a surge in cloud-specific threats and misconfigurations that demand a proactive approach to security. Now more than ever, professionals must understand how to effectively secure cloud environments to prevent breaches, ensure compliance, and maintain trust.

This course offers an in-depth exploration of cloud security, covering critical areas such as cloud infrastructure security, cloud application security, identity and access management, data protection, security operations and monitoring, incident response, and compliance with global standards. Additionally, by analyzing real-world cloud breaches and understanding the shared responsibility model, learners will gain practical skills to secure cloud-native applications, mitigate risks, and apply cloud security best practices.

Finally, with insights from industry experts and optional hands-on labs, this course equips professionals with the essential knowledge and strategies to tackle today's cloud security challenges and safeguard critical systems.

- Explain fundamental cloud-specific security concepts and threats.
- Learn to evaluate security risks in cloud architectures and applications.
- Analyze real-world cloud security breaches to understand root causes and extract lessons learned.
- Understand how to implement cloud data protection.
- Develop effective cloud security operation, monitoring, and incident response strategies.
- Ensure compliance with relevant cloud security standards and regulations.
- Assess emerging cloud security technologies.

## INSTRUCTORS

**Dan Boneh**
*Professor Computer Science and Electrical Engineering*

**Neil Daswani**
*Cybersecurity Executive, Investor, Author, and Educator*

**ENROLL NOW**

## COURSE OUTLINE

- **Introduction to Cloud Security**
  Uncover the fundamentals of cloud security and see some examples of cloud breaches. Receive an introduction to cloud architecture, including components of cloud applications, major cloud providers, fundamental security considerations, and the shared responsibility model.

- **Cloud Infrastructure Security and Cloud Application Security**
  Dive deep into two critical areas of cloud security: cloud infrastructure security and cloud application security. Understand cloud infrastructure security and explore various strategies to secure containers and Kubernetes environments.

- **Data Protection and Access Security in Cloud Environments**
  Receive an overview of data protection and access security in cloud environments. Become acquainted with the core data protection steps: data classification, setting access policy, and support for encrypting data at rest and in transit. Understand Key Management Systems (KMS), including details on the different types of keys, key policies, and key rotation.

- **Cloud Security Operations and Monitoring**
  Uncover the unique considerations for cloud security operations and monitoring. Learn best practices for bot protection and cloud configuration.

- **Cloud Security Frameworks and Compliance Standards**
  Investigate cloud security frameworks and compliance standards. Review the frameworks relevant to cloud security, including Cloud Security Alliance's Cloud Controls Matrix and AWS Well-Architected Framework.

- **Ensuring Privacy in Cloud Environments**
  Dive into advanced topics on ensuring privacy in cloud environments and how to harness the power of machine learning without compromising sensitive information. Learn about Slalom, a novel technique for accelerating machine learning classification.

# AI Security

This course introduces you to the security challenges of modern AI systems and examines how vulnerabilities can be introduced during system architecture design, model development, training, and deployment. You'll explore how attacks like prompt injection, adversarial inputs, data poisoning, and model extraction exploit foundation models, retrieval-augmented systems, and AI agents. You'll also learn about common AI misapplications and the risks introduced by multi-agent collaboration. Alongside these threats, you'll examine emerging defenses such as secure architectures, verifiable training, and prompt-level protections, gaining a deeper understanding of how to assess and improve AI system security.

By analyzing real-world breaches and misapplications and engaging in hands-on exercises, you will gain valuable insights into the limitations of current AI systems and be equipped with the knowledge and skills to build more secure, robust, and trustworthy AI applications.

- Learn how vulnerabilities can be introduced during system architecture design, model development, training, prompt handling, and deployment.
- Identify potential vulnerabilities in AI systems—including prompt injection, adversarial examples, model extraction, data poisoning, and jailbreaks—and assess their impact on system behavior.
- Assess security implications of foundation models, retrieval-augmented generation (RAG), and multi-agent or agentic AI systems.
- Interpret real-world breaches and misuse cases, such as deepfakes and model leaks, to understand emerging threat patterns.
- Apply defenses, including verifiable training and inference, prompt-level protections, and secure code generation, and understand their limitations.

## INSTRUCTORS

**Dan Boneh**
*Professor Computer Science and Electrical Engineering*

**Neil Daswani**
*Cybersecurity Executive, Investor, Author, and Educator*

**John Mitchell**
*Mary and Gordon Crary Family Professor, Computer Science*

ENROLL NOW

## COURSE OUTLINE

- **Foundations of AI and Cybersecurity**
  Understand why AI is a dual-use technology and how it can be harnessed for powerful, positive advancements, but also misused for harmful purposes. Gain a solid foundation for understanding the critical role cybersecurity plays in the development and deployment of AI systems, and how these two fields are now more connected than ever.

- **AI Systems, Architectures, Design, and Security**
  Take a closer look at different types of AI systems, what they're useful for, and the security considerations that come with them. Learn about key security challenges that arise in both traditional and modern AI systems, and why AI must be secure and trustworthy in ways that depend on its specific application. Understand how modern AI systems are structured, what they're used for in real-world settings, and the key security risks that come with each type.

- **Security Considerations for AI Misapplications**
  Explore the risks that come with applying the wrong type of AI for the wrong problem or relying on it too heavily, even when the task seems appropriate. View concrete examples of misapplied AI, and learn about identifying which type of AI, if any, is suitable for a given task, and how to weigh the risks involved.

- **Adversarial Methods in AI Systems**
  From data poisoning during training to prompt injection at inference time, discover how AI introduces new security risks at nearly every stage of the pipeline. Explore how attackers can manipulate training data, extract sensitive information from models, and exploit vulnerabilities in cloud-hosted AI services.

- **Real-World AI Breaches, Attacks, and Misuses**
  Examine high-profile examples of AI misuse, such as DeepFakes used for fraud and cases where large language models have been manipulated to leak private data or bypass safety controls. Gain insight into jailbreak attacks–techniques adversaries use to circumvent a model's built-in safeguards–which have become a serious and evolving threat.

- **Defending and Verifying AI Systems**
  What can be done to defend and verify AI systems, while keeping a realistic perspective? Gain a clear understanding of the defenses that exist today, the limitations they face, and why securing and verifying AI remains an active area of research, with many solutions still in early stages of research and development.

- **The Future of AI & Cybersecurity**
  Listen to industry experts share their insights on where AI is headed and the challenges still ahead. Comprehend the evolving landscape of AI and cybersecurity careers—what skills are becoming essential, how roles are changing, and how to prepare for a future shaped by intelligent systems.

Stanford | ONLINE

Updated October 2025