About this course

Focusing on the areas of applied cryptography, system security, and the principles and practices of network security, this course explores the necessary tools, techniques, and concepts of network security for modern computer networks. The course’s coverage of advanced network security includes both cutting-edge technologies and research topics, primarily at the MAC layer and above. The course not only provides students with exposure to burgeoning areas of network security but also hands-on experience using the tools essential for computer network and cybersecurity today and in the future.

Specific topics covered include:

- Public key and symmetric key based cryptography
- Access control models
- Network security policies
- Authentication protocols
- Secure protocol standards
- Public Key Infrastructure and its development trends
- Virtual Private Network and its restrictions
- Attack graphs and attack trees
- SDN/NFV based Security Solutions
- Cloud network security
- ML and AI for computer network security
- Moving target defense in computer networks
- Key management (Public key, shared key, group key, distributed key management)

Required prior knowledge and skills

- **Knowledge:** Basic computer network concepts such as TCP/IP, packet switching, network services architecture, network protocol stack (MAC layer and above), and basic network security concepts such as encryption/decryption, authentication, access control, identity/key management
- **Skills:** Java, Python, C/C++, HTML programming

Learning Outcomes

*Learners completing this course will be able to:*

- Explain basic security terminologies, models, architectures, and techniques.
- Apply proven methodologies to design secure networks that address enduring and emerging issues.
- Apply network security standards and cryptography algorithms.
- Document the process of designing and implementing secure networking systems.
- Build a secure networking system to counter given network attacks.
Adhere to standards of computer security ethics.
Manage a network security establishment effort.
Assess networking systems to identify security vulnerabilities.
Represent security system setup and process results in written form.
Discuss cutting-edge network security research and development.

Creator

Dijiang Huang

Dijiang Huang is an associate professor in the School of Computing Informatics and Decision Systems Engineering. He teaches Computer Network and Security (CSE468) at the undergraduate level and Advanced Computer Network and Security (CSE548) at the graduate levels. In addition, he had taught computer science courses such as Computer Networks (CSE434), Cloud Computing (CSE 546), Concepts of Computer Science and Data Structure (CSE 205), Data Structures and Algorithm (CSE 310), and Introduction to Computer Science and Engineering (CSE 101) at Arizona State University. Dr. Huang received his Bachelor of Science degree in Telecommunications from Beijing University of Posts & Telecommunications, China, and his Computer Science and Telecommunications Master of Science degree and Ph.D. from the University of Missouri-Kansas City.

Dr. Huang's research interests are in computer and network security, mobile ad hoc networks, network virtualization, and mobile cloud computing. His research is supported by the federal agencies NSF, ONR, ARO, and NATO, and organizations such as Consortium of Embedded System (CES), Kern Family Foundation, Hewlett-Packard, and China Mobile. He is a recipient of ONR Young Investigator Award and HP Innovation Research Program (IRP) Award, a Distinguished Lecturer of IEEE ComSoc, and a co-founder of Athena Network Solutions LLC (ATHENETS) and CyNET LLC. He currently leads the Secure Networking and Computing (SNAC) research group at ASU.