Computer Science (COMP) 660

Enterprise Information and Network Security (Revision 3)

Status:	Replaced with new revision, see the **course listing** for the current revision
Delivery mode:	**Grouped study**
Credits:	3
Area of study:	Information Systems
Prerequisites:	**COMP 604**
Precluded:	None
Faculty:	**Faculty of Science and Technology**
Notes:	This is a graduate level course and students need to apply and be approved to one of the graduate programs or as a non-program **School of Computing and Information Systems** graduate student in order to take this course. Minimum admission requirements must be met. Undergraduate students who do not meet admission requirements will not normally be permitted to take this course.

Instructor: Dr. Hongxue (Harris) Wang

Overview

The security of computer networks and information is a serious concern for all organizations and enterprises, and it has become increasingly so, as organizations and people are more and more connected through, and dependent on, the internet. Computer Science 660: Enterprise Information and Network Security provides students with opportunities to review and explore definitions of network and information security; vulnerabilities of network and information assets; and threats and attacks to the security of enterprise networks and information.

This course covers many topics and is both problem-driven and research-based. Within each unit, students are led by topics of study and leading questions to review and explore important concepts, principles, theories, algorithms, protocols, schemes, standards, tools, systems, policies, and government regulations in specific areas of information and network security.

For each assignment, students conduct in-depth research and write a paper on a topic approved by the instructor, and then solve various security-related problems.

While efforts have been made to accommodate students who come to the course with different backgrounds and depths of knowledge, students taking this course are assumed to have a science degree or equivalent and a background in computing and information systems.

Outline

Unit 1: Defining Enterprise Network and Information Security

Securing the information assets of an enterprise can be very technical and costly; however, even with advanced and expensive technologies, systems, and personnel in place, the security of an enterprise's network and information assets cannot be guaranteed if the technologies and systems are not used properly or the personnel is poorly trained. In this unit, you will explore topics related to information security management. After completing this unit, you will be able to explain the roles of security training and security audit, as well as security assessment and planning at enterprises. You will be able to discuss the policies, standards, and government regulations that are helpful—even critical—for enterprises in managing their information security.

Unit 2: Fundamental Technologies Enabling and Defending Security

Certain security goals, such as confidentiality, integrity, availability, and authenticity, can only be achieved and protected by using appropriate enabling and defending technologies. In this unit, you will explore topics related to cryptography and other technologies essential in maintaining the confidentiality and integrity of enterprise data. You will also study algorithms and schemes for hashing and keyed hashing, and you will explore topics related to authentication, as well as access control of users, services, and data.

The focus of this unit is on the essential principles, theories, algorithms, schemes, and technologies in cryptography, authentication, and access control. After completing this unit, you will be able to explain what symmetric and asymmetric cryptography are, and how some classical and modern cryptographic schemes and algorithms work, such as Caesar cipher, RSA, Diffie-Hellman, and public key cryptography. You will also be able to explain how some fundamental authentication and access control schemes/models work, as well as their strengths and weaknesses in ensuring the authenticity and availability of network and information assets. Finally, you will be able to choose appropriate security schemes and algorithms, as well as authentication and access control schemes, to achieve required security goals for a given application.

Unit 3: Vulnerabilities, Risks, Threats, Attacks, and Challenges

To win a battle, it is very important to know the strengths and weaknesses of both you and your enemy. This also applies to enterprise network and information security. In this unit, you explore various vulnerabilities in computer systems and networks, as well as threats to enterprise network and information security. These threats include various computer worms; viruses; bots; phishing schemes; and potential intrusions and attacks on enterprise networks and information, as well as network services. You will also learn about the challenges in ensuring the security of enterprise network and information assets.

Unit 4: Protocols, Standards, Tools, and Systems for Network and Information Security

In a networked environment (like the internet), certain security goals can only be achieved through the collaboration of clients and servers. Computers collaborate by following certain standards and protocols, with the assistance of security systems. In this unit, you will study some well-known protocols and standards, such as DES, Triple DES, AES, IDEA, the Kerberos protocol, and public key infrastructure (PKI). You will also study security protocols designed and implemented at different network layers, particularly secure IP protocol (IPSec), Secure Socket Layer (SSL), and transport layer security (TLS). Protocols and systems designed for special purposes, such as firewalls, VPNs, IDS, and IPS, are also explored.

Unit 5: Systems Security

Today's enterprises are heavily dependent on many types of computer-based systems, which store or transmit their information assets. The security of such systems is essential and critical to enterprises. In this unit, you will study security issues and the technological requirements of systems commonly deployed and used by enterprises. After completing this unit, you will be able to explain the principle of firewalls. You will also be able to describe the main security features of some well-known systems, as well as their weaknesses.

Unit 6: Enterprise Information and Network Security Management

Securing the information assets of an enterprise can be very technical and costly; however, even with advanced and expensive technologies, systems, and personnel in place, the security of an enterprise's network and information assets cannot be guaranteed if the technologies and systems are not used properly or the personnel is poorly trained. In this unit, you will explore topics related to information security management. After completing this unit, you will be able to explain the roles of security training and security audit, as well as security assessment and planning at enterprises. You will be able to discuss the policies, standards, and government regulations that are helpful—even critical—for enterprises in managing their information security.

Learning outcomes

After successfully completing this course, you will be able to

- clearly define the scope and purposes of enterprise information and network security.
- analyse, design, and use security protocols, policies, tools, and systems to achieve confidentiality, integrity and availability of information and services.

- analyse, design, and use security protocols, policies, tools, and systems to achieve authenticity of users, service, and data.
- analyse, design, and use security protocols, policies, tools, and systems to achieve accountability of users in cyberspace.
- explain the roles of security training, security audit, and security assessment and planning at enterprises, and discuss the policies, standards, and government regulations that are either helpful or critical for enterprises in managing their information security.
- identify research problems related to computer, network, and information security, and conduct research and write publishable technical papers.

Evaluation

To **receive credit** for COMP 660, you must achieve a cumulative course grade of **B- (70 percent)** or better, and must achieve an average grade of at least 60% on the assignments and 60% on the final exam. Your cumulative course grade will be based on the following assessments.

Activity	Weight
Assignment 1	20%
Assignment 2	20%
Assignment 3	20%
Class participation in the COMP 660 General Forum	10%
Final Examination	30%
Total	**100%**

Materials

There is no assigned textbook for this course. Students are directed to find articles and other documents related to the topics covered in each unit from libraries and online sources, such as the IEEE and ACM digital libraries. Students who are completely new to the subject are encouraged to get a copy of a university textbook that covers the general topics and standard technologies related to information security.

Other Materials

The following materials are distributed online as part of the course:

- Course orientation
- Study guide
- Study plan
- Assignment requirements
- Course evaluation form

Other materials may be distributed through the course forum when necessary.

Course Workload

The estimated weekly workload is approximately five hours of reading and three hours of synthesis/exercises, plus an additional eight hours of assignment work, for a total of approximately 16 hours of coursework per week.

The above numbers represent averages only. The actual workload for each individual depends on the individual’s background knowledge and skills in the areas of mathematics, computer networks, and general computing.

Software Tools

Some of the general system development tools that may be needed for coursework and assignments are publicly available on internet. Students are not required to have specific network security software on their computers.

Special Course Features

Delivery Platform

The basic delivery model for this course is internet home study. The AU-produced textual and graphical material is supplemented by use of applications software for some content, exercises, and assignments.

Computer and Data Communications Resource Requirements

Students must provide their own Internet access.

Special Note

Students registered in this course will NOT be allowed to take an extension due to the nature of the course activities.

Important links

- Future Course Offerings
- Important Dates and Deadlines
- MSc IS Contact Information

Athabasca University reserves the right to amend course outlines occasionally and without notice. Courses offered by other delivery methods may vary from their individualized study counterparts.

Opened in Revision 3, November 16, 2020

Updated January 27, 2025

View **previous revision**