CSCI 5301 – MODERN COMPUTER SECURITY AND CONTEMPORARY ISSUES IN COMPUTER SCIENCE

CREDIT HOURS: 3

CATALOG DESCRIPTION:

This course addresses concerns applicable to computer users. It covers the issues and practical aspects of modern computer security, with an overview of relevant laws and regulations (including HIPAA – the Health Insurance Portability and Accountability Act) concerning computer security. It also addresses relevant issues with large-scale computer usage, including big data, user interfacing, cloud computing, and ethical issues in computing.

PURPOSE OF COURSE:

The purpose of this course is to acquaint students with practical aspects of computer applications and computer security, and to discuss contemporary issues involving computing that involve other disciplines. This course is designed for the non-computer science major that wishes to gain insight and keep current with security and legal issues involving practical uses of computing. The contemporary issue topics will include but not limited to security, legal aspects, ethics, big data, and data analytics. No programming is involved.

EDUCATIONAL OBJECTIVES

Upon successful completion of the course, students should be able to:

1. Understand theoretical and practical aspects of computer security.
2. Understand practical aspects of physical security related to computing.
3. Explain the trade-offs of using cloud-based storage, involving confidentiality, access, and data integrity.
4. Explain legal aspects of computing, including HIPAA and other relevant laws.
5. Know and be able to explain ethical issues involving the use of computers.
6. Explain and apply principles of cybersecurity.

COURSE CALENDAR

This course meets for a minimum of 37.5 lecture contact hours during the semester, including the final exam. Students have significant assignments based on readings from the primary literature, participate in classroom discussions regarding current research topics, complete periodic homework and laboratory assignments, and periodic exams in addition to the final exam. Students are expected to prepare for any class assignments or quizzes over the material covered in class or in the reading material. Successful completion of these activities requires at a minimum six additional hours of outside of classroom work each week.

CONTENT

<table>
<thead>
<tr>
<th>Security</th>
<th>HOURS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer security – confidentiality, integrity and accessibility</td>
<td>12</td>
</tr>
<tr>
<td>Implementing real-world security practices</td>
<td></td>
</tr>
<tr>
<td>Physical security and how it impacts computer security</td>
<td></td>
</tr>
</tbody>
</table>
Cybersecurity and cyberterrorism

Legal aspects of computing ................................................................. 9
  Relevant legal issues, to include the Health Insurance Portability and Accountability Act (HIPAA)

Cloud-based storage and security ......................................................... 9
  Types of cloud service (platform, infrastructure, and software)
  Trade-offs of cloud storage

Data Analytics......................................................................................... 9
  Big data
  Analysis and storage

Ethical issues in computing .................................................................. 3
  Ethics and the law
  ACM/IEEE codes of ethics and conduct

Exams (plus a comprehensive final) ...................................................... 3

TOTAL 45

REFERENCES


Smith, R. Information Security, Jones and Bartlett Learning, 2011.

Assorted papers and web sites to cover topics such as data analytics, big data, and other relevant topics.