Course Objectives: The objective of this course is to expose students to advanced topics in information security and privacy across emergent cyber systems. Topics covered will include security issues like authentication, anonymity, traceback, denial of service, encryption, forensics etc. in both wired and wireless computing systems. At the conclusion of the course, students will be expected to get a clear and in-depth understanding of state of the art in information security and privacy in emergent computing systems from the perspective of attacks and defenses.

Student Workload: There will be regular homework assignments and two exams for the course based on content covered.

Grading for Students:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Homework Assignments</td>
<td>50%</td>
</tr>
<tr>
<td>Exam 1</td>
<td>25%</td>
</tr>
<tr>
<td>Exam 2</td>
<td>25%</td>
</tr>
</tbody>
</table>
Tentative Schedule of Topics Covered

**Topics Covered**

- Anonymity in Peer-to-Peer Systems
- Secure Forwarding in Overlay Networks
- Key Management in Sensor Networks
- Intrusion Detection in Sensor Networks
- Security in RFID Devices
- Security in Vehicular Networks
- Human-Centered Cyber Security
- Project Discussions and Presentation

**CLASS POLICIES**

Students are expected to attend all classes unless they have a reasonable excuse for being absent.

Assignments/Tests cannot be submitted/taken late unless there is prior approval from the Instructor, or there is formally documented evidence of medical/other emergencies.

Classes will be taught using power point slides.

Exams and homeworks must be an individual effort.