CS6601 - Privacy-Preserving Data Integration and Analysis


Course Description

This course covers basic tools, in statistics and cryptography, commonly used to design privacy-preserving and secure protocols in a distributed environment as well as recent advances in the field of privacy-preserving data analysis, data sanitization and information retrieval. Students are expected to complete a course project on a relevant topic of their choosing.

Intended Audience & Prerequisite

This course is aimed at graduate students in any science or engineering degree program. The prerequisite: CS5300 and CS3600.

Course Policies

Academic Alert System

The purpose of the Academic Alert System is to improve the overall academic success of students by improving communication among students, instructors and advisors; reducing the time required for students to be informed of their academic status; and informing students of actions necessary by them in order to meet the academic requirements in their courses.

Disabilities

If you have a documented disability and anticipate needing accommodations in this course, you are strongly encouraged to meet with the instructor as early as possible in the semester. You will need to request that the Disability Support Services staff send a letter to the instructor verifying your disability and specifying the accommodation you will need before the instructor can arrange your accommodation. Disability Support Services is located in 204 Norwood Hall, their phone number is 341-4211, and their E-mail is dss@mst.edu.

Academic Dishonesty

Every student enrolled in this course is expected to be familiar with Missouri S&T’s Student Academic Regulations, including the section on Conduct of Students which on pages 30-31 defines several forms of Academic Dishonesty such as cheating, plagiarism, and sabotage. Incidences of Academic Dishonesty will typically result in zero grades for the respective course components, notification of the student’s advisor, the student’s department chair, and the campus undergraduate studies office, and further academic sanctions.
may be imposed as well in accordance with the regulations. Note that those who allow others to copy their work are just as guilty of plagiarism and will be treated in the same manner.

**Attendance & Participation**

Attendance is mandatory for this course. If a student misses more than two lectures, the instructor will drop the student from the course.

**Assignments**

Some assignments need to be done individually, and other assignments can be done in a group of most three. The types of assignments are programming, problem solving, paper presentation, and among others.

**Makeups & Extensions**

There will be no makeups and late assignments. On the other hand, if a posted exam date or assignment deadline is known in advance to pose an irresolvable conflict, with feasible early notice, the instructor may accommodate all reasonable requests for alternative dates.

**Title IX Statement**

Missouri University of Science and Technology is committed to the safety and well-being of all members of its community. US Federal Law Title IX states that no member of the university community shall, on the basis of sex, be excluded from participation in, or be denied benefits of, or be subjected to discrimination under any education program or activity. Furthermore, in accordance with Title IX guidelines from the US Office of Civil Rights, Missouri S&T requires that all faculty and staff members report, to the Missouri S&T Title IX Coordinator, any notice of sexual harassment, abuse, and/or violence (including personal relational abuse, relational/domestic violence, and stalking) disclosed through communication including but not limited to direct conversation, email, social media, classroom papers and homework exercises. Missouri S&Ts Title IX Coordinator is Vice Chancellor Shenethia Manuel. Contact her directly (manuels@mst.edu; (573) 341-4920; 113 Centennial Hall) to report Title IX violations. To learn more about Title IX resources and reporting options (confidential and non-confidential) available to Missouri S&T students, staff, and faculty, please visit http://titleix.mst.edu.

**Instructor Information**

<table>
<thead>
<tr>
<th>Name</th>
<th>Wei Jiang, Ph.D.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office</td>
<td>333 Computer Science Building</td>
</tr>
<tr>
<td>Office Hours</td>
<td>MW 11:00 - 11:50AM, or by appointment</td>
</tr>
<tr>
<td>E-mail</td>
<td><a href="mailto:wjiang@mst.edu">wjiang@mst.edu</a></td>
</tr>
<tr>
<td>Homepage</td>
<td><a href="http://web.mst.edu/~wjiang/">http://web.mst.edu/~wjiang/</a></td>
</tr>
<tr>
<td>Office Phone</td>
<td>(573) 341-4989</td>
</tr>
<tr>
<td>Office Fax</td>
<td>(573) 341-4501</td>
</tr>
</tbody>
</table>
Course Information

<table>
<thead>
<tr>
<th>Lecture Sessions</th>
<th>MWF 9:00-9:50AM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location</td>
<td>Toomey Hall 00260</td>
</tr>
<tr>
<td>Egress map</td>
<td>TBA</td>
</tr>
<tr>
<td>Course Schedule</td>
<td>TBA</td>
</tr>
</tbody>
</table>

Grading Information (Tentative)

<table>
<thead>
<tr>
<th>Assignments</th>
<th>60%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exam</td>
<td>20%</td>
</tr>
<tr>
<td>Course project</td>
<td>20%</td>
</tr>
</tbody>
</table>

Grade for Graduate

| A (90 - 100%) | B (80 - 89%) | C (70 - 79%) | F (< 70%) |

Tentative Topics

- Private distributed functionalities
  - What is privacy-preserving?
  - Data partitions
  - Adversary models

- Privacy definitions
  - Randomization - additive and multiplicative noise, generalization
  - Cryptography - computationally and theoretically secure
  - The trusted third party model

- Common techniques
  - Distribution reconstruction
  - $k$-Anonymity
  - Secure multi-party computation

- Basic primitives
  - Secure sum
  - Secure dot product
  - Secure set operations
  - Secret sharing
  - Oblivious transfer
  - Zero knowledge proof

- Privacy-preserving data analysis and integration
- Decision tree
- Association rule mining
- Algebraic operations
- Distributed $k$-Anonymity