# ISA 763 Security Protocol Analysis

Thabet Kacem, PhD
Department of Computer Science
George Mason University

## Course Description

Spring 2018

Teaches how to design, understand, verify, and test communication protocols so they meet their security objectives of recognizing the basic components of a communication protocol. These include specifying security properties accurately, modeling actors and mal-actors against whom a protocol ought to be secure and discussing verification and testing methods, including their limitations. This is a graduate level class where we read many papers and apply their methods to model and verify the properties of protocol that are being used today.

### Class Details

*Prerequisites: ISA 656 or permission of instructor*
*Co-requisites: None*

*Classes*

* *Wednesdays, from 4:30 p.m. to 7:10 p.m.*
* *Room 2026 of the Art and Design building.*

*Office hours*

* *By appointment only.*
* *Dr. Thabet Kacem Email: tkacem@gmu.edu*

*Administrative*

* *Registration and drop without tuition penalty deadline: January 29th.*
* *Drop with tuition penalty: February 23th.*

## Course Logistics

1. All course communication will be done via the Blackboard system. Students are expected to have access and be able to use the system before classes start. Blackboard is accessible via the MyMason portal at https://mymasonportal.gmu.edu/. Instructions for using the Blackboard system are provided in the "resources" link at the bottom of the portal page.
2. Volgenau School Computing Resources has answers to many questions about school systems on their web site: http://labs.vse.gmu.edu and will try to help you if have problems connecting to school computing systems. However, they will not provide assistance with general computing questions or course assignments. Please contact me if you have any questions about how to use software to complete your assignments.
3. Accommodations for disability: If you have a documented learning disability or other condition that may affect your academic performance you should: a) make sure this documentation is on file with Office for Disability Services (SUB I, Rm. 4205; 993-2474; http://ods.gmu.edu) to determine the accommodations you need; and b) let me know about your accommodation needs as soon as possible. If you have contacted the Center for Disability Services and are waiting to hear from a counselor, please keep me updated during the whole process.
4. Inclement weather: Class sessions may be cancelled due to inclement weather or other University emergencies. Check the Announcements area of the course website for updates.

## Expected Behavior

1. Attendance in class is essential. Information will be presented that will not necessarily be in the book, and is almost certain to be required for successfully completing the project.
2. You can enter or leave at any time, provided you do your best to avoid disrupting the activity going on.
3. Please make sure you have your cell phone, tablet, pager, etc., in silent mode. *Should you find yourself in extreme need of answering an incoming call, just leave the room to do so*.
4. All course deliverables will be submitted electronically and scheduled in advance. I do have some flexibility regarding scheduled assignments; provided requests are made prior to the event. Should any scheduled event impact a student's participation in class activities and assignments, it is the student's responsibility to coordinate with me in advance.
5. Religious observances are one common example of events that might impact students' activities. Students are responsible for planning ahead. Please, refer to the GMU's calendar of religious holidays at http://ulife.gmu.edu/religious_calendar.php.
6. Academic Policy: All academic policies as given in the Honor System and code will be strictly followed. These are available at http://catalog.gmu.edu/content.php?catoid=19&navoid=4113.
7. General Policies: All general policies defined in the University Catalog are in place for this course. You can access those at http://catalog.gmu.edu/content.php?catoid=19&navoid=4114.

8. George Mason University is an Honor Code university. Please see the Office of Academic Integrity website (http://academicintegrity.gmu.edu/honorcode/) for a full description of the honor code and the honor committee process.

**Exercise planning, be proactive and do your best to stay ahead of schedule.**

**Course Outline:**

Unit 0: Course Overview and Introduction
Unit 1: Security Protocol Verification Syntax: Basic Concepts
Unit 2: Security Protocol Verification Syntax: Specifying Security Objectives
Unit 3: Protocols for Anonymity
Unit 4: Trusted Computing

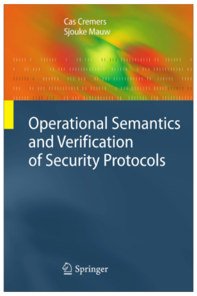
**Grading**

The grading structure of this course is as follows:

- Projects (80% of grade – 4 total, 20% each Project)
- Class presentations (20% of grade)

**Textbook and References**

The course will be based on the class notes. However, the following book is recommended:



Operational Semantics and Verification of Security Protocols Cas Cremers and Sjouke Mauw
Springer, 1st Edition (October 31, 2012). 172 pp.
ISBN-10: 354078635X.
ISBN-13: 978-3540786351.
GMU Library Link: http://magik.gmu.edu/cgi-bin/Pwebrecon.cgi?BBID=2956956

Other main references for this course are:

- Lowe, Gavin. A Hierarchy of Authentication Specifications. *Proceedings of 10th IEEE Computer Security Foundations Workshop*, 1997.
  Available at: http://www.cs.ox.ac.uk/gavin.lowe/Security/Papers/authentication.ps
- Meier, Simon. Advancing Automated Security Protocol Verification. PhD Thesis. ETH Zürich. 2013. Available at: http://www.infsec.ethz.ch/research/meiersi_thesis_final_draft_20130130.pdf

Please, note that all of the above references are also available either from the course Blackboard website or from the GMU Library.

### Software

The course includes usage of the following software, which is freely available from their associated websites listed below.

*Scyther tool*

Scyther is a tool for the automatic verification of security protocols. It is available from:

http://www.cs.ox.ac.uk/people/cas.cremers/scyther/

*GO Language*

**Go** is an expressive, concurrent, garbage-collected programming **language**. It is available from: https://code.google.com/p/go/

### Group Projects

***Overview***: The course grade is based on 4 group projects and individual presentations. Groups will be defined during the first class and all assignments must be submitted via Blackboard by their respective due date.

***Oral presentations***: Each student will present an assigned research paper related to the covered topic in class. The presentation(s) account for 20% of the course grade. Each presentation should take 20 to 30 minutes.

### Tentative Schedule

The following schedule is provided for planning purposes only. The course’s blackboard website includes a schedule of the activities, and students are responsible for keeping themselves updated with the changes

| | | | | | |
|---|---|---|---|---|---|
| 1/24 | Week | 1 | Course | Overview and Introduction, group assignments | |
| 1/31 | Week | 2 | Unit | 1, | Yahloom protocol, Scyther tool |
| 2/7 | Week | 3 | Unit | 1, | Project preparation meetings<br>Oral Presentations |
| 2/14 | Week | 4 | Unit | 1, | group presentation |
| 2/21 | Week | 5 | Unit | 2, | JFK protocol |
| 2/28 | Week | 6 | Unit | 2, | Project preparation meetings<br>Oral Presentations |
| 3/7 | Week | 7 | Unit | 2, | group presentation |
| 3/14 | Spring Break: | | No Classes ----------------------------------------------------------------- | | |
| 3/21 | Week | 8 | Unit | 3, | Dinning cryptographers protocol, GO language |
| 3/28 | Week | 9 | Unit | 3, | Project preparation meetings<br>Oral Presentations |
| 4/4 | Week | 10 | Unit | 3, | group presentation |
| 4/11 | Week | 11 | Unit | 4, | a zero knowledge protocol |
| 4/18 | Week | 12 | Unit | 4, | Project preparation meetings<br>Oral Presentations |
| 4/25 | Week | 13 | Unit | 4 | Group presentations |
| 5/2 | Week | 14 | | | Oral Presentations |

**BEST WISHES FOR A GREAT SEMESTER!!!**