Course manual & Organization AI & Cyber Security in Module IID (6) for TCS & BIT

Organization & Hybrid teaching

This course will be taught in hybrid mode, with some parts online and some parts on campus. All lectures will be prerecorded and made available before the scheduled lecture of the respective week. The scheduled time for the lecture can be used to watch the pre-recorded videos. There is no live session during that time. An exception is that during the first lecture (November 16th, 8:45), a short online live introduction to the course setup will be provided. Exams will be held on campus. See section on `Availability of TAs and teachers' below for information about how to ask questions about the course material.

Half of the tutorial sessions is conducted online, and half on campus (see table below). For the on campus tutorials, there is enough space for all students to attend. The location of on campus tutorials can be found in the timetable online. For students who are unable to attend on campus tutorials for health reasons, we will have limited opportunities for online Q&A.

Week	Lecture	Tutorial
1	Pre-recorded & Online live intro course setup Nov 16th, 8:45 (Bouali)	Online Q&A
2	Pre-recorded	On campus
3	Pre-recorded	Online Q&A
4	Pre-recorded	On campus
5	Pre-recorded	On campus
6	Pre-recorded	Online Q&A
9	-	On campus: repair assignments

Online platforms

In this course we will use the following online platforms:

- Canvas: this is used for posting teaching materials of the course, grades, and critical announcements relevant for all students.
- Teams: this is used for the live course introduction.
- Discord: this is used for the online tutorials and for asking questions to teachers about lecture content.
- Horus: this is used for queuing questions for online tutorials.

<u>Discord usage rules and guidelines</u>

1. It is required to use your real name. Nicknames are not allowed.
2. Messages should concern the content and organization of the course. Feedback for individual teachers should be sent via email to the teacher and/or coordinator.
3. Post your message in the channel corresponding to the topic of your question. In particular, use the channel "qa-weekN" for questions about the content of week N.
4. When posing a question, mention the topic and number of the assignment question it pertains to, or the slide set and number. Ensure that your question is as concrete as possible and show what you have already done to try to solve the problem. If your post does not adhere to these guidelines, it may not get answered.

5. If you posted your question on Discord, and you also joined a queue in Horus, make sure to remove yourself from the queue if it was answered on Discord, or vice versa, indicate on Discord that your question was already answered via Horus.

Availability of TAs and teachers

TAs are your first point of contact for this course. They are available during the weekly tutorial session to answer your questions about the content and organization of the course. During tutorial sessions, teachers will also monitor Discord and may address questions that are specific to the lecture material or that TAs forward to teachers. Outside tutorial sessions, you can use Discord to interact with other students about the course material. Depending on availability, TAs and teachers may sometimes answer your questions outside tutorial hours as well, but this is not to be expected. However, on the day of the lecture, you can post questions that come up while watching the pre-recorded lectures to the corresponding channel in Discord which teachers will then monitor. Teachers and TAs are not expected to be available during the two-week Christmas break.

Below is an overview of who to contact for which questions and how to do so:

- *Teaching Assistants (TAs):* questions about the weekly tutorial and practical assignments, and the connected lecture material
    - How? During the weekly tutorial sessions - on campus or online
- *Coordinating TAs:* questions about grading of the practical assignments, or administrative questions connected to this
    - How? Via Discord.
- *Teachers:* questions about the lecture material or practical assignments, in case these could not be answered by the TAs
    - How? Via Discord or e-mail.
- *Course coordinator:* questions, remarks or suggestions about the overall organization of the course, special requests (for example due to personal circumstances), accommodations
    - How? Via E-mail.

Contact information

Below is an overview of the teachers, coordinating TAs, and regular TAs for the course.

Teachers:

- Birna van Riemsdijk (coordinator): m.b.vanriemsdijk@utwente.nl
- Nacir Bouali: n.bouali@utwente.nl
- Andrea Continella: a.continella@utwente.nl
- Estefania Talavera Martínez: e.talaveramartinez@utwente.nl

Coordinating TAs:

- Aachi Garg: garg.aachi01@gmail.com
- Andrei Popa: a.popa@student.utwente.nl

TAs:

- Aly Afia
- Judith Bravo de Medina Arribas
- Gergana Georgieva
- Long Huynh Quang Long

- Noor Mansour
- Ioana Mazilu
- Humaid Mollah
- Priya Naguine
- Can Ölmezoğlu
- Evana Reuvers
- Olga Solovyeva
- Daan Strijbosch
- Irvine Verio
- Zihao Xu
- Zhiyong Zhu

Schedule of topics and teachers

Week	Topic	Lecturer	Practical Assignment	
1	Intro AI Propositional Logic	Van Riemsdijk	Prolog (not handed in)	B O N U S
2	Predicate Logic Search	Van Riemsdijk	Prolog	
3	Probabilistic Reasoning, Bayesian Networks	Bouali Talavera Martínez	Probabilistic reasoning (Python notebook)	
4	Machine Learning Decision Trees	Talavera Martínez Bouali	Decision trees (Python notebook)	
5	Neural Networks Reinforcement Learning	Talavera Martínez Bouali	Neural networks and RL (Python notebook)	
6	AI for Security	Continella	Security	

Practical assignments

The practical assignments consist of 5 separate assignments corresponding with weeks 2-6 of the course, respectively. The practical assignment from Week 1 is not handed in and not graded. There is furthermore a bonus practical assignment based on the material of Week 1-6, which is to be made throughout these weeks. The practical assignment is made in **pairs**.

All 5 regular assignments have to be a PASS in order to get a pass for the practical part of the course. A PASS will be given if all components of the assignment are sufficient. If the bonus assignment is a PASS, it can be used to either 1) compensate for a FAIL in 1 of the 5 regular practical assignments, or 2) if all 6 practical assignments (week 2-5 + bonus) have a PASS in the first round (i.e., without repairs), a 0.5 point bonus will be added to the exam grade of the AI theory part.

Repair opportunity

If an assignment is graded as a FAIL, there is the opportunity to repair it. The repair consists of handing in an improved version of the original assignment, as well as a (small) additional assignment on the topic of that week. Both the improved original assignment and the additional assignment need to be graded as PASS to get a PASS on that week's assignment. A maximum of 3 of the regular practical assignments can be repaired. There is no repair opportunity for the bonus assignment.

The deadlines for handing in the practical assignments are detailed below.

Week	Deadline
1	**not** handed in/graded
2	Monday Nov 29th 23.59
3	Monday Dec 6th 23.59
4	Monday Dec 13th 23.59
5	Monday Dec 20th 23.59
Bonus	Friday Dec 24th 17.00
6	Tuesday Jan 11th 23.59
Repair	Wednesday Jan 26th 23.59

Study material

AI Book (Week 1-5)

For this course we use the following book:

> *Artificial Intelligence. A Modern Approach* by S. Russell & P. Norvig **(4th edition)**

The 3rd edition of the book can also be used. However, note that the chapter and section numbers sometimes differ slightly from the 4th edition of the book.

In this course we treat material from the following chapters of the book: 1-3, 7-9, 12,13,19,22,23. See the weekly schedule below for the relevant sections per week.

Week	Read
Week 1	Chapter 1, 2, Chapter 7 (up to & including 7.5)
Week 2	8.1-8.3, 9.1, 9.2, 9.5, Chapter 3
Week 3	Chapter 12 and 13 up to and including 13.3
Week 4	Chapter 19 up to and including 19.6
Week 5	Chapter 22 up to and including 22.2 and Chapter 23

Cyber Security reading material (Week 6)

Sections 1.1 – 1.2, 2.1 – 2.3, 3.1, 4.1 – 4.2, and 4.4.2 in K. Rieck, *Machine Learning for Application-Layer Intrusion Detection*. PhD thesis, TU Berlin, 2009.
Available at: https://user.informatik.uni-goettingen.de/~krieck/docs/2009-diss.pdf

Further reading material can be found in R. Sommer and V. Paxson, *Outside the Closed World: On Using Machine Learning For Network Intrusion Detection*. S&P, IEEE, 2010.
Available at: https://personal.utdallas.edu/~muratk/courses/dmsec_files/oakland10-ml.pdf

Exam

The exam will be a multiple choice exam, to be made on campus using the Remindo system. A practice exam will be made available at the end of the course, before the first exam opportunity. During the exam, a dictionary can be used and it is allowed to bring a 1A4 cheat sheet on which you can write/print/draw on both sides anything that you think will help you during the exam.