UNIVERSITY OF TWENTE.

MOD6/AI & CYBER SECURITY: INTRODUCTION

NACIR BOUALI, M. BIRNA VAN RIEMSDIJK

TEACHERS

Birna van Riemsdijk
(Course coordinator)

Nacir Bouali

Estefanía Talavera

Andrea Continella

UNIVERSITY OF TWENTE.

TEACHING ASSISTANTS

Coordinating TAs:

- Aachi Garg
- Andrei Popa

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

ABOUT THE AI & CS COMPONENT

- It is an introductory course covering the basic formalisms of (modern) AI and the application of AI (Machine Learning) in Cyber Security.
  - History of AI
  - Agents
  - Knowledge Representation and Reasoning
  - Search
  - Reasoning under Uncertainty
  - Machine Learning: Decision Trees & Neural Networks
  - Reinforcement Learning (Basics)
  - Machine Learning for Cyber Security

LEARNING GOALS

After passing this course the student should be able to:

1. Recall the historical development of the AI field.
2. Construct, understand, formalize and deduce rather complex sentences in proposition and first order predicate logic.
3. Explain, compare and apply basic search techniques.
4. Model probabilistic inference problems as Bayesian Networks and reasoning about such networks.
5. Model and solve simple classification problems using Decision Trees and Neural Networks. (Machine Learning)
6. Understand and apply Reinforcement Learning in simple learning problems (Machine Learning).
7. Apply and evaluate machine learning techniques in the cyber security context of network intrusion detection.

ONLINE PLATFORMS

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

DISCORD ACCESS

- You need to fill in the intake form before you can access the server: https://docs.google.com/forms/d/e/1FAIpQLSfxFzOCz7TBB-lOaUrjd1d3u-aRycyX2ku1uHt1zF3GlLptkw/viewform

DISCORD RULES AND GUIDELINES

1. 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.

SETUP OF THE COURSE

- Theory (3EC)
  - lectures and tutorial assignments (week 1-6, prerecorded)
  - MC exam, closed book (week 7/resit week 10, on campus)
- Practice (3EC)
  - weekly practical assignment connected with lecture of that week (week 1-6, only week 2-6 are handed in), self-study
  - bonus assignment (week 1-6)
  - performed in groups of 2 students (make your pairs by Thursday the latest, otherwise we will pair you randomly!)
- Contact hours
  - Thur: weekly Q&A with TAs about tutorials and practical combined, online or on campus, see schedule
  - Questions about lecture: pose on Discord on day of the lecture
  - See course manual for details on who to contact and how
- Self study!

SCHEDULE

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

DEADLINES PRACTICAL ASSIGNMENTS

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

- Start with the bonus assignment in Week 1 and extend throughout the course; **don't wait until Week 6!**
- Week 6 deadline is after the Christmas break to avoid deadlines during the holidays; it is not expected to work on it during the break, TAs and teachers are not available.
- Jan 24th: on campus tutorial for questions regarding repairs

ASSESSMENT

- Final grade =
  - exam grade if practical assignment is pass
    - exam grade + 0.5 bonus if condition 2 below is met
  - insufficient if practical assignment is fail

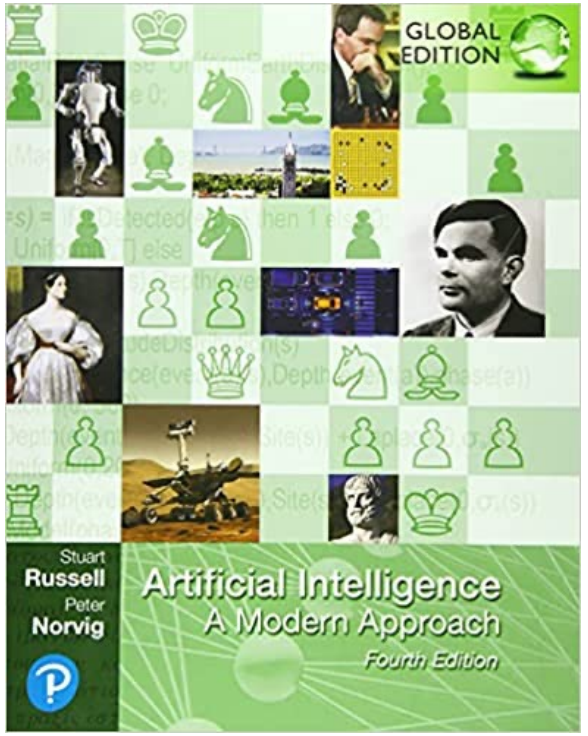
- Practical assignment grade
  - pass if all 5 assignments (week 2-6) are pass (with repair option/you can repair a maximum of 3 assignments/no repair for the bonus)
  - if bonus assignment is a pass, it can be used to either
    1. compensate for a FAIL in 1 of the 5 regular practical assignments, or
    2. if all 6 practical assignments (week 2-6 + 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.
  - fail otherwise

ASSESSMENT OF PRACTICAL ASSIGNMENTS

- Practical assignment receives a pass if all questions of the assignment are graded as sufficient.
- For machine learning exercises, sufficient is given if the minimum threshold of accuracy is passed
  - For assignments that do not make the threshold, it will be checked if the code is nevertheless of sufficient quality to give a pass
  - Otherwise, a fail will be given.

COURSE MATERIAL AI

- Book: *Artificial Intelligence. A Modern Approach* by S. Russel & P. Norvig
  - 4th edition!
- Slides and lecture videos (on Canvas).
- Exercises for tutorials and practical (on Canvas).
- Readers for Cyber Security.



CHANGES FROM LAST YEAR

- Overarching understanding of AI
  - New bonus assignment Week 1-6
  - Extended introduction about the overall course topics
- More attention to neural networks
- Workload distribution
  - Also Week 6 assignment made in pairs
  - Assignment deadline on Mondays instead of Sundays
  - Week 6 deadline after break
  - But: content of Week 4-6 may still be experienced as more challenging!
- 4th edition of R&N book

WE WISH YOU AN INTERESTING AND FUN COURSE! - THE TEACHING TEAM