PSI-AdvaSP-M Syllabus

Summer Semester 2022 · v1 / 2022-04-27

Prof. Dr. Dominik Herrmann
www.uni-bamberg.de/psi
dh.psi@uni-bamberg.de
☎ +49 951 863-2661

Head of Privacy and Security in
Information Systems Group

University of Bamberg
96045 Bamberg, Germany

This course is called **Advanced Security and Privacy**. It offers insights into various security and privacy topics, e. g., authentication mechanisms, web tracking, anonymity on the internet, protection against state level censorship, security ethics, usable security, software security, and advanced cryptography building blocks.

Some of these topics will be covered in depth, some topics will only be introduced superficially. By the end of the semester, you will have a better understanding of security and privacy and how research is done in those areas.

PSI-AdvaSP-M is a module with 6 ECTS credits consisting of a lecture and a tutorial (2 + 2 hours per week). All materials are provided through the corresponding VC course. In the first two weeks you do not need an enrollment key to join the VC course. After that, please contact our office.

This syllabus is an attempt to provide all relevant pieces of information about PSI-AdvaSP-M in one place. The syllabus helps managing expectations, and it gives reasons for the course design. It should answer most if not all of your organizational questions. Please read it carefully because it also contains guidelines and rules. Feel free to approach us if anything is unclear or missing.

A “syllabus” is a document that summarizes information on the organization and content of a course. The term is used mainly in Anglo-Saxon countries.

If you read this syllabus on a small screen, we recommend the responsive and mobile-friendly HTML version.

1. Flipped Classroom

This year’s course will use the *flipped classroom model*: We will provide material and extensive self-learning opportunities. In addition, there will be face-to-face offerings.

1.1 Self-learning Offerings

There are **four kinds of self-studying offerings**: lecture videos, lecture slides, task sheets, and a self-learning web-based environment called PSI Arena. These offerings allow you to acquire **all the material** that is relevant for the exam on your own.

All videos are made permanently available via the VC course and can also be downloaded from there. Save the links to the recordings in your browser or – even better – download the videos in order to have access to them in case of failures or overloads.

Lecture slides consist mostly of illustrations and visualizations. We try to keep the amount of text on the slides low to avoid fatigue (“Death by PowerPoint”). Take notes during the videos!

1.2 Optional Face-to-Face Sessions

In addition, there are face-to-face sessions, which are optional, i. e., attendance is not mandatory. You can find the rooms and times for the face-to-face sessions in UnivIS.

If you participate in the face-to-face sessions, you must adhere to the infection control regulations of University of Bamberg.

At the time of the lecture, we meet several times during the semester for the **plenary** (but not in the first week of the lecture period). Here you can consolidate and review the knowledge you have acquired so far. In the plenary **no additional content** will be taught, so you will not miss any material for the exam if you do not attend. The plenary is not recorded.

The plenary is not a lecture with frontal presentations which you are supposed to consume. During this time, you will work on questions and discuss them with your peers. Please only come to the plenary if you are prepared and bring your notes with you.

Furthermore, there is a **tutorial**. In the tutorial you can work on the exercises either alone or as a group. Use the time to work and to help each other. In the tutorial, there is **no frontal teaching**, i. e., we will not present or discuss solutions or discuss individual questions in front of the whole group.

During the tutorial, a teaching assistant is present whom you can ask for tips – but only after you have already attempted to solve a task yourself.
In general, there will not be enough time in the tutorial to work on all the assignments. We recommend that you work on some of the tasks before you come to the tutorial so that you can ask questions.

1.3 Asking Questions

Do not hesitate to ask your questions! It is quite likely that you are not alone with your question. You are, of course, welcome to answer other students' questions if you feel that you can help.

Too scared to ask questions? Maybe the article The Fear of Publicly Not Knowing will help you.

We would like to help you as quickly and effectively as possible. Supporting you becomes more efficient – and more effective – if you ask **informative questions**. Informative questions provide the following information:

- what you have already tried (e. g., relevant excerpt of source code or functions you used),
- what result you observed or where exactly you got stuck (including the exact wording of the error message), and
- what you would have expected.

For more information on asking informative questions, see the Teaching Philosophy.

In general, we do not give you solutions to exercises on the task sheets. However, if you get stuck on the assignments, feel free to contact us for clarification and tips on how to solve them.

For very specific questions that can best be clarified interactively, please approach a tutor in the tutorial. Alternatively, please describe your issue in an email (see section Contact and Support).

1.4 Questions on the VC Forum

For online interaction we use the VC forums and emails.

For information on contact and support options, see the contact and support section.

We would like to lower the threshold for asking questions in the VC forums. Your questions and answers can be asked **informally** - as it is done in other help forums, e. g., Stackoverflow. This means you do not have to add a formal salutation at the beginning or a greeting at the end of your posts.

Some of you may prefer to ask **anonymous questions**. You can use our anonymous user account *psi-student* for this purpose. The password and further instructions for login can be found in the VC course.

1.5 Study Groups

We strongly recommend that you form study groups to work through the material, to work on the tasks, to support and motivate each other.

1.6 Keeping up

It is crucial that you stay on top of the course content throughout the semester. Catching up with the material at the end of the semester or shortly before the exam is usually not successful. Therefore, in PSI-AdvaSP-M we use different incentive systems to motivate you, bonus points and the booklet, which will be described in later sections of the syllabus.

2. Prerequisites

For the module PSI-AdvaSP-M, we recommend to be familiar with basic concepts in information security and privacy, which can be acquired, for instance, by taking the module "Introduction to Security and Privacy" (PSI-IntroSP-B).

This includes basic knowledge about the commonly used security terminology, common types of malware and attacks, buffer overflows and related attacks, cryptography, network security, web security, and concepts of privacy. Moreover, participants should have practical experience with at least one scripting or programming language such as Python or Java.

If you feel that you do not understand fundamentals, it is important that you take the time to familiarize yourself with them so that you can follow this course.

You can join the IntroSP VC course of the previous semester to check out the material. Instructions for joining the IntroSP VC course are available in the AdvaSP VC course.

3. Bonus points

One of the incentive systems for keeping up is the possibility to score up to 20 bonus points. There are two activities with which you can earn bonus points: task sheets and essays.

3.1 Task Sheet Submissions

The first source of bonus points are task sheets with exercises that are related to the material covered in the lecture. Typically, there will be 1–2 weeks between publication of task sheet and the submission deadline. We plan to have **4 task sheets**.

In order to obtain bonus points, you have to submit your solution via VC. Please upload your solution as a **single PDF file**, i. e., do not upload your whole project folder as a ZIP file. In the PDF, please include any **relevant** pieces of code with proper syntax highlighting. In general, use a clean layout that is pleasant to read. Include your name and student number in the PDF. This makes it easier to review your solution.

You have **one token for late submission** (up to 5 days after the deadline). If you submit late, state in your submission that you want to use your token to get points for your solution despite late submission. If no token is used, we may tolerate late submission of a few minutes at our discretion.

At the end of the semester, we will **randomly select two of the task sheets** to review them for bonus points. If you submitted a solution for both task sheets, you can score up to 12 bonus points, **6 points per sheet**.

The task sheets are to be solved **by every student individually**. To ensure that everyone has an incentive to work on the task sheets on their own, we **will not accept team work**.

3.2 Essays

The second source of bonus points are essays about scientific papers. You will be asked to write **essays for 4 papers** during the semester. Responses are due 7 days after the release of a paper.

After the deadline, every essay is **reviewed** by three randomly chosen students within 7 days, i. e., every student receives three anonymous essays. Reviewers are asked to rank the three assigned essays according to their quality. They are also asked to provide a short justification. These reviews are also anonymous and te essay authors receive their ranks and the other essays after the review process.

Essay and review submission is handled via our web application **Peery**, which can be reached via VC.

The bonus points for every paper are determined as follows. If a response is submitted and it is obvious that an effort was made (not too short and no dummy submission), the author gets **1 bonus point**. If an essay is ranked on 1st position by at least 50 % of the reviewers, the author gets **2 bonus points**. Authors who do not submit a review will not receive any bonus points for their essay in the respective round.

You can collect 4 times 2 points, which equals up to 8 points in total.

4. Booklet

One of the most effective learning techniques is to take notes while reading and listening (active reading or active listening). We observe that many students, however, cannot motivate themselves to take notes continuously.

As an additional motivation to take notes on a regular basis, we have introduced the instrument of **personal exam booklets**. A booklet consists of up to 15 pages (A5 size). Each week you can submit one A5 page by a certain deadline (the exact deadline will be announced online). You can fill your booklet pages with any content you deem useful for the exam (subject to the conditions set out in Section Conditions). Before the exam, we will print your booklet pages **in color** and assembe them into a stapled booklet. You will receive your personal booklet on the day of the exam with the exam questions. At the end of the examination, you hand in the booklet with your exam so that it can be archived with the exam. If you fail the exam, you will receive your booklet in the repeat exam.

Creating the pages for your booklet requires critical thinking. What is the best way to condense the material and write it down clearly and concisely? What content do you want to outsource to the booklet, what can you remember on your own? The booklet thus stimulates an active learning process. If you are working in a learning group it is advisable that each member of your group prepares his or her own draft for every page. Then you can discuss the drafts in your learning group before all group members compile their own pages based on the discussion.

4.1 Conditions

Booklet pages may be submitted **only during the summer semester** and are acceptable aids to the examination *only during the current semester and the following winter semester*.

The conditions may seem pedantic. However, they are necessary to maintain the examination principle of *equal opportunity*.

All booklet pages must be written in **your own handwriting**, either on paper or using a tablet. Writing by hand assists your brain in remembering what you have written. Ideally, by the end of the semester, you will know what is in the booklet and what is not, so all lookups during the exam will be quick.

Screenshots of slides, the lecture notes, or from the videos are not allowed – unless you have transferred them in your own handwriting into your booklet. One printed heading in a typewritten font is allowed per page, which is the default behavior of some note-taking apps for tablets.

Scaling down and arranging multiple handwritten elements on a page is allowed. The key condition is that all of the content is in your own handwriting.

You do not have to include citations on the pages, which means, lecture slides, answers to exercise questions, content from Wikipedia etc. can be included without mentioning the source. It is also irrelevant whether booklets of different students contain the same drawings – as long as they have been drawn independently by each person.

Working out booklet pages in learning groups is allowed – as long as each booklet page has been completely handwritten by each person.

If you have taken the course in the past, it is permitted to re-submit your own pages from a past course run once again. While this practice saves work, it has the disadvantage that you will not get the incentive of regular note-taking and the benefit of active learning during the present semester.

4.2 Submission of the Booklet Pages

The submission process is handled via our booklet web application at https://booklet.psi.uni-bamberg.de. The booklet tool requires authentication via the university's single sign-on service. An invitation code is required the first time you use it. The code can be found in the VC course.

There are two ways to submit your booklet pages: **uploading an image** or **submitting on paper**.

For **submission on paper** You have to print the paper template provided in the booklet tool (available after selecting "Submit on paper in our postbox"), put your content into the designated A5 area and submit the page *before the weekly deadline* at the PSI Chair's office (WE5/05.063). If no one is present, you can slide your page under the door. We will then scan your page in color at 300 dpi.

You can also scan your pages in good quality, e. g., in WE5/04.006. To do this, insert your student ID card into the terminal, press the "Fax/Scan" button on the multifunction device and select "campusprint" as the recipient on the touch display. You can insert your page into the upper feeder and then press the start button. After the scanning process is finished, you can download your page at https://campusprint.uni-bamberg.de/ and then upload it to the booklet tool.

The alternative, **uploading an image**, is best done via a desktop browser. In the following, we provide some tips to achieve a good result. First, note that we will print your pages in A5 format on a laser printer. If you write very small, you must take care to upload a sharp image with high contrast. Check that your submissions are not too pale, cut off at the edges, or fuzzy. If you take photos of your pages, ensure sufficient and – more importantly – *even* illumination and use a sufficiently high resolution. Consider using a dedicated app that helps with digitizing paper documents. Prepare a suitable setup early on, that you are not pressed for time.

Uploading is also possible directly from the smartphone. However, the booklet web application is not yet designed for smartphone browsers.

What is a high enough resolution? Printouts are easy to read if their resolution is at least 300 dpi. So the short side of your image should have at least 1771 pixels, the long side at least 2480 pixels.

Use the **preview** function of the booklet web application to adjust the cropping and improve the contrast. To get a feel for readability, change the scaling on the computer screen so that the displayed size corresponds to a sheet of A5 sheet of paper laid on top of it. If you can read your writing at this scale, everything should be fine. The booklet application also allows you to download a **preview booklet** after uploading, which you can print yourself.

4.3 Problem Handling

After successfully uploading a booklet page, the booklet application displays a verification code. Please **make a copy of this code and the uploaded file**. The code serves as proof that you have successfully uploaded a particular file before the deadline.

If at a later time you find that a booklet page is missing, please send us an email with the image file (the exact same file you previously uploaded) and the code previously displayed in the booklet application. Only if our check shows that this code matches the file, we will add the file to your booklet afterwards.

Often, just before a booklet deadline, the internet is down – or the WiFi at the university is overloaded. If you cannot upload your image file in time because of this, please calculate a cryptographic hash value of the file you wanted to upload. Use a hash function like SHA-256 for this purpose. The obtained hash value uniquely identifies your file. Send us the hash value (and the hash function used) by e-mail before the deadline. You can also take a photo of the hash value and email it to us over the mobile network. Only if our check after the deadline shows that the hash value matches your image, we will add the file to your booklet.

If you want to prepare for this scenario, it is best to familiarize yourself in advance with how to calculate a cryptographic hash value of a file locally on your computer (in Linux there are command line tools for this). It is also a good idea to prepare everything so that you can quickly send an e-mail over the mobile network using a smartphone, if you have one.

We recommend that you do not upload booklet pages until just before the deadline. Test the upload process before the deadline to avoid any surprises. You can upload each page as many times as you like until the deadline.

We will not subsequently accept booklets for which you have not provided us with a hash value before the deadline – unless you immediately provide a suitable doctor's certificate of incapacity.

5. Examination

There will be a **written exam of 90 minutes** at the end of the summer semester. The exam will **require your on-site presence**. The repeat exam will take place at the end of the winter semester. The exam questions will be in English but you can answer in English or in German.

5.1 Relevant Material

What is relevant for the exam? Examination tasks are based on contents from the lecture videos, the exercises, the PSI Arena, and the paper readings. For a good result it is not enough to focus only on the exercises. You will also have to work through the examples given in the lecture and read the provided papers.

No additional content relevant for the exam will be taught in the face-to-face sessions.

We recommend that you look at the exams from previous semesters in VC to familiarize yourself with familiarize yourself with the style of the exam questions. You will find that for many questions it is not enough to restate facts; on the exam you must show that you can apply your knowledge and transfer it to problems with which you are not familiar. Keep in mind that the exams vary considerably in terms of task types and focal points differ considerably from one another. Do not infer from previous exams which content might be asked in the future.

Take the style of the exam questions into account when considering what content to transfer to your booklet pages.

5.2 Authorized Aids

We will give you your booklet together with the exam tasks. Only the **booklets distributed by us** are authorized, i. e. you are not allowed to bring any further notes to the exam. You are also **not allowed to add notes to your booklet before or during the exam**. Adding highlights with highlighters, however, is allowed.

Booklets that have **not been entirely handwritten by yourself** are **no authorized aids**. It is your responsibility to check whether your booklet meets this criterion. If you find that one of your pages does not meet the requirements after the deadline for that page, you can ask us to delete it from your booklet (before the deadline of the last booklet page). Replacing the content of deleted pages is not possible. After the deadline of the last page, pages cannot be deleted any more.

Furthermore, it is permitted to use a **non-programmable calculator**. Pocket calculators are considered programmable, when you can store data sets or programs, which remain available after switching off and on again. The Casio FX-5800P, for instance, is not authorized, while the Casio FX-991DE is an authorized aid.

Additionally, a **dictionary** from any language to English is allowed.

If we discover during or after the examination that unauthorized aids have been used, we must proceed in accordance with §7 (4) APO, i. e., **you will fail the exam**. In severe cases and cases of repeated misconduct, additional measures may be imposed by the examination board.

6. Expectations

We love teaching, and we care for you. On occasion, however, we have to make unpopular decisions to make you (more) successful. For me, it is "more important to be a good professor than your favorite professor."

Please find more information on my expectations in the Teaching Philosophy.

We will not focus on teaching you facts. Instead, we want to **teach you how to think**. In some parts of the course you will have to learn concepts by yourself.

It is your responsibility to

- abstain from cheating and plagiarism,
- acquire necessary background knowledge,
- invest sufficient time for self-studying,
- prepare before attending lecture and tutorials,
- consider switching to a part-time studies program if you cannot handle the workload, and
- to learn to ask effective questions.

We strongly recommend that you engage with the lectures and exercises each week. Take handwritten notes, rework your notes, and form study groups in which everyone works on all assignments rather than dividing assignments among the members.

Of course, we also expect you to be **in conformity with the law**. In addition, we would like you to treat each other in a professional and considerate manner. Hate speech and any form of discrimination is not tolerable.

Please ask us if you are unsure if a particular activity is in line with our expectations.

7. Academic Integrity

We are investing much time to offer you a high-quality academic education. In response, **we expect you to act with integrity**, namely by behaving per the commonly shared values of honesty, trust, fairness, respect, and responsibility.

Any (attempted) act that violates the core values associated with academic integrity constitutes *academic misconduct*. Deception during the examination, during obtaining bonus points, and during the preparation of the booklets

- abuse the trust between you and me,
- aim at creating an unfair advantage,
- are disrespectful toward me as your professor, your fellow students, and the institution as a whole, and
- represents a failure to take personal responsibility.

Parts of this section are inspired by the Academic Integrity Tutorial of University of Waterloo (CC BY-NC 4.0).

Acts of academic misconduct can interfere with your intellectual development as they obstruct the opportunity to meet a university education's challenges. Moreover, such actions can potentially undermine our students' and faculty's reputation and credibility, which degrades the value of a degree our university. Thus, we cannot tolerate academic misconduct.

Academic misconduct is often a result of **overwhelming pressure**. Please seek help instead of giving up your integrity. The university offers psychological counseling services to all students. We are also there for you if you struggle, but you have to get in touch with us for that.

Counseling Services for students of University of Bamberg

8. Contact and Support

Your instructors are Prof. Dr. Dominik Herrmann and Andreas Kirsch, M.Sc.

Please ask questions when you are stuck or when you do not understand something.

We prefer to get **questions about the content** in the Q&A forum in VC. Please also *post answers* if you can answer a question of your peers.

Asking questions in German is fine if you are uncomfortable with English. Alternatively, use available tools such as deepl.com for translation.

Don't hesitate to approach us.

If you have a **question about organizational or examination matters**, which you do not want to post publicly, you can reach Dominik Herrmann via e-mail at dominik.herrmann@uni-bamberg.de.