# Introduction to Security and Privacy (PSI-IntroSP-B)

*Syllabus for Winter Semester 2023 · v1.0 / 20231022*

**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 introduces you to fundamental concepts in the fields of information security and the protection of privacy. It provides a broad overview of the most relevant topics from a technical perspective. The focus lies on practical issues that have to be considered when professional and personal information systems are built and operated.

This course is worth 6 ECTS, consists of a lecture and tutorials (2 + 2 hours per week), and is taught in English. You cannot collect bonus points ("semester-begleitende Studienleistung") in this course. All materials will be made available via its corresponding VC course. During the first two weeks of the semester, you do not need an enrollment key. After that, please contact our office.

**Learning Objectives.** Successful students will know, understand, and apply basic security and privacy concepts. Moreover, they will know how to take useful notes and how to understand academic texts. Finally, they will have improved their skills to implement tools to automate security analyses tasks.

This **syllabus** provides all relevant pieces of information one place. The syllabus helps managing expectations, gives reasons for the course design, and answers all organizational questions. Please read it carefully since 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.

**A word of warning.** This module has the reputation of requiring a significant amount of work to pass the exam. Some of the assignments are very challenging. Working on them, however, is insightful, and finding the solution can be quite rewarding. Moreover, the assignments allow you to hone your problem-solving skills.

## 1. Flipped Classroom

This lecture runs in the *flipped classroom model*. The flipped classroom model aims to overcome the problems of classical face-to-face lectures. Classical lectures, in which a lecturer presents slides, result in an environment where consume lectures passively in the lecture hall. After the lecture, students struggle to post-process the contents of the lecture. As a result, there is little engagement with the content.

In a flipped classroom, the locations where students acquire knowledge and where students practice are switched. Students acquire new information by watching lecture videos at home whenever it fits their schedule (instead of in the lecture hall at a fixed point in time). After that, they come to face-to-face sessions (the "Plenary") in the lecture hall. There, they are asked to apply the newly acquired knowledge via exercises and discussions, i. e., practicing takes place as a group during the lecture hours (instead of at home). This design promises to be more engaging – and more fun – which hopefully results in more students mastering the material.

## 1.1 Materials

We provide materials for self-studying. There are **six types of materials**: lecture videos, lecture slides, plenary slides, tutorial tasks, readings, and a lecture script. You are expected to watch the lecture videos and study the slides and (if announced) the readings before you attend the face-to-face sessions ("Plenary"). Plenary slides will be published after the plenary.

Slides and documents will be made available via VC, videos will be released on Panopto (accessible via the VC course). **Videos** can either be viewed in the browser or downloaded. We recommend downloading the videos to have access to them in case of network failures or overloads.

All **lecture slides** have already been published in VC. Most slides show figures and visualizations that support the lecture. We like to keep the amount of text on the slides small to avoid fatigue ("death by PowerPoint").

Complementary to the lecture slides and the videos, there is also a draft version of a **lecture script** that will be released on VC throughout the semester. For now, reading the lecture script is **optional**. We appreciate, however, notifications about errors or ambiguous explanations in the script.

In addition, we also provide some **mandatory readings**.

For some tutorials, we publish **in-presence task sheets** in VC. You are expected to work on these *during* the tutorial on your own, supported by tutors.

In addition to the in-presence task sheets, there are **homework tasks** for self-study.

There are also some tasks in the **PSI Arena** (https://arena.psi.uni-bamberg.de), which is our interactive web-based learning tool based on the Insekta platform.

Some of the exercises involve coding and analyzing programs. You can perform these tasks on your machine or the **PSI Playground**, a Linux server provided by us. Instructions to access the PSI Playground will be published on VC. In case you run into problems with that, approach a tutor in the tutorials.

You will need access to a working C compiler to work on the first homework tasks, so please, get set up quickly.

## 1.2 Face-to-Face Sessions: Plenaries

At the time of the lecture, we meet for the **Plenary**. The plenary takes place roughly every two weeks. These face-to-face sessions will not be recorded.

You can find the rooms and times for the Plenary in UnivIS. As with all other lectures at the WIAI Faculty, attendance in lectures is not mandatory but, of course, recommended. Watch for VC announcements that inform you when face-to-face sessions take place. Typically, the next plenary will be announced at end of the plenary slides.

In the plenary, you can consolidate and review the knowledge you have acquired so far. In contrast to a lecture, the plenary does not consist of a presentation that you are supposed to consume. Instead, you will work on questions and discuss them with your peers. In the plenary, I will call on you and engage in discussions with you. Please come to the plenary only if you have studied the material provided up to that point. Bring your notes and be prepared to take notes during the plenary.

## 1.3 Tutorials

All tutorials during the week discuss the same content, i. e., it is sufficient to attend one of the tutorials. Attendance in the tutorials is not mandatory but recommended.

What happens during the tutorials? Let us start with what does *not* happen: The tutors will not present the solution to the homework tasks during the tutorials. The tutorials are meant as a working space for you and your fellow students. You may use the time to meet up with your study group, e. g., starting to work on the homework assignments while having a tutor available if you get stuck.

Secondly, in some of the tutorials there may be *in-presence tasks*. These tasks are typically shorter than the homework assignments. You are supposed to work on them and complete them during the tutorial. You can work on these tasks alone or in study groups of two to three students.

We may publish solutions for selected homework tasks. The solutions do not contain all intermediary steps. They allow you to check whether you have obtained the correct solution. For some tasks, the solutions will also contain a short description of the idea on how to solve the task. In contrast to the homework assignments, we will not publish solutions for the in-presence tasks.

## 1.4 Asking Questions

In case you get stuck, first consult your study group. Maybe someone else has already figured out how to solve a particular problem. If this is not the case, approach a tutor, preferably in the tutorial. Outside of the tutorials, you may use the **VC Forum**.

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., considered concept, 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.

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 questions anonymously**. You can use our anonymous user account *psi-student* to ask questions in the forum. The password and further login instructions are available in VC.

### 1.5 Study Groups

We strongly recommend that you form study groups to work on the material and the cases. Within the group it is easier to support each other and keep motivated. Study groups also help reduce frustration and loneliness.

### 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 will, most likely, not work out.

We provide two incentives to help you with that. Firstly, there is the **Booklet**, which we will explain in the section Booklet.

Secondly, we will publish multiple-choice **quizzes** in the PSI Arena throughout the semester. The Arena assesses the correctness of your answers immediately and you can try again if necessary. You should not need more than 30 minutes for each quiz. Attempting the quizzes is beneficial as you can train to work on problems under time constraints, and you get an understanding of our expectations.

## 2. Prerequisites

Security and privacy are often only meaningful in the context of a concrete application. PSI-IntroSP-B introduces you to the breadth of the field, i. e., you will be exposed to various application areas and technologies, some of which may be unfamiliar.

We recommend taking this course only once you have passed PSI-EiRBS-B or other courses on computer architectures and operating systems. While having completed lectures on computer networks, web technologies, and software engineering may flatten the learning curve, we will only depend on specific basics of these areas, which you can also acquire on the fly.

We assume that you are familiar with the basics of the **Linux command line**.

You should be familiar with fundamentals of **computer architecture** (binary representation of strings and numbers in computers, bitwise operators such as XOR, operation of a CPU, basics of assembly language), and **operating systems** (memory layout and process management).

Some parts of the course assume that you are familiar with practical aspects of **computer networks** (basic IP routing and addressing, TCP/IP connection establishment), common web technologies (HTTP, HTML, JavaScript, PHP), and relational database systems (SQL).

Finally, you should have working knowledge in at least one **programming language** (e. g., Python, C, or Java) so that you can write small tools that automate some tasks, such as decrypting some ciphertext.

**We offer self-study materials** for some of the specifically required preliminaries, for instance, memory layout on the stack, computer networks, and web technologies. Please let us know whether these offers are helpful and whether essential preliminaries are missing.

## 3. Booklet

One of the most effective learning techniques is to take notes while reading and listening (active reading or active listening).

We observe, however, that many students cannot motivate themselves to take notes continuously. Instead, many students procrastinate throughout the semester. Shortly before the exam period, students engage in frantic binge-learning activities. This form of studying is not only stressful but not an effective technique to master the material and adopt sustainable skills (besides stress resistance).

As a motivation to take notes on a regular basis instead, we have introduced the instrument of **personal exam booklets**. A booklet consists of up to 15 pages of size A5.

Every week you can submit one 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 Requirements). If you submit pages every week, your booklet will consist of 15 pages, otherwise it will consist of less pages.

The pages that you submit can have any size and any format. Before the exam, we will scale down your pages to A5, print them **in color**, and assemble 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 study 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 study group before all group members compile their own pages based on the discussion.

Submitting booklet pages is a voluntary activity. You can pass the exam without a booklet, and we do not create exam questions that assume that you have a booklet.

### 3.1 Requirements

Booklet pages may be submitted **only during the semester that the lecture is offered** and are acceptable aids to the examination *only in this semester*. If you do not submit a page by the deadline, your booklet will have less pages than possible. Changing pages after the deadline is not possible.

The requirements 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. 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.

Whether handwritten or computer-generated notes are more effective for learning success cannot yet be answered unequivocally. Recent studies come to different conclusions. See the seminar study by Mueller and Oppenheimer (2014), its replication by Morehead et al. (2019), the online article by Haring and Kelner (2021) as well as the more recent studies by Umejima et al. (2021) and Wiechmann et al. (2022).

*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 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 – if they have been drawn independently by every person.

Working out booklet pages in study groups is allowed – if 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. While this practice saves work, it has the disadvantage that you will not get the incentive of regular notetaking and the benefit of active learning during the present semester.

### 3.2 Page Submission

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.

To submit a page, you **upload an image**, ideally using a desktop browser. In the following, we provide some tips to achieve a good result.

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

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.

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 an 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.

### 3.3 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 later 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.

Sometimes, just before a booklet deadline, the internet is down – or the Wi-Fi 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.

## 4. Examination

There will be two opportunities to take a **written exam** at the end of the winter semester. You must pass only one of the exams to pass the module. The exam will **require your on-site presence**. The dates of the exams will be announced in VC. Note that besides the two exams in the winter semester, there will be no further exams. The next exams will be offered about one year later.

The exam will be an **e-exam**, i. e., you will write the exam on a laptop that is provided by us. More details on the logistics of the e-exam will be released during the semester in VC. There will be a test exam so that you can familiarize yourself with the electronic examination environment.

The exam questions will be in English, but you can answer in English or in German.

## 4.1 Relevant Material

Exam tasks may focus on content from the lectures, the tutorials, the in-presence assignments, the homework assignments, and the mandatory readings.

Content in the lecture script that is not mentioned in the lecture slides is not relevant for the exam.

Please have a look at the previous exams in VC to become familiar with the style of the exam tasks. You will notice that most questions **do not ask you to reproduce facts** but apply your knowledge or analyze a problem. For a good result it is not enough to focus only on the exercise; also work with the examples from the lecture.

Our examinations often differ considerably regarding the types of tasks used and the focus. Do not draw conclusions from previous exams as to what topics might be on the next exam.

## 4.2 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 has passed, you can ask us to delete it from your booklet by the deadline of the last booklet page. Replacing the content of deleted pages is not possible.

Furthermore, using a **non-programmable calculator** in the exam is permitted. Pocket calculators are considered programmable, where 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.

Finally, a **dictionary** is also an allowed aid during the exam.

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.

We would like to know if this syllabus is read. If you have read this text, we would be pleased if you send us a picture via this link showing an animal you like.

## 5. Expectations

We love teaching, and we care for you. On occasion, however, we must 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 in VC.

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 work on the lectures and exercises each week. Take handwritten notes, rework your notes, and form study groups where everyone works on all assignments rather than dividing assignments among yourselves.

Of course, we also expect you to be legally compliant. This applies, in particular, to the PSI Playground, which you may only use for self-study. In addition, we would like you to treat each other in a professional and considerate manner.

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

## 6. 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.

Cheating on the exam or on the booklet pages

- 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.

Any action or attempted action that breaches one or more of the fundamental values associated with academic integrity is considered *academic misconduct*.

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

## 7. Contact and Support

**Please ask questions** when you are stuck or when you do not understand something. You can ask questions during the tutorials or asynchronously.

While some of the pre-recorded videos still mention Rocket.Chat as communication option, according to our experience and feedback from students there is little benefit in having a group chat for a course. Therefore, there **will not be any Rocket.Chat support** this semester.

We prefer to get **questions about the content** in the Q&A forum in VC. We encourage you to *post answers* if you can answer a question of your peers. Explaining concepts to others or answering their questions is one of the best ways to improve your own understanding.

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

Do not hesitate to approach us, for instance, during the in-presence tutorials or via mail.

Contact details for the **tutors** are available in the VC course.

If you have a **question about organizational or examination matters**, which you do not want to post publicly, you can reach me via e-mail at dominik.herrmann@uni-bamberg.de. Preferably, approach the tutors first because they can answer most of the questions.

## 8. Textbooks and Readings

Two textbooks that cover most aspects of this lecture on a high level:

- W. Stallings & L. Brown: *Computer Security: Principles and Practice*.
- C. P. Pfleeger et al.: *Security in Computing*.

We can also recommend the following three books:

- J. Erickson: *Hacking: The Art of Exploitation* – strong focus on software and web security.
- R. Anderson: *Security Engineering* – covers a large number of topics, very thorough and broad.
- A. Shostack: *Threat Modelling* – contains some best practices for handling security in professional environments.

We will publish links to more focused readings in VC. Some of these readings are **mandatory readings**.

## 9. Outline of the Course

Finally, let's preview the content of the course. We will cover the following areas in the order given below:

*Security Terminology* threats, risk, protection goals, attacks, countermeasures;

*Software Security* issues in C and Assembly programs, e. g., buffer overflows and memory safety defenses;

*User Accounts* Authentication and Authorization Fundamentals;

*Cryptography* e. g., historic ciphers, symmetric and asymmetric cryptosystems, Diffie-Hellman key exchange, the TLS protocol;

*Network Security* e. g., spoofing, denial of service, firewalls, intrusion detection systems;

*Web Security* e. g., attacks and defenses related to the OWASP Top 10 including SQL injections and Cross Site Scripting; and

*Privacy and Data Protection Techniques* re-identification risks, anonymization networks, k-anonymity, and the idea of differential privacy.

**Learning Outcomes.** Successful students will know the mathematical background behind basic cryptographic primitives and be able to explain fundamental concepts of information security and privacy, including classical attacks and defenses. They will be able to apply their knowledge when implementing simple attack programs as well as building and operating defensive techniques.