PSI-IntroSP-B Syllabus

Winter Semester 2021/22 · v1.1 / 20211017

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 syllabus is an attempt to provide all relevant pieces of information about PSI-IntroSP-B in one place. The syllabus helps managing expectations, and it gives reasons for the course design. Please read it carefully and inform us if anything is unclear or missing.

1. Practicalities

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 a VC course. During the first two weeks of the semester, you do not need an enrolment key.

The first lecture takes place on Oct 18 from 12:15 o'clock as a livestream with Q&A in Rocket.Chat during the lecture. After the lecture, there will be a 30-minute "meet and greet" session so that you can show your face and say "Hello".

We offer video recordings of all lectures. **Recordings** will be available via VC and Panopto (access limited to the course, i. e., a closed group). We also offer video recordings for all tutorials.

We publish all **lecture slides** 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"). We also provide some **readings**.

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

In addition to the in-presence task sheets, there are **homework tasks** for self-study. We expect you to work on these on your own *before* the tutorials, ideally in learning groups.

To support self-studying, we publish some tasks in the **PSI Arena** (https://arena.psi.uni-bamberg.de), which is our web-based training 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 are available in VC.

One of the tutors will show how to access the Playground during the first tutorial.

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

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.

2. Online Teaching

Given the current situation, we have decided, with a heavy heart, to avoid face-to-face on-campus lecture and tutorial sessions for the time being. We believe that everyone should have equal opportunities, including those who are not in Bamberg and those who are reluctant to come to the university at the moment. Initially, we planned to have optional on-campus and online sessions in this course. Still, we could not develop a pedagogically sound concept that wouldn't have interfered with course workload and examination equality while still being worth your time.

Lecture and tutorials run synchronously *and* asynchronously. We produce pre-recorded videos, which are **live-streamed** during the lecture timeslot announced in UnivIS. We offer a live stream because it helps to establish a sense of community.

Recordings will be available for download after the lecture in Panopto so that everyone has access to the same content.

Captions (subtitles) have been shown to improve understanding, especially if English is not your native tongue. We will, therefore, transcribe all videos to **provide captions**. If we complete the transcript on time, the live stream will contain *open captions*, which are rendered into the video and cannot be disabled. The recordings, which are published after the live stream, will have *closed captions*, i. e., you can enable them if desired. The recordings will also offer a scrollable transcript that allows you to quickly jump to the desired part of the lecture.

2.1 Interaction

TL;DR: Q&A will be handled via Rocket.Chat during lecture and tutorial livestreams, in Whereby video conferences after the livestreams, and asynchronously in the VC Forum. You can also make an appointment to meet with us on campus for Q&A. For contact and support options, see the section Contact and Support.

https://wiai.whereby.com/meet-psi

We are reluctant to use US-based service providers. Whereby is based in Norway and offers a decent web interface as well as lightweight apps for iOS and Android devices.

Rocket.Chat is useful for asking shorter questions, e. g., during the lecture and the tutorials.

The **Forum** is more suitable for more extended questions, e. g., when you seek help for a task. In this case, please describe what you have attempted so far, what unexpected outcome you observed, and what you would have expected.

Please follow the advice on asking questions in the Teaching Philosophy.

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. Note that this account only works in VC but not in Rocket.Chat.

2.2 Tutorials

We will broadcast tutorial videos in a live stream at one point in time during the week. The videos will be available after the live stream so that you can attend asynchronously if you have a scheduling conflict.

For the live stream, we will select the time slot which suits most of you. Please **vote on the preferred time slot** for the tutorial live stream in VC.

Tutorial videos consist of explanations of the homework assignments, "now it's your turn" sessions in which you are supposed to work on the in-presence assignments, and explanations of the in-presence assignments. This means, you should set up your environment so that you can work on assignments during the tutorials.

Generally, we will not give you solutions to homework tasks in advance. We will, however, answer clarification questions and give you tips if you are stuck.

2.3 Learning Groups

We highly recommend building learning groups to discuss the material and work on the tasks. Learning groups reduce frustration and loneliness.

2.4 Keeping Up

It is paramount that you keep up during the semester. We provide three incentives to help you with that.

Firstly, there is the **Booklet**, which we will explain in the section Booklet.

Secondly, there will be four multiple-choice **quizzes** in the PSI Arena. Each quiz is available for a fixed amount of time (e. g., 30 minutes). The Arena assess the correctness of your answers immediately and you can try again if necessary. After the time is up, we will review the tasks in the tutorial. Participation in the quizzes is beneficial as you can train to work on problems under time constraints, and you get an understanding of our expectations.

Thirdly, we ask you to **share your work** with others. Looking at the solutions of your peers fosters reflection and analysis – and may ultimately improve your understanding. Therefore, we will ask you to share your work – anonymously – within the course by **uploading it to VC**. Access to your peers' solutions is only granted to those who have uploaded their solution themselves. We hope that this setup incentivizes participation and ultimately helps to establish a community of learners. After all, all of you are in this together.

3. 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 invite you to complete our **self-assessment quiz** in the PSI Arena to check your pre-existing knowledge.

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.

4. Booklet

One of the most effective learning techniques is to write notes and refine them during the semester. For more techniques, see the Teaching Philosophy. We observe that many students cannot motivate themselves to write notes on a regular basis.

As an incentive for extensive note-taking, we implement the **personal booklet technique** in this course. The booklet consists of up to 15 pages of size A5. Every week you can submit or upload one A5 page by a certain deadline. You can fill this page with any content you deem useful for the exam (subject to the conditions described in section Requirements). We will assemble your pages and **print them in color** to create a booklet. We will give you your personal printed booklet together with the exam tasks. You will have to hand in your booklet together with the exam again.

Creating pages for your booklet requires you to think critically. What is the best way to compress the material and write it down clearly and concisely? The booklet encourages this active learning process. If you work in a learning group, it is probably most beneficial if each member of your group prepares a draft of the page, and you discuss the drafts in your group before all group members assemble their pages.

4.1 Requirements

All pages must be in **your handwriting**, either on paper or by using a tablet. Copying by hand helps your brain remember what is in the booklet. Ideally, you will know precisely what is and what is not in the booklet so that looking up content during the exam is fast.

Screenshots from slides or recordings are not acceptable – unless they are drawn by yourself. A non-handwritten headline inserted by some note-taking apps (showing the current date, etc.) is permissible.

Arranging and resizing several handwritten pieces on a page or resizing them is permissible. The decisive factor is that the content is in your handwriting.

You do not have to include citations on the pages, i. e., it is allowed to copy lecture slides, tutorial task answers, content from Wikipedia, etc. without mentioning the source. It is irrelevant whether booklets of different students contain the same images – as long as they are in the respective students' handwriting.

Developing booklet pages in learning groups is allowed – as long as each booklet page has been entirely handwritten by the respective student.

This rather strict set of regulations may seem pedantic, but it is necessary to maintain equal opportunities.

4.2 Page Submission

The submission of booklet pages is handled via our booklet web application at https://booklet.psi.uni-bamberg.de. The booklet application requires you to authenticate via single sign-on. During the first sign-on, the application may ask for your student number. Please enter your student number correctly.

There are two ways to hand in your booklet pages: **uploading a scan** or **submitting on paper**. For the latter, you have to use the paper template provided in the booklet tool for the respective page, write your content on it and drop it in the mailbox of the PSI Chair in the foyer of the building WE5. You will find further instructions on the template. We will scan your page at 300 dpi in color.

In the following, we provide some tips for those who intend to *upload a scan*.

First of all, note that we will print your pages in A5 format on a laser printer. If you write very small, you must take special 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.

What is a sufficiently high resolution? Printouts are easy to read when they have at least 300 dpi. Thus, the short side of your page should have at least 1771 pixels, the long side at least 2480 pixels.

You can use the preview function of the booklet tool to adjust the cropping and improve the contrast. To get a feeling of the readability, change the scaling on the computer screen so that the displayed size corresponds to an A5 sheet placed on top of it. If you can read everything at this scale, you should be fine.

4.3 Problem Handling

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

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

If you are unable to upload your image, for example because your internet connection is down, please calculate a cryptographic hash value of the file you want to upload. Use a secure hash function for this, for example SHA-256. The hash value obtained will uniquely identify your file. Send us the hash value (and the hash function used) by email or Rocket.Chat before the deadline. You can also take a photo of the hash value and transmit it over the mobile network. If our post-deadline verification shows that the hash value matches your image, we will still accept the image after the deadline.

If you want to prepare for this scenario, it is best to familiarize yourself in advance with how to compute a cryptographic hash value of a file locally on your computer (in Linux there are several command line tools for that).

We recommend that you do not upload booklet pages until shortly before the deadline. We will not accept booklets for which you have not sent us a hash value before the deadline - unless you immediately submit a suitable medical certificate of incapacity.

5. Examination

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

5.1 Relevant Material

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

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.

Our examinations often differ considerably with regard to 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.

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 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 poossible.

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.

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 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 recommend attending the lectures “live” instead of postponing watching the recordings. Also, take notes in hand-writing, post-process your notes, and build learning groups in which everyone works on all tasks instead of distributing the load.

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.

- 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

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. You can ask questions during the lectures, during the tutorials, or asynchronously.

We prefer to get **questions about the content** in Rocket.Chat or 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.

Do not hesitate to approach us, for instance, by directly messaging us in Rocket.Chat. We will chat with you or set up an audio or video call to help you with your issue. We consider this approach superior to discussing particular problems synchronously during the tutorials.

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.

9. 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 numbers 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**.

10. 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.

11. PSI Talks: Informal On-campus Interaction

Mentoring and inspiring students are dear to us, but meaningful interaction has proven difficult during hybrid and online teaching. We had, however, interesting discussions at the PSI chair in the past, for instance, when students and tutors were around.

With PSI Talks, we aim to make these informal academic exchanges accessible for a larger audience. If you want to socialize in an informal academic setting on campus, sign up for a (not-for-credit) PSI Talks event. At a PSI Talks event, students and staff of PSI will share insights from their research, learning, teaching, reading, writing, and academic scholarship. We will also discuss topics from the lectures and current affairs about security, privacy, ethics, and more. Each PSI Talks event will consist of a small group to foster interaction, take place in the WE5 building, and last 60 minutes. The first PSI Talks event takes place in the second week of the semester in German; events in English will follow.

Sign up in the PSI Talks VC course with the times that fit your schedule and your topics of interest. A few days before the event, we will send out invitations with time and location.

PSI Talks VC Course