Fraunhofer AISEC

Fraunhofer Institute for Applied and Integrated Security AISEC

SEMINARS SUMMER TERM 2025:
- CYBER-PHYSICAL SYSTEMS SECURITY (CPSS)
- EXPLOITED - INVESTIGATING SECURITY FAILS (EIS)
- CONCEPTS OF SECURITY AND AUTHENTICITY (COSA)
- PRIVACY MATTERS - ENSURING CONFIDENTIALITY (PEC)

PRE-COURSE MEETING 04.02.2025

Contents

Fraunhofer AISEC

Facts & figures

- **Founded:** 2009
- **Employees**: approx. 250

- **Locations**: Garching near Munich (main locaton), Berlin, Weiden i.d. Oberpfalz
- **International**: Partner institute of Fraunhofer Singapore
- **University connections:**

Technische Universität München — Prof. Dr. Eckert und Prof. Dr. Sigl

Freie Universität Berlin — Prof. Dr. Margraf

Ostbayerische Technische Hochschule Amberg-Weiden — Prof. Dr. Loebenberger

© Hans Georg Esch

Last updated: October 2024

Fraunhofer AISEC

Areas of expertise

Service and Application Security
Cloud and container infrastructures, distributed applications

Secure Operating Systems
Security of hardware-facing software and operating systems

Product Protection and Industrial Security
Anti-counterfeiting, automotive security, industrial security, IoT, smart building

Hardware Security
Trustworthy electronics and secure embedded systems

Cognitive Security Technologies
Security for, with and through AI

Secure Infrastructure
Application of cryptographic methods, secure network protocols

Secure Systems Engineering
Secure and user-friendly digital systems

Security from Hardware to the Cloud

Course Objectives

Assessing the state of the art regarding a specific topic in the context of security

- **Write a paper** about your findings
- **Give feedback** to (two of) your fellow students' papers (peer review)
- **Give a talk** in order to **discuss** your topic with your fellow students at the end of the semester

Previous Knowledge?

- **no formal requirements**
- **ITsec knowledge necessary!**

Orga

Communication

- TUM Moodle
- Video Calls via MS Teams
- E-mail – **always use "reply-all"** when writing or answering to us!
- Language of instruction and deliverables will be **English**

Individual work (no groups)

Registration in matching system (http://docmatching.in.tum.de/)

Motivational e-mail to security-seminar@aisec.fraunhofer.de

About, e.g., your relation to (IT-)security, your preferred seminars(!), your preferred topics, which topic you like most, and why

Process (1/4)

04.02.2025 (today)

- Organizational information
- Overview on topics

Until 19.02.2025

- Registration via DocMatching: http://docmatching.in.tum.de/
- **Motivational email** to security-seminar@aisec.fraunhofer.de

28.02.2025

- Automated assignment of courses

Until 05.03.2024

- Please send us an ordered list of your 5 preferred topics via email (if not already done in your motivational email)

Process (2/4)

Until 10.03.2025

- Response from organizers with assigned topic
- Possibility to withdraw without penalty - non-attendance after this point is graded with 5.0

Until 31.03.2025

- Familiarize with literature
- Deep dive into your topic
- As soon as possible: Schedule a kickoff meeting with your supervisors – **obligatory**!

Until 19.05.2025

- Preparation of the draft version of the paper
- Submission of the draft is **obligatory**!

Process (3/4)

Until 20.05.2025

- Assignment of two of your fellow students' paper for review

Until 27.05.2025

- Preparation of written review of these papers

Until 01.06.2025

- Rebuttal period

Until 22.06.2025

- Preparation of the final paper
- Revision based on reviews/rebuttal

Process (4/4)

Until 02.07.2025

- Slide preparation

Until 10.07.2025

- Comments on the slides from supervisor

Until 13.07.2024

- Revision of slides

14./15./16.07.2024

- Final presentations + discussion (in-person at Fraunhofer AISEC)
- Length of each presentation 25 minutes + 15 minutes of discussion
- Participation in your seminar is **obligatory** (1 of the 3 days)

Deadlines for Obligatory Deliverables

	Due to	Grading
Schedule 1-to-1 Kick-Off Meeting with supervisors	31.03.2025	Obligatory
Submission of Draft Paper	18.05.2025	10%
Reviews	27.05.2025	5%
Rebuttal	01.06.2025	Obligatory
Submission of Final Paper	22.06.2025	50%
Presentation	14./15./16.07.2025	30%
Presentation Discussion	14./15./16.07.2025	5%
		Σ 100 %

-> Missing any deadline will have a major impact on your grade.

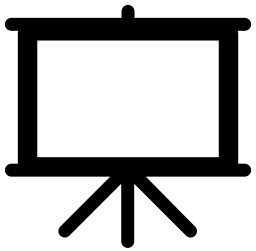
Paper writing and presentation

Paper

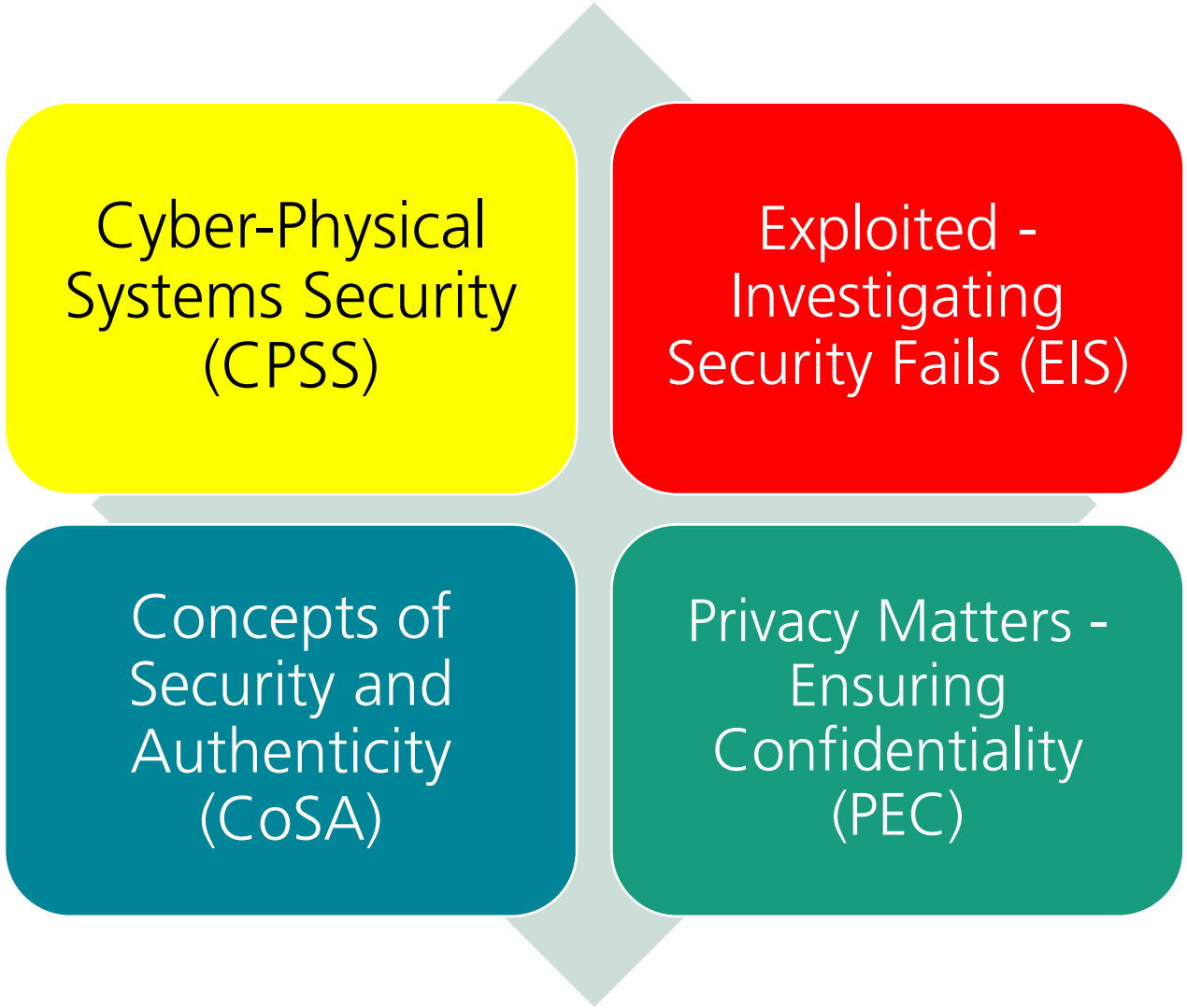
- Systematization of Knowledge (SoK)
- ~10 pages excl. list of references and appendices
- IEEE conference proceedings template
- Utilization of LaTeX (highly recommended)
- Note the *Scientific writing guide* in the Moodle course

Presentation

- MS Powerpoint or similar
- 25 minutes presentation
- 15 minutes discussion - moderated by you

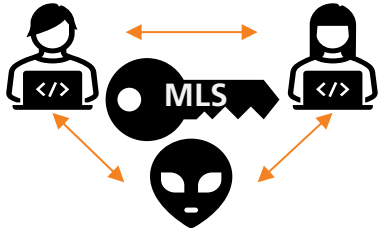


Four Seminars



Cyber Physical Systems Security (CPSS)

Topic 1: Applicability of Messaging Layer Security (MLS) in P2P networks



Possible questions to be answered: How mature is the Messaging Layer Security (MLS) protocol? What applications currently exist with MLS? What are the strengths and weaknesses of the protocol? How about Peer-to-Peer scenarios?

Literature to start from:

- The Messaging Layer Security (MLS) Protocol - https://datatracker.ietf.org/doc/rfc9420/
- On Post-compromise Security - https://doi.org/10.1109/CSF.2016.19
- TreeKEM: Asynchronous Decentralized Key Management for Large Dynamic Groups - https://inria.hal.science/hal-02425247/file/treekem+%281%29.pdf
- TreeSync: Authenticated Group Management for Messaging Layer Security - https://eprint.iacr.org/2022/1732.pdf

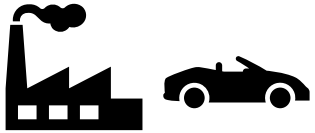
Topic 2: Comparative Analysis of Regulatory Requirements for Automotive Cybersecurity

Possible questions to be answered: Compare the regulatory requirements for automotive cybersecurity in different regions (e.g., Europe, USA, Asia). What are the key regulations such as UNECE WP.29, China's GB 44495-2024? How do these regulations influence Original Equipment Manufacturers (OEMs) and suppliers in terms of compliance and implementation? Are there contradictions or inconsistencies between different regional regulations? What aspects of automotive cybersecurity might be missing or insufficiently addressed in current regulations? How do regulations such as the EU's Euro 7 regulation, primarily focused on emissions, indirectly impact automotive cybersecurity requirements?

Literature to start from:

- UNECE WP.29 Regulation No. 155 – Cyber Security and Cyber Security Management System
- UNECE WP.29 Regulation No. 156 – Software Update and Software Update Management System
- GB 44495-2024 – Technical Requirements for Vehicle Cybersecurity (China)
- European Union's Euro 7 Regulation – Emission standards and indirect effects on vehicle cybersecurity

Topic 3: Automotive Supply Chain Security



Possible questions to be answered: What are the main cybersecurity risks and vulnerabilities in the automotive supply chain? How do third-party components and software introduce security risks into vehicles? What strategies can be implemented by Original Equipment Manufacturers (OEMs) and suppliers to enhance supply chain cybersecurity? How can companies assess and manage the cybersecurity posture of their suppliers and partners? Are there real-world examples of supply chain cybersecurity breaches in the automotive industry, and what lessons can be learned from them?

Literature to start from:

- Securing Automotive Software Supply Chains https://www.ndss-symposium.org/wp-content/uploads/vehiclesec2024-15-paper.pdf
- Open Problems when Mapping Automotive Security Levels to System Requirements https://www.scitepress.org/Papers/2018/66653/66653.pdf
- Driving with sharks: Rethinking connected vehicles with vehicle cybersecurity https://ieeexplore.ieee.org/document/7908939

Topic 4: Risk Assessment Methodologies for Automotive Cybersecurity

Possible questions to be answered: Compare risk assessment methodologies proposed for or used in automotive cybersecurity. What are the key differences in their approaches, scopes, and applications within the automotive context? Which methods are useful to analyze both onboard vehicle systems (Electronic Control Units) and offboard systems (e.g. IT backend servers, production systems)? What are the strengths and weaknesses of each methodology in terms of effectiveness, complexity, and resource requirements?

Literature to start from:

- Security Risk Assessments: Modeling and Risk Level Propagation https://dl.acm.org/doi/10.1145/3569458
- A Risk Assessment Framework for Automotive Embedded Systems https://dl.acm.org/doi/10.1145/2899015.2899018
- A Systematic Risk Assessment Framework of Automotive Cybersecurity https://link.springer.com/article/10.1007/s42154-021-00140-6
- A Systematic Review of Threat Analysis and Risk Assessment Methodologies for Connected and Automated Vehicles https://dl.acm.org/doi/10.1145/3600160.3605084

Topic 5: Group Key Agreement for Industrial Busses

Assume you have an industrial bus system (could be CAN, Ethernet, etc.) with multiple embedded devices communicating on the bus. How to secure their communication? You need some form of group key agreement!

Possible questions to be answered: Which group key agreement protocols exist? How to categorize them? What relevant characteristics do industrial busses have? Which group key agreement protocols could be suitable? Which protocols work for embedded devices with only limited resources (minimize asymmetric operations)?

Literature to start from:

- Recommendation of secure group communication schemes using multi-objective optimization - https://link.springer.com/article/10.1007/s10207-023-00692-0
- A secure key agreement protocol for dynamic group - https://link.springer.com/article/10.1007/s10586-017-0853-0
- A Secure and Receiver-Unrestricted Group Key Management Scheme for Mobile Ad-hoc Networks - https://ieeexplore.ieee.org/document/9771870

Topic 6: A practical approach on authentic date and time in mobile and cyber-physical systems

Possible questions to be answered: What are possible time sources for mobile and cyber-physical systems? E.g., GNSS, Wi-Fi, Mobile data, DCF77/MSF/TDF/WWVB, SDARS, and other satellite or terrestrial systems (be creative!)? Evaluate their authenticity and discuss attacker scenarios. Which algorithms could be used for error minimization and sensor/time fusion? Which gradations for trustworthiness of (external sources of) time exist? According to which criteria/events should the trust level be decreased?

Literature to start from:

- A Security Analysis and Revised Security Extension for the Precision Time Protocol - https://ieeexplore.ieee.org/abstract/document/8025399
- RFC 5905 Network Time Protocol Version 4: Protocol and Algorithms Specification - https://datatracker.ietf.org/doc/html/rfc5905
- Security Assessment of Time Synchronization Mechanisms for the Smart Grid - https://ieeexplore.ieee.org/abstract/document/7397831
- DCF77 Receiver authorization and availability - https://www.ptb.de/cms/en/ptb/fachabteilungen/abt4/fb-44/ag-442/dissemination-of-legal-time/dcf77/dcf77-receiver-authorization-and-availability.html

Topic 7: Secure Logging for Cyber-Physical Systems – A requirements analysis

Possible questions to be answered: What are the important requirements for Logging in Industrial and Cyber-Physical systems? Which requirements overlap? Based on NIST Guide to OT Security, BSI ICS Security Kompendium, NERC CIP, and other standards. [strong focus on norms/standards/requirements]

Literature to start from:

- NIST SP 800-82r3 Guide to OT Security - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf
- NERC CIP - https://www.nerc.com/pa/Stand/Reliability%20Standards%20Complete%20Set/RSCompleteSet.pdf
- BSI ICS Security Kompendium 2024 - https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security_kompendium_pdf.html
- A Secure Event Logging System for Smart Homes - https://dl.acm.org/doi/abs/10.1145/3139937.3139945
- LogSafe: Secure and Scalable Data Logger for IoT Devices - https://ieeexplore.ieee.org/abstract/document/8366984
- Facilitate Security Event Monitoring and Logging of Operational Technology (OT) Legacy Systems - https://link.springer.com/chapter/10.1007/978-3-030-98741-1_38

Topic 8: Passkeys - state of development and possible applications in industrial and cyber-physical use-cases

Possible questions to be answered: What are passkeys? What characterizes industrial and cyber-physical systems? How to bring passkeys to CPS? What are the obstacles of passkeys in IT? What are or could be the obstacles in OT?

Literature to start from:

- Why Aren't We Using Passkeys? Obstacles Companies Face Deploying FIDO2 Passwordless Authentication (Extended Version) - https://elleenpan.com/files/lassak-fidoobstacles-ext-2024.pdf
- BSI Verbraucherbefragung zur passwortlosen Authentisierung mit Passkeys - https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/passwortlose-authentisierung-bericht.html?nn=1107468
- Challenges with Passwordless FIDO2 in an Enterprise Setting: A Usability Study - https://ieeexplore.ieee.org/abstract/document/10305624
- "You still use the password after all" - Exploring FIDO2 Security Keys in a Small Company - https://www.usenix.org/conference/soups2020/presentation/farke

Topic 9: Security of EV Charging Infrastructure – Protocols and Standards

Possible questions to be answered: What are the relevant standards in public charging? How is the protocol flow? Which security measures are in place? How is trust established? Where does authentication take place? Which additional security measures are recommended? (Defensive and regulatory perspective)

Focus should be on German/EU charging infrastructure: CCS Type2: The plug, IEC 61851 & 62196: Electric charging, ISO 15118 Smart Charging, OCPP & OCPI: Managing charging stations

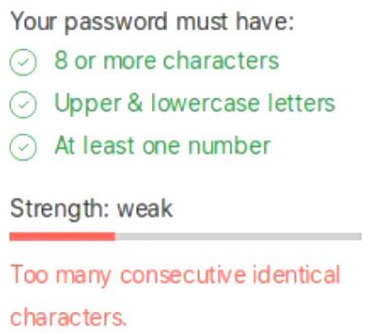
Literature to start from:

- Overview
  - Security of EV-Charging Protocols - https://doi.org/10.48550/arXiv.2202.04631
  - A Detailed Security Assessment of the EV Charging Ecosystem - https://ieeexplore.ieee.org/abstract/document/8994200
- Protocol Specific
  - OCPP Protocol: Security Threats and Challenges - https://ieeexplore.ieee.org/document/7857099
  - Electric Vehicle Charging: A Survey on the Security Issues and Challenges of the Open Charge Point Protocol (OCPP) - https://ieeexplore.ieee.org/abstract/document/9800931
  - Security Analysis of OCPI Protocol v3.0: Evaluating an electric-vehicle roaming protocol using STRIDE and DREAD frameworks - https://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1897681&dswid=-9386 (MA only!)
  - A threat analysis of the vehicle-to-grid charging protocol ISO 15118 – https://doi.org/10.1007/s00450-017-0342-y
- Proposed additional measures:
  - Extending ISO 15118-20 EV Charging: Preventing Downgrade Attacks and Enabling New Security Capabilities - https://doi.org/10.1109/PST62714.2024.10788058

Exploited – Investigating Security Fails (EIS)

Offensive perspectives

Topic 1: No double letters and one of three special characters – The Impact of Bad Password Policies

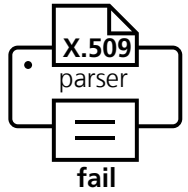


Possible questions to be answered: We all know what is best (if it has to be passwords at all): long random passwords and a password manager. So why are there always (in the best case) strange policies? E.g. "no double letters" or "max. 12 characters". What kinds of poor password policies exist? Which composition rules are stupid, which are dangerous? What temptations could drive responsibles to do this?

Literature to start from:

- Please do not use !?_ or your License Plate Number: Analyzing Password Policies in German Companies - https://www.usenix.org/conference/soups2021/presentation/gerlitz
- Do Differences in Password Policies Prevent Password Reuse? - https://dl.acm.org/doi/abs/10.1145/3027063.3053100
- Password policies of most top websites fail to follow best practices - https://www.usenix.org/conference/soups2022/presentation/lee
- Relevant public collections of poor password policies: https://dumbpasswordrules.com/sites/ and https://x.com/PWTooStrong and https://github.com/publicarray/password-policy-wall-of-shame (non-scientific)

Topic 2: Fails vs Best Practices in Certificate Parsing



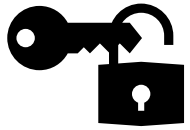
Inspired by publications, such as FrankenCert, the task of this work is to collect and structure Certificate Parsing Best Practices.

Possible questions to be answered: What is Certificate Parsing and why is it important? What are learnings from weaknesses (relevant CVEs?) in Certificate Parsing? Systematize and compile a collection of best practices.

Literature to start from:

- ParsEval: Evaluation of Parsing Behavior using Real-world Out-in-the-wild X.509 Certificates - https://dl.acm.org/doi/pdf/10.1145/3664476.3669935
- Using Frankencerts for Automated Adversarial Testing of Certificate Validation in SSL/TLS Implementations - https://ieeexplore.ieee.org/document/6956560
- Systematic Parsing of X.509: Eradicating Security Issues with a Parse Tree - https://arxiv.org/abs/1812.04959
- ITU-T X.509 Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks - https://www.itu.int/rec/T-REC-X.509-201910-I/en
- Introduction to ASN.1 - https://www.itu.int/en/ITU-T/asn1/Pages/introduction.aspx
- Relevant CVEs

Topic 3: Smart Locking Systems Unlocked

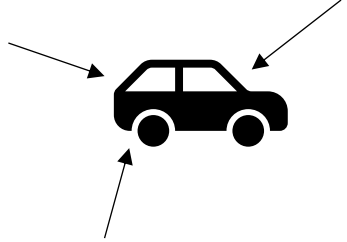


Possible questions to be answered: Which approaches on Smart Locking Systems exist? Which physical and upper layer protocols do the use? What relevant attacks were carried out on them? How to categorize them? How is their use percevied?

Literature to start from:

- Smart Locks: Lessons for Securing Commodity Internet of Things Devices - https://dl.acm.org/doi/pdf/10.1145/2897845.2897886
- Exploring the Usability, Security, and Privacy of Smart Locks from the Perspective of the End User - https://www.usenix.org/system/files/soups2023-hazazi.pdf
- Innovative IoT Smart Lock System: Enhancing Security with Fingerprint and RFID Technology - https://www.mjsat.com.my/index.php/mjsat/article/view/335/183 (careful with quality)
- Review Paper on Door Lock Security Systems - https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9318636&tag=1 (careful with quality)
- The Best Smart Locks - https://www.nytimes.com/wirecutter/reviews/the-best-smart-lock (non-scientific)
- Relevant CVEs

Topic 4: Analysis of multi-vector attacks and vulnerabilities in the automotive industry



Possible questions to be answered: Analyze real-world cyber attacks and vulnerabilities that had an effect on both onboard vehicle systems (Electronic Control Units) and offboard systems (e.g. IT backend servers, production systems). What are the attack methods used and the vulnerabilities exploited as well as (possible) impacts for Original Equipment Manufacturers and Road Users?

Literature to start from:

- Manipulated Automotive Fleet Telemetry - https://nvd.nist.gov/vuln/detail/CVE-2023-3028
- Upstream's 2024 Global Automotive Cybersecurity Report https://upstream.auto/reports/global-automotive-cybersecurity-report/
- BMW ConnectedDrive Vulnerabilities (2018) https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=BMW
- Relevant CVEs

Topic 5: Pwn2Charge: Vulnerabilities in the EV Charging Infrastructure

Possible questions to be answered: How was public charging exploited in the past? Which layers have been under attack? Can these attacks be categorized? (Offensive perspective)

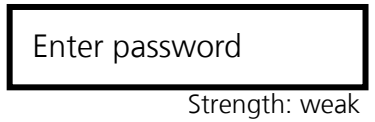
Focus should be on German/EU charging infrastructure: CCS Type2: The plug, IEC 61851 & 62196: Electric charging, ISO 15118 Smart Charging, OCPP & OCPI: Managing charging stations

Literature to start from:

- Attack Systematization: STRIDE / MITRE (ICS) ATT&CK / OWASP / ... by affected charging infrastructure component
- Overview
  - Security Threats in Electric Vehicle Charging - https://doi.org/10.1109/SmartGridComm52983.2022.9961027
  - Review of Electric Vehicle Charger Cybersecurity Vulnerabilities, Potential Impacts, and Defenses - https://doi.org/10.3390/en15113931
- Exemplary Vulnerabilities
  - Brokenwire : Wireless Disruption of CCS Electric Vehicle Charging - https://doi.org/10.48550/arXiv.2202.02104
  - Power jacking your station: In-depth security analysis of electric vehicle charging station management systems - https://doi.org/10.1016/j.cose.2021.102511
  - Losing the Car Keys: Wireless PHY-Layer Insecurity in EV Charging - https://www.usenix.org/conference/usenixsecurity19/presentation/baker
  - Vulnerability Analysis of an Electric Vehicle Charging Ecosystem - https://doi.org/10.1007/978-3-031-62139-0_9
  - Uncovering Covert Attacks on EV Charging Infrastructure: How OCPP Backend Vulnerabilities Could Compromise Your System - https://dl.acm.org/doi/abs/10.1145/3634737.3644999
- CVEs and Vulnerabilities
  - Pwn2Own Automotive 2024 & 2025: Electric Vehicle Chargers - https://vicone.com/pwn2own-automotive
  - Common exploit databases – https://www.cve.org/CVERecord/SearchResults?query=EV+Charging → https://csirt.divd.nl/cases/DIVD-2024-00035/

Concepts of Security and Authenticity (CoSA)

Topic 1: Password Strength Estimators - Nonsense or Helpful?

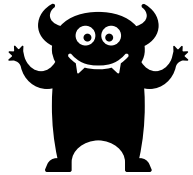


Possible questions to be answered: Which different approaches exist to measure, display, and communicate the strength of passwords? What do they have in common and which aspects are different? What is the latest state of research in that field (apart from transitioning to Passkeys and MFA)?

Literature to start from:

- On the Accuracy of Password Strength Meters - https://dl.acm.org/doi/abs/10.1145/3243734.3243769
- From Very Weak to Very Strong: Analyzing Password-Strength Meters - https://spectrum.library.concordia.ca/id/eprint/978105/
- An Explainable Online Password Strength Estimator - https://link.springer.com/chapter/10.1007/978-3-030-88418-5_14
- zxcvbn: Low-Budget Password Strength Estimation - https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_wheeler.pdf
- Almost one in 10 people use the same four-digit PIN - https://www.abc.net.au/news/2025-01-28/almost-one-in-ten-people-use-the-same-four-digit-pin/103946842 (non-scientific)

Topic 2: FrankenCert revived - Comparison of Certificate Parser Testing Approaches

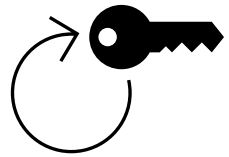


Possible questions to be answered: Which approaches exist on Certificate Parser Testing? What has changed since the famous 'FrankenCert' publication from 2014? Focus on parsing, less on generic testing as already done by Swierzy et al.

Literature to start from:

- SoK: Automated Software Testing for TLS Libraries - https://dl.acm.org/doi/pdf/10.1145/3664476.3670871
- ParsEval: Evaluation of Parsing Behavior using Real-world Out-in-the-wild X.509 Certificates - https://dl.acm.org/doi/pdf/10.1145/3664476.3669935
- Using Frankencerts for Automated Adversarial Testing of Certificate Validation in SSL/TLS Implementations - https://ieeexplore.ieee.org/document/6956560

Topic 3: Authentication Recovery - What is your mother's maiden name?



Most efforts in securing authentication are focusing on strengthening the 'main' login, usually by implementing a second factor. However, what if users forget or loose their methods for access? This topic deals with Methods for Account Recovery.

Possible questions to be answered: Which methods exist? How can they be categorized? What are their differences in usability, security, and user acceptance?

Literature to start from:

- A Comparative Long-Term Study of Fallback Authentication Schemes - https://dl.acm.org/doi/10.1145/3613904.3642889
- Email as a Master Key: Analyzing Account Recovery in the Wild - https://ieeexplore.ieee.org/document/8486017
- Secure Fallback Authentication and the Trusted Friend Attack - https://ieeexplore.ieee.org/document/6888835
- Account Recovery Methods for Two-Factor Authentication (2FA): An Exploratory Study - https://digitalcommons.odu.edu/psychology_etds/351/ (careful, only masters thesis)
- Moving Account Recovery beyond Email and the "Secret" Question - https://www.usenix.org/conference/enigma2017/conference-program/presentation/hill (only presentation)

Topic 4: Attacks and Mitigations on Centralized Network Architectures

Centralized network architectures allow future-proof high-performance networking. Unfortunately, they also increase the attack surface and allow attackers new capabilities if they are not protected accordingly. The seminar topic should assess which potential risks and attacks are possible on centralized network architectures. Additionally, it should discuss which measures do exist and where potential blind spots are.

Possible questions to be answered: What new attack surfaces in centralized network architectures do exists? Which different threat modelling approaches do exist? What different types of attacks have been shown? What measures have been taken to protect different parts of modern centralized network architectures? Are there existing blind spots either on a certain layer or regarding a certain technology / protocol?

Literature to start from:

- TSN Security: https://ieeexplore.ieee.org/document/9473542/
- PTP Security: https://cybersecurity.springeropen.com/articles/10.1186/s42400-021-00080-y
- Secure Resource Allocation Protocol: https://ieeexplore.ieee.org/document/10711053/
- TSN Security Considerations: https://ieeexplore.ieee.org/document/9988000/

Note: I focus on TSN, any other centralized network architecture (SDN, IBN, …) is also fine

Topic 5: Security of High Availability

High-availability is a topic that is usually interesting from a pure networking perspective. Due to safety-critical applications in modern networks, it starts to become more and more a serious cybersecurity issue. Therefore, it is required to categorize and analyze the current work done on the topic of threat modelling to different availability threats and how mitigations, usually developed for equipment failure mitigate those threats.

Possible questions to be answered: What existing mitigations do exists in the contexts of different technologies (wireless vs wired)? What different threats do exist for availability attacks? How does the mitigations match those threats? Are there open threats that are currently not mitigated properly?

Literature to start from:

- IEC 62439 – HSR
- IEEE 802.1CB - FRER: 802.1CB-2017 - IEEE Standard for Local and metropolitan area networks--Frame Replication and Elimination for Reliability | IEEE Standard | IEEE Xplore
- Ethernet Ring Protection Switching
- Multi-level High-availability system: http://ieeexplore.ieee.org/document/6086313/

Topic 6: eBPF and Security: State of the Art

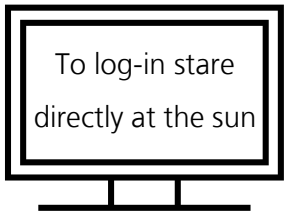
eBPF (Extended Berkeley Packet Filter) is a technology that allows for running sandboxed programs in the Linux kernel without changing kernel source code or loading kernel modules. It is used for performance monitoring, networking, and security by enabling the execution of custom code in response to events. eBPF programs are efficient and safe, as they are verified before execution to ensure they do not harm the system.

Possible questions to be answered: Investigation of the current state of technology of the extended Berkeley Packet Filter (eBPF) framework within the Linux operating system. What are the current challenges and future directions for eBPF technology in Linux environments according the operating system's security?

Literature to start from:

- https://ieeexplore.ieee.org/abstract/document/10733575/
- https://webthesis.biblio.polito.it/secure/33909/1/tesi.pdf
- https://ieeexplore.ieee.org/abstract/document/10579531
- https://fosdem.org/2025/schedule/track/ebpf/

Topic 7: Security, does it have to hurt? A meta-analysis on usable security



Possible questions to be answered: Is security and usability always a tradeoff or are we doing security wrong? In which contexts does get usability/security evaluated? Which methods are used? What makes a good usability/security study good? What are best practices?

Literature to start from

- Towards Robust Experimental Design for User Studies in Security and Privacy
  https://www.usenix.org/conference/laser2016/program/presentation/krol
- Exploring the meaning of usable security – a literature review
  https://doi.org/10.1108/ICS-10-2020-0167
- Analyzing Cyber Security Research Practices through a Meta-Research Framework
  https://doi.org/10.1145/3607505.3607523
- Security and Usability: Analysis and Evaluation
  https://doi.org/10.1109/ARES.2010.77
- What Parts of Usable Security Are Most Important to Users?
  https://doi.org/10.1007/978-3-030-80865-5_9

Motivation

- When Security Gets in the Way (Essay)
  https://dl.acm.org/doi/pdf/10.1145/1620693.1620708
- Exemplary Usability Studies
  - Users are not the Enemies (1999)
    https://doi.org/10.1145/322796.322806
  - Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0 (1996)
    https://www.usenix.org/conference/8th-usenix-security-symposium/why-johnny-cant-encrypt-usability-evaluation-pgp-50

Privacy Matters – Ensuring Confidentiality (PEC)

Topic 1: Privacy & Data Protection

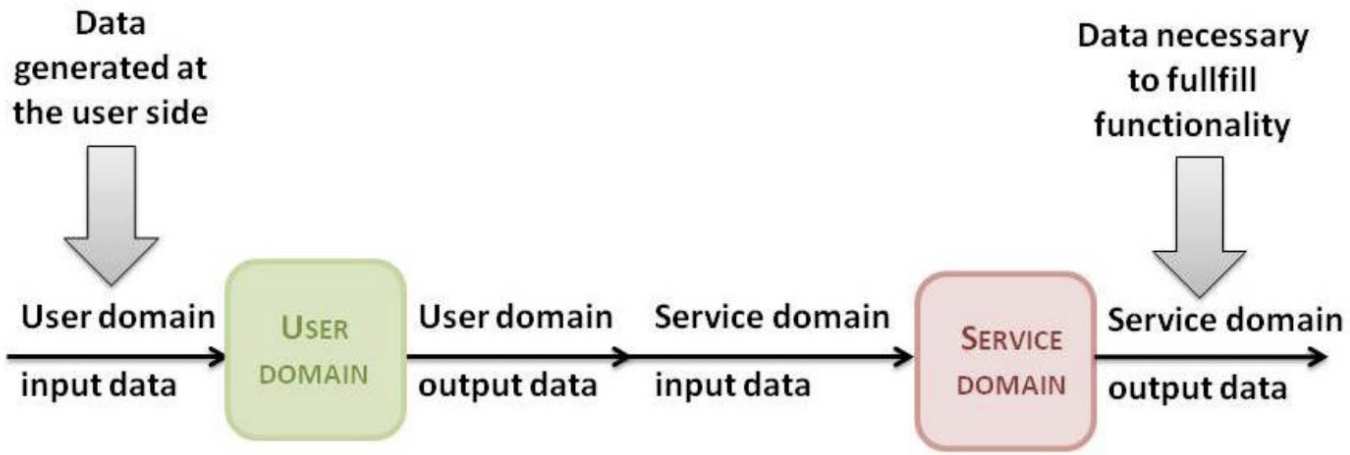
What is the difference between privacy and data protection (and security)?

- Which protection goals are relevant for privacy, data protection, and security?
- Compare STRIDE, LINDDUN, and possibly other approaches
- Compare GDPR, CCPA, and possibly others, and carve out their focus on risk methods
- Compare the personal data classifications in different regulations

Topic 2: Privacy by Design

What is “Privacy by Design“ and how has it evolved?

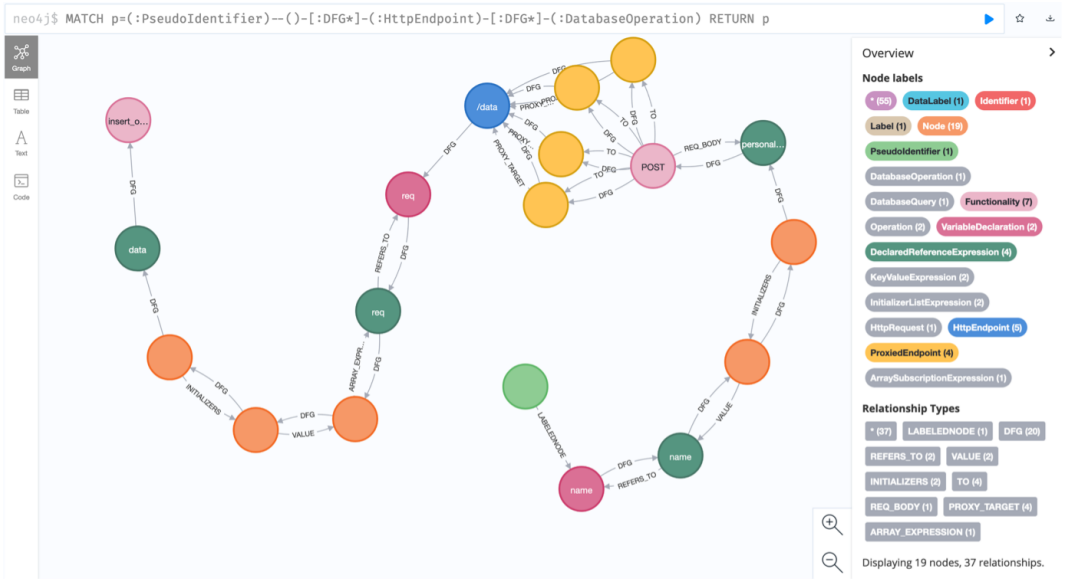
- Which approaches to PbD exist?
- How do existing approaches build upon each other?
- Compare approaches based on use case



Topic 3: Privacy Data Flow Analysis

How can Data Flow Analysis improve Privacy?

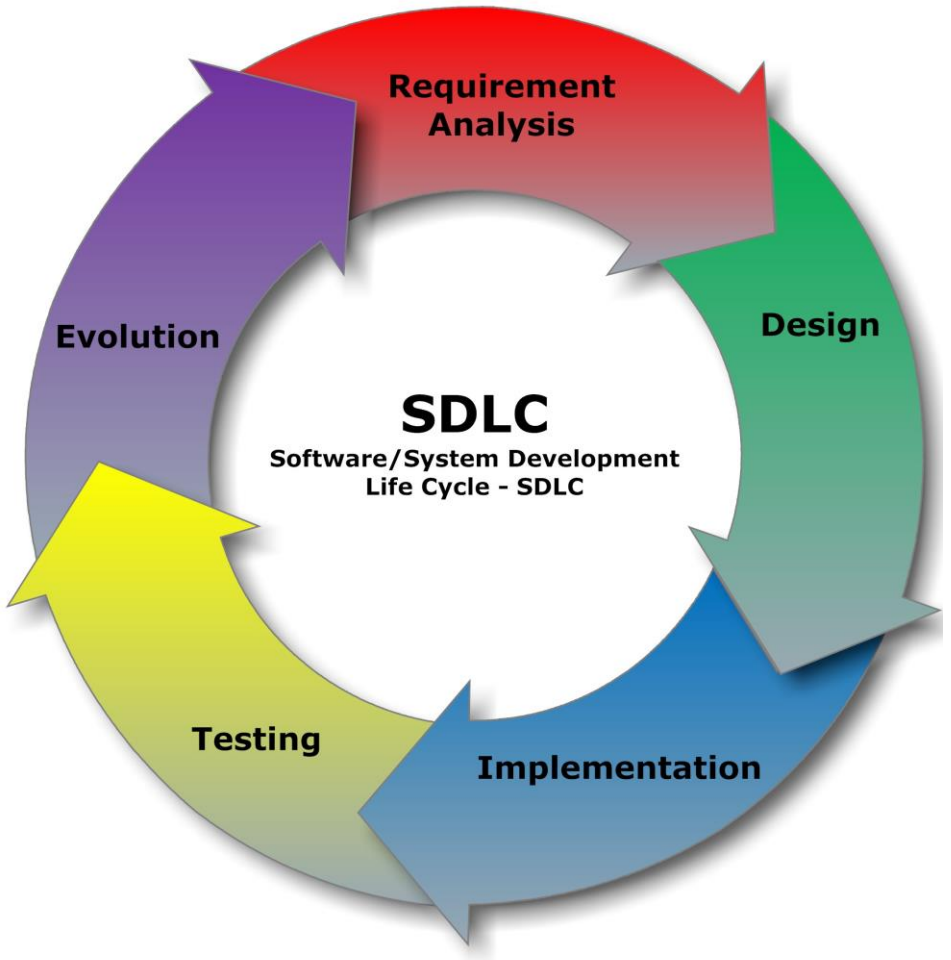
- How does data flow tracking work and what tools exist?
- What approaches are used to utilize personal data flow tracking?
- What are differences and similarities between different approaches?



Topic 4: Privacy in the Software Development Lifecycle

Privacy protection in Secure Development Lifecycles (SDLs)

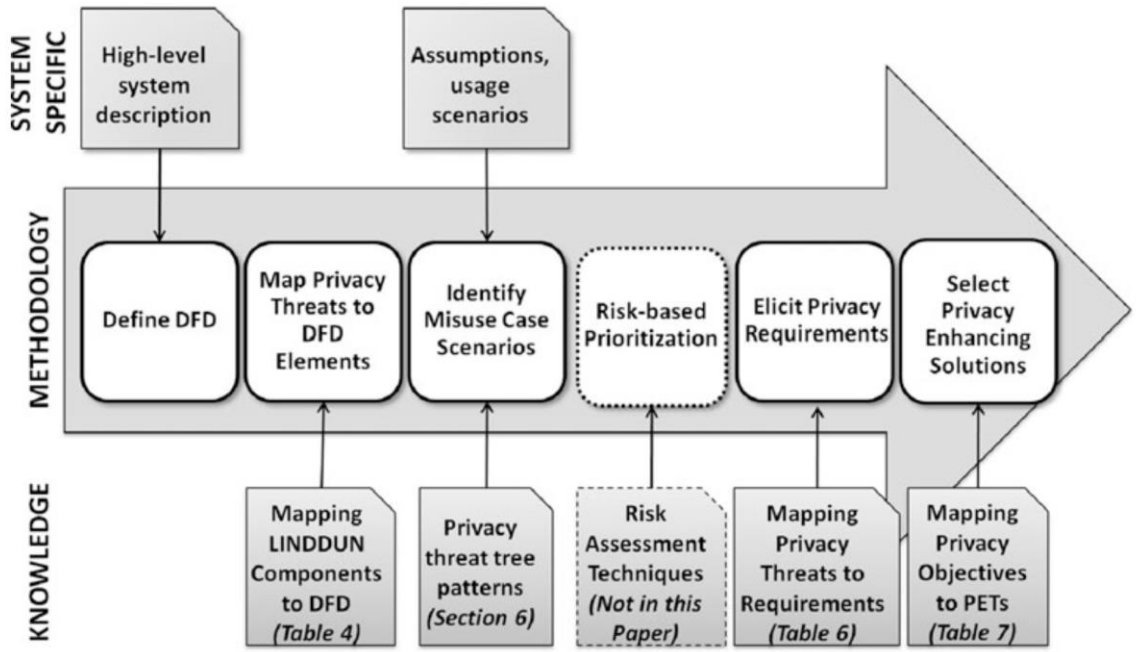
- How are Privacy Engineering tasks reflected in SDLs?
- Compare MS-SDL, Privacy-aware V-Model
- Highlight challenges in Privacy Engineering and SDLs



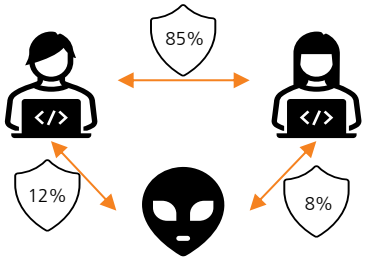
Topic 5: Privacy Threat Modeling and Risk Assessment

Which threat modeling techniques exist and how do they compare?

- Which methodical steps are taken?
- How are threats elicited?
- How are mitigations elicited?
- Use case-based comparison possible



Topic 6: Trust Value Scoring between Peers

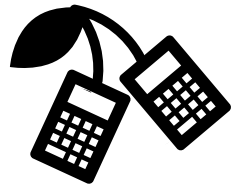


Possible questions to be answered: How are trust and reputation defined? What approaches are used to derive a computational trust score from parameters like the quality and quantity of data, like cyber threat intelligence data a peer distributes, and the connectedness and reputation of a peer in a network? How can anonymity still be achieved in an environment where trust is paramount?

Literature to start from:

- A Quantitative Evaluation of Trust in the Quality of Cyber Threat Intelligence Sources - https://dl.acm.org/doi/10.1145/3339252.3342112
- A topological potential weighted community-based recommendation trust model for P2P networks - http://link.springer.com/10.1007/s12083-014-0288-9
- Trust and Reliance in Multi-Agent Systems: A Preliminary Report - https://www.researchgate.net/publication/2269307
- Survey on Computational Trust and Reputation Models - https://dl.acm.org/doi/10.1145/3236008
- Trust and Quality Computation for Cyber Threat Intelligence Sharing Platforms - https://doi.org/10.1109/CSR51186.2021.9527975
- A Novel Trust Taxonomy for Shared Cyber Threat Intelligence - https://doi.org/10.1155/2018/9634507
- Anonymity vs. Trust in Cyber-Security Collaboration - https://doi.org/10.1145/2808128.2808134
- A survey of attack and defense techniques for reputation systems - https://doi.org/10.1145/1592451.1592452

Topic 7: Early Works of Cryptographic Pairings and their Application

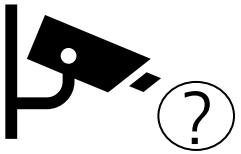


Possible questions to be answered: What are cryptographic pairings? How are they defined? When were pairings introduced, and how did they evolve to lead to today's application scenarios? What are groups with bilinear maps? How are they used for anonymous credential systems (zero-knowledge proofs), group signatures, and encryption (attribute-based encryption, somewhat homomorphic encryption)?

Literature to start from:

- Miller 1986: Short Programs for functions on Curves - https://crypto.stanford.edu/miller/miller.pdf
- A. Menezes 1993: Reducing elliptic curve logarithms to logarithms in a finite field - https://ieeexplore.ieee.org/document/259647
- A. Joux 2000: A One Round Protocol for Tripartite Diffie-Hellman - https://link.springer.com/chapter/10.1007/10722028_23
- Sakai, Ohgishi, Kasahara 2000: Provably secure non-interactive key distribution based on pairings - https://www.sciencedirect.com/science/article/pii/S0166218X05002337
- Boneh, Franklin 2001: Identity-Based Encryption from the Weil Pairing - https://dl.acm.org/doi/10.5555/646766.704155
- Berlin, Heidelberg 2004: Signature Schemes and Anonymous Credentials from Bilinear Maps - http://link.springer.com/10.1007/978-3-540-28628-8_4

Topic 8: The FAQ is Privacy?



Possible questions to be answered: What is the definition of privacy? When did the first discussions about it start, and when did it become a technical term? What are the differences between privacy and confidentiality? What is the privacy paradox? What is the current status quo of privacy research?

Literature to start from:

- Privacy and Freedom, Alan F. Westin, 1968 - https://muse.jhu.edu/article/894334/
- Technical Privacy Metrics: a Systematic Survey, 2015, Wagner et al. - https://arxiv.org/abs/1512.00327
- Information Disclosure and Privacy Paradox: The Role of Impulsivity 2020, Aivazpour et al. – https://doi.org/10.1145/3380799.3380803
- Benefits in Privacy Research: A Literature Review, Status Quo and Future Research Directions, 2020, Wirth et al. - https://doi.org/10.1145/3378539.3393854
- Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems, Belanger et al., 2011 - https://doi.org/10.2307/41409971
- A Taxonomy of Privacy, 2006 - https://papers.ssrn.com/sol3/papers.cfm?abstract_id=667622
- Privacy as contextual integrity, Nissebaum, 2004 - https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=534622

Topic 9: Attacks and Countermeasures of Mixnets

Possible questions to be answered: What are Mixnets? How were they created, and who invented them? How do they hide metadata for private communication? What are the known strengths, weaknesses, and attacks for those networks? What does current research say about them, and what is the level of anonymity they grant?

Literature to start from:

- How Secure Are The Main Real-World Mix Networks - 10.1145/3579856.3595785
- Untraceable electronic mail, return addresses, and digital pseudonyms - https://dl.acm.org/doi/10.1145/358549.358563
- The Loopix Anonymity System - https://arxiv.org/abs/1703.00536
- Two Cents for Strong Anonymity: The Anonymous Post-office Protocol - https://link.springer.com/chapter/10.1007/978-3-030-02641-7_18
- Generalising Mixes - https://link.springer.com/chapter/10.1007/978-3-540-40956-4_2
- Let the Users Choose: Low Latency or Strong Anonymity? Investigating Mix Nodes with Paired Mixing Techniques - https://dl.acm.org/doi/pdf/10.1145/3664476.3664516
- Sphinx: A Compact and Provably Secure Mix Format - https://ieeexplore.ieee.org/document/5207650

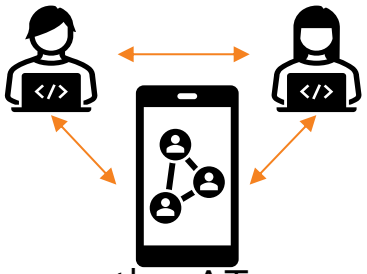
Topic 10: Confidential Automotive Data

Possible questions to be answered: Which electronic control units (ECU) store confidential data? What classifies data "confidential" inside of cars? How could attackers locate confidential data in cars? What about the storage of confidential data in vehicular ad hoc networks? Does Secure Onboard Communication (SecOC) fail to ensure data confidentiality?

Literature to start from:

- can-train-and-test: A curated CAN dataset for automotive intrusion detection, Lampe et al., 2024 - https://www.sciencedirect.com/science/article/pii/S0167404824000786
- Access to In-vehicle Data and Resources, McCarthy et al., 2017 - https://www.cetraa.com/wp-content/uploads/documentacion/informe-trl.pdf
- Security, Privacy, and Decentralized Trust Management in VANETs: A Review of Current Research and Future Directions, AlMarshoud, 2024 - https://dl.acm.org/doi/abs/10.1145/3656166
- A hierarchical and secure approach for automotive firmware upgrades, Luo et al., 2024 - https://www.sciencedirect.com/science/article/pii/S1319157824003471

Topic 11: Decentralized Social Media – Protocols without Privacy Violations?



Possible questions to be answered: Which privacy risks does social media pose to users? Compare the AT-Protocol, ActivityPub, Nostr- and Farcaster designed to achieve security in a decentralized social media network. Have they implemented Privacy-By-Design, or are they lacking in it? Find the winner with the best privacy design and availability.

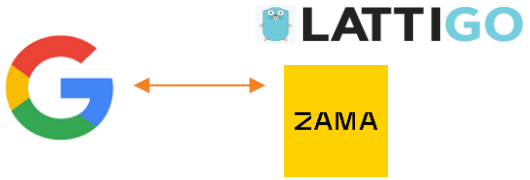
Literature to start from:

- Bluesky and the AT Protocol: Usable Decentralized Social Media, Kleppmann, 2024 - https://dl.acm.org/doi/abs/10.1145/3694809.3700740
- Decentralized Social Networking Protocol (DSNP) and User Empowerment, Nay, 2024: https://dspace.mit.edu/handle/1721.1/156782
- How to decentralize the internet: A focus on data consolidation and user privacy, Kwon et al., 2023: https://www.sciencedirect.com/science/article/pii/S1389128623003560
- DeMedia: Decentralization of Social Media, Perere et al., 2024 - https://ieeexplore.ieee.org/abstract/document/10545716/

Additional resources:

- https://fed.brid.gy/docs#compare
- https://zeroknowledge.fm/331-2/

Topic 12: PETs for Privacy Preserving Data Analytics – Homomorphic Enc.

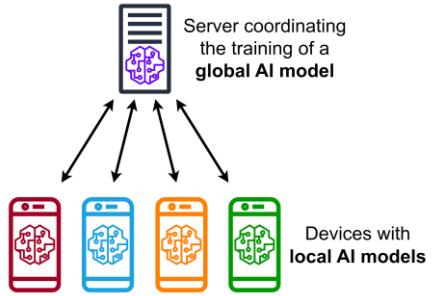


Possible questions to be answered: How did Homomorphic Encryption evolve? What is the current state regarding efficiency? What is the difference between the current development approaches, compiler based (i.e. Google HEIR) vs. Code/library based (i.e. zama.ai-concrete/lattigo). Which use cases fit which approach? What are the efficiency boundaries of both approaches?

Literature to start from:

- FHE Graph (most important literature on HE)
  https://kumu.io/iliailia/fhe-graph
- SoK: Fully Homomorphic Encryption Compilers
  https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9519484
- Lattigo: A multiparty homomorphic encryption library in go
  https://infoscience.epfl.ch/record/299025/files/wahc20.pdf
- CONCRETE: Concrete Operates oN Ciphertexts Rapidly by Extending TfhE
  https://inria.hal.science/hal-03926650/file/wahc20_demo_damien.pdf

Topic 13: PETs for Privacy Preserving Federated Learning – Functional Encryption



Possible questions to be answered: How can Functional Encryption be used in PETs, especially in Privacy Preserving Machine Learning? Which ML algorithms/training models can be protected by FE? What are possible drawbacks and advantages compared to other PETs like Homomorphic Encryption or Federated/Split Learning?

Literature to start from:

- Reading in the Dark: Classifying Encrypted Digits with Functional Encryption https://eprint.iacr.org/2018/206.pdf
- Privacy-Enhanced Machine Learning with Functional Encryption https://eprint.iacr.org/2019/1129.pdf
- Cryptographic Primitives in Privacy-Preserving Machine Learning: A Survey https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10269692

Topic 14: Balancing Privacy and Usability: Strategies for Sharing and Protecting Confidential Data

Possible questions to be answered: How can sensitive data, mainly Intellectual Property (IP) but also private personal data, be pre-processed locally to reduce risk when sharing? What approaches from various fields are available for this purpose? Which privacy-enhancing technologies (PETs) are suitable for protecting intellectual property? How does the trade-off between usability and privacy/confidentiality behave with different techniques? How can we quantify the gains in privacy and confidentiality? How can critical data be identified? What examples exist for cross-company collaboration where sensitive data is shared?

Literature to start from:

- MINERVA: Secure Collaborative Machine Tool Data Utilization Leveraging Confidentiality-Protecting Technologies [Related background research project]
  https://dl.gi.de/items/0763885c-3556-4e2e-bda5-45b91f4c2144
- A taxonomy for privacy enhancing technologies
  https://www.sciencedirect.com/science/article/abs/pii/S0167404815000668
- Edge-computing enhanced privacy protection for industrial ecosystems in the context of SMEs
  https://ieeexplore.ieee.org/document/8962138

Topic 15: Beyond the Payload: Protecting Communication Metadata in Data Sharing

Possible questions to be answered: When sensitive data, such as personally identifiable information (PII) and intellectual property (IP), is shared, it is essential to protect the payload and communication metadata. If the metadata is not adequately safeguarded, it may be possible to infer the identities of individuals, their behaviors, or even the contents of the payload itself. How can we secure or obscure the metadata exchanged between clients and servers? What techniques can be employed to protect clients' identities, regardless of the content of their messages? How can we quantify the gains in privacy and confidentiality? How can critical data be identified? Lastly, what are the advantages and disadvantages of the existing solutions?

Literature to start from:

- MINERVA: Secure Collaborative Machine Tool Data Utilization Leveraging Confidentiality-Protecting Technologies [Related background research project]
  https://dl.gi.de/items/0763885c-3556-4e2e-bda5-45b91f4c2144
- SoK: Metadata-Protecting Communication Systems
  https://petsymposium.org/popets/2024/popets-2024-0030.php

Topic 16: Exposing Weaknesses: Risks in Federated Learning and Their Impact on Data Privacy

Possible questions to be answered: Federated Learning (FL) is a widely used approach for preserving privacy in machine learning. However, it is often mistakenly assumed to be the only adequate solution for protecting sensitive data such as Personally Identifiable Information (PII) and Intellectual Property (IP), overlooking its inherent weaknesses and associated risks. What exactly is Federated Learning, and what are the different approaches within this framework? What attack vectors exist that could compromise data protected by FL? Additionally, what possible solutions can enhance the protection of sensitive data while using Federated Learning, mainly through the combination of various techniques?

Literature to start from:

- MINERVA: Secure Collaborative Machine Tool Data Utilization Leveraging Confidentiality-Protecting Technologies [Related background research project]
  https://dl.gi.de/items/0763885c-3556-4e2e-bda5-45b91f4c2144
- When the Curious Abandon Honesty: Federated Learning Is Not Private
  https://arxiv.org/abs/2112.02918
- Beyond federated learning: On confidentiality-critical machine learning applications in industry
  https://www-sciencedirect-com.eaccess.tum.edu/science/article/pii/S1877050921003458

Topic 17: Strategies for Privacy Protection in Machine Learning: Solutions, Benefits, and Drawbacks

Possible questions to be answered: What methods are available to enhance privacy and confidentiality in machine learning? How do these various solutions operate, and what are their advantages and disadvantages? What principles support the protection of sensitive data? Is it possible to quantify this protection, and how does the performance (usability) of machine learning change when privacy and confidentiality are considered? How can critical data be identified?

Literature to start from:

- MINERVA: Secure Collaborative Machine Tool Data Utilization Leveraging Confidentiality-Protecting Technologies [Related background research project]
  https://dl.gi.de/items/0763885c-3556-4e2e-bda5-45b91f4c2144
- When Machine Learning Meets Privacy: A Survey and Outlook
  https://dl.acm.org/doi/abs/10.1145/3436755
- Preserving data privacy in machine learning systems
  https://www.sciencedirect.com/science/article/pii/S0167404823005151

Topic 18: Resilience in Machine Learning: Analyzing Privacy Violations and Risks to Confidentiality, Integrity, and Availability

Possible questions to be answered: Decentralized machine learning presents a wide range of potential vulnerabilities that could be exploited to intercept sensitive information, compromise model accuracy, or disrupt the overall availability of the system. What specific types of attacks are known, and what harm do they aim to inflict? At what stages can privacy or confidentiality be compromised? How can insights be drawn about sensitive training data? What risks, including intellectual property (IP) and personally identifiable information (PII), are associated with a fully trained model? How do manipulations impact model quality (integrity), and what measures can be taken to prevent failures during the learning process or in model distribution (availability)?

Literature to start from:

- MINERVA: Secure Collaborative Machine Tool Data Utilization Leveraging Confidentiality-Protecting Technologies [Related background research project]
  https://dl.gi.de/items/0763885c-3556-4e2e-bda5-45b91f4c2144
- When Machine Learning Meets Privacy: A Survey and Outlook
  https://dl.acm.org/doi/abs/10.1145/3436755
- A taxonomy and survey of attacks against machine learning
  https://www.sciencedirect.com/science/article/abs/pii/S1574013718303289

FAQ

FAQ

Do I need to answer all the *„possible questions“*?

No. They are just an orientational starting point.

Do I need to include all the listed publications in my SoK paper?

No. Not even a single one, if you find better/more interesting/more fitting ones on your topic.

Many listed publications = lots of work?

No. Just lots of hints ;-)

Are the listed publications to be considered conclusively?

No. You are expected to find and read a lot more!

Do I need to read each publication completely?

No. Learn quick-reading to quickly sort out less interesting publications.

How can I access publication xyz or specification abc?

Check the university library tools. University VPN. Main authors webpage.

How to find scientific literature?

Attend a course on scientific writing! References of the listed papers. Google Scholar, ResearchRabbit, and ConnectedPapers

FAQ cont.

Does the 1-to-1 kickoff meeting have to take place until 31.03.2025?

No. The meeting only has to be organized within this period but can take place after the 31.03.2025

Do I have to participate in all presentations?

Yes. To facilitate the discussion, participation is mandatory, and your discussion will be graded. In seminars with many participants, we usually make only one day obligatory.

When should I start working on the seminar?

Right after your topic is assigned to you!

How close to the final paper should my draft paper be?

Content-wise we expect about 2/3 of your final paper

In general, it should be as close as possible – that way you can make the most from the reviewer's feedback and are more relaxed in June/July.

Will the slides be available after the meeting?

Yes! We will upload them to the chair's website and/or in the TUMonline course description

Is this seminar lots of work?

It depends! For example, on how well you can structure and write. We set high expectations, as all topics come from our own research areas.

Contact

Sebastian N. Peters
Veronique Ehmes
Patrick Wagner
Nikolai Puch
Lukas Lautenschlager
Stefan Tatschner
Andy Ludwig
Immanuel Kunz
Georg Bramm
Andreas Binder

security-seminar@aisec.fraunhofer.de