Research & Teaching Statement

Dr. Vladislav Mladenov

January 9, 2026

My work focuses on practical IT security, including investigating the security and privacy of network communication, cryptographic attacks on applications, and strengthening users' authentication and access to restricted resources. I have excellent publication record, industry contributions, and over ten years of teaching experience with excellent feedback. In addition, I provide part-time training and consulting on the protection of IT systems for numerous companies, further strengthening my practical profile.

Research: I have authored more than 30 peer-reviewed papers, with 15 of them published in the most prestigious conferences, including top-tier venues (A* and A)[1]. These conferences have 10-20% acceptance rates[2], such as *USENIX Security*, *NDSS*, *ACM CCS*, *Security & Privacy*, *RAID*, and *Euro S&P*. I am a regular Program Committee (PC) member of top security conferences, contributing to the review and selection process for high-quality research. My research earned two Best Paper Awards and is recognized in industry through presentations at CCC and OWASP. With my strong publication record and practical experience in protecting IT systems, I am well-prepared to lead impactful research projects at FernUniveristät Hagen.

Teaching: In 2024, my lecture Message-Level Security received the Excellent Teaching Award for the best course in the Computer Science faculty at Ruhr University Bochum. In 2022, I was granted the 5x5000 award for an innovative e-learning platform, which I would like to introduce at FernUniveristät Hagen as well. I can contribute to teaching offers at FernUniveristät Hagen with practical lectures on defensive and offensive security, seminars, practical courses, and hands-on theses.

[1] `http://portal.core.edu.au/conf-ranks/?search=security&by=all&source=CORE2023&sort=arank`

[2] `https://github.com/puzhuoliu/Computer-Security-Conference-Acceptance-Rate`

Research Statement

Today, attackers do not break in, they log in. The entry points into companies, critical infrastructures, or governmental services are identity management flaws [1, 2], malware campaigns [3, 4, 5], and insecurely connected devices [6, 7]. My expertise in IT security, including the security and privacy of connected systems, threat analysis of identity and access management, as well as data protection for critical software applications, addresses these challenges by identifying vulnerabilities and strengthening system resilience.

I have *extensive experience with real-world threats, cryptographic attacks, and corresponding defenses*, combining theory and practice. This is reflected in my research and my teaching. My work covers state-of-the-art technologies, supporting the development of trustworthy and secure solutions for both academic and enterprise applications.

- **Security & Privacy in Networked Systems.** Every device, person and piece of data being connected to the internet, could be vulnerable to hacking and unauthorized access. To prevent a weak point in a network, allowing attackers to compromise the entire communication, complex cryptographic protocols and identity management technologies are used. A key research challenge in the security and privacy of authentication is developing secure systems for digital identities, as demonstrated by eIDAS 2.0's effort to create a standardized electronic identification across Europe [8] or FAPI 2.0 [9] for secure high-value financial API access.

  Research Scope: My research concentrates on *analyzing, monitoring, and protecting authentication protocols* used to identify users or devices and authorize data access by third parties. This topic is complemented by new fundamental research on the *systematic evaluation and protection of APIs* used by websites, mobile applications, IoT devices, and industrial or financial sector.

- **Threat Intelligence for Data & Application Security.** Secure data processing refers to the ability of software to handle and process data in a reliable and safe manner. Today, this concerns not only structured data, but also electronic documents such as PDFs and Office files, which users and devices handle and exchange in both private and professional settings. Attackers systematically weaponize these formats in large-scale malware campaigns to *attack software applications* enabling remote code execution, sophisticated phishing, denial-of-service attacks, and even bypassing cryptographic mechanisms. Despite significant progress, *threat detection and analysis for malicious data* remain an open challenge, and even state-of-the-art approaches still suffer from substantial false negatives.

  Research Scope: In earlier work, I uncovered vulnerabilities in the insecure processing of structured data, with impacts ranging from physical damage to IoT devices to breaking the cryptographic protection. Building on this, my *current DFG-funded project focuses on understanding why malware detection for Office documents* so often fails in practice. By systematically identifying these weaknesses, we aim to address them one by one and significantly improve state-of-the-art detection mechanisms for malware documents.

Security & Privacy in Networked Systems

In the recent years, I performed several security studies on the most important authentication protocols used on the Internet and in major industries. These include investigation on state of the art protocols like SAML [10, 11, 12, 13, 14, 15, 16], OpenID [17], OAuth, and OpenID Connect [18, 19, 20, 21, 22, 23]. These protocols are used by companies like Google, Microsoft, Apple, and Facebook to authenticate billions of end-users and authorize the access to restricted resources.

Ongoing Research The fully automated analysis and monitoring of multi-party authentication protocols in the wild is still an unsolved challenge. In a joined research with the *Heilbronn University of Applied Sciences* and *Northeastern University in Boston*, we work on the fully automated security and privacy evaluation of identity management in web. Our project covers a comprehensive threat analysis, but it also discovers privacy violations leaking users' data.

Research Plan My future research covers three main aspects: continuous threat analysis of authentication protocols and web APIs, extended security evaluation, and new privacy issues. Such monitoring allows us to depict the evolution of authentication and identity management technologies, geo-based differences, and integration of new services. Furthermore, we can observe how newly standardized security protocols, such as FIDO2 and Passkeys, are being adopted in real-world implementations and deliver cutting-edge analyses of their deployment. I am currently in the drafting phase of a DFG proposal for this project.

My research will be complemented by authentication protocols used in Internet-of-Things (IoT) devices like sensors or Smart-Home devices. Due to the limitations of such devices (e.g., missing keyboard or browser) new challenges regarding the authentication, the authorization, and the security analysis occur.

Threat Intelligence for Data & Application Security

Achieving secure and reliable processing of data has become a critical goal to ensure the integrity and trustworthiness of digital workflows. Until now, my research has discovered novel threats and critical flaws in processing cryptographically protected data [24, 25, 26, 27, 28]. In 2022 and 2023, our research on unprivileged code execution and insecure signature verification in office documents appeared in the proceedings of *USENIX'22* [29] and *USENIX'23* [30]. Such attacks could be used by malicious campaigns distributing malware and infecting billions devices. Beyond office documents, we analyze the security of printing technologies including classical printing devices and additive manufacturing. Until now, we discovered critical vulnerabilities in all printers and many related technologies [31, 32, 33, 34].

Ongoing Research My research group elaborates on three security topics: *cryptographically protected data*, security and privacy aspects in digital office, and software-based vulnerabilities. With respect to IoT devices, our ongoing research reveals security issues affecting all 3D printing devices worldwide by allowing attackers to steal intellectual property, manipulate printing jobs, or even destroy the device.

Research Plan My research has identified a significant gap in the security guarantees of virtual workspaces, encompassing vulnerabilities such as insecure data formats, inadequate cryptographic protections, privacy breaches, and the risks associated with physical device damage. By developing and analyzing *new attacks*, I can systematically test *state-of-the-art malware detection* and reveal their weaknesses. This offensive perspective directly supports defensive security: it shows where detection fails, why evasion works, and how real-world threats bypass current protections. At present, I am working on evasion techniques against malware detectors and using these insights to harden and improve their threat detection capabilities.

In addition, a collaboration between the excellence cluster at the Ruhr University Bochum (CASA) and research groups at FernUniveristät Hagen can be established. As part of a collaboration project with the University of Paderborn, I will continue my investigations on the security of additive manufacturing.

Teaching Statement

Teaching Experience I have over ten years of teaching experience, during which I have consistently received above-average positive feedback from students. My courses provide practical experience, solid fundamentals, and a comprehensive theoretical background in cybersecurity, tailored to both bachelor and master students, as well as individuals with or without prior knowledge in the field. I have taught my own lectures at multiple universities, including Paderborn, Konstanz, Wuppertal, Bochum, and Erlangen. My teaching excellence has been recognized with awarding my lectures, including the 2022 Center for Science Didactics' 5x5000 e-learning competition and the 2024 Excellent Teaching Award from the Faculty of Computer Science.

In addition, I gave talks and courses at the Chaos Computer Congress (CCC), OWASP AppSec Europe, OWASP Germany, or directly for various companies. This shows that I have established teaching skills, proven by the lectures taught at the university as well as by the workshops provided in the industry. I can also teach in both German and English and provide the needed experience.

Industry Experiences in IT-Security Since 2014, I work as a freelance IT security consultant, offering consulting, penetration testing, and tailored training to help organizations proactively defend against cyber attacks. My clients include medium and large companies across Europe, among them several DAX-listed firms. I incorporate the practical insights and lessons learned from these industry projects into my lectures and lab courses, which students consistently report as engaging and highly relevant to real-world practice.

Implementation of Modern Teaching Concepts *Research-based Learning.* In my lecture *Message-Level Security*, I consistently integrate current research findings to enhance the learning experience. These findings stem either from recent publications at scientific conferences or from my own research work. An important part of learning is developing a responsible way to handle security vulnerabilities in software, including sharing them responsibly when they are discovered. This ensures that students understand both the ethical considerations and practical steps involved. In 2024, my teaching approach was appreciated and awarded by the students and the faculty with the Excellent Teaching Award.

e-Hacking Platform (Winner of the 5x5000 contest). Students need both formal exercises to deepen their comprehension and gain an abstract overview of the problems as well as exercises to practice the lecture material. The latter is harder to achieve since the creation of practical exercises is time-consuming, requires constant updates and is more susceptible to errors. Nevertheless, the learning effect is indispensable for modern study courses such as IT-security. For this purpose, I developed an *e-Hacking platform* containing six different vulnerable services covering the security of web applications, JSON, XML, OAuth & OpenID Connect, SAML, and REST APIs. Two new modules are currently under development: SOAP and Passkeys.

The advantage of the e-Hacking platform is that students can practice attacks *without causing any damage on production systems*. It is being used in lectures at multiple universities (Bochum, Paderborn, Wuppertal, and Erlangen) and it is constantly updated to cover modern technologies. The usage is well-received by the students in all courses where it has been used. The e-Hacking platform is freely available at `https://e-hacking.de/`.

Tool/Bug of the Week. As supervisor of the exercises for the mandatory lecture "Computer Networks" at the RUB, I was commissioned to develop a practical learning module called "Tool of the Week". Since the lecture is attended by more than 300 students, the challenge is to choose the learning content in such a way that it fits the lecture thematically and contributes to the understanding of the topics covered. Furthermore, the content should be easily reproducible and repeatable. My task was to develop the content of the module and present it in a 45-minute presentation as part of the exercise. The concept resonated widely with students and is still taught today. Later, this concept was adopted in other lectures.

PhD Supervision In my work as a postdoctoral researcher, I contribute with my skills in teaching PhD students how to organize the research projects. For this purpose, I developed an educational concept supporting PhD students to improve their writing, presentation, research, and management skills.

At the beginning, I work with the PhDs on the publication of their master thesis. By this means, the PhDs learn how to write scientific articles, have their first experience with the peer review process, and practice presenting to international audiences. I also use my contacts to other researcher groups to exchange valuable knowledge and establish collaborations. I actively support my students to participate educational workshops, scientific conferences and summer schools. For example, my PhDs participate networking

conferences such as MyPhD[3] and RuhrSec[4] to present their research.

Teaching Style At the beginning of each lecture, it is essential to establish an open and encouraging level of communication. This is quite challenging with respect to the diversity of the audience. Based on my experience in working with small groups and lectures with more than 300 students, I established best practices independent of the group size.

At the beginning of each lecture, I present and discuss with the participants three main topics: the goals of the lecture, the structure of the lecture (including the exercises), and the code of conduct. The first two blocks allow me to evaluate the achieved goals of the lecture together with the students during and at the end of the semester. The third block describes the rules with respect to the communication regarding problems, expectations by the lecturers, and a summary of good and bad practices learned from previous semesters. Thus, a ground truth for the joined work between the lecturer and the students is established. According to my experience, this ground truth promotes a more focused and efficient communication.

To make my lectures easier to understand, I use slides that are shared with students before the lecture so they can follow along and take notes easily. In addition, important aspects of the lecture are highlighted by showing practical examples. If possible, the source code and the test environment are also provided.

I am constantly improving my teaching skills by visiting different seminars and studying books on didactic, teaching and communication.

Integration at the FernUniversität Hagen

In this section, I outline how I plan to integrate my research and teaching expertise at the FernUniveristät Hagen.

Research Directions

Overall, the focus of my work would help to diversify and extend the expertise within the research groups. This would create strong synergistic effects. Building on my work in network and data security, I see potential for many collaborations with chairs in the faculty of mathematics and computer science. For example, my expertise on network protocols position me as a valuable collaborator for the research groups *communication networks*, *parallelism & VLSI*, and *applied stochastics*. My expertise in safeguarding sensitive data can also support groups focusing on *data science*, *multimedia and internet applications*, and *databases and information systems*. By using my specialized knowledge, I am prepared to offer security assessments and practical evaluation of vulnerabilities, e.g., in the context of *software engineering*. In the area of intelligent systems, I offer insights into counteracting attacks that bypass AI-based security measures. I also bring a depth of experience in web protocols, along with strategies to address security

[3] `https://www.fh-muenster.de/hochschule/aktuelles/pressemitteilungen.php?pmid=9323`
[4] `https://www.ruhrsec.de/2023/`

and privacy violations online. Based on my experience with e-learning platforms and online teaching, I can contribute to research groups focusing on *collaborative work and learning in virtual organizations.*

External Collaborations My goal is to build an internationally visible group perceived by the community as the leading player in practical analysis of security protocols and office technologies. I will extend my existing collaborations with the groups of Prof. Jörg Schwenk at Ruhr University Bochum, Prof. Thorsten Holz at Max-Plank Institute, Prof. Juraj Somorovsky at the Paderborn University, Prof. Tibor Jager and Prof. Christian Mainka at the Wuppertal University, and Prof. Sebastian Schinzel at the Münster University of Applied Sciences. My PhD students will visit these groups to strengthen our cooperation. My national and international contacts to companies and universities facilitate the establishment of constant exchange.

Teaching Plans for Bachelor/Master Students

In the course of my professional career, I had responsibilities for my own lectures and exercises. I plan to offer future-oriented courses at FernUniveristät Hagen that focus on cutting-edge cybersecurity research. These courses will cover both theoretical foundations and practical hands-on exercises, ensuring students gain deep knowledge and real-world skills. All my lectures can be offered in German or English.

Mandatory Lectures. Thanks to my extensive field of expertise, I am well-equipped to support any fundamental lecture, and I would particularly enjoy teaching topics related to IT security, such as "Security in Internet". If the need arises, I can give lectures in topics, like "Introduction in object-oriented Programming" and "Computernetworks".

Elective Lectures. I can offer a lecture for bachelor students about *web security*, *data security*, or *foundational lecture on applied cryptography.* In such lectures basic knowledge about web technologies, structured data and cryptographic systems including practical exercises will be covered. Such lectures serve as a basis for further lectures in the master's program that deal with advanced attacks on complex technologies.

Specialized Courses: Practical Lab Courses and Projects. As part of specialized courses, different applications including the used communication protocols will be analyzed in-depth. First, classic attacks will be executed. Afterwards, the students will carry out state-of-the art attacks abusing modern network protocols. Finally, countermeasures and security best practices will be implemented.

I will also offer different projects on current research topics in the field of IT-security. The idea of such projects is to provide students with insights regarding an ongoing security research and increase their excitement and motivation. I also actively support existing *Capture the Flag* activities organized by the university and encourage students and PhDs to participate.

References

[1] Crowdstrike. 2025 crowdstrike threat hunting report: Adversaries weaponize and target ai at scale, 2025.

[2] Natalia Trojanowska-Korepta. The year in review: The most interesting single sign-on vulnerabilities of 2024, January 2025.

[3] Zimperium. Zimperium reveals new advanced pdf-based cyber threat exploiting mobile devices, January 2025.

[4] Microsoft Security. Threat actors leverage tax season to deploy tax-themed phishing campaigns b, April 2025.

[5] ESET Research. Emotet launches major new spam campaign. Welivesecurity.com, November 2018.

[6] Heise Online. Security vulnerabilities in nearly 750 multifunction printers of various brands, June 2025.

[7] Dr. Christopher Kunz. Terrapin-attacke: Millionen ssh-server angreifbar, risiko trotzdem überschaubar. Heise Online, January 2024.

[8] European Commission. eidas regulation, shaping europe's digital future.

[9] OpenID Working Group. Financial-grade API (FAPI 2.0), apr 2025.

[10] Nils Engelbertz, Nurullah Erinola, David Herring, Juraj Somorovsky, Vladislav Mladenov, and Jörg Schwenk. Security analysis of eidas–the cross-country authentication scheme in europe. In *12th {USENIX} Workshop on Offensive Technologies (WOOT 18)*, 2018.

[11] Nils Engelbertz, Vladislav Mladenov, Juraj Somorovsky, David Herring, Nurullah Erinola, and Jörg Schwenk. Security analysis of xades validation in the cef digital signature services (dss). *Open Identity Summit 2019*, 2019.

[12] Christopher Späth, Christian Mainka, Vladislav Mladenov, and Jörg Schwenk. Sok: Xml parser vulnerabilities. In *10th USENIX Workshop on Offensive Technologies (WOOT 16), Austin, TX*, 2016.

[13] Vladislav Mladenov, Christian Mainka, Florian Feldmann, Julian Krautwald, and Jörg Schwenk. Your software at my service: Security analysis of SaaS single sign-on solutions in the cloud. In *Proceedings of the 6th Edition of the ACM Workshop on Cloud Computing Security*, 2014.

[14] Andreas Mayer, Marcus Niemietz, Vladislav Mladenov, and Jörg Schwenk. Guardians of the clouds: When identity providers fail. In *Proceedings of the 6th Edition of the ACM Workshop on Cloud Computing Security*. ACM, 2014.

[15] Andreas Mayer, Vladislav Mladenov, Jörg Schwenk, Florian Feldmann, and Christopher Meyer. Strengthening web authentication through tls – beyond tls client certificates. *Open Identity Summit*, 2014.

[16] Detlef Hühnlein, Vladislav Mladenov, Florian Feldmann, Jörg Schwenk, Tobias Wich, Andreas Mayer, Johannes Schmölz, Bud Bruegger, and Moritz Horsch. Options for integrating eid and saml. In *Proceedings of the 2013 ACM workshop on Digital identity management*, 2013.

[17] Christian Mainka, Vladislav Mladenov, and Jörg Schwenk. Do not trust me: Using malicious idps for analyzing and attacking single sign-on. In *2016 IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 321–336. IEEE, 2016.

[18] Louis Jannet, Vladislav Mladenov, Christian Mainka, and Jörg Schwenk. Distinct: Identity theft using in-browser communications in dual-window single sign-on. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (CCS)*, November 2022.

[19] Vladislav Mladenov, Christian Mainka, Tobias Wich, and Jörg Schwenk. Sok: Single sign-on security – an evaluation of openid connect. In *2017 IEEE European Symposium on Security and Privacy (EuroS&P)*, 2017.

[20] Mike Jones and John Bradley. Oauth 2.0 mix-up mitigation. IETF Draft, January 2016.

[21] Dennis Detering, Juraj Somorovsky, Christian Mainka, Vladislav Mladenov, and Jörg Schwenk. On the (in-) security of javascript object signing and encryption. In *Proceedings of the 1st Reversing and Offensive-oriented Trends Symposium*, page 3. ACM, 2017.

[22] Max Westers, Tobias Wich, Louis Jannett, Christian Mainka, Andreas Mayer, and Vladislav Mladenov. Sso-monitor: Fully-automatic large-scale security and privacy analyses of single sign-on in the wild. In *2024 IEEE European Symposium on Security and Privacy (EuroS&P)*, August 2024.

[23] Tommaso Innocenti, Louis Jannett, Christian Mainka, Vladislav Mladenov, and Engin Kirda. "only as strong as the weakest link": On the security of brokered single sign-on on the web. In *2025 IEEE Symposium on Security and Privacy (SP)*, pages 24–24, Los Alamitos, CA, USA, May 2025. IEEE Computer Society.

[24] Vladislav Mladenov, Christian Mainka, Karsten Meyer zu Selhausen, Martin Grothe, and Jörg Schwenk. 1 trillion dollar refund: How to spoof pdf signatures. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 2019.

[25] Jens Müller, Fabian Ising, Vladislav Mladenov, Christian Mainka, Sebastian Schinzel, and Jörg Schwenk. Practical decryption exfiltration: Breaking pdf en-

cryption. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, CCS '19, 2019.

[26] Christian Mainka, Vladislav Mladenov, and Simon Rohlmann. Shadow attacks: Hiding and replacing content in signed pdfs. In *In Proceedings of the Network and Distributed System Security Symposium (NDSS)*, 2021.

[27] Jens Müller, Dominik Noss, Christian Mainka, Vladislav Mladenov, and Jörg Schwenk. Processing dangerous paths – on security and privacy of the portable document form. In *In Proceedings of the Network and Distributed System Security Symposium (NDSS)*, 2021.

[28] Simon Rohlmann, Vladislav Mladenov, Christian Mainka, and Jörg Schwenk. Breaking the specification: Pdf certification. In *2021 IEEE Symposium on Security and Privacy (SP)*, 2021.

[29] Simon Rohlmann, Christian Mainka, Vladislav Mladenov, and Jörg Schwenk. Oops... code execution and content spoofing: The first comprehensive analysis of opendocument signatures. In 31^{st} *USENIX Security Symposium (USENIX'22)*, 2022.

[30] Simon Rohlmann, Vladislav Mladenov, Christian Mainka, Daniel Hirschberger, and Jörg Schwenk. Every signature is broken: On the insecurity of microsoft office's ooxml signatures. In 32^{st} *USENIX Security Symposium (USENIX'23)*, 2023.

[31] Jens Müller, Vladislav Mladenov, Juraj Somorovsky, and Jörg Schwenk. Sok: Exploiting network printers. In *2017 IEEE Symposium on Security and Privacy (SP)*, pages 213–230. IEEE, 2017.

[32] Jens Müller, Vladislav Mladenov, Dennis Felsch, and Jörg Schwenk. Postscript undead: Pwning the web with a 35 years old language. In *International Symposium on Research in Attacks, Intrusions, and Defenses (RAID '18)*, pages 603–622. Springer, 2018.

[33] Jost Rossel, Vladislav Mladenov, and Juraj Somorovsky. Security analysis of the 3mf data format. In *International Symposium on Research in Attacks, Intrusions, and Defenses (RAID' 23)*, October 2023.

[34] Jost Rossel, Vladislav Mladenov, Nico Wördenweber, and Juraj Somorovsky. Security implications of malicious g-codes in 3d printing. In 34^{th} *USENIX Security Symposium (USENIX'25)*, 2025.