Maciej Sawka

✉ maciejsawka@gmail.com   📍 Kraków, Poland   in Maciej Sawka   ⌂ msaw328

Experience

Penetration Tester, Comarch

Kraków, Poland
Oct. 2020 to Present
4 years+

- Found vulnerabilities in web, mobile and desktop applications both manually and using variety of automated tools.
- Tested cloud deployments (AWS) of applications for security misconfiguration.
- Assessed the severity of found vulnerabilities using industry-standard frameworks such as CVSS and OWASP RRM.
- Provided guidance to the developers on how to fix security bugs.
- Developed and maintained tools for internal team use, including exploits for testing vulnerabilities as well as a report-generating tool.
- Was solely responsible for the inclusion of the CVSS3.1 standard into the testing process, including research, adapting the tools and educating other team members on the matter.

Penetration Tester - Intern, Comarch

Kraków, Poland
Jul. 2020 to Sept. 2020
3 months

- Learned the essentials of penetration testing and methodology used by the team.
- Developed necessary skills using both real-life examples and lab environments.

C++ Developer - Intern, IGE-XAO

Kraków, Poland
July 2016
1 month

- Maintained and fixed bugs in CAD software product in C++.
- Fixed and implemented test cases in VBS.

Education

BEng	**AGH University of Science and Technology**	Oct. 2018 to Mar. 2022
	Information and Communication Technology	
	Thesis title: *Design, Implementation and Verification of a New Block Cipher*	
IT Tech.	**Upper–Secondary Schools of Communications**	Oct. 2013 to Jun. 2017
	Information Technology	

Certifications

eWPTXv2, eLearnSecurity

May 2023

Web Application Penetration Tester eXtreme v2

Certification ID: 7727309 ↗

Technical Skills

- Programming languages and their security features, including C, Rust, Python, Java, JavaScript and others.
- Other languages, such as SQL, HTML, CSS.
- Experience with penetration tests of Linux, Windows, Android and iOS, as well as Cloud environments such as AWS.
- Software: Burp Suite Pro, Docker, Hashcat and John the Ripper, Wireshark, Ghidra, Bash and Python scripting and other tools used during penetration tests.
- Very good understanding and knowledge of cryptography, networking, containerization and virtualization.
- Good knowledge of reverse engineering.

Languages

- Polish - native
- English - B2/C1

Projects

IJON - Symmetric Block Cipher ↗

- Created a fully functional symmetric block cipher, with sponge-based key expansion algorithm.
- Implemented the cipher in C and performed statistical tests of the quality of the key expansion sequence.
- Submitted the project as my bachelor thesis and was awarded second place in a competition organized by the Director of Institute of Telecommunications of AGH.
- Published an article ↗ describing the cipher and its construction in a peer-reviewed scientific journal.

SHA1extend - Command-Line Utility ↗

- Researched the Length Extension Attack on hash functions.
- Developed a command-line utility in C to perform the attack on the SHA1 hash function.

MSAES - Cipher Implementation ↗

- Implemented the AES block cipher in C in the form of a shared library.
- Ensured correctness of the implementation by including automated tests based on the test vectors from the original AES publication.
- Included an implementation of the ISO9797 method 2 padding in the library.

Publications

A Sponge-Based Key Expansion Scheme for Modern Block Ciphers   *Energies*, Sept. 2022

M. Sawka, M. Niemiec

10.3390/en15196864 ↗

Soft Skills

- Ability to explain complex vulnerabilities and security topics in a way that is simple and understandable.
- Continous self-development in cybersecurity as well as other areas of IT.
- Personal focus on understanding difficult concepts in depth, instead of at the surface level.