CSAW Middle East North Afrika (MENA) 2024 Recognition: Paper on Statistical Timing Side-Channel Analysis Achieves Second Place

The paper "With Great Power Come Great Side Channels: Statistical Timing Side-Channel Analyses with Bounded Type-1 Errors" has been awarded second place at the CSAW' 24 Applied Research Competition MENA, held in Abu Dhabi from November 6th to 9th, 2024. The paper introduces a robust statistical framework to detect timing side-channel vulnerabilities in TLS implementations.

Timing side channels occur when attackers exploit the time taken by cryptographic operations to infer sensitive information. The research presented in this paper equips cryptographers with statistical tools to detect such vulnerabilities reliably, while type-1 errors are strictly controlled. By providing a statistically sound and reliable testing methodology, the paper enables large-scale analyses of cryptographic implementations, including widely used libraries like OpenSSL. In the paper, various known vulnerabilities and seven new vulnerabilities were found through the statistical tool. The authors of the paper are:

- Martin Dunsche, Marcel Maehren, Nurullah Erinola, Nicolai Bissantz, and Jörg Schwenk from Ruhr-Universität Bochum,
- Robert Merget from the Technology Innovation Institute,
- Juraj Somorovsky from Paderborn University.

Link to the paper:

https://www.usenix.org/conference/usenixsecurity24/presentation/dunsche