

LITHUANIAN COMPUTER SOCIETY

VILNIUS UNIVERSITY, INSTITUTE OF DATA SCIENCE AND DIGITAL TECHNOLOGIES

LITHUANIAN ACADEMY OF SCIENCES



16th Conference on

DATA ANALYSIS METHODS for Software Systems

November 27–29, 2025

Druskininkai, Lithuania, Hotel “Europa Royale”

<https://www.mii.lt/DAMSS>

VILNIUS UNIVERSITY PRESS

Vilnius, 2025

Co-Chairs:

Dr. Saulius Maskeliūnas (Lithuanian Computer Society)

Prof. Gintautas Dzemyda (Vilnius University, Lithuanian Academy of Sciences)

Programme Committee:

Dr. Jolita Bernatavičienė (Lithuania)

Prof. Juris Borzovs (Latvia)

Prof. Janusz Kacprzyk (Poland)

Prof. Ignacy Kaliszewski (Poland)

Prof. Bożena Kostek (Poland)

Prof. Tomas Krilavičius (Lithuania)

Prof. Olga Kurasova (Lithuania)

Assoc. Prof. Tatiana Tchemisova (Portugal)

Assoc. Prof. Gintautas Tamulevičius (Lithuania)

Prof. Julius Žilinskas (Lithuania)

Organizing Committee:

Dr. Jolita Bernatavičienė

Prof. Olga Kurasova

Assoc. Prof. Viktor Medvedev

Laima Paliulionienė

Assoc. Prof. Martynas Sabaliauskas

Prof. Povilas Treigys

Contacts:

Dr. Jolita Bernatavičienė

jolita.bernatavicienne@mif.vu.lt

Prof. Olga Kurasova

olga.kurasova@mif.vu.lt

Tel. (+370 5) 2109 315

Copyright © 2025 Authors. Published by Vilnius University Press.

This is an Open Access article distributed under the terms of the Creative Commons Attribution Licence, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

<https://doi.org/10.15388/DAMSS.16.2025>

ISBN 978-609-07-1200-9 (digital PDF)

© Vilnius University, 2025

Preventing Memory Based Data Leaks Through Cryptographic Remote Attestation Mechanisms

**Damian Olgierd Zykovič, Virgilijus Krinickij,
Linus Bukauskas**

Cybersecurity Laboratory
Institute of Computer Science
Faculty of Mathematics and Informatics
Vilnius University
olgierd.zykovic@mif.stud.vu.lt

Modern commerce platforms are frequent targets for cybercriminals. Attackers usually try to exfiltrate customers' private data, which in most cases is an essential resource in organisational data stores. Most breaches lead to monetisation through the resale of data on various platforms. Today, organisations rely on strong, unbreakable encryption without a key, but encryption alone cannot guarantee complete protection. In the majority of conventional system configurations, decrypted data resides in system memory in plaintext once accessed for legitimate use. If the machine is compromised by malware, the attackers can extract the data directly from memory, thus bypassing encryption entirely. Modern malware is fully capable of residing stealthily in memory and stealing decrypted data in real time.

To address this challenge our research investigates the possibility for integration of remote attestation mechanisms with Trusted Platform Modules (TPMs) to cryptographically prove to a remote verifier that the firmware is in an unaltered state and is trusted before any sensitive operation is allowed. Remote attestation enables the system to cryptographically prove that the current state of software and hardware configuration matches a previously known, safe state. To achieve this, we will explore the use of Platform Configuration Registers (PCRs), a special register within the TPM module that holds the cryptographic fingerprints of system components. With special registers, we can bind the use of a TPM-based key to a certain state of the device; the key can be sealed

to an expected set of PCR values. In the event that the machine fails remote attestation, due to malicious activity or undocumented changes, access to cryptographic keys will be denied. We expect to reduce the risk of memory-based data leaks by enforcing decryption only on verified with remote attestation systems. This approach focuses on establishing and keeping Zero Trust Architecture (ZTA) from the system boot to data access. The success metrics will rely on the rate of successful attestations under controlled versus compromised conditions, system performance overhead that was introduced by attestation checks and the mean time to detection and denial in tampered environments.