f

Center for Cybercrime Studies

presents

Trusted Code: The Missing Link of True Information Security

Syed Waqas Jafri

Date: Tuesday, March 21, 2017

Time: 1:40 – 2:40 pm
Math & CS Conference Room (6.63.37), 6th Floor, New Building

Abstract:

- System security has been a reactive or a defense strategy where a system or network is characterized to be secure or protected solely on the basis of known threats and vulnerabilities.
- Malicious code and zero-day attacks are still serious threats to both information and system security.
- Platform integrity is some what managed via TPM bases solutions like the TPM Chip, Intel's Software Guard Execution (SGX) and Samsung's Knox.
- This paper is an attempt to fill gaps, where each executable code could be attested and authenticated prior to execution thus providing a robust and on-demand code integrity and thereby eliminating malicious code execution, or if required, isolating the execution of untrusted code, if needed.