CT Advanced Computing Center (CACC) Security Seminar Series 2022-2023

Speaker: Marten van Dijk
Date: Wednesday, February 1, 2023
Time: 2:00pm - 3:30pm
Location: ITE 401
Meeting Link : https://uconn-cmr.webex.com/uconn-cmr/j.php?MTID=m8f2bf56f871cd64624aafcfc4e6f6156
Meeting number (access code): 2623 541 3543
Meeting password: qfGvdEjs366

Towards Remote Verifiable Computation without Digital Secrets

The development of secure processor architecture technology has seen many challenges. It turns out difficult to implement efficient resource sharing and at the same time eliminate or protect against side channels as a result of shared caches and other buffers. For this reason, implemented hardware isolation cannot provide confidential computing (as of yet). Nevertheless, the hardware isolation for access control as implemented by micro code and added circuitry cannot be circumvented and this allows for verifiable computation. However, even though computations can be isolated in enclaves, how can we provide remote attestation of computed output? Remote attestation requires digital secrets which may leak due to side channels. We show two puzzle pieces which together can be used to implement remote attestation without secure digital computation or digital secrets: We use a strong PUF for masking 'session signing keys' and we use these in a new one-time signature primitive. In essence, computing a signature for an output boils down to directly reading out a signature from unmasked digital storage.

Joint work with W. Burleson, D. Gurevin, C. Jin, O. Khan, K. Mahmood, P. H. Nguyen, U. Ruhrmair, and D. P. Sahoo

UCONN

CACC