VirginiaTech
VIRGINIA POLYTECHNIC INSTITUTE AND STATE UNIVERSITY

Computer Science Seminar Series, 2013

National Capital Region

Secure Computation on Encrypted Data

Speaker: Dr. Marten van Dijk
MIT Computer Science and Artificial Intelligence Laboratory

Tuesday, February 19, 2012
1:00PM- 2:00PM, NVC T3

Abstract

One of the key issues in cloud computing is how to keep private data private. From financial information to medical records, sensitive data is stored and computed upon in the cloud. Computation requires the data to be exposed to the cloud servers, which may be attacked by malicious applications, hypervisors, operating systems, or by insiders. Encrypted computation has the potential to solve this data privacy problem: e.g., Fully Homomorphic Encryption (FHE) has been coined the Holy Grail of cryptography since it allows an untrusted server to perform computation directly on an encrypted ciphertext without having access to the decryption key. As opposed to current secure hardware solutions (e.g., Intel+TXT, XOM or Aegis), FHE does not require the user to trust any component on the server side -- even the application program can be untrusted.

I will first explain recent work showing that, for encrypted execution of general programs, even efficient FHE schemes will necessarily suffer a large performance loss compared to plain computation. Motivated by large FHE overheads and FHE's limitations, the main part of this talk describes how to solve the problem of placing trust in programs by designing a tamper-resistant single-chip processor called Ascend (Architecture for Secure Computation on ENcrypted Data) that can run untrusted batch programs without leaking information about private input data over its external input/output and power pins. Surprisingly, Ascend incurs only 6.1x performance overhead relative to insecure computation, which is orders of magnitude better than what FHE can achieve.

Biography

Marten van Dijk is a research scientist at the MIT Computer Science and Artificial Intelligence Laboratory with over 10 years research experience in system security both in academia and industry: Most recently he worked for two and a half years at RSA Laboratories in cybersecurity. Prior to RSA he was a research scientist at MIT CSAIL working together with Prof. Srini Devadas with an emphasis on processor architectures that offer strong security guarantees; most notably, this collaboration led to the design of Aegis, the first single-chip secure processor that verifies integrity and freshness of external memory, and led to the introduction of circuit realizations of Physical Unclonable Functions (PUFs), which resulted in a commercialization by Verayo and Intrinsic-ID. His work received the NYU-Poly AT&T Best Applied Security Paper Award, 3rd place, 2012, and the ACSAC'02 outstanding student paper award. Prior to working in system security he was a research scientist at the digital signal processing group at Philips Research where he became the lead inventor of the error correcting codes used in Blu-ray disc. He received a Ph.D. in mathematics, a M.S. in mathematics, and a M.S. in computer science from Eindhoven University of Technology.