



Computer Engineering

CE Program Seminar



Dr. Edward Suh

CE Faculty Candidate from Pufco, Inc.

THURSDAY, MARCH 9, 2006 ~ 9:00 am ~ Engineering Science Bldg (ESB), Room 2001

AEGIS: Architectural EnGine for Information Security

The Internet is expanding into the physical world, connecting billions of devices. In this expanded network, two contradictory trends are appearing. On the one hand, the cost of security breaches is increasing as we place more responsibilities on the devices that surround us. On the other hand, computing elements are becoming small, disseminated, unsupervised, and physically exposed. Unfortunately, existing computing systems do not address physical threats, presenting a significant vulnerability in future embedded systems.

We have built a tamper-resistant platform using a single-chip secure processor called AEGIS. Our platform protects applications from physical attacks as well as software attacks. This enables several applications such as secure sensor networks, certified execution, and copy protection of media and software. This talk will describe the architecture of the AEGIS secure processor and its key primitives, namely, physical random functions, memory encryption and integrity verification.

Physical Unclonable Functions (or PUFs) are a tamper resistant way of establishing shared secrets with a physical device. They rely on the inevitable manufacturing variations between devices to produce an identity for a device. This identity is arguably unclonable.

Memory encryption and integrity verification protect content stored in external memory, and are essential to build a secure computing system that is powerful enough to run applications requiring large memory. The talk will discuss memory encryption and integrity verification schemes that are secure, yet efficient and practical.

We have fabricated and tested Physical Unclonable Function chips in TSMC 0.18u technology, and implemented the AEGIS processor on an FPGA.

Speaker Bio

Edward Suh has recently received a Ph.D. degree in Electrical Engineering and Computer Science from the Massachusetts Institute of Technology (MIT). Currently, he is leading an effort to develop secure embedded processors at Pufco Inc. He has worked in the areas of high performance memory systems, embedded processors, and secure hardware architecture, and has co-authored over a dozen papers in these areas. His current research focuses on secure computing systems, in particular, secure processors and their applications.

