Secure Embedded System Design: A Tale of Three Gaps

Speaker: ***Dr. Anand Raghunathan*** — NEC Labs America

Abstract: Our experiences with personal computers, the Internet, and the digital information revolution, have clearly identified security as a major challenge (a simple web search reveals that identity theft has affected over 28 million Americans, and costs over $50 Billion/year; e-commerce fraud cost merchants $2.6 Billion last year; the ILOVEYOU virus alone affected over 60% of US companies, causing over $10B in damages). As embedded computing systems pervade various aspects of our daily lives, capturing, storing, accessing, and manipulating a wide range of sensitive personal data, security will become a daunting challenge, and will bring into question the very viability of many future electronic products, applications, and services.

While major advances have been achieved in developing theoretical underpinnings (such as cryptographic algorithms) and functional security measures (such as secure communication protocols), they are hardly sufficient to ensure security in practice. Most real security attacks do not directly take on the theoretical strength of cryptographic algorithms, choosing instead to target weaknesses in a system's implementation. This implies that security cannot be added as an afterthought, but must be built-in through careful consideration during various stages of the design process.

This talk will highlight the "gaps" that exist in secure embedded system design. The assurance gap refers to the gap between functional security measures and secure system implementations. The security processing gap and battery gap arise due to the computational and energy requirements of the additional computations that must be performed for the purpose of security. The talk will identify how hardware designers, software engineers, and system architects can contribute to bridging them. Opportunities for design methodologies and tools to assist in this process will also be discussed.

Speaker Bio: Anand Raghunathan is a Senior Researcher and Project Leader at NEC Labs America, where he leads research efforts on advanced system-on-chip architectures and design methodologies. He concieved and architected MOSES, a programmable security processing engine for mobile appliances, and led a design team that implemented the security architecture that is being used in NEC's mobile application processor products.

Anand holds M.A and Ph.D degrees from Princeton University, and received a B.Tech. degree from the Indian Institute of Technology, Chennai, all in Electrical Engineering. He is a Golden Core member of the IEEE Computer Society and a Senior member of the IEEE.