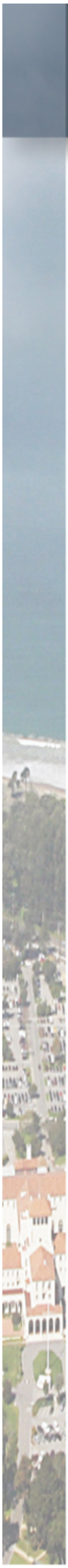
NAVAL
POSTGRADUATE
SCHOOL

Computer Science Department



Nathan Dautenhahn

University of Pennsylvania

Abstractions, Mechanisms, and Policies for Intra-Kernel Protection

**** GE-104, 1500-1600, 15 February 2018 ****

Abstract: Many layers of our computing stacks are implicitly trusted, but are themselves no more secure than the applications they seek to protect. In this talk I describe one of my explorations into making *trusted* software more trustworthy. The Nested Kernel modifies monolithic operating system design to include a small security kernel that protects memory within the operating system itself. The core insight is to partition the operating system so that the security kernel abstracts memory protection hardware and to show how this abstraction can be enforced at a single privilege level in a single address space. The benefits are that the development effort is minimal, it works incommodity systems on commodity hardware, performance costs are low, and the design is portable to diverse hardware (ARM, x86, Hypervisor privilege) and software (FreeBSD, Linux, Xen) environments. Overall, the Nested Kernel FreeBSD prototype demonstrates that it is possible to retrofit powerful security into existing and popular systems. In the talk I will sketch a path forward to "micro-evolving" over privileged commodity systems, which I plan to exploit for security and verification: a must for gaining high assurance in our computing stacks.

Biography: **Nathan Dautenhahn** is a postdoctoral researcher at U. Penn. He earned his doctorate in CS from UIUC in 2016. His research investigates trustworthy system design by developing experimental operating systems, compilers, and hardware components, which has led to publications in key security and systems venues, including IEEE S&P, CCS, NDSS, ASPLOS, and ISCA.