Abstract: Blurring the line between software and hardware, reconfigurable devices strike a balance between the raw high speed of custom silicon and the post-fabrication flexibility of general-purpose processors. While this flexibility is a boon for embedded system developers, who can now rapidly prototype and deploy solutions with performance approaching custom designs, this results in a system development methodology where functionality is stitched together from a variety of soft IP cores, often provided by multiple vendors with different levels of trust. Unlike traditional software where resources are managed by an operating system, soft IP cores necessarily have very fine grain control over the underlying hardware.

To address this problem, the embedded systems community requires novel security primitives which address the realities of modern reconfigurable hardware. This talk will describe a novel isolation primitive, moats and drawbridges, built around four design properties: logical isolation, interconnect traceability, secure reconfigurable broadcast, and configuration scrubbing. Each of these is a fundamental operation with easily understood formal properties, yet maps cleanly and efficiently to a wide variety of reconfigurable devices. After carefully quantifying the required overheads on real FPGAs, this talk will explain how these primitives can be applied to the practical problem of memory protection.

Biography: Ted Huffmire is a Ph.D. Candidate at UC Santa Barbara. The common thread through his research in hardware security is the development of efficient policy-driven mechanisms to enhance the security of special-purpose devices. Ted’s advisor is Dr. Tim Sherwood.