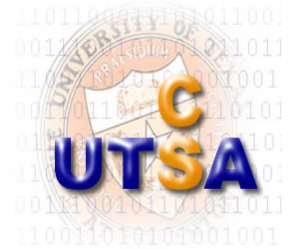




**Invited Talk Series:**  
**Computer Information Assurance and Security**  
**Tuesday, October 4, 2005**  
**2:00 - 3:30 p.m.**  
**BioScience Building, Loeffler Room 3.03.02**



The UTSA's Center for Infrastructure Assurance and Security (CIAS) and The UTSA's Computer Science Department are proud to host:

## **INVITED TALK SERIES: COMPUTER INFORMATION ASSURANCE AND SECURITY**

**Speaker:** **David Evans**  
*Assistant Professor*  
*University of Virginia*

**Topic:** **The N-Variant Systems Framework: Polygraphing Processes for Secretless Security**

**Abstract:** The current computing monoculture leaves our infrastructure vulnerable to a massive, rapid attack. One technique that has been proposed to mitigate this threat is to artificially increase software diversity by transforming programs to produce diverse executables. These techniques depend on keeping a key used to control the transformation secret from potential attackers. Previous techniques have used artificial diversity in a way that depends on keeping a key secret from attackers.

In the first part of this talk, I will discuss one proposed diversification technique, instruction set randomization (ISR), and describe our work on evaluating its security. ISR defuses all standard code injection attacks by hiding the instruction set of the target machine from the attacker. A motivated attacker may be able to circumvent ISR by determining the randomization key. I will describe a remote attack for determining an ISR key using an incremental guessing strategy and present a method for injecting a worm in an ISR-protected network. The attack is plausible under realistic conditions and can infect an ISR-protected server in under 6 minutes.

In the second part of the talk, I will introduce the N-variant systems framework that uses artificial diversity to enhance security. Unlike previous approaches such as ISR, it does not rely on keeping any secrets. Instead, the framework requires an attacker to compromise one of the system variants without producing detectable behavior on another system variant processing the same input. By constructing variants with disjoint exploitation sets, we can make it impossible to successfully carry out large classes of important attacks. In this talk, I will describe our framework and prototype implementations, identify some useful variations, and introduce a model for analyzing security properties of N-variant systems.

**Note:** This talk includes joint work with Ben Cox, Jack Davidson, Adrian Filipi, John Knight, Anh Nguyen-Tuong, Nathanael Paul, Jonathan Rowanhill, and Nora Sovarel funded by grants from DARPA (SRS program) and NSF (Cyber Trust).

**Speaker's bio:** David Evans is an Assistant Professor at the University of Virginia. He has SB, SM and PhD degrees in Computer Science from MIT. His research interests include program analysis, exploiting properties of the physical world for security, and applications of cryptography.  
For more information, see <http://www.cs.virginia.edu/evans/>

*Everyone is Welcome!!!*  
*Refreshments will be served.*

**Upcoming talk: October 18, 2005, at 2:00 p.m. – BioScience Building 3.03.02**  
**Speaker: Radha Poovendran– Assistant Professor, University of Washington**  
**Please visit [www.utsa.edu/cias](http://www.utsa.edu/cias) for updates.**