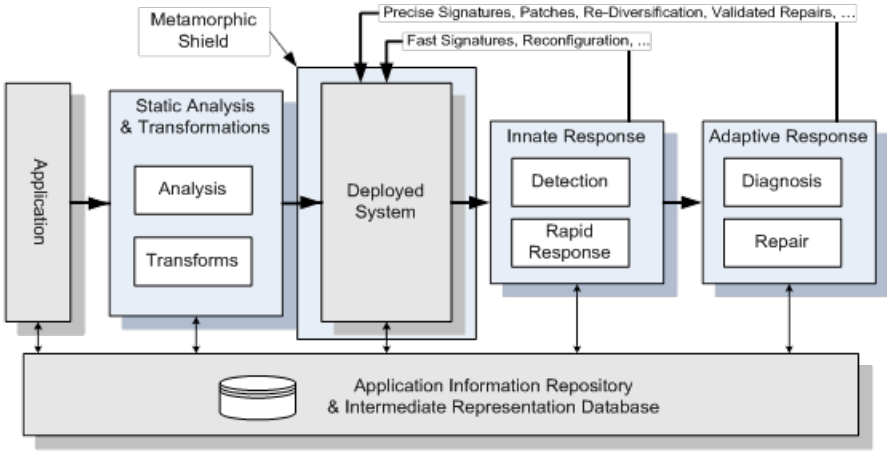
Dependability Research Group



My interests span the areas of programming languages, computer architecture, embedded systems, computer security, and computer science education. My current research interests are focused on the areas of computer security, run-time management of applications running on multi-core systems, and computer science education.

I am also involved in a wide range of professional activities including serving as co-chair of the Association of Computing Machinery's (ACM) Publications Board. The Board oversees the publication of over 40 journals and manages ACM's digital library. I also serve as a founding member of the Digital Asset Protection Association (DAPA). DAPA is dedicated to the advancement and successful deployment of technologies for protecting the privacy and integrity of digital asses including software, content, keys and other valuable digital information.

Jack Davidson

Professor
jwd@virginia.edu
www.cs.virginia.edu/~jwd/

Department of Computer Science
University of Virginia
Charlottesville, VA
434.982.2209

"The best programmers, like the best craftsmen, understand the tools they use."

UNIVERSITY of VIRGINIA ENGINEERING

Computer Security

Society increasingly relies on computer systems to provide a wide range of facilities from critical infrastructures to routine services to entertainment. Many such computer systems have to achieve a high level of dependability, because the consequences of failure are often extreme. The current approach to software development is to try to remove software faults before deployment, but despite years of intense research, technology that permits finding and removing all software faults has proved an elusive goal. We seek to develop technologies that armor binary programs and protect them from attacks which could arise from the inevitable vulnerabilities that remain after deployment.

Strata

Strata is a high-performance software dynamic translator (SDT) that enables software malleability and adaptability at the instruction level by providing facilities for run-time monitoring and code modification. SDT can affect an executing program by injecting new code, modifying existing code, or by controlling which portions of code may be executed. These capabilities give system designers unprecedented flexibility to control and modify a program's execution. Using Strata we are exploring novel approaches for protecting programs from attack by malicious entities, protecting valuable intellectual property, improving the run-time performance of applications, and simplifying the software development process.

REEact

REEact: A Robust Execution Environment for Fragile Multicore Systems is one of the research projects of the Consortium for Adaptive CMP Compilation and Optimization including Penn State, University of Pittsburgh, and the University of Virginia. With the emergence of the chip-level multiprocessor (CMP) comes the promise of integrating enormous computing power in a single chip, thereby enabling parallel computing in all types of platforms including handheld computers and desktop machines. Nonetheless, there are significant barriers and challenges to exploiting the power of CMPs. Very simply we must rethink every aspect of these systems-the underlying architecture(s) of the individual processing elements, the on-chip and off-chip memory architectures, the on-chip and off-chip communications structures and mechanisms, the operating system, the software architecture of applications, and the programming language paradigms and support required.

RECENT RESEARCH DEVELOPMENTS

- Developed and patented a novel algorithm to protect software from malicious tampering and reverse engineering.
- Lead research team that developed ILR (Instruction Location Randomization) an efficient, powerful approach for thwarting attacks against critical software.
- Lead a research team that is developing powerful analysis techniques to detect vulnerabilities in binaries.

RECENT GRANTS

- Intelligence Advanced Research Projects Agency (IARPA): Preventing Exploits Against Software of Untrusted Provenance.
- Army Research Office (ARO): Securing Untrusted Binaries with Acceptance Testing and Field Monitoring.

SEAS Research Information
Pamela M. Norris, Associate Dean
University of Virginia
Box 400242
Charlottesville, VA 22903
pamela@virginia.edu
434.243.7683

UNIVERSITY of VIRGINIA ENGINEERING