Ducson Nguyen
ducson.nguyen@gmail.com • ducsonnguyen.com • linkedin.com/in/ducsonnguyen

Summary
C/C++/Python developer. Experience in binary analysis, software dynamic translation, and reverse engineering. iOS development in Swift on the side. TS/SCI clearance.

Work Experience

GrammaTech
Software Engineer – September 2009 to present, Ithaca, NY
Member of the research team:

- Proteus/HACCS: Stitched together GrammaTech and open source technologies to discover potential vulnerabilities and analyze their exploitability. (Python/C++)
- Cyber Grand Challenge: Built the distributed infrastructure for automated binary defense and exploit generation integrating PEASOUP (below) and University of Virginia technology. 2nd place team. (Python/C++)
- Preventing Exploits Against Software of Uncertain Provenance (PEASOUP): Automated defenses against vulnerabilities in binaries. Added support for file, network and X11 inputs to Grace, an automatic test input generator that explores programs using concolic execution. Implemented a machine learning-driven identifier of stack variables, allowing our binary rewriting technology to insert guards against memory violations. (Python/C++/Scheme)
- KATE: a kernel-level software dynamic translator (useful for real-time observation and transformation). Implemented management of guest memory, interrupts, and CPU privilege level changes. (C/C++/x86 assembly)
- CodeSonar: bug-finding tool for C/C++/x86. Extended taint tracking through variadic function arguments. (C)

L-3 Communications
Senior Member of the Engineering Staff – October 2005 to August 2009, Camden, NJ
Embedded software development in C++ and Java for data security devices:

- Joint Strike Fighter data security module: Implemented driver for cryptography ASIC, driver for Freescale MPC8347 (PowerPC) Security Engine (random number generation, hashing, SHA-1), flash memory key management module, data management module. (C/C++)
- Next-generation Electronic Key Management System: Implemented electronic key processing functionality using Spring Framework. (Java)

Computer Sciences Corporation
Software Engineer – June 2002 to October 2005, Egg Harbor Township and Mount Laurel, NJ

- U.S. Navy's Aegis Combat System: Developed a graphical (Java Swing) testing tool to simplify data extraction for all versions of Aegis software. Designed and implemented components of Aegis radar hardware's self-diagnostic test system (Element Test Function) in C++.
- FAA Controller-to-Pilot Data Link Communications (CPDLC): Developed a Java GUI for supervisory CPDLC functions. Created an in-house C++ unit testing framework for development team's use

Education

Master of Science in Computer Science, May 2006
Villanova University, Villanova, PA

Bachelor of Science in Computer Science, May 2002
Rutgers University, New Brunswick, NJ