Keynote #3

Software Security: Building Security In

Gary McGraw
Cigital, Inc.

ABSTRACT
Software security has come a long way in the last few years, but we’ve really only just begun. I will present a detailed approach to getting past theory and putting software security into practice. The three pillars of software security are applied risk management, software security best practices (which I call touchpoints), and knowledge. By describing a manageably small set of touchpoints based around the software artifacts that you already produce, I avoid religious warfare over process and get on with the business of software security. That means you can adopt the touchpoints without radically changing the way you work. The touchpoints I will describe include

- Code review using static analysis tools
- Architectural risk analysis
- Penetration testing
- Security testing
- Abuse case development
- Security requirements

Like the yin and the yang, software security requires a careful balance-attack and defense, exploiting and designing, breaking and building-bound into a coherent package. Create your own Security Development Lifecycle by enhancing your existing software development lifecycle with the touchpoints.

BIO
Gary McGraw, Cigital, Inc.’s CTO, is a world authority on software security. Dr. McGraw is co-author of five best selling books: Exploiting Software (Addison-Wesley, 2004), Building Secure Software (Addison-Wesley, 2001), Software Fault Injection (Wiley 1998), Securing Java (Wiley, 1999), and Java Security (Wiley, 1996). His new book Software Security: Building Security In (Addison-Wesley 2006) was released in February 2006. As a consultant, Dr. McGraw provides strategic advice to major software producers and consumers. Dr. McGraw has written over ninety peer-reviewed technical publications and functions as principal investigator on grants from DARPA, National Science Foundation, and NIST’s Advanced Technology Program. He serves on Advisory Boards of Authentica, Counterpane, and Fortify Software, as well as advising the CS Department at UC Davis, the CS Department at UVa, and the School of Informatics at Indiana University. Dr. McGraw holds a dual PhD in Cognitive Science and Computer Science from Indiana University and a BA in Philosophy from UVa. He is a member of the IEEE Security and Privacy Task Force, and was recently elected to the IEEE Computer Society Board of Governors. He is the producer of the Silver Bullet Security Podcast for IEEE Security & Privacy magazine, writes a monthly column for darkreading.com, and is often quoted in the press.