Cards on the table: Low-cost tool spots software security flaws during development process

February 24 2009

A new risk management tool can help software developers identify security vulnerabilities in their programs early in the planning process, effectively solving problems before they exist, simply by having the developers lay their cards on the table. The system, called "Protection Poker," was developed by computer security experts at North Carolina State University and is already being used in a pilot project to identify security problems.

In Protection Poker, lead researcher Dr. Laurie Williams explains, software development managers are asked to present ideas for new software features or applications to their team of programmers. Members of the software development team are then asked to vote on two questions: how valuable is the data that the new feature will be using? And how easy will it be to attack the new feature?

The development team members use a special deck of cards to vote that allows them to rank the value and ease of attacking the new feature on a scale of 1 to 100. Everyone on the team flips over his or her cards simultaneously. Members who voted with the highest and lowest cards are asked to explain their votes. If one member of the team has ranked the vulnerability as a 40, while the rest of the team ranked it as a three, that member may know something the others don't, Williams says. This process takes advantage of the diversity of knowledge and perspective within the development team.

This process, while simple and inexpensive, is effective - particularly if it takes place during the planning stage, so that potential problems can be addressed before any coding has taken place. For example, Williams and her research team launched a Protection Poker pilot project with Red Hat IT in October 2008 - and have already identified vulnerabilities and prevented them from being included in software projects at that company.

Williams is currently in discussions with other private companies and government agencies about the possibility of launching additional pilot projects to test the Protection Poker system. Williams is an associate professor of computer science at NC State. The Protection Poker research team includes two NC State doctoral candidates in computer science: Michael Gegick and Andrew Meneely.

In addition to identifying security flaws, Protection Poker is also a valuable training tool. Having an individual explain his or her vote results in that person's security knowledge being shared with the entire software development team, Williams explains.

The Protection Poker research, "Protection Poker: Structuring Software Security Risk Assessment and Knowledge Transfer," was presented at the first-ever Engineering Secure Software and Systems (ESSoS) Conference in Leuven, Belgium, earlier this month.

Gegick and Williams have also co-authored research, with Pete Rotella of Cisco Systems, that effectively allows software developers to identify the elements of their software that are most likely to have security vulnerabilities. While the program does not identify the vulnerabilities, it does evaluate reports of non-security problems with a program (or "bugs") to determine which elements of the program should be prioritized as possibly having security flaws. This research, "Toward Non-security Failures as a Predictor of Security Faults and Failures,"

was also presented at the ESSoS conference.

Source: North Carolina State University