Software That's Resilient Against Hacker Attack

October 29 2009, by John Messina

Image Credit: Technology Review

(PhysOrg.com) -- A team of researchers headed by Martin Rinard, a professor of computer science at MIT, have developed new software that automatically patches errors in deployed software in a matter of minutes.

The software is called ClearView and is designed to apply patches whenever it detects that something has gone wrong with the program. ClearView operates by monitoring a program's normal behavior and establishing a set of rules.

ClearView looks for certain types of errors that are mostly caused by an attacker introducing malicious code into the operating program. When ClearView detects a software intrusion, it identifies the rule that has been compromised and generates a set of repair patches designed to

force the software to follow the compromised rules. ClearView then studies all possibilities to determine which selected rule is the most successful patch.

ClearView can be very successful when it is installed on multiple computers running the same software. By ClearView analyzing the malicious code and applying the most effective rule on one machine, it can then apply the patch to all other machines. ClearView applies the patch to the binary code, bypassing the source code which enables it to fix programs without human intervention.

ClearView was tested on a group of computers running Firefox and an independent team to launch an attack on the [Web browser](#). The attack team used 10 different attacks to inject malicious code into Firefox. ClearView was successful in all 10 attacks by blocking the malicious code and shutting down the program before its intended attack took effect.

ClearView created patches that corrected the errors introduced by the malicious code and discarded any corrections that had a negative effect. ClearView, on average, came up with a working patch within five minutes of its first attack.

In a TR interview, Rinard stated: "What this research is leading us to believe is that software isn't in itself inherently fragile and brittle because of errors. It's fragile and brittle because people are afraid to let the software continue if they think there's something wrong with it." Some software engineering approaches, such as "failure-oblivious computing" or "acceptable computing," share this philosophy.

More information: Automatically Patching Errors in Deployed Software, 22nd ACM Symposium on Operating Systems Principles. [Paper] [Slides]

Via: [Technology Review](#)

Citation: Software That's Resilient Against Hacker Attack (2009, October 29) retrieved 27 April 2024 from https://phys.org/news/2009-10-software-resilient-hacker.html