Battling Botnets With An Awesome OS

April 9 2010

(PhysOrg.com) -- Despite security software, patches and updates, your computer remains threatened by attack and takeover from hackers and cyber-criminals who will turn your PC into their networked robot -- or "bot" -- creating mischief to mayhem by everything from spreading spam to looting bank accounts.

"Today's computer operating systems are thoroughly penetrated and unfixable," said University of Illinois at Chicago computer security expert Jon Solworth. "Every year we spend more and more on the problem, but every year the problem gets worse because we're working at the edges instead of at the heart of the problem."

Solworth, associate professor of computer science at UIC, along with cryptography expert Daniel Bernstein, research professor of computer science, just received a $1.15 million grant from the National Science Foundation to build a new computer operating system -- or OS -- that plugs holes against intruding bugs, viruses and other harmful e-critters.

Solworth is building an operating system he calls Ethos -- essentially a blueprint for an OS that ratchets up security in ways not yet considered or believed necessary when operating systems like Windows, Mac and Linux were conceived.

Today, the applications that run on your computer are more vulnerable than the OS itself, Solworth said. He and his laboratory staff are working to make Ethos OS guard against attacks that target the applications that run on it.

"Our goal is to learn what a security OS looks like," he said. "The attacker needs to find only one way into the system, whereas we as defenders have to protect against every way in. Security is not a field where you're going against a fixed target. You're going against the intelligence of another human."

Solworth's team has begun the laborious task of building this new generation of secure, robust operating systems one cyber-brick at a time, examining new ways to make sub-systems attack-proof and eliminate vulnerabilities in what are known as system calls, used to communicate with computers on the Internet.

While Solworth and his team are building the Ethos OS, Bernstein's primary role is as the hacker, exposing vulnerabilities that need fixing. Bernstein's expertise in cryptography and networks will also be tapped in the construction of Ethos.

The new OS will run on so-called "virtual machine" computers that run one or more operating systems together, like Windows and Mac. Older applications written for those OS systems where security is not a big issue, like games, will continue to work, but new OS like Ethos will simultaneously handle applications such as online banking and other sensitive business transactions as part of the evolution to tomorrow's more secure operating systems.

Solworth thinks that new OS will also free software developers from worrying about security so they can spend more time writing programs that make applications work better.

But Solworth doesn't underestimate the task at hand.

"This is a huge undertaking, with complex scientific aspects," he said. "But an equally large concern is the logistics of such a project, and my

job is to sequence things so that they go smoothly.

"If we succeed, we'll have achieved what many thought couldn't be done. It's a little scary, daunting and humbling, yet it's extraordinarily exciting."

Provided by University of Illinois at Chicago