Inspired by nature, researcher develops new cyber security techniques

May 13 2014, by Kathryn Bold

UC Irvine computer science professor Michael Franz has devised a way to individualize software programs to help keep hackers from inflicting widespread damage. Credit: Steve Zylius/UC Irvine

(Phys.org) —Imagine a cyber world in which hackers, identity thieves, spammers, phishers, foreign spies and other miscreants have a much tougher time plying their trade. Thanks to UC Irvine computer science professor Michael Franz and his research group, such a world is closer to a reality.

Franz, director of UC Irvine's Secure Systems & Software Laboratory, is borrowing the idea of "biodiversity" from nature and applying it to the software that runs on digital devices from smartphones to supercomputers. His promising ideas have already won a U.S. patent and make it much harder for attackers (including those with the resources of a nation state) to compromise their targets.

A major player in government-funded digital defense, Franz has been awarded more than $11 million as a principal investigator for UC Irvine—including more than $7 million as sole principal investigator—from the Defense Advanced Research Projects Agency, the U.S. intelligence community, the Department of Homeland Security and other funding entities.

Here, he describes his revolutionary concept for thwarting cyber attacks:

Why is our cyber infrastructure so vulnerable to attacks?

Today, if hackers discover a weakness in one piece of software, they can take over all of the devices that run the software. Unfortunately, the same software—with the exact same bugs—runs on large numbers of digital devices. For example, the vast majority of smartphones use either Android or iOS, and most computers use Windows.

This makes it easy for attackers. They need to find just one way in, and

it will work on lots of targets. They can create viruses that jump from computer to computer while exploiting the same path of entry on each of them. And it enables attackers to practice their attacks before they unleash them, because they can replicate the exact software environment that will later exist on the target.

What's the solution that you and your research group have developed?

Our solution is to make every software program unique, so that hackers have to find different attacks for different targets. It's inspired by biology—appropriately so, since biological viruses existed long before the term was applied to computers. The plague wiped out a third of humanity, but it didn't wipe out everyone because different people have different genetics.

Just as in biology, diversity is strength. Using this concept to diminish the effect of software errors, we have developed mechanisms that can potentially create a unique version of every program for every person in the universe. This won't eliminate hacking completely, but it will prevent widespread damage, dramatically increase the cost of attempting cyber attacks and make it much more difficult to target a specific person or entity.

How does your work break new ground?

While using multiple versions of software is not new—fly-by-wire controls in airplanes and other high-assurance systems often use "n-version" programming, in which a small number of alternative implementations are built separately from scratch—it has never before been attempted on the scale or at the low price point delivered by our solution. In the traditional n-version approach, you basically multiply the

development cost by the redundancy factor n.

In our approach, on the other hand, subtly different versions of the same software are created automatically "in the cloud," in a matter that is invisible to both the software developers and the end users. The magic of creating the different versions happens inside of the app store from which users download the software. When software is downloaded from our version of the app store, different users automatically get different, but functionally identical, versions.

We have a fully functioning prototype and a few institutions are already experimenting with it. Preliminary benchmarks suggest that the cost of our approach is surprisingly small—not zero, but so low that lots of people will want to be using this. Meanwhile, the cost of not using it keeps rising.

Provided by University of California, Irvine

Citation: Inspired by nature, researcher develops new cyber security techniques (2014, May 13) retrieved 28 April 2024 from https://phys.org/news/2014-05-nature-cyber-techniques.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.