

HP to use Professor Sal Stolfo's host-based defense technology for embedded devices

September 25 2015

Computer Science Professor Sal Stolfo and his former student Ang Cui PhD'15, whose cybersecurity research has discovered dozens of serious flaws, have developed Symbiote defense technology that significantly reduces the threat of embedded device malware attacks on end users and organizations. This work originated from Stolfo's laboratory at Columbia University's Engineering School and is now commercially available through his company, Red Balloon Security.

HP has just announced that it is deploying the host-based defense technology on four new HP LaserJet Enterprise printers and multi-function printers coming out later this fall. The company will also deliver a firmware update enabling these capabilities on all Future Smart-enabled HP LaserJet Enterprise printers already in operation going back as far as 2011.

"It has taken us nearly five years from concept to prototype to deployment in scale to millions of users of HP printers," Stolfo says. "This is quite a remarkable achievement and marks a great success from the Columbia Engineering security group!"

Stolfo and Cui began their work in response to increased and forecasted exploitation of embedded devices. "Our technology is the culmination of almost a decade of working together," notes Cui, Red Balloon's chief scientist and CEO. "It was clear embedded devices were a major target and so we designed software that could install easily on any device without modifying the hardware or source code and that works on any

CPU and all operating systems."

Printers have become a major target for hackers and Stolfo and Cui focused on trying to protect them and other embedded devices, such as VOIP telephones, from security breaches. They developed technology that is the first intrusion defense to provide persistent implant detection, in-device memory monitoring, and situational awareness to protect against malicious attacks. Their technology is broadly compatible with printers, routers, cars, telephones, peripherals, point-of-sale systems, industrial control, aviation systems, medical equipment, and more.

"We are very grateful to have the backing of both the Department of Defense and Department of Homeland Security on this project," Stolfo adds. "Until now, hardening all types of embedded devices has proven intractable and prohibitively costly at scale. Embedded devices are quite varied in their hardware architectures and the operating systems they employ. But now we can automate the process of embedding intrusion detection functionality directly into the binary firmware of any device without knowing what operating system is used."

Columbia Technology Ventures, the University's tech-transfer office, exclusively transferred the technology to Red Balloon Security to make advanced anti-malware available to the commercial market.

"This is an excellent example of Columbia researchers, administration, and students working together to create real economic and technology change in the world," says Calvin Chu, Red Balloon's COO and former Columbia senior technology licensing officer. HP is the first company to deploy this secured embedded devices technology on select LaserJet printers. Stolfo and Cui plan next to license the [technology](#) to other large vendors of embedded devices.

Provided by Columbia University School of Engineering and Applied Science

Citation: HP to use Professor Sal Stolfo's host-based defense technology for embedded devices (2015, September 25) retrieved 20 September 2024 from <https://phys.org/news/2015-09-hp-professor-sal-stolfo-host-based.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.