Famed obfuscator proving thus far to be unhackable

February 5 2014, by Bob Yirka

Professor Amit Sahai is a co-author of this research. Credit: UCLA

(Phys.org) —This past summer a team of researchers from MIT and UCLA, with affiliations with IBM and Microsoft published two papers on Cryptology ePrint Archive. The first described a protocol the team had developed that described how software could be scrambled to prevent someone else from seeing its code. The second paper added more information. The protocol describes a method of creating an obfuscator—as it's known in computer science—a means for hiding everything about the workings of a computer program except inputs and outputs. For most of the history of computer science the possibility of creating a real obfuscator was more dream than reality. Now, it appears that after extensive testing (attempting to hack the code), it appears,

according to an in-depth article published in *Quanta Magazine*, that not only is it possible to create such a virtual device, but it has been done—successfully.

Protecting code from prying eyes is just the tip of the iceberg—if code can be hidden and not cracked, then so too can other information, such as passwords or keys for using other systems. It would be the ultimate encryption scheme—a means for sending anything to anyone else without fear of it being snooped on (even by the government).

The obfuscator does its magic by adding code that is not really code and by mixing pieces of the real code around—like a jigsaw puzzle. To a hacker the code would be nonsensical. And thus far, it seems the scheme is working as envisioned—all attempts at hacking the code have failed.

Amid the good news there is still some bit of caution—while the obfuscator does indeed obfuscate the code, it requires a hefty amount of overhead to do so—too much at this point for it to be used in real world applications. But that, the team suggests, will likely become less and less of an issue as other teams set to work using the ideas the team developed to create leaner code that hopefully will one day soon result in a wide range of products—applications that prevent hackers from stealing identities or other personal information, comes to mind. Of course, it should be noted that the same technology could also be used for other types of applications such as rendering DVD's (or digital videos) impervious to copying, a development some might find a little less exciting.

More information: Paper 1. Candidate Indistinguishability Obfuscation and Functional Encryption for all circuits: eprint.iacr.org/2013/451.pdf
Paper 2. How to Use Indistinguishability Obfuscation: Deniable Encryption, and More: eprint.iacr.org/2013/454.pdf