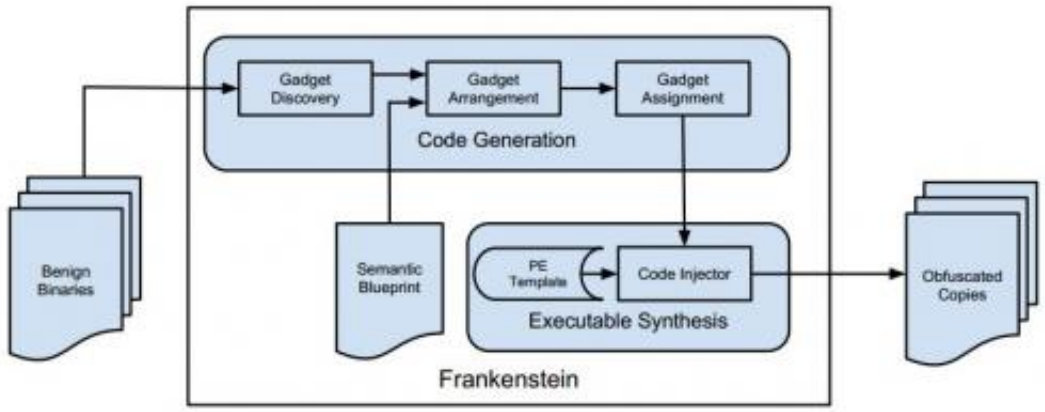
Researchers create 'Frankenstein' malware made up of common gadgets

August 21 2012, by Bob Yirka



High-level architecture of Frankenstein. Image: Kevin W. Hamlen

(Phys.org)—In the ever ongoing struggle between good and evil, or in this case, the battle between those that create malware and those that seek to detect and destroy it, the good guys appear to have mimicked the bad by creating a computer virus that can evade detection by building itself from pieces of code that normally reside harmlessly on people's computers. The result, the team of Vishwath Mohan and Kevin Hamlen of the University of Texas, say, is a cyber version of Frankenstein's monster.

The research, which was partly funded by the US Air Force, was described to attendees at this year's USENIX Workshop on Offensive

Technologies. There the team said their aim in creating the malware was to see if it might be possible to create a virus that is made up of nothing but gadgets, snippets of code used by such commonly installed programs as Internet Explorer or Notepad. Theoretical research over the past several years suggested it could be done. The overall purpose of such a project would be to see if using the technique could result in the creation of a virus that could not be detected by conventional anti-virus programs. And it seems the answer is yes, though the malware the team created isn't a virus in the technical sense because it doesn't cause any harm, it's merely a proof of concept. Their code resulted in the creation of new code made from gadgets that ran two harmless algorithms. But, of course, those algorithms could just as easily been very, very harmful. One of the more clever aspects of the code the team created was the part where the original kernel, the part that infects the computer, was itself modified and caused to look like part of a normal gadget, thus, leaving no trace of itself to be found.

The point, of course, in creating new kinds of malware is to help people on the right side of the law stay one step ahead of those that hide in the dark toiling in earnest to conceive and construct ever more malevolent software that once unleashed might prey on others and do their bidding. Getting there first allows researchers time to build ways to circumvent such malware before the bad guys figure out how to do it themselves. In this case, some have suggested the best way to detect the new so-called undetectable malware is by creating security software that is able to detect objectionable behavior by code, rather than scanning it for identifying markers, which is how virtually all anti-virus software currently find infections on computer systems.

More information: Kevin W. Hamlen's page: www.utdallas.edu/~hamlen/research.html

Press release