MEMO

To: Karen Pluemer

From: Brianna Muleski

Subject: Program-Tampering Detection

Date: October 4, 2013

Researchers from MIT and Israel’s Technion and Tel Aviv University developed a new system that can quickly identify if a program running on the cloud is executing properly.

Their program improves several things:

* Hackers cannot hijack a legitimate program or application and interfere with their execution.
* Researchers can look for patterns in data without actually seeing what the data is (protecting the privacy of the data).
* The use of a probabilistically checkable proof and cryptographic encoding makes the process much faster.

The probabilistically checkable proof, or PCP, method:

* Instead of using the method of going line by line, which is done in any standard mathematical proof, the PCP can essentially “flip a coin” and probabilistically sample three of four lines.
* This makes checking if the program is working correctly exponentially faster.
* But, this only gives a probabilistic guarantee that it’s correct.

So, the use of cryptographic encoding ensures a working program:

* The PCP theory assumes that anyone trying to produce a fraudulent proof has an infinite computational capacity.
* Using the cryptographic encoding, it forces the user to use only linear evaluations,
* Thus sidestepping the inefficiencies of the theorem.