8-16-2016

Fighting Fire with Innovation

USU Jon M. Huntsman School of Business

Fighting Fire with Innovation

08/16/2016

Jeffrey Johnson

Associate Professor

Email:jeffrey.johnson@usu.edu
Office Phone: 435.797.2350

This summer MIS Associate Professor Jeff Johnson was granted a patent for his unique form of information security, one that has the potential to revolutionize online security. Patent #9391962, “Multi-node Encryption”, is an idea that could potentially upset the entire internet industry.

Describing the genesis of his idea, Professor Johnson offered the following analogy, “In the cyber world we have bad guys who are constantly trying to hurt us. Our defense against these bad guys is to build great stone walls that act as a shield. Unfortunately, over time the bad guys obtain machines that can crush stone. Surprisingly, our solution is to simply use more stones in the wall.” So, why then are we building our defenses out of the very source of our enemy’s strength?

He went on to explain that the defensive “stone wall” represents math encryption (the traditional form of cyber security). The bad guys’ “stone crushing machines” are computers designed with the very purpose of processing mathematical codes better and faster than humans ever could. Professor Johnson realized the insanity of fighting fire with fire. Soon after this realization, his idea was born.

Computers struggle with some forms of language based information. Proof of this observation is readily apparent when looking at errors caused by the auto-correct function programed in any computer operated device. The solution: language based encryption!

The idea of language based authentication dates back to biblical times. Armies would use a particular word as a form of authentication for soldiers passing in and out of guarded borders. Each word used was selected because it was extremely difficult for their enemies to pronounce correctly. Thus, making it even more effective.

Within the cyber security realm, a similar communication process is made possible through an (A-Z) chain of paired nodes that spans the network. Professor Johnson proposed that each pair of nodes in that chain would speak its own slang language that only that pair understands. (A) talks to (B) in a language that (C) doesn’t understand, so then (B) turns around and translates the message to (C) in a language that (C) understands, and so forth and so on throughout the chain. Once you have established these links then (A) will be able to send a message to (Z) and it will simply go through a process of repeated translations between each pair of nodes until it arrives at (Z) in a word form that both (Z) and (A) understand. Following this method (A) and (Z) then have their own language on top of this.

Even if a cyber eavesdropper were to intercept or gain access to any one of the messages passed between a pair of nodes it will simply be an abstract word out of context and afford the threat no help in understanding the true message of (A-Z). If at any time threats are sensed the nodes will simply each change their randomized slang word and continue the process.

After spending the last five years researching and developing his idea, Professor Johnson was granted a patent on the second section of his project. He is continuing his efforts to obtain the patent for the first section of his proposal. In the meantime, he plans to refine his work by building and testing prototype systems.

Some have said that if Professor Johnson’s “one-time pad” approach is someday realized, it would be considered the holy grail of information security.