PUFFIN offers graphics card breakthrough versus break-in

October 9 2012, by Nancy Owano

(Phys.org)—The PUFFIN Project has come up with research that suggests GPU manufacturing processes leave each product with a unique kind of fingerprint. PUFFIN stands for physically unclonable functions found in standard PC components. What might appear to be identical graphics processors nonetheless differ. The differences cannot be duplicated. According to Threatpost, the Kasperksy Lab Security News Service, the project's lead researcher, Dr. Tanja Lange of Eindhoven Institute for the Protection of Systems and Information, said that the manufacturing differences were unclonable. The researchers have software that can spot the fine differences between GPUs.

The team's work is seen as significant in that it might lead to a new kind of user authentication.

In explaining their findings, they said that Physically Unclonable Functions (PUFs) offer a way to protect objects against counterfeiting. They allow "a root of trust" in a hardware system through generating unique "fingerprints" and deriving secret keys from the underlying physical properties of the silicon.

"Today they are typically found in specially designed hardware components and result from the silicon properties of individual transistors. They exist in many forms, among which are the so-called SRAM PUFs."

This is a collaborative research effort that includes the Technische Universiteit Eindhoven in The Netherlands, Technical University of Darmstadt in Germany, Katholieke Universiteit Leuven in Belgium, and the Dutch security firm, Intrinsic ID. The so-called fingerprinting for a piece of hardware is seen as especially relevant to the online gaming industry, for both vendors and players.

Heavy gamers with high-end graphics cards and customized machines accessing games from their computers could benefit from an online gaming company's installation of PUFFIN software on its servers. When a gamer logs into the game, the software scans the graphics card for its unique "fingerprint," and matches it against the fingerprint on file. If the log-in name and password do not match the fingerprint, the company asks for more authentication and if that does not bring satisfactory results, the user is blocked.

"Any passionate gamer knows the investment it takes to create a good character and the dangers of identity theft to which he is exposed by playing," said the project team. They pointed out that the operator of the gaming platform can push the extra security feature via a software update without any need for action on the user side.

The PUFFIN Project is to run its research until February 2015 with a total budget of 1.3 million euros. Moving forward, the project team intends to study and show the existence of SRAM PUFs and other types of PUFs, from standard PCs and laptops to mobile phones and consumer electronics.

More information: www.puffin.eu.org/