

IBM patentovala systém zabezpečující kryptografické klíče a kódy na ochranu dat

Armonk - 27 VII 2017: Firma IBM oznámila, že její inženýři získali patent na systém, který využívá vlastní struktury desky plošných spojů (DPS) k ochraně kryptografických klíčů a kódů. Systém je navržen tak, aby byl vysoce odolný vůči neoprávněné manipulaci. Patentovaný systém nevyžaduje velké množství pryskyřice nebo jiných materiálů pro zapouzdření modulu nebo obalu obsahujícího klíče a kódy. Toho lze využít k výraznému zvýšení ziskovosti výroby a díky spolehlivosti obalu současně k omezení rozsahu nezbytných oprav. Tento vynález by mohl pomoci chránit klíče a kódy šifrující data uložená na jakékoli platformě, ať už v cloudu nebo ve firemním úložném systému.

Ochrana kryptografických klíčů a kódů pro šifrování a dešifrování dat je zásadní pro účinnou bezpečnost informací. V případě, že jsou kryptografické klíče a kódy uloženy na modulech v elektronickém zařízení, musí být tyto moduly chráněny proti neoprávněné manipulaci nebo přístupu, aby nemohly být klíče a kódy zneužity.

Firma IBM si tento vynález patentovala pod číslem 8 938 627: Mnohvrstvá zabezpečovací struktura a metoda na ochranu kryptografických klíčů a kódů. Moduly se na ochranu proti neoprávněné manipulaci běžně zapouzdřují nebo zalévají plastovou hmotou nebo epoxidovou pryskyřicí. Tímto postupem většinou dochází k zajištění bezpečnosti proti neoprávněné manipulaci.

Výroba je ale náročná a problematická, protože desky plošných spojů se zalévanými moduly se mohou během vytvrzování pryskyřice deformovat nebo zkroutit. „V IBM se vynálezům a inovacím v rámci ochrany a bezpečnosti dat věnují celé týmy. Tuto oblast totiž považujeme za základ naší globální digitální budoucnosti, a proto také tato myšlenka stála u zrodu této inovace,“ říká technický manažer IBM Systems a jeden z vynálezců patentovaného přístupu Stefano Oggioni.

Patentovaný přístup využívá systém obvodů ve vrstvách DPS nebo jiné laminované struktury ke kódování kryptografických klíčů a kódů. Další vrstvy DPS nebo laminované struktury, které se přidávají nad nebo pod vrstvy obsahující klíče a kódy, zabraňují fyzickému přístupu. Obvody chránící klíče a kódy lze v rámci DPS nebo laminované struktury rozmístit v nahodilých schématech nebo místech, takže jsou dokonale skryty.

Pro ještě vyšší zabezpečení klíčů a kódů se tento systém obvodů skládá z materiálů, které nelze odhalit ani pomocí rentgenového záření nebo akustického mikroskopu. Firma IBM se této oblasti věnuje už desítky let a minulý týden ohlásila spuštění IBM Z – nové generace nejvýkonnějšího transakčního systému na světě schopného zvládnout více než 12 miliard zašifrovaných transakcí denně. Patentovaný systém patří k nastupujícím technologiím, se kterými už IBM Z a další systémy společnosti počítají.

Informace o kontaktu

Vladislav Doktor

IBM Central External Communications Manager vladislavdoktor@sk.ibm.com