VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

Příjemci podpory:

Vysoké učení technické v Brně
Fakulta informačních technologií

Poskytovatel:

Ministerstvo vnitra ČR

***Integrovaná platforma pro zpracování digitálních dat z bezpečnostních incidentů* (TARZAN)**

Identifikační kód VI20172020062

Název předkládaného výsledku: *Towards Fully Automated Infinitely Scalable and Maximally Effective Password Cracking of Encrypted Documents*

Typ výsledku dle UV č. 837/2017	Evidenční číslo (příjemce)	Rok vzniku
A audiovizuální tvorba		2019
ISBN-ISSN	**Webový odkaz na výsledek**	**Kde a kdy publikováno**
	https://www.fit.vut.cz/research/publication/12147/	ISS World Europe 2019

Anotace k výsledku:

Přednáška nastíní případy použití crackingu heslem, použité formáty, současné výkonnostní limity GPU / FPGA a stávající (ne) komerční crackerové nástroje. Kromě toho představíme našeho hypervizora pro distribuované praskání hesla, které pomáhá vyšetřovatelům využít potenciál jejich infrastruktury. Ukážeme, jak: a) automaticky extrahovat hash ze šifrovaných dokumentů; b) připravit a vyhodnotit klíčový prostor pro heslo (např. generovat hesla pomocí Markovových řetězců / gramatik založených na pravidlech a nakládání s hesly obsahujícími národní znaky); c) organizovat různé krakovací strategie (např. kombinace slovníků). V neposlední řadě budeme hovořit o našich zkušenostech při vývoji naší vlastní platformy pro praskání hardwaru založené na GPU, která je konkurenceschopná s průmyslovými standardy od známých dodavatelů.

Řešitelský tým: *Petr Matoušek (manažer a hlavní řešitel), Vladimír Veselý (realizační tým)*