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**<br>audiovizuální tvorba | | 2019 |
| **ISBN-ISSN** | **Webový odkaz na výsledek** | **Kde a kdy publikováno** |
| | https://www.fit.vut.cz/research/publication/11953/ | ISS World MEA 2019 |

## Anotace k výsledku:

*Na přednášce jsou popsány pouţívané případy pro pouţívání hesel, pouţívané formáty, běţné limity výkonnosti GPU / FPGA a stávající (ne) komerční nástroje pro trhání. Navíc představíme náš hypervisor pro rozptýlené rozprogramování hesel, které pomáhá vyšetřovatelům využít potenciálu jejich infrastruktury. Ukážeme, jak: a) automaticky extrahovat hash z šifrovaných dokumentů; b) připravovat a vyhodnocovat prostor klíče hesla (např. generovat hesla pomocí gramatik Markovových řetězců / pravidlům a manipulace s hesly obsahujícími národní znaky); c) organizovat různé strategie rozbíjení (např. kombinace slovníků).*

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