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: *TLS/SSL Decryption Workshop*

Typ výsledku dle UV č. 837/2017	Evidenční číslo (příjemce)	Rok vzniku
A audiovizuální tvorba		2018
ISBN-ISSN	**Webový odkaz na výsledek**	**Kde a kdy publikováno**
	https://www.fit.vut.cz/research/publication/11852/	ISS World Europe 2018

Anotace k výsledku:

SSL/TLS je používaný způsob šifrování chránící soukromí při prohlížení webových stránek. Tento workshop vysvětluje základy SSL/TLS protokolu a názorně demonstruje možnosti, jak zabezpečení obejít za pomoci sondy vyvinuté na FIT VUT. V rámci ukázky demonstrujeme, jak snadno se dá šifrovaná komunikace odposlechnout, za pomoci již existujících nástrojů, a následně vložit škodlivý kód zachycující všechna zadaná data z formulářů.

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