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: *SSL/TLS Interception 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/11874/	ISS World Asia 2018

Anotace k výsledku:

Prezentace uvádí metody pro dešifrování připojení TLS / SSL. Důraz je kladen na útok typu man-in-middle využívající protokol TLS / SSL proxy a další způsoby, jak získat soukromé klíče relace. Přednášející demonstrují, jak dešifrovat zachycený provoz pomocí nástrojů s otevřeným zdrojovým kódem, jako jsou Wireshark a NetFox Detective. Účastníci získají přístup k testovacímu lůžku, které se skládá ze skutečných zařízení (a jejich provozu), včetně naší 40Gbps intercepční sondy, která ukládá klíč relace TLS / SSL a zrcadlí provoz na monitorovacím rozhraní.

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