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		2019
ISBN-ISSN	**Webový odkaz na výsledek**	**Kde a kdy publikováno**
	https://www.fit.vut.cz/research/publication/12146	ISS World Europe 2019

Anotace k výsledku:

Prezentace představuje metody pro zachycení připojení TLS / SSL. Důraz je kladen na útok typu člověk ve středu využívající proxy proxy TLS / SSL a další způsoby, jak získat soukromé klíče relace. Přednášející nastíní potřebnou teorii (včetně historie designu SSL / TLS), známé útoky (včetně OpenSSL Hearthbleed, Logjam nebo BEAST) a standardní průmyslové nástroje (jako Wireshark, NetFox Detective, Fiddler Proxy a SSL-Split). Relace bude také zahrnovat živou demonstraci útoku MitM na připojení HTTPS vylepšenou injekcí JavaScriptu s protokolováním formuláře. Účastníci získají bezplatný přístup do zkušebny, která se skládá ze skutečných zařízení (a jejich provozu), včetně prototypu naší hardwarové sondy dešifrující SSL / TLS za běhu.

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