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 (TLS1.3 edition)*

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/12145/	ISS World Asia 2019

Anotace k výsledku:

Prezentace představuje metody pro zachycení připojení TLS / SSL. Důraz je kladen na útok typu člověk uprostřed" pomocí proxy a dalšími způsoby, jak získat nezašifrovaný obsah relace TLS / SSL. Přednášející nastíní potřebnou teorii (včetně zpráv o TLS 1.3), známé útoky (např. Opětovné vyjednávání, downgrade, změnu šifry a další) a průmyslové nástroje (jako Wireshark, NetFox Detective, Fiddler Proxy a SSL-Split). Relace také zahrnuje živou demonstraci útoku MitM na připojení HTTPS rozšířeného o vkládání JavaScriptu do protokolování formulářů. Účastníci získají bezplatný přístup k testovacímu stanovišti, které 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)*