E-Bezpečí 2019, 4(1): Page 23-25. Univerzita Palackého v Olomouci. ISSN 2571-1679.
Online: https://www.e-bezpeci.cz/index.php?view=article&id=1417

DEEP FAKE - STRUČNÝ ÚVOD DO PROBLEMATIKY

Kamil KOPECKÝ

Deep fake je fenomén, který v budoucnu zásadním způsobem ovlivní práci s informacemi - významným způsobem zasáhne především ověřování jejich pravdivosti. Bude pak pravděpodobně velmi obtížné, či dokonce nemožné odhalit, zda je materiál - v případě deep fake videozáznam - autentický, nebo zda byl upraven. Dostupnost této technologie posílí šíření dezinformací online prostředím a postupně posílí úloha autorit - informace budou posuzovány podle toho, kdo je publikoval, odpovědnost za jejich pravdivost bude stále více přenášena na vydavatele/autora.

Deep fake je označení pro realistickou úpravu videa - především tváří zobrazených osob - která umožňuje např. velmi věrohodně změnit mimiku, tedy i samotnou řeč jednotlivých aktérů videa. V praxi tak můžeme osobám na videu vkládat do úst věty, které nikdy nepronesly, provádět záměny postav, obličejů atd. Deep fake využívá pokročilého počítačového zpracování dat s využitím umělé inteligence (využívá neurální sítě se schopností učit se) a kvalita výsledného produktu - upraveného videa - se neustále zvyšuje.

Ačkoli se deep fake videa objevují masověji především v oblasti parodických videí a pornografie a první videa byla s trochou práce odhalitelná, s rozvojem strojového učení (neuronových sítí) se kvalita videí neustále zlepšovala a komunita nadšených vývojářů, kteří se na deep fake videa zaměřovala, stále rostla. S příchodem prvních aplikací se pak

technologie deep fake úprav rozšířila i mezi laiky a upravená videa začala stále více kolovat internetem.

Zdroj: Bloomberg YouTube Channel

Nastala celá řada problémů spojených logicky s porušováním autorských práv, etikou, ochranou osobnostních práv apod. a v tuto chvíli zdaleka není jasné, jak se vlastně budou videa na bázi deep fake právně posuzovat (legislativa na tuto formu manipulace s obrazem zatím není dostatečně připravena).

Pavel Kasík ve svém textu na Technetu upozorňuje na to, že v několika letech může nastat situace, kdy zcela přestaneme důvěřovat videoobsahu - nepůjde totiž rozeznat, kdy jde o původní neupravený záznam a kdy o jeho deep fake úpravu. To znamená obrovský potenciál pro šíření dezinformací - laický uživatel nebude mít šanci ověřit si autenticitu videa.

Logicky se tak dostaneme do fáze, kdy se falešná videa (upravená či zcela zfalšovaná) masově rozšíří sociálními sítěmi a budou cílit na uživatele, kteří nedokáží jejich autenticitu rozpoznat. Nástroje, které by deep fake umožnily odhalit, nestíhají držet krok s rychlostí, jakou nástroje na vytváření deep fake vznikají.

Čemu pak bude možné věřit, když půjde snadno podvrhnout obraz (fotografii), zvuk i video? Nebo bude nutné pochybovat o všem, co vidíme a slyšíme? Přestane existovat důvěra? Nebo bude nahrazena důvěrou v konkrétní autoritu a instituci, tj. zprávám budeme věřit prostě proto, že je vytvořilo veřejnoprávní médium? To vše ukáže čas.

Pro E-Bezpečí
Kamil Kopecký
Univerzita Palackého v Olomouci

Zdroje:

Počítač umí přelepit tvář. Internet zaplaví parodie a falešné porno. https://www.idnes.cz/technet/internet/deep-fake-videomontaze-porno-neuronova-sit-falesne-video.A180225_010517_sw_internet_pka

Budoucnost falešných zpráv: za tři roky budou videa nedůvěryhodná https://www.idnes.cz/technet/internet/budoucnost-fake-news-obama-video.A170801_114510_tec_technika_dvz

Po fake news přijde fáze deep fake. Falešné video se Zemanem, Babišem a Trumpem neodhalíte http://forum24.cz/po-fake-news-prijde-faze-deep-fake-falesne-video-se-zemanem-babisem-a-trumpem-neodhalite/

O tom, co nám řekne Trump, Babiš či Zeman, rozhodnou tvůrci „deep fake“. https://hlidacipes.org/o-tom-co-nam-rekne-trump-babis-ci-zeman-rozhodnou-tvurci-deep-fake/

Jak donutit Obamu mluvit sprostě: fake news budoucnosti napodobí hlas i mimiku https://hlidacipes.org/budoucnost-fake-news-bude-o-dost-hur-nebudeme-verit-vlastnim-usim-a-ocim/