Výskumníčka z FIIT STU ukázala spôsob, akým je možné z mikročipu odhaliť duševné vlastníctvo vývojára

Tlačová správa

Bratislava 19. 10. 2021 – **Neurónové siete sú jedným zo základných stavebných prvkov umelej inteligencie. Ich model a interné parametre sú spravidla niečo, čo si autori chránia ako obchodné tajomstvo, ktoré je predmetom ich konkurenčnej výhody. Výskumníčka Dr. Xiaolu Hou, ktorá na Fakultu informatiky a informačných technológií STU (FIIT STU) prišla zo Singapuru, vo svojej poslednej publikácii poukázala na spôsob, akým je možné hotový model neurónovej siete z mikročipu extrahovať a odhaliť.**

„Náš výskum preukázal, že neurónové siete sú zraniteľné voči útokom spôsobujúcim chyby. Tieto útoky zmenia fyzické správanie zariadenia počas výpočtu, čo má za následok zmenu hodnoty, ktorá sa práve vypočítava. Predchádzajúce práce väčšinou skúmali útoky na chyby kvôli nesprávnej klasifikácii výstupu, čo ovplyvňovalo spoľahlivosť neurónových sietí. My sme skúmali možnosť reverzného inžinierstva neurónových sietí s chybovými útokmi," konštatujú vo svojej práci výskumníci okolo Dr. Xiaolu Hou z FIIT STU.

Článok s ich zisteniami bol publikovaný v prestížnom karentovanom časopise IEEE Transactions on Reliability, ktorý patrí do najvyššej kategórie Q1 v počítačových vedách a pýši sa vysokou citovanosťou.

„V tejto práci sme vyvinuli metódu, ktorá poskytuje dokázateľne presnú extrakciu parametrov neurónovej siete pomocou vkladania chýb. Cieľom našej metódy je obnoviť konkrétne vrstvy neurónovej siete, čím je možné odhaliť jej kľúčové parametre a odhaliť tak to, čo vývojári považujú za svoje duševné vlastníctvo," hovorí Dr. Xiaolu Hou.

„Kybernetická bezpečnosť je mimoriadne dôležitá téma, ktorej sa niektorí naši kolegovia venujú dlhé desaťročia. V posledných rokoch dôležitosť počítačovej bezpečnosti rastie oveľa dynamickejšie ako v minulosti a omnoho viac sa priamo dotýka každého z nás. Je skvelé vidieť, že príchod nových kolegov zo zahraničia na našu fakultu sa prejavuje aj v podobe takýchto kvalitných vedeckých publikácií, o ktorých môžeme bez preháňania povedať, že sú na špičkovej svetovej úrovni," konštatuje prof. Ivan Kotuliak, dekan FIIT STU.

Dr. Xiaolu Hou v súčasnosti pôsobí ako odborná asistentka na Fakulte informatiky a informačných technológií Slovenskej technickej univerzity v Bratislave. V roku 2017 získala doktorát z matematiky na Nanyang Technological University (NTU) v Singapure. Vo svojom výskume sa zameriava na hardvérovú bezpečnosť kryptografie a neurónových sietí. Má tiež skúsenosti s výskumom v oblasti ochrany súkromia polohy, výpočtov viacerých strán (multiparty computation) a diferenciálneho súkromia. Vďaka širokému spektru výskumných záujmov publikovala svoje práce na špičkových konferenciách a v časopisoch v rámci rôznych

Ilkovičova 2
842 16 Bratislava 4
www.fiit.stuba.sk
press@fiit.stuba.sk

oblastí, od matematiky až po počítačovú bezpečnosť. Na FIIT STU začala pôsobiť začiatkom roku 2021, čím sa zaradila medzi viacerých expertov zo zahraničia, ktorí nedávno prišli na túto fakultu. Dnes okrem aktívneho výskumu na fakulte pôsobí aj vo výučbe a vedie diplomové práce študentov.

Fakulta informatiky a informačných technológií STU v Bratislave

- Jediná fakulta v ČR a SR s medzinárodnou akreditáciou od najväčšej profesijnej organizácie IET, ktorú má aj Cambridge či Ofxord na svojich technických smeroch (http://bit.ly/FIIT_akred).
- Jediná fakulta na Slovensku so zameraním výhradne na oblasť informatiky a informačných technológií.
- Najmladšia fakulta Slovenskej technickej univerzity v Bratislave.
- Jedna z dvoch slovenských fakúlt v medzinárodnom združení Informatics Europe, ktorého cieľom je zlepšovanie kvality výskumu a výučby v oblasti informatiky a IT.
- Absolventi majú najvyššie priemerné platy a sú najžiadanejší na trhu práce.
- Fakulta s najlepšou návratnosťou financií vynaloženými na študentov. Už po 2,16 roku od úspešného ukončenia štúdia sa vrátia štátu všetky financie vynaložené na študenta.