XIAOLU HOU

Fakulta informatiky a informačných technológií
Slovenská technická univerzita

Číslo projektu
2130/01/01

Trvanie projektu
10/2021 -9/2024

"Do programu SASPRO som sa prihlásila, pretože mi poskytuje vynikajúcu príležitosť venovať sa vlastnému výskumu v jednej z popredných výskumných inštitúcií na Slovensku. Plánovaný výskum rozšíri moje skúsenosti v oblasti hardvérovej bezpečnosti, ako aj bezpečnosti neurónových sietí. Tieto skúsenosti mi pomôžu v mojej akademickej kariére. Získané zručnosti v oblasti projektového manažmentu a líderstva posilnia moju kompetenciu pri snahe o získanie profesúry. Vedecké úspechy počas pracovného pobytu, ako sú publikácie v renomovaných vedeckých časopisoch a nadviazanie spolupráce s rôznymi výskumnými organizáciami v rámci Európy, mi pomôžu naštartovať moju akademickú kariéru v rámci EÚ a poskytnú mi dobrú východiskovú pozíciu v úvodnej fáze získania titulu profesora. "

BIOGRAFIA

Xiaolu Hou získala titul Ph.D. z matematiky na univerzite Nanyang Technological University (NTU) v Singapure v roku 2017. Jej výskum sa zameriava na vnášanie chýb a útoky postrannými kanálmi. Má tiež skúsenosti s výskumom v oblasti bezpečnosti neurónových sietí, utajenie polohy, skupinových výpočtov a diferenciálneho utajenia. So širokým spektrom výskumných záujmov publikovala svoje práce na špičkových miestach v rôznych oblastiach, od matematiky po počítačovú bezpečnosť.

ZHRNUTIE PROJEKTU

Hardvérové zabezpečenie neurónových sietí - HARSONN

Rozhodovacie úlohy vykonávané pomocou neurónových sietí sa úspešne zavádzajú v mnohých oblastiach, vrátane tých, ktoré sú kritické z hľadiska bezpečnosti, ako je zdravotníctvo, doprava a inteligentné siete, kde úmyselné a neúmyselné zlyhania môžu byť katastrofálne. Implementácie neurónových sietí sa spoliehajú na hardvérové platformy (napr. FPGA, GPU a mikrokontroléry) na urýchlenie výpočtov. Ako sa ukázalo v oblasti aplikovanej kryptografie tieto systémy sú citlivé na fyzické útoky, ktoré boli útoky vykonávané za účelom obnovy tajného kľúča alebo za účelom porušenia/obídenia bezpečnostných kontrol. Preto je potrebné vyhodnotiť potenciálne útoky, ktoré môžu byť zamerané na neurónové siete na hardvérovej úrovni.

V tomto projekte sa zameriavame na dva hlavné typy hardvérových útokov na neurónové siete, a to útoky bočným kanálom a chybové útoky, ktoré boli predtým skúmané najmä v súvislosti s ich kryptografickými implementáciami. Útoky bočným kanálom sú pasívne útoky, ktoré sledujú fyzické veličiny súvisiace s výpočtom citlivých premenných a zneužívajú ich na získanie neoprávnených informácií. Chybové útoky sú aktívne útoky, ktoré narušia zariadenie počas výpočtu v prospech útočníka.

Cieľom projektu je preskúmať možné útočné vektory a navrhnúť protiopatrenia v rámci všetkých aspektov rozvoja neurónových sietí (údaje o výcviku, tréningový program, nasadená sieť). Najprv vykonáme komplexnú štúdiu o súčasných útočných metódach a obranných opatreniach. Ďalej vyvinieme nové útoky a navrhneme možné protiopatrenia.

Naše výsledky môžu slúžiť ako základ pre načrtnutie citlivosti neurónových sietí na fyzické útoky, ktoré možno považovať za životaschopný vektor útoku vždy, keď je zariadenie nasadené v nepriateľskom prostredí.

Projekt bude taktiež čerpať zo spolupráce a poznatkov o vlastnostiach neurónových sietí z oblasti matematiky s cieľom zlepšiť stratégie útoku.

XIAOLU HOU

Fakulta informatiky a informačných technológií
Slovenská technická univerzita

Číslo projektu
2130/01/01

Trvanie projektu
10/2021 -9/2024

PUBLIKÁCIE

1. Won, Yoo-Seung, **Xiaolu Hou,** Dirmanto Jap, Jakub Breier, and Shivam Bhasin. "Back to the basics: Seamless integration of side-channel pre-processing in deep neural networks." IEEE Transactions on Information Forensics and Security 16 (2021): 3215- 3227. [PDF]

2. Breier, Jakub, **Xiaolu Hou,** and Yang Liu. "On evaluating fault resilient encoding schemes in software." IEEE Transactions on Dependable and Secure Computing 18, no. 3 (2019): 1065-1079. [PDF]

3. Breier, Jakub, Mustafa Khairallah, **Xiaolu Hou,** and Yang Liu. "A countermeasure against statistical ineffective fault analysis." IEEE Transactions on Circuits and Systems II: Express Briefs 67, no. 12 (2020): 3322-3326. [PDF]

4. Breier, Jakub, Dirmanto Jap, **Xiaolu Hou,** and Shivam Bhasin. "On side channel vulnerabilities of bit permutations in cryptographic algorithms." IEEE Transactions on Information Forensics and Security 15 (2019): 1072-1085. [PDF]

5. Breier, Jakub, **Xiaolu Hou,** Dirmanto Jap, Lei Ma, Shivam Bhasin, and Yang Liu. "Practical fault attack on deep neural networks." In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, pp. 2204-2206. 2018. [PDF]

Tento pprojekt získal financovanie z výskumného a inovačného programu Európskej únie Horizont 2020 v rámci Marie Skłodowska-Curie Dohody o grante č. 945478.