Faktablad

Avdelningen för cybersäkerhet och säkra kommunikationer

Publ.nr MSB1762 – maj 2021

Sårbarheter och hotanalys från sidokanaler med maskininlärning i fokus

Under det senaste decenniet har cyberattacker flyttat från att existera högt upp i programvarustacken till att även appliceras på den underliggande fysiska implementeringen. Trots det växande erkännandet av problemet finns det inga allmänna lösningar för att säkra de fysiska enheter som för närvarande är i användning.

I det här projektet kommer vi att undersöka användningen av automatiserade verktyg och maskininlärningstekniker för att extrahera hemlig information från fysiska implementationer via läckage från olika sidokanaler. En av uppgifterna i projektet är att bestämma om det är möjligt att extrahera den hemliga nyckeln från SIM-kort inbäddade på mobilen, en typ som förväntas bli standard i 5G. Vi kommer att kvantitativt utvärdera attackens möjligheter under begränsningar för den tillgängliga sidokanalsinformationen.

Parallellt kommer vi att undersöka hur en tillverkare inom AI-industrin kan skydda den detaljerade arkitekturen för ett neuralt nätverk från att läcka genom sidokanaler om det implementeras i en enhet som är tillgänglig för motståndaren.

Den förvärvade kunskapen gör det möjligt för oss att utveckla nya metoder för bedömning av mobila, inbäddade och personliga datorenheter och AI-hårdvaruacceleratorer, samt att hantera det pressande behovet av att säkerställa säkerhet på hårdvarunivå. Den stora utmaningen är att skapa försvarsmekanismer som motstår attacker även när attackernas kapacitet växer.

Projektet förväntas leverera utmärkta vetenskapliga resultat som leder till en bättre förståelse för möjligheter och begränsningar för maskininlärningbaserad sidokanalsanalys. Våra resultat hoppas att stödja processen för sårbarhets- och hotanalys, samt utvärdering av säkerhetskontroller och säker produktutveckling.

Bakgrund

Sidokanalsattacker utnyttjar korrelationen mellan fysiska mätningar som gjorts vid exekvering och det inre tillståndet för den beräknande enheten för att extrahera känslig information. Sidokanalsattacker kan användas för att extrahera hemliga nycklar från fysiska implementeringar av kryptosystem, stjäla immateriell egendom och rekonstruera proprietära algoritmer från dess hårdvaruimplementering.

Avancerad teknik som maskininlärning möjliggör dessutom en ny typ av sidokanalsattacker. Angriparen tränar först en modell för att ``lära sig'' hur läckaget för en attackerad implementering ser ut, och attackerar sedan det verkliga målet med mindre beräkningsresurser . Det ger motståndaren möjlighet att kringgå vissa skyddsåtgärder och attackera skyddade implementationer.

Projektorganisation

KTH Kungl Tekniska Högskolan
LTH, Lund tekniska högskola

Koordinator

Prof Elena Dubrova, KTH
Telefon: 08-7904114
dubrova@kth.se

Kontakta oss:
Tel: 0771-240 240
registrator@msb.se
www.msb.se

Myndigheten för samhällsskydd och beredskap