Defence-related Research Action - DEFRA

ACRONIEM: INES

Titel: INtegrated Embedded Security

Duur van het project: 01/12/2025 – 01/03/2030

Totaal budget: 2 448 000€

waarvan bijdrage KHID: 2 000 000€

Kernwoorden : side-channel attacks, fault injection attacks, post-quantum cryptografie

BESCHRIJVING VAN HET PROJECT (tussen 4000 en 5500 karakters, spaties inbegrepen)

Context

INES speelt in op de dringende noodzaak van robuuste ingebedde beveiliging voor cryptografische implementaties tegen side-channel attacks (SCA's) en fault-injection attacks (FIA's), met bijzondere aandacht voor post-quantum cryptografie (PQC). Hoewel PQC-schema's (bijv. ML-KEM/Kyber en ML-DSA/Dilithium) momenteel worden gestandaardiseerd, is bij hun ontwerp zelden rekening gehouden met fysieke dreigingen op implementatieniveau, waardoor nationale veiligheidssystemen kwetsbaar blijven wanneer ze in vijandige omgevingen worden ingezet. Het INES-consortium — UCLouvain (coördinator), NXP, STMicroelectronics, Thales Belgium en de Koninklijke Militaire School — streeft naar een holistische aanpak die ontwerp, implementatie, meting en evaluatie omvat.

Algemene doelstellingen

Het project is opgebouwd rond vier SMART-doelstellingen:

1. Verbeteren van de bescherming tegen SCA's en FIA's voor PQC door middel van gevoeligheidsanalyses en gelaagde implementaties (bijv. tegenmaatregelen concentreren waar het lekken het meest kritiek is).
2. Behoud van beveiligingseigenschappen tijdens compilatie/synthese voor software en hardware (FPGA's), inclusief onderzoek naar externe SCA's op algemene processors.
3. Opzetten van betrouwbare, geharmoniseerde testopstellingen voor lokale lekmetingen en foutinjectie, plus VM-gebaseerde omgevingen voor externe aanvallen.
4. Vooruitgang in solide beveiligingsbeoordeling door worst-case aanvalsstudies te combineren met verkorte extrapolaties om weerstand te schatten buiten laboratoriumlimieten en tooling uit te breiden (bijv. SCALib - https://www.simple-crypto.org/activities/scalib).

Methodologie

INES volgt een geïntegreerde, iteratieve workflow:

- **WP1 (Ontwerp):** Selecteer prioritaire PQC-schema's; voer gevoeligheidsanalyse uit van subcomponenten (bijv. NTT, her-encryptiestappen) en specificeer tegenmaatregelen op algoritmisch niveau.
- **WP2 (Compilatie & synthese):** Vertaal tegenmaatregelen naar beschermde implementaties — software (embedded & algemene CPU's) en hardware (FPGA's) — waarbij wordt gewaarborgd dat compiler/synthesizer de beveiliging behoudt. Een publieke challenge-implementatie zal aan de gemeenschap worden vrijgegeven.
- **WP3 (Opstellingen):** Definieer referentielabs voor SCA's en FIA's en bouw VM-netwerken om de haalbaarheid en omstandigheden van externe SCA's te beoordelen.
- **WP4 (Evaluatie):** Versterk evaluatiemethodologieën (worst-case vectoren, extrapolatie) en breid SCALib uit met functies gericht op de industrie.
  Het consortium zal waar mogelijk open-source resultaten ontwikkelen (datasets, code) en eigendomsimplementaties ter ondersteuning van industriële exploitatie en defensietoepassingen.

Potentiële impact op Defensie

INES ondersteunt rechtstreeks de CYBER-prioriteiten van Defensie door:

- **Capaciteitsontwikkeling:** Belgische Defensie uitrusten (via KMS, Cyber Command, NSA/NVO) met reproduceerbare tests, verbeterde beoordelingsmethoden en know-how om veilige cryptografische producten te evalueren en te produceren die bestand zijn tegen SCA's/FIA's — zelfs bij veldinname of vijandige manipulatie.
- **Procesoptimalisatie:** Geharmoniseerde labs en kwantitatieve evaluatieraccourts bieden om certificeringsprocessen en inkooprisicoanalyses te versnellen.
- **Commerciële producten & banen:** Industriële partners integreren resultaten om apparaten die door Defensie worden gebruikt te versterken; kennisoverdracht en nieuwe evaluatietaken zullen gespecialiseerde functies binnen Defensieorganisaties doen groeien.

Verwachte eindresultaten & valorisatie op korte/middellange termijn

- **Beschermde implementaties:** Minstens drie implementaties (≥1 software, ≥1 hardware, ≥1 open source), inclusief een publieke challenge-release (M42) en eigendomsleveringen voor Defensie (M48).
- **Demonstraties van externe SCA's:** Twee aanvallen aangetoond in realistische netwerkomgevingen, met richtlijnen over praktische relevantie en mitigaties (M24).
- **Referentietestopstellingen:** Gedocumenteerd ontwerp van een meet- en foutinjectielab dat reproduceerbaarheid en kostenefficiënte adoptie mogelijk maakt (M42).
- **Evaluatietools:** SCALib uitgebreid met ≥2 nieuwe functionaliteiten, plus evaluatierapporten en verkorte formules voor betrouwbare extrapolatie (M48).
- **Publicaties & verspreiding:** ≥6 peer-reviewed artikelen; datasets en code gedeeld waar niet-gevoelig; workshops en gerichte briefings voor Defensie-stakeholders (Cyber Command, NSA/NVO).

Valorisatieperspectieven

Korte termijn (binnen het project):

- Adoptie van beoordelingsprocessen en tools door Defensie-evaluatoren en industriële labs; onmiddellijke inzet van verbeterde SCALib en VM-netwerk voor externe aanvallen.

Middellange termijn (3–5 jaar):

- Integratie van tegenmaatregelen in Defensie-producten van Thales Belgium, NXP en ST; versterking van het nationale traject naar certificering van ingebedde beveiliging; blijvende opleiding met open datasets en challenge-platforms.

CONTACTINFORMATIE

Coördinator

UCLouvain / ICTEAM – Crypto Group
François-Xavier Standaert
francois-xavier.standaert@uclouvain.be

Partners

STMicroelectronics Belgium / Connected Security, SW development, Security architecture
Jean-François Dhem
Jean-francois.dhem@st.com

NXP Semiconductors Belgium NV / Competence Center Crypto & Security
Joppe Bos
joppe.bos@nxp.com

Thales Belgium / Innovation & Product Policy
Jonathan Pisane
jonathan.pisane@be.thalesgroup.com

Royal Military Academy / ALICE (cryptography group), MWMW (mathematics)
Julien Petit
julien.petit@mil.be

LINK(S) NAAR PROJECT

Nog niet beschikbaar