

NOTA AAN DE VLAAMSE REGERING

Pagina 1 van 18

- (1) Uitvoeren van top strategisch basisonderzoek voor het gericht ontwikkelen van nieuwe kennis, wetenschappelijke doorbraken en talent op wereldniveau daar waar Vlaanderen reeds excellent presteert én waar synergie kan bekomen worden met de vraag-gedreven implementatie-agenda van het Vlaamse bedrijfsleven;
- (2) Een centrale focus op de implementatie van CS-toepassingen in het bedrijfsleven. Een vraag-gedreven agenda vanuit het bedrijfsleven moet via open, goed georganiseerde kanalen en netwerken gebracht worden tot bestaande overheidsinstrumenten van het Vlaams Agentschap Innoveren en Ondernemen (VLAIO) en relevante instellingen;
- (3) Een sterk flankerend beleid waarin wordt gewerkt aan de significante opleidingsnoden gericht op de arbeidsmarkt. Verder ligt er een focus op een correcte doch ambitieuze “outreach” zodat vernieuwende cybersecurity-kennis, inzichten en technologieën worden gedeeld, waardoor zo veel mogelijk Vlaamse actoren actief kunnen participeren.

In uitvoering van dit beleidsplan duidde de Vlaamse regering op 7 juni 2019 de stuurgroep van het beleidsplan CS aan (VR 2019 0706 DOC.0866/1BIS).

Op 4 en 5 juli 2019 heeft de internationale wetenschappelijke adviesraad het voorgestelde programma positief beoordeeld.

2. INHOUD

A. DOELSTELLING EN INHOUD VAN HET CYBERSECURITY-ONDERZOEKSPROGRAMMA

In de voorbije maanden is door het gezamenlijk onderzoeksveld in Vlaanderen gewerkt aan een onderzoeksprogramma voor “Cybersecurity”. In samenspraak hebben de Vlaamse universiteiten met toonaangevende expertise rond cybersecurity (KU Leuven, U Gent, VU Brussel) en het strategisch onderzoekscentrum imec een onderzoeksplan opgesteld. Dit plan “Cybersecurity Initiative Flanders” is bijgevoegd als bijlage 1.

Vertegenwoordigers van bovengenoemde organisaties hebben een onderzoeksprogramma gedefinieerd dat inspeelt op alle aanwezige sterktes en alle aanwezige onderzoekcompetenties rond CyberSecurity (CS) in Vlaanderen, en dat gestructureerd werd zodat de diverse actoren met vraaggedreven noden rond CS zo vlot mogelijk kunnen aansluiten bij de toepassingsgerichte resultaten van dit onderzoeksprogramma.

Er werd met andere woorden een structuur gemaakt met vier onderzoekslijnen of 'Research Tracks' waarbij rekening wordt gehouden met de aanwezige sterktes in Vlaanderen en het toepassingsgericht onderzoek. Vervolgens werden deze 'Research Tracks' opgesplitst in onderzoeksthema's ('Research Themes') die nauw aansluiten bij dezelfde sterktes en die aanknopingspunten bieden voor vraaggedreven implementatietrajecten met de industrie.

De inhoud van deze ‘Research Tracks’, zoals uitgebreid in het CS-onderzoeksprogramma beschreven, werd voorgelegd aan de stakeholders in een ‘validatieworkshop’ en aan een Internationale Adviesraad, zoals verder toegelicht.

De vier Research Tracks die in het CS-onderzoek worden uitgevoerd, worden kort toegelicht, zoals reeds beschreven in de nota aan de Vlaamse Regering (VR 2019 2203 DOC.0317/1QUATER). Daarbij wordt telkens per Track vermeld:

////////////////////////////////////

De Track Leader: een top-expert uit de corresponderende research track die de verantwoordelijkheid heeft genomen om een Research Track te definiëren en te coördineren, en samen met de experts van de verschillende organisaties te verfijnen (in onderzoeksthema's die op hun beurt zijn samengesteld uit onderzoeksactiviteiten).

Core Principal Investigators: de Principal Investigators (PI) zijn professoren of vaste onderzoekskaders die internationaal erkend zijn in hun expertise en die verantwoordelijkheid hebben genomen om samen met de collega's uit de verschillende organisaties inhoud te geven aan de specifieke activiteiten en themas's. Het CV van de betrokken onderzoekers is opgenomen in Bijlage 2 (CS Consortium). De betrokken onderzoekers behoren tot de onderzoeksgroepen COSIC, DistriNet en CiTiP (KU Leuven), CSL (U Gent), SOFT (VU Brussel) en imec.

De positionering van de Research Track in het onderzoeksprogramma is op basis van de aanwezige excellentie. De budgetten voor de eerste twee jaar worden opgenomen in bijlagen 3 en 4.

We herhalen hier de korte beschrijving van de vier ‘Research Tracks’ die het validatieproces doorlopen hebben. Hierbij dient opgemerkt dat de finale beschrijving in het programma “Cybersecurity Initiative Flanders” geëvolueerd is zonder afbreuk te doen aan de essentie van de basisbeschrijving (VR 2019 2203 DOC.0317/1QUATER). We voegen vervolgens de hierboven opgesomde kerngegevens en positionering toe. De volledige beschrijving van het programma is te vinden in bijlage 1.

Onderzoekslijn 1 : Software- en Applicatiebeveiliging

Voor een grote fractie van de veiligheids-incidenten is de uitbuiting van een of andere software-zwakheid een sleutelelement. Dit bevestigt de nood aan basisonderzoek over de kwaliteit van beveiligingssoftware en applicatielogica en de betrouwbare koppeling tussen beide. Er wordt ingezet op drie belangrijke uitdagingen: (1) het ondersteunen van een beveiligingsmethodiek die toepasbaar is in de volledige levenscyclus van software en applicaties; (2) het ontwikkelen van verificatietechnologie die harde garanties kan leveren voor belangrijke (beveiligings)kritische eigenschappen van software en (3) kerntechnologie die toekomstige softwareontwikkelingen inherent veiliger kan maken.

(II) *SDLC, beveiliging gedurende de levenscyclus van softwareapplicaties*

De creatie, ontwikkeling en ondersteuning van veilige softwareapplicaties en diensten vormt een inherent grote uitdaging. Er werd al heel wat vooruitgang geboekt op dit terrein: op het vlak van (1) het modelleren van kwetsbaarheden, aanvalsscenario's en misbruiken, (2) het modelleren van beveiligde oplossingen (*Security by Design* en *Privacy by Design*, o.a. met beveiligingspatronen) en (3) het aanleveren van veilige code en het ontwikkelen van systematische beveiligingstesten.

Verdere verbeteringen zijn noodzakelijk, samen met de georkestreerde toepassing van deze technieken in de context van een volledige levenscyclus waarin ook andere ontwikkelingsactiviteiten aan bod komen die deels los staan van beveiliging. Hierbij moeten een aantal “best of breed” technieken gecombineerd worden. In functie van de maturiteit van de organisatie die het interne beveiligingsproces wil verbeteren kan dit leiden tot lichtvoetige (*agile*) beveiliging of tot intensieve processen met uitgebreide testprocedures en certificatie.

(III) Programmaverificatie en testen voor cybersecurity

Statische programma-analyses leiden informatie over het gedrag van een applicatie volautomatisch af uit diens broncode en laten toe om zwakheden of ongewenst gedrag te detecteren. Het is een belangrijke uitdaging om de precisie en schaalbaarheid van een analyse te garanderen voor applicaties met inherent niet-determinisme en om statische analyse geschikt te maken om garanties

////////////////////////////////////

Dynamische programma-analyses zijn complementair aan statische analyses: zij voeren een applicatie uit om het gedrag ervan te observeren of om over datzelfde gedrag controle uit te oefenen en het te wapenen tegen zwakheden. De belangrijkste uitdagingen zijn het combineren van transparantie (geen beïnvloeding van het gedrag), volledigheid en het omgaan met dynamische applicaties, waarbij componenten van derden geïntegreerd worden tijdens de uitvoering (bv. de cliëntzijde van webapplicaties).

Veel aanvallen tegen software zijn gebaseerd op het uitbuiten van implementatie-details van de software of de onderliggende infrastructuur. Heel bekende klassieke voorbeelden zijn de geheugenbeheer-zwakheden zoals buffer overflows, of injectie-aanvallen zoals SQL injection of script injection. Nieuwere voorbeelden zijn de recente micro-architecturale zijkanaal-aanvallen zoals Spectre, Meltdown en Foreshadow.

Voor software die niet op één computer draait, maar op een gedistribueerd systeem, kan deze ondersteuning worden ingebouwd in programmeertalen of raamwerken die op een geschikte manier abstractie maken van details rond “deployment”, coördinatie en communicatie. Door deze abstracties vervolgens te voorzien van de nodige parametrisaties, kunnen veiligheidsaspecten op een samenstelbare wijze worden uitgedrukt. Dat laatste is cruciaal nu software bijna per definitie gedistribueerd is en opgebouwd is uit componenten die in verschillende programmeer-paradigma’s en talen werden geschreven, en meestal ook ontwikkeld worden door verschillende teams.

////////////////////////////////////

Challenge 1 organisatie, structuur en positionering

- Track leader: Bart Jacobs¹
- Core PI's en kaders: Bart Jacobs¹, Wouter Joosen¹, Frank Piessens¹, Vincent Naessens¹, Lieven Desmet¹, Dimitri Van Landuyt¹, Koen Yskout¹, Elisa Gonzales Boix³, Wolfgang De Meuter³, Coen De Roover³, Dominique Devriese³
- Lijst van onderzoeksthema's – Secure Software and Applications
 - o Thema 1 – SDLC: *Secure Software Development Life Cycle*
 - o Thema 2 – Programmaverificatie en Security Testing
 - o Thema 3 – Veilige programmeertalen en veilige compilatie
- Positionering: op basis van voorstel van de eerste 16 maand, september 2019 – december 2020) heeft Track 1 ongeveer 18% van globale personele inzet van het onderzoeksprogramma (excl. management).

(1) KU Leuven, (2) U Gent, (3) VU Brussel, (4) imec

Onderzoekslijn 2: Kritische beveiligingsdiensten voor diverse platformen

Een groot aantal beveiligingsoplossingen steunt op de controle van gebruikers, op basis van hun identiteit of toegekende rechten en permissies, en op de evaluatie of de gebruiker in kwestie de toelating heeft om functionaliteit uit te voeren, toegang te krijgen tot informatie, enz. Deze beveiligingsfunctionaliteit wordt geleverd door kritische beveiligingsdiensten die gebaseerd zijn op authenticatie, autorisatie en audit. Dit domein evolueert zeer snel en wordt bovendien uitgebreider, aangezien het verregaand gebruik van diverse databronnen de complexiteit van deze uitdaging aanzienlijk heeft verhoogd. Deze onderzoekslijn bevat ook een multidisciplinair luik dat de nodige aandacht geeft aan policy en regelgeving.

(I) Identiteitsbeheer en Authenticatie

De creatie van authenticatiesystemen die op naadloze wijze kunnen samenwerken met een groeiend palet van applicaties en platformen vormt een belangrijke uitdaging. De kosten die gepaard gaan met het betrouwbaar beheren van gebruikers, identiteit en de daaraan gekoppelde platformen voor toegangscontrole is zeer hoog, zowel voor de gebruikers als voor de partijen die onlinediensten en applicaties aanbieden. Het vereiste onderzoek streeft dan ook naar oplossingen die enerzijds beveiliging, transparantie en privacy verhogen, en tegelijk de drempel en lasten (*friction*) voor de gebruiker beperken. Een belangrijk onderzoeksthema in deze context is het benutten van een groot aantal sensoren die meer en meer aanwezig zijn in slimme apparaten en omgevingen: deze maken het mogelijk oplossingen te bouwen die het gedrag van de gebruiker nauwkeurig herkennen (gedragsgebaseerde biometrie). Uiteraard volgt hieruit een grote en bijkomende uitdaging om de beveiliging (authenticatie) in kwestie te beschermen tegen nieuwe aanvallen en misbruik. Het wordt belangrijk de robuustheid van diverse oplossingen te verhogen en meteen ook een antwoord te bieden voor de belangrijke vereisten op het vlak van privacy.

(III) Autorisatie en Audit

Autorisatie en audit vormen samen met authenticatie de zogenaamde AAA-diensten: wanneer een gebruiker correct herkend werd door middel van authenticatie, dan dient een digitaal platform vervolgens na te gaan of de gebruiker in kwestie wel degelijk de toestemming krijgt om bepaalde acties en operaties uit te voeren. Dit gebeurt in principe door middel van autorisatie. Het is een bijzondere uitdaging autorisatie aan te leveren die gelijktijdig veilig en performant is, robuust in een omgeving met aanvallers en bovendien duidelijk voor alle belangrijke actoren: eindgebruikers, beheerder van de platformen en eigenaars (exploitanten) van digitale applicaties. Precies omwille van

////////////////////////////////////

is een belangrijke hefboom om alle maatschappelijke actoren mee te laten evolueren met de snelle technologieontwikkeling binnen cybersecurity.

Onderzoekslijn 2 organisatie, structuur en positionering

- Track Leader: Frederic Vercauteren¹
- PI's en kaders: Frederic Vercauteren¹, Bart Preneel¹, Nigel Smart¹, Enrique Argones Rua¹, Dave Singelée¹, Peggy Valcke¹, Bart De Decker¹, Wouter Joosen¹, Bert Lagaisse¹, Davy Preuveneers¹
- Lijst van onderzoeksthema's: Track 2 – Security Services
 - o Thema 1 – Identity Management en Authenticatie
 - o Thema 2 – Autorisatie en Audit
 - o Thema 3 – Geavanceerde encryptie en toegangscontrole voor data
 - o Thema 4 – Policy en regelgeving
- Positionering: op basis van voorstel van de eerste 16 maand, september 2019 – december 2020) heeft onderzoekslijn 2 ongeveer 20% van globale personele inzet van het onderzoeksprogramma (excl. Management).

(1) KULeuven, (2) U Gent, (3) VU Brussel, (4) imec

Onderzoekslijn 3: Systeem- en infrastructuurbeveiliging

Deze onderzoekslijn bevat naast de voor de hand liggende systeem- en infrastructuurdimensie ook een activiteit die de beveiligingsbeheer en -operaties ondersteunt.

(II) *Systeembeveiliging*

Elk systeem, gaande van diensten in de cloud tot kleinschalige “embedded” sensoren, vergt een combinatie van hard- en software om correct te functioneren. Systeembeveiliging wordt geadresseerd op twee vlakken: schaalbare basistechnieken en ondersteuning voor gedecentraliseerde beveiliging.

Schaalbare basistechnieken. Systeembeveiliging wordt gekenmerkt door een voortdurende wedloop tussen aanvals- en verdedigingstechnieken. Dit vereist verregaand basisonderzoek waarbij noodzakelijke beveiligingseigenschappen nagestreefd worden: mogelijkheid tot fijnkorrelige isolatie, run-time attestatie en garanties omtrent de integriteit van software, data en control flow. Ook het in kaart brengen van de beschikbare en meest waarschijnlijk geëxploiteerde aanvalsvectoren vereist continu onderzoek. Oplossingen voor systeembeveiliging vertrekken van hard- en software co-design en moeten schaalbare mechanismen opleveren, bijvoorbeeld op basis van beperkte uitbreidingen van de instructieset, of door het toevoegen van processormodi of nieuwe componenten in het run-time systeem, etc. Het gebruik van de ontwikkelde oplossingen dient zoveel mogelijk geautomatiseerd en moet voldoen aan niet-functionele beveiligingsvereisten die aangepakt worden met de nodige tools (o.a. compilers). Indien voorgestelde oplossingen immers teveel manuele interventies vereisen door ontwikkelaars, dan is de kans op fouten te groot en het praktisch gebruik te duur en te omslachtig.

Gedecentraliseerde beveiliging. Een tweede onderzoeksactiviteit in dit luik adresseert gedecentraliseerde beveiliging. Dit thema vormt een essentiële vereiste voor het beheren en opereren van autonome systemen. Hierbij wordt er onderzoek geleverd op het vlak van gedecentraliseerde detectie van bedreigingen.

(III) *Netwerkbeveiliging*

Kerntechnologie van het moderne Internet werd in de 70er jaren geïntroduceerd. Vandaag zijn de bouwstenen waarmee gewerkt wordt zoals bv. routing met BGP en adressering met DNS relatief bekend. Daarbij zijn er ook een aantal securitybeperkingen zeer zichtbaar en vaak te gemakkelijk exploiteerbaar door aanvallers. Vergelijkbare observaties kunnen gemaakt worden voor een aantal andere infrastructuurcomponenten zoals PKI (public key infrastructure) die essentieel is voor het web en voor heel wat mobiele ecosystemen. In een aantal gevallen zijn beveiligingsoplossingen bekend maar duur qua exploitatie. Daarnaast stellen draadloze en mobiele protocollen unieke beveiligingsuitdagingen, zoals bv. recent geïllustreerd met de *KRACK attack* die een beperking in het WPA2 protocol aantoonde.

Dit alles is ongetwijfeld van groot en voortdurend belang voor netwerkkoperatoren en service providers (ISPs). Deze korte schets motiveert zonder twijfel de nood aan een doorgedreven onderzoeksinspanning op het vlak van de beveiliging en robuuste exploitatie van huidige en toekomstige netwerken, en voor de ontwikkeling van nieuwe oplossingen die alle elementen van de netwerkprotocolstapel adresseren. De toepassing van geavanceerde cryptografie vormt een belangrijk element in de oplossingen die verder onderzocht moeten worden.

(III) *Monitoring en Management*

Het beveiligen van systemen, netwerken en kritische infrastructuur gaat gepaard met een beheeraspect. Hoe robuust het initieel geïnstalleerd systeem ook is, de evolutie van software, diensten en systemen, de voortschrijdende inzichten van aanvallers en de inherente beperkingen die gepaard gaan met eender welke beveiligingsoplossing, vergen in principe een actieve bewaking en mogelijk verdediging van heel wat omgevingen. Een belangrijk doel van onderzoek in deze context is het ontwikkelen van middelen die de verzameling, opslag, en representatieve monitoring van informatie mogelijk maken. Hierbij is de bruikbaarheid van deze informatie, in het bijzonder voor de beveiligingsanalyse en digitale bewaking, van groot belang.

Onderzoekslijn 3 organisatie, structuur en positionering

- Track leader: Frank Piessens¹
- Core PI's en kaders: Frank Piessens¹, Danny Hughes¹, Wouter Joosen¹, Vincent Naessens¹, Stijn Volckaert¹, Lieven Desmet¹, Sam Michiels¹, Jan Tobias Mühlberg¹, Bart Preneel¹, Ingrid Verbauwhede¹, Danny De Cock¹, Benedikt Gierlichs¹, Dave Singelée¹, Bjorn De Sutter²
- Onderzoeksthema's Track 3: *System en Infrastructure Security*
 - o Thema 1 – Systeembeveiliging
 - o Thema 2 - Netwerkbeveiliging
 - o Thema 3 – Monitoring en management voor cyberssecurity
- Positionering: op basis van voorstel van de eerste 16 maand, september 2019 – december 2020) heeft Track 3 ongeveer 32% van globale personele inzet van het onderzoeksprogramma (excl. management).

(1) KU Leuven, (2) U Gent, (3) VU Brussel, (4) imec

Onderzoekslijn 4: Technologische bouwblokken: veilige hardware, cryptografie en veilige communicatie

Beveiligingstechnologie steunt op een aantal kernbouwblokken, die in deze onderzoekslijn bestudeerd en ontwikkeld worden: veilige hardware, cryptografische algoritmen en protocollen (met inbegrip van de veilige implementatie ervan) en oplossingen voor veilige communicatie.

(1) *Veilige Hardware*

Halfgeleidertechnologieën ondergaan een sterke evolutie: naast het schalen volgens de wet van Moore zijn er ook andere belangrijke trends ("More than Moore"); het onderzoek bestudeert hoe procesvariaties en halfgeleiderruisbronnen kunnen aangewend worden voor beveiligingsdoeleinden zoals Physical Unclonable Functions (PUFs) en nieuwe True Random Number Generators (TRNG's). Daarnaast worden de beveiligingseigenschappen van toekomstige geheugentechnologieën bestudeerd zoals Magnetoresistive Random Access Memory (MRAM) en Resistive Random Access Memory (ReRAM). Belangrijke onderzoeksproblemen zijn veilige opslag van cryptografische sleutels, maar ook veilige berekeningen direct in het geheugen. Het samenspel van toekomstige logica en beveiliging is een ander cruciaal onderzoeksgebied dat kan leiden tot nieuwe vormen van logica of een betere bescherming tegen fysieke aanvallen. Daarnaast wordt er onderzoek gepland naar nieuwe hardware-gebaseerde aanvalsvectoren door middel van kwaadwillige manipulatie van de toekomstige hardware, zoals bijvoorbeeld Trojaanse paarden op laag niveau. Een laatste onderzoeksgebied zijn beveiligde hardware-ontwerpstromen die onderzoeken hoe beveiligings- en privacy-functionaliteit geïntegreerd kan worden in de ontwerpmethodologie.

(III) Cryptografische algoritmen en protocollen

Cryptografie bestudeert wiskundige technieken om gegevens te beschermen tijdens communicatie, opslag en tijdens de verwerking ervan; het vormt de kern van de bescherming van digitale gegevens en processen.

Uitdagingen op het gebied van symmetrische cryptografie omvatten (1) het verbeteren van de wisselwerking tussen beveiliging, kosten en prestaties en in het bijzonder lange-termijn beveiliging, (2) cryptografische primitieven voor low-end processoren en knopen met strikte beperkingen op beschikbare energie en (3) nieuwe constructies die geschikt zijn voor white-box cryptografie, Multi-Party Computation (MPC) en post-kwantum digitale handtekeningen, dat wil zeggen, digitale handtekeningen die aanvallen op kwantumcomputers kunnen weerstaan. Voor publieke sleutel cryptografie wordt er onderzoek gevoerd naar de ontwikkeling en evaluatie van post-kwantumprimitieven op basis van roosters, isogenieën en kwadratische systemen in meerdere veranderlijken (Multivariate Quadratic systems). Een derde aspect is de ontwikkeling van efficiënte cryptografische software en hardware-bibliotheken met ingebouwde beveiliging tegen fysische aanvallen zoals aanvallen gebaseerd op nevenkanalen en op foutinjectie. Voor elk van deze onderzoeksonderwerpen wordt er gesteund op wiskundig onderzoek naar harde problemen om de beveiliging op te baseren. Er worden beveiligingshulpmiddelen ontwikkeld voor de evaluatie van de veiligheid die zowel statistisch, logisch als algebraïsch kunnen zijn en die kunnen gecombineerd worden met formele verificatiemethoden.

(III) *Veilige communicatie*

Het veilig verbinden van twee of meer knopen is een essentieel bouwblok om een veilig ecosysteem op te bouwen. Hierbij wordt onderzoek gedaan naar cryptografische protocollen op de netwerklaag, datalinklaag en fysieke laag om na te gaan welke knopen dichtbij liggen, om een veilige verbinding op te zetten met nieuwe knopen, om sessiesleutels overeen te komen en te updaten en om gecompromitteerde knopen te herroepen. Voor het eerste doel kunnen gesofisticeerde protocollen voor *distance bounding* gebruikt worden, die cryptografie vermengen met fysieke eigenschappen. Voor al deze problemen vormt het beperken van de vertraging een belangrijke onderzoekuitdaging. Daarnaast is het essentieel dat het protocol robuust is, d.w.z. voorwaartse veiligheid biedt als een of meer knopen gecompromitteerd worden en dat het gebruikte algoritme op een veilige manier kan onderhandeld worden. Daarnaast is het ook zeer belangrijk om de veiligheid van implementaties te analyseren. Naast het voorstellen van nieuwe protocollen zal de veiligheid van belangrijke relevante standaardprotocollen zoals Bluetooth Low Energy (BLE), SSH en TLS bestudeerd worden. Een belangrijk aspect is het beschermen van de metadata op elk niveau van de communicatie. Hierbij wordt bestudeerd hoe metadata lekt op verschillende manieren en worden technieken ontwikkeld

om metadata op een efficiënte en effectieve manier te beveiligen op alle relevante niveaus (vb. mix netwerken).

Onderzoekslijn 4 organisatie, structuur en positionering

- Track leader: Ingrid Verbauwhede¹
- Core PI's en laders: Ingrid Verbauwhede¹, Claudia Diaz¹, Nele Mentens¹, Bart Preneel¹, Vincent Rijmen¹, Nigel Smart¹, Frederik Vercauteren, Elena Andreeva¹, Benedikt Gierlichs¹, Svetla Nikova¹, Emmanuela Orsini¹, Dave Singelee¹, Dimitri Linten⁴, Jo De Boeck⁴
- Lijst van thema's: Technologiebouwstenen
 - o Thema 1 – Hardware Security
 - o Thema 2 – Cryptografie: algoritmes
 - o Thema 3 – Cryptografie: protocollen
 - o Thema 4 – Veilige en efficiënte crypto-implementaties
- Positionering: op basis van voorstel van de eerste 16 maand, september 2019 – december 2020) heeft Track 4 ongeveer 30% van globale personele inzet van het onderzoeksprogramma (excl. management).

(1) KU Leuven, (2) U Gent, (3) VU Brussel, (4) imec

B. ORGANISATIE EN GOVERNANCE VAN HET ONDERZOEKSPROGRAMMA

Algemene governance van het hele Cybersecurity-programma

In de nota aan de Vlaamse regering van 22 maart 2019 (VR 2019 2203 DOC.0317/1QUATER) werd volgende governance voor het globale CS-programma voorzien (voor de drie luiken samen):

"Het globale programma wordt opgevolgd door een stuurgroep die opgezet wordt onder leiding van het departement EWI en VIAIO met een vertegenwoordiging van de relevante stakeholders uit het bedrijfsleven en het onderzoeksveld. Om deze stuurgroep slagkrachtig te laten beslissen telt zij maximaal 12 leden, waarbij de verschillende stakeholders werken via het principe van vertegenwoordiging uit hun bestaande overlegstructuren.

Op deze stuurgroep wordt de werking en impact van het programma geëvalueerd en waar nodig bijgestuurd. Er wordt in het bijzonder aandacht besteed aan de industriële relevantie van het programma door het betrekken van relevante bedrijven als klankbord voor de implementatie en de wetenschappelijke relevantie door het programma op gezette tijden extern te laten benchmarken op zijn wetenschappelijke impact op internationale schaal door internationale experts, teneinde de focus te behouden op die onderzoeksdomeinen waar Vlaanderen het verschil kan maken. De samenstelling van de stuurgroep zal voorwerp uitmaken van een afzonderlijke beslissing van de Vlaamse Regering.”

Op 7 juni 2019 duidde de Vlaamse regering de Stuurgroep van het beleidsplan CS aan (VR 2019 0706 DOC.0866/1BIS). Volgende leden maken er deel van uit:

7. Stijn Bijmens (Cegeka)
2. Alex Van Cauwenbergh (Cranium)
3. Nele Van Malderen (Proximus)
4. Freddy Van Bogget (KBC)
5. Herman Derache (Agoria)

////////////////////////////////////

6. Hans Maertens (Voka)
7. Rik van de Walle Rector (UGent)
8. Paul Van Dun (KULeuven)
9. Steven Latré (UAntwerpen – rotatie met VUB en UHasselt)
10. Luc Van den Hove (imec)
11. Dirk Torfs (Flanders Make)
12. Ria Bollen (VLHORA)

Operationeel management van het Onderzoeksprogramma CS

In de nota aan de Vlaamse regering van 22 maart 2019 (VR 2019 2203 DOC.0317/1QUATER) werd gesteld dat de coördinatie van het onderzoeksprogramma CS bij KULeuven gelegd wordt. Deze coördinatie wordt gerealiseerd onder leiding van Prof. Bart Preneel en Prof. Wouter Joosen. Deze verantwoordelijkheid houdt het organiseren en opleveren van de rapportering van het programma in, het opzetten van de programma reviews, het organiseren van alle programma-activiteiten (actualiseren van de roadmap, de vernieuwing van programma-activiteiten door een oproep voor nieuwe ideeën enz.). Dit centraal programmamanagement vergt 1 (senior) FTE.. KULeuven zal daartoe een programmamanager aanstellen, of een tandem van twee deeltijdse managers.

Het centraal programmamanagement zal worden ondersteund door en samenwerken met de managementondersteuning in elk van de research tracks. Hiervoor wordt een budget voorzien per onderzoeksgroep, dit budget is evenredig met de rol van de onderzoeksgroep. De managementondersteuning per research track zorgt o.a. voor de toelevering van de nodige gegevens over de voortgang van de specifieke research tracks, voor de doorstroming van informatie, de organisatie en oplevering van Proof-of-Concepts (PoCs), prototypes, enz.

Het Programmamanagement en de leiders van de Research Track zullen de synergie en kruisbestuiving tussen de verschillende research tracks aansturen, naast de samenwerking met het programma Artificiële Intelligentie (AI). Verder worden er valorisatieopties onderzocht, met een sterke nadruk op het stimuleren en faciliteren van Luik 2 en 3 van het CS-programma (samenwerkingsprojecten met industrie met het oog op implementatie, industrie training en outreach activiteiten).

Het budget voor management van het basisonderzoekprogramma bedraagt iets meer dan 7% van het totale budget voor basisonderzoek.

Inhoudelijke dynamiek van het Onderzoeksprogramma

Uiteraard zijn de research track leaders van groot belang. Zij organiseren elke kwartaal een managementmeeting voor hun specifieke track. Hierbij gaat er specifieke aandacht naar de vooruitgang en prioriteiten binnen de research track, met inbegrip van:

- het stimuleren van samenwerking in de verschillende thema's en onderzoeksactiviteiten met de collega's van andere instellingen;
- het actief ondersteunen van kruisbestuiving tussen de verschillende research tracks;
- het evalueren van hoe is rekening gehouden met de opmerkingen van de industriële feedback en internationale raden;
- Het opzetten van de nodige acties en activiteiten voor het dynamisch maken van het programma in overleg met het centraal programmamanagement (zelfevaluatie, off-sites, prospectie voor specifieke nieuwe thema's, opzoeken van jonge 'high-potentials' met vernieuwende ideeën etc.).

Het centraal programmamanagement brengt naast de research tracks, ook de deelnemende onderzoeksgroepen en hun onderzoeksgroepsleiders samen. Naast bovenstaande elementen is er specifieke aandacht voor

- het verzekeren van de steun van alle geledingen binnen de deelnemende organisaties (instellingen engroepen) voor de uitvoering van het programma en de valorisatie van de resultaten;
- het assessment van de portfolio aan activiteiten en het faciliteren van een dynamisch programma door actieve programma-vernieuwing.

Het programmamanagement zal geregeld “*off-site sessies*” organiseren met de deelnemende PI’s en kaders om de voortgang te bespreken en de interactie, die moet leiden tot een sterke cohesie en een gedragen ambitie voor het ganse programma, te bevorderen.

Om dit verder te onderbouwen zal jaarlijks een validatie-workshop met de Vlaamse industriële en andere stakeholders worden georganiseerd. Zie verder voor een beschrijving van deze workshop, die reeds op 3 april een eerste keer samenkwam.

Daarnaast wordt ook jaarlijks de *Internationale Adviesraad (IAB)* samengeroepen voor een opvolging van de aanbevelingen van de laatste IAB alsook het opmaken van een nieuw rapport met aanbevelingen. Verder wordt meer informatie gegeven over de eerste IAB die op 4 en 5 juli samenkwam voor een eerste evaluatie van het onderzoeksprogramma.

Budgettaire aspecten en personeelsinzet van het onderzoeksprogramma

In bijlage 3 wordt het budget gegeven voor september 2019 – augustus 2020 (jaar 1). Ter informatie kan men in bijlage 4 het budget vinden voor jaar 2 (september 2020 – augustus 2021).

De volgende categorieën zijn hierin te onderkennen:

1. Gedeelde kosten voor het programma:
 - Programmamanagement (door KU Leuven aan te stellen)
2. Per deelnemende organisatie
 - een budget voor onderzoekers, uitgedrukt in mensmaanden. De VTE's kunnen worden toegewezen aan PhD, PostDoc, (senior) researchers. De VLAIO tarieven werden gehanteerd om tot een opmaak van het budget te komen.

Hieronder wordt een samenvattende overzichtstabel gegeven die de persoonsmaanden-verdeling over de Research Tracks en de verschillende deelnemers weergeeft.

2020 - Person Months	KU Leuven	VUB	UGent	imec	Totals
Programme Management	13				
TRACK 1	124	92	-	-	216
TRACK 2	230	-	-	-	230
TRACK 3	311	-	69	-	379
TRACK 4	269	-	-	48	317
Person Months per partner	947	92	69	48	
Total Person Months 2020					1.155

Een van de grootste uitdagingen (internationaal erkend) is het vinden en opleiden van voldoende talent. Een goede link met het onderwijsveld zal hiertoe ook worden opgezet.

[illegible]

Het is een van de belangrijke resultaten van dit onderzoeksprogramma dat er nieuw talent wordt opgeleid voor de Vlaamse industrie in de meest geavanceerde nieuwe cybersecurity-technologie. Deze talenten komen uit Vlaanderen, Europa en 'Rest-of-World'.

Validatie door de Vlaamse industrie

Van deze workshop is een rapport opgemaakt en kan worden besloten dat er een groot draagvlak is voor de activiteiten in het CS-onderzoeksprogramma en dat er grote interesse is om een dergelijke workshop in de loop van het programma geregeld te herhalen. Dit zal de aansluiting van de Vlaamse actoren met het onderzoek en de opname van resultaten in toekomstige projecten (luik 2 van het CS-programma in Vlaanderen) verder activeren.

Op 4 en 5 juli 2019 werd vervolgens een internationale wetenschappelijke adviesraad (International Scientific Advisory Board) gehouden, georganiseerd door KU Leuven. De IAB werd samengesteld in samenspraak met het FWO en er werd zorggedragen voor een gebalanceerde samenstelling met betrekking tot inhoudelijke achtergrond en gender.

Sandrine Blazy	University of Rennes 1, France
Sinja Buchegger	KTH Royal Institute of Technology, Sweden
George Danezis	University College London and Facebook Calibra, UK
Riccardo Focardi	Ca'Foscari University, Venice, Italy
Aurélien Francillon	Eurecom, France
Bart Jacobs	Radboud University, Nijmegen, The Netherlands
Stefan Mangard	TU Graz, Austria
Ahmad-Reza Sadeghi	TU Darmstadt, Germany
Haya Shulman	Fraunhofer SIT, Germany

////////////////////////////////////

De IAB begint het rapport met de volgende executive summary:

“Overall the IAB was extremely impressed with the quality of the research program, and the quality of the partners and their track record in cybersecurity research. They have a top international standing and indeed represent the strongest research groups in Flanders doing cybersecurity research and advanced development. They are working at the forefront of international cybersecurity research already for many years and have published a wide range of results with high impact on both industry and academic research.

The value for money of the programme is excellent since the funding is provided to existing and established groups, the overheads are very low as 90%+ of the funding is committed to substantive research activities, and the leadership of the programme is in the hands of extremely experienced international research leaders who can flexibly allocate it to important fields as they develop in cybersecurity. The consortium has a track record of successful collaborations between partners and industry, that will be strengthened. The fields covered by the current plan are excellent in breadth and depth, and address some of the hottest topics in cybersecurity research, with key industrial applications, and have the critical mass of talent to succeed in their goals.

We strongly encourage Flanders to provide a financial commitment for this initiative at the minimum for the next 10 years as soon as possible to allow institutions and lead researchers in the consortium to plan their investments in time and resources accordingly, and multiply the impacts and value of the project. Some of those impacts include key novel technologies, building capacity to support industrial projects and collaborations, attracting key international cybersecurity industries to Flanders, strategic hires in important new cybersecurity fields, as well as the potential for start-ups based on technologies developed by the programme. The plans of the programme to materialize those impacts through great research, collaborations with industry, and the AI programme are credible and very strong. They allow for quickly reacting to new research demands, i.e., support agility without too much bureaucratic overhead, which is key to success in the area of cybersecurity.”

Het volledige onderzoeksprogramma zal worden geëvalueerd binnen 18 maand na de start. Aanbevelingen van het IAB, met het oog op de volgende bijeenkomst, zijn als volgt geformuleerd:

Following a review of the application, and a 2-day in person discussion with the consortium we recommend that in our subsequent meetings the consortium presents progress on the following items:

An update on the success around recruitment and retention of key staff that both strengthens and extends the expertise of the consortium. We are aware that human capital in cybersecurity is prized in the current industrial environment and invite the consortium to develop a deliberate strategy to retain and extend its excellent expertise.

An update on the joint activities between partners in the consortium, as well as the vehicles developed to foster those formally or informally. Core funding represents an opportunity to create strong ties, and synergies, but fostering those requires a deliberate effort.

A review of the current research topics within tracks, with a view to identifying any opportunities for new topics of key academic and industrial importance. We recommend that the funding is secured in the long term, so as to allow the consortium institutions to implement long-term plans if they identify key areas of expertise that would benefit Flanders.

A plan on how engagements with the AI programme as well as more industrial focused activities are developing. As well as any potential for direct commercialization of cybersecurity technologies through academic-led start-ups. A dual strategy of strengthening current industry in Flanders as well

[illegible]

as creating more innovation-focused industry is key. We recommend that the academic leaders in this consortium are involved in developing an overall cybersecurity industrial strategy for Flanders.

De internationale adviesraad telt 17 leden en heeft de wil uitgesproken om het programma verder te willen opvolgen. We stellen daarom voor om de voorgestelde leden van de ISAB voor de komende 3 jaren te benoemen.

D. HEFBOOMWERKING VAN DE VLAAMSE OVERHEIDSFINANCIERING

De voorziene 8 miljoen euro vanuit de Vlaamse begroting voor het CS-onderzoeksprogramma moet een hefboomwerking realiseren naar andere financieringsbronnen.

De belangrijkste prioriteit is uiteraard het faciliteren en inhaken op luik 2 en 3 van het globaal programma CS (CyberSecurity), met de nadruk op het implementatieluik (luik 2).

Door interacties met de diverse industriële sectoren (ook individuele bedrijven) en overheidsorganisaties, door interactie met relevante intermediaire organisaties (bv. VOKA, Agoria, Sirris, LSEC, speerpuntclusters, IBNs, enz.) zal een belangrijke groei aan opportuniteiten voor samenwerking van de industrie met het onderzoeksveld ontstaan. Deze samenwerkingen zullen gericht zijn op de implementatietrajecten van de onderzoeksresultaten, vaak als deel van het implementatieluik van het impulsprogramma en op industrie-training, mogelijk als deel van het derde luik van het impulsprogramma.

Verder is het uiteraard ook van belang een hefboomwerking te realiseren naar andere financieringsbronnen, met name EU-financiering en andere bronnen van competitieve financiering. Verder gaat er aandacht naar bilaterale samenwerkingen en “venturing”. Door gerichte contacten met industriële partners (netwerking, community ontwikkeling en gerichte acties naar doelgroepen) kunnen bilaterale contracten worden afgesloten voor samenwerking rond de activiteiten van de programma’s met de ‘early adopters’ van nieuwe technologische ontwikkelingen rond CS. Zulke bilaterale contracten zijn een erg ambitieuze manier om de activiteiten te benchmarken tegen de internationale stand van de technologie. Er zal zorg gedragen worden dat de Vlaamse industrie maximaal kan profiteren van het vroeg inzetten van first-of-a-kind technologie door regionale samenwerking. De internationale samenwerking in deze vorm zal in vele gevallen nodig zijn om de waardenketen voor het implementeren van de producten, diensten, processen e.d. mogelijk te maken.

E. KEY PERFORMANTIEINDICATOREN VAN HET CS-ONDERZOEKSPROGRAMMA

In een aantal voorbereidende werkdocumenten werden voorstellen geformuleerd voor de KPI's van het CS-onderzoeksprogramma. Hieronder volgen de belangrijkste elementen:

1. Het aantal publicaties in internationale topconferenties voor cybersecurity, in relevante top-journals, en de deelname aan standaardisatie-comités in industrie fora gericht op de activiteiten van het cybersecurityprogramma;
2. Het aantal lopende en afgelegde doctoraten in cybersecurity
3. Het aantal Proof-of-Concepts gegenereerd in het programma, PoC's die verdere validatie en industriële implementatie faciliteren;
4. Het aantal projecten die mogelijk gemaakt worden door de programmaresultaten: projecten met Vlaamse stakeholders in het implementatieluik van het cybersecurityprogramma;
5. Bijkomende financiering rond programma-activiteiten die de hefboomwerking van de Vlaamse financiering realiseren;
6. Het aantal lopende Baekelandmandaten en Innovatiemandaten.

////////////////////////////////////

In januari 2020 zal een eerste versie van realistische en ambitieuze doelstellingen voor deze KPI's worden voorgelegd ter goedkeuring aan de stuurgroep van het CS-programma en dit voor 2020 met een concept voor de 4 volgende jaren. Deze KPI's zullen aan de Vlaamse regering medegedeeld worden.

F. IP-OVEREENKOMSTEN

Voor de gezamenlijke activiteiten zullen de betrokken partijen de nodig overeenkomsten sluiten om de kennis uit het onderzoeksprogramma op de geijkte manieren te kunnen beschermen en valoriseren, volgens de doelstellingen van het programma: spin-off, subsidieprojecten met de industrie, Europese subsidieprojecten, bilaterale contracten en dergelijke. Dit alles met het oog om een maximale impact van de onderzoeksresultaten in Vlaanderen – en globaal – te realiseren en de beoogde leiderschapspositie te kunnen claimen.

3. BESTUURLIJKE IMPACT

A. BUDGETTAIRE IMPACT VOOR DE VLAAMSE OVERHEID

Voor het eerste jaar (september 2019 – augustus 2020) wordt er een subsidie toegekend voor een bedrag van maximaal 7.996.360 euro voor het onderzoeksprogramma cybersecurity in Vlaanderen. De begunstigden zijn universiteiten KULeuven, UGent, VUBrussel en het strategisch onderzoekscentrum imec.

Deze subsidie wordt aangerekend op begrotingsartikel EBO-1EEB2JA-WT van de algemene uitgavenbegroting van de Vlaamse Gemeenschap voor het begrotingsjaar 2019.

Het gunstig advies van de Inspectie van Financiën werd verleend op 12/11/2019.

Het begrotingsakkoord werd verleend op (datum).

B. ESR-TOETS

Aangezien de beschikbare middelen binnen het budget van het begrotingsjaar 2019 voorzien zijn, is een ESR-toets niet van toepassing.

C. IMPACT OP HET PERSONEEL VAN DE VLAAMSE OVERHEID

Het voorstel heeft geen weerslag op het personeelsbestand en het personeelsbudget van de Vlaamse Gemeenschap.

D. IMPACT OP DE LOKALE EN PROVINCIALE BESTUREN

Het voorstel van beslissing heeft geen weerslag op de werking van de lokale besturen.

4. VERDER TRAJECT

In januari 2020 zal een voorstel voor de KPI's worden voorgelegd ter goedkeuring aan de stuurgroep van het CS-programma en dit voor 2020 met een concept voor de 4 volgende jaren. De goedgekeurde KPI's zullen aan de Vlaamse regering medegedeeld worden.

Deze nota betreft het eerste werkingsjaar van het strategisch onderzoek voor cybersecurity. Volgend jaar zal er een nota voorgelegd worden voor de financiering van het tweede werkingsjaar.

5. VOORSTEL VAN BESLISSING

De Vlaamse Regering beslist:

1° haar goedkeuring te hechten aan het onderzoeksprogramma “Cybersecurity Initiative Flanders” zoals toegelicht in deze nota en beschreven in bijlage 1;

2° de leden en de werkzaamheden van de internationale adviesraad te verlengen met drie jaar;

3° haar goedkeuring te hechten aan het ontwerpbesluit van de Vlaamse Regering betreffende de toekenning van een subsidie aan het onderzoeksprogramma voor het eerste werkingsjaar;

4^o de Vlaamse minister, bevoegd voor het wetenschapsbeleid en het technologisch innovatiebeleid, te belasten met de uitvoering van deze beslissing.

De Vlaamse minister van Economie, Innovatie, Werk, Sociale economie en Landbouw,

Hilde CREVITS

Bijlagen:

Bijlage 1 – Programma “Cybersecurity Initiative Flanders”

Bijlage 2 – Cv's van de deelnemende onderzoekers

Bijlage 3 – Budget 2019 -2020 (jaar 1)

Bijlage 4 – Budget 2020 – 2021 (jaar 2)

Bijlage 5 – Rapport van de Internationale Adviesraad, 2019

Bijlage 6 – Advies Inspectie van Financiën

Bijlage 7 – Begrotingsakkoord

Bijlage 8 – Besluit van de Vlaamse Regering

////////////////////////////////////