Rijksdienst voor Ondernemend Nederland

Samenvattingen winnaars SBIR Cyber Security III fase 1

Balancing Security and Mobility

Dit SBIR project wordt medegefinancierd door het Fonds voor interne veiligheid van de Europese Unie

SB1CS17002

Projecttitel	NATAN: Network Assisted Track and Neutralize
SBIR-projectnummer	SB1CS17002
Bedrijfsnaam	Embedded Acoustics BV
In samenwerking met	TNO

Projectsamenvatting

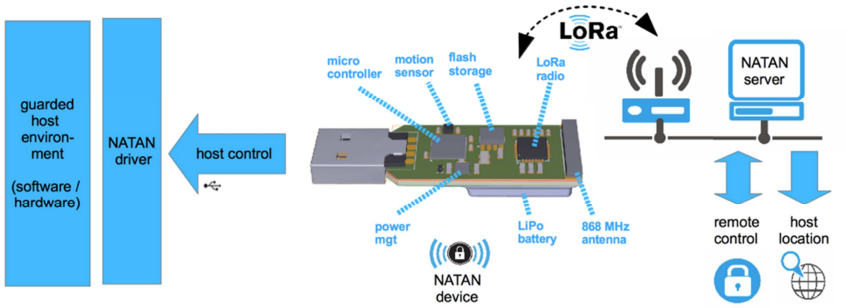
Zolang voor veel criminelen het stelen van een laptop gemakkelijker is dan het hacken van een database is het zinvol om de mogelijkheden voor controle op hardware in de fysieke wereld te vergroten. Kort samengevat is het doel van dit projectvoorstel: het ontwikkelen van een zeer simpel, goedkoop en klein apparaatje (uiteindelijk een compacte chip) waarmee op afstand kan worden ingegrepen wanneer een (mobiel) device of datadrager in verkeerde handen gevallen is. De functionaliteit is vergelijkbaar met diensten als “find my iPhone”, maar volledig uitgevoerd in hardware, platform-onafhankelijk, en met een eigen, host-onafhankelijke draadloze infrastructuur via IoT netwerken (zoals LoRa).

In het haalbaarheidsonderzoek worden 20 devices, in eerste instantie uitgevoerd als USB-sticks, verspreid onder proefpersonen in verschillende delen van het land. Vervolgens wordt bepaald of de USB-sticks (en de apparatuur waaran deze worden gekoppeld) inderdaad voldoende betrouwbaar op afstand kunnen worden bereikt en geblokkeerd.

Embedded Acoustics ontwikkelt, produceert en verkoopt sensortechnologie voor toepassingen op het gebied van defensie, veiligheid en wetshandhaving.

Contactpersoon (+eventueel contactgegevens) en website

Sander van Wijngaarden, Algemeen Directeur
sander@embeddedacoustics.com, 088 8770700
www.embeddedacoustics.com



SB1CS17003

Projecttitel	CySECURE: Advies en implementatie voor laagdrempelige informatiebeveiliging in het MKB
SBIR-projectnummer	SB1CS17003
Bedrijfsnaam	Spru IT BV
In samenwerking met	The Habit Agency BV VrolijkeNoodzaak

Projectsamenvatting

Inleiding | CySECURE is een advies- en implementatiedienst inclusief e-coaching voor laagdrempelige informatiebeveiliging in het midden- en kleinbedrijf (MKB). Wij benaderen informatiebeveiliging vanuit het perspectief van de benodigde gedragsverandering van de medewerkers. CySECURE bestaat uit drie onderdelen: CySCAN, CyPLAN en CyCAN.

Haalbaarheidsonderzoek | Uitgaande van de reeds ontwikkelde en getoetste ISFAM familie van volwassenheidsmodellen voor informatiebeveiliging gaan wij de haalbaarheid onderzoeken voor het realiseren van één alomvattend meetinstrument (1) voor persoonlijk informatiebeveiligingsadvies, (2) voor het gehele MKB, (3) inclusief persoonlijke ondersteuning, (4) gedurende het implementatieproces.

Illustratie

Over
CySECURE bundelt expertise in ICT wetenschap, e-coaching, e-infrastructuur, en MKB accountmanagement rondom informatiebeveiliging.

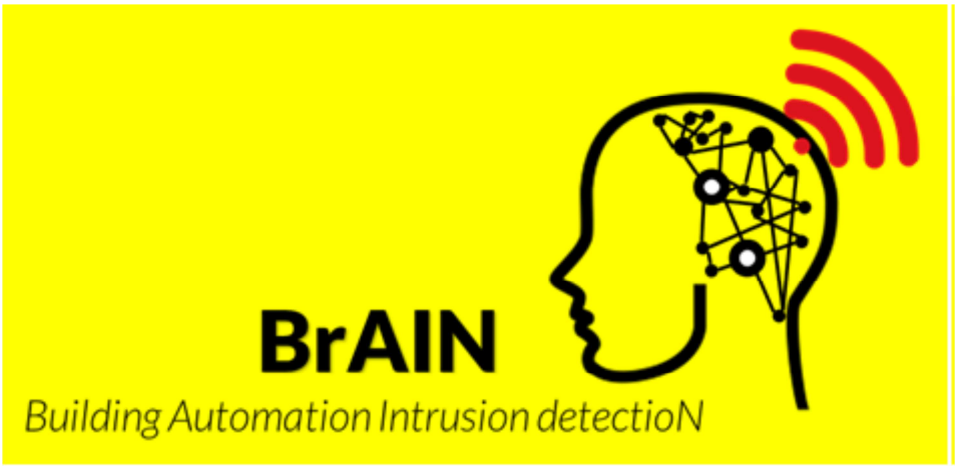
Contactpersoon (+eventueel contactgegevens) en website
Dr. Marco Spruit
www.cysecure.nl

SB1CS17005

Projecttitel	Building Automation Intrusion DetectioN (BrAIN)
SBIR-projectnummer	SB1CS17005
Bedrijfsnaam	KPN
In samenwerking met	Security Matters

Inleiding
Binnen de kritieke infrastructuur, gebouwautomatisering en bijvoorbeeld fabrieken en smart grids, wordt er veel gebruikt gemaakt van zogenoemde 'control systems'. Met deze systemen kan het gedrag van fysieke processen worden geregeld, gemonitord en gereguleerd. Dankzij communicatie netwerken- en protocollen, kunnen deze control systems van een afstand worden bestuurd, door gebruik van sensoren en controllers. Deze technologie wordt ook wel 'networked control systems' (NCS) genoemd. Voorbeelden van NCS technologie zijn ICS (industrial control systems) en BAS (building automation systems). Bij toepassingen van deze systemen kun je onder andere denken aan klimaatbeheersing en beveiliging van kantoorgebouwen. Sinds enkele jaren wordt steeds pijnlijker duidelijk dergelijke control systems kwetsbaar zijn voor kwaadwillenden. Denk bijvoorbeeld aan de Oekraiense stroomuitval in december 2015 of aan de gehackte auto van Chrysler, ook in 2015. Een relatief onbekende component binnen cybersecurity is gebouwautomatisering. Binnen gebouwautomatisering wordt van oudsher gebruik gemaakt van stand-alone BAS, echter is de ontwikkeling dat ook steeds vaker IP-gebaseerde technologie gekoppeld wordt en dat er een uitstrekking is naar IoT technologie. BAS is merendeel non-IB-gebaseerd, IoT apparaten zijn deels wel IP-gebaseerd. Dit biedt een enorme uitbreiding van het aantal toepassingen, maar het zorgt ook voor een vergroting van de kwetsbaarheid van dergelijke systemen, zonder dat er direct een oplossing in zicht is. KPN en Security Matters maken zich zorgen over de cyberdreigingen voor deze technologie.

Beknopte beschrijving van het haalbaarheidsonderzoek
Security Matters en KPN willen samen een oplossing ontwikkelen voor **'Building Automation Intrusion DetectioN' (BrAIN)**'. BrAIN staat voor een IDS – Intrusion Detection System – oplossing, specifiek ontwikkeld voor BAS (Buidling Access Systems) en BMS (Building Management Systems) om cyberaanvallen te detecteren en eventueel misconfiguratie te signaleren zodat deze systemen en daarmee de gebouwen die afhankelijk zijn van deze systemen beter beschermd zijn.



Beknopte feitelijke beschrijving van de organisatie
Security Matters en KPN werken samen aan dit project. KPN is de grootste telecompartij in Nederland en biedt vanuit het onderdeel "KPN Security Services" haar klanten diensten om zich te beschermen tegen cybercriminaliteit. Security Matters is opgericht in 2009 en richt zich op het beveiligen van ICS/SCADA1 netwerken binnen OT-omgevingen2. De start van dit project betreft het uitvoeren van het haalbaarheidsonderzoek, verdeeld in een commercieel, juridisch en een technisch deel.

Security Matters zal zich primair focussen op de technische haalbaarheid, KPN richt zich op de commerciële en juridische haalbaarheid. Vanuit Security Matters zal Elisa Constante, hoofd R&D direct betrokken zijn, vanuit KPN zal Suzanne Rijnbergen, portfoliomanager security, direct betrokken zijn.

Contactpersoon (+eventueel contactgegevens) en website
Suzanne Rijnbergen, 070-3434343, https://www.kpn.com/zakelijk/grootzakelijk/security.htm

---

SB1CS17008

Projecttitel	Mobiel als ID
SBIR-projectnummer	SB1CS17008
Bedrijfsnaam	InnoValor
In samenwerking met	-

Projectsamenvatting
Er is een groeiende interesse in online en fysieke identiteitsvaststelling. Niet alleen om identiteitsfraude tegen te gaan, maar ook om online dienstverlening op een veilige en privacyvriendelijke manier mogelijk te maken. Hierbij spelen twee belangrijke trends waar dit project op inspeelt:

- **Mobile first** – onze mobiel vervangt ons cash geld, onze bankpasjes en als volgende stap hierin, ons rijbewijs en paspoort.
- **Integratie van fysiek en online** – waar in het verleden we gescheiden online en fysieke identiteiten hadden, integreren deze steeds meer.

Het doel van het Mobiel als ID project is om **een unieke middleware oplossing te ontwikkelen waarmee een mobiel gebruikt kan worden voor zowel online als fysieke identiteitsvaststelling**. Dus de mobiel vervangt niet alleen de portemonnee, maar ook je paspoort en je DigiD. Daartoe moeten echter de volgende technische onderzoeksvragen beantwoord worden:

- Security van de mobiel, met name hoe veilige opslag van credentials te realiseren en hoe om te gaan met de diversiteit van mogelijkheden die mobiele telefoons hiervoor bieden?
- Hoe vast te stellen van wie de telefoon is en of niet iemand anders toegang tot de telefoon heeft gekregen, door gebruik te maken van biometrische, context en continuous authenticatie?
- Gebruiken van de mobiel als fysiek identiteitsdocument zonder deze *ongelocked* aan bijvoorbeeld een politieagent te hoeven geven?

Naast deze technische onderzoeksvragen zal in fase 1 zal de economische haalbaarheid inclusief het business model onderzocht worden.

Een mogelijke toepassing die gemaakt kan worden op basis van de resultaten van dit projecten zijn werknemers die zowel toegang tot hun online werkomegeving als hun kantoor kunnen krijgen met hun mobiel. Een andere toepassing die mogelijk uitdagender is, is het vervangen van ons rijbewijs, paspoort en DigiD door een mobiele app.

Dit project wordt uitgevoerd door InnoValor BV. InnoValor is een research-based advies en softwareontwikkelingsbedrijf gericht op digitale innovaties, met een focus op digitale identiteiten, privacy en vertrouwen. InnoValor werkt voor met name overheid (bijvoorbeeld DigiD doorontwikkeling en Idensys), financiële instellingen (bijvoorbeeld online zelf-registratie) en service providers (bijvoorbeeld blockchain en identiteiten). Ook geeft InnoValor advies aan met name de overheids- en financiële sector over business model innovatie en digitalisering.

Contactpersoon (+eventueel contactgegevens) en website
Maarten Wegdam
maarten.wegdam@innovalor.nl | 0651993485
https://innovalor.nl

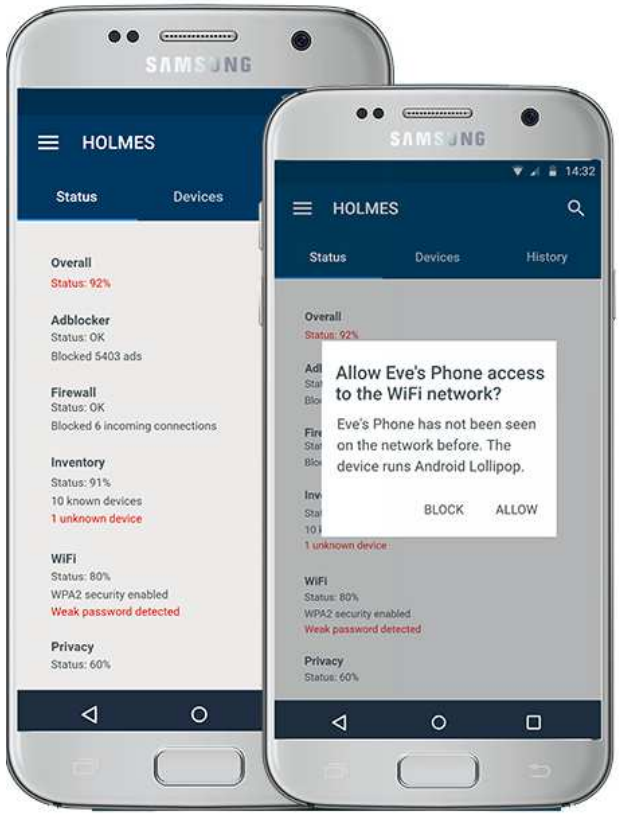
SB1CS17009

Projecttitel	HOLMES: Securing the Internet of Things at Home
SBIR-projectnummer	SB1CS17009
Bedrijfsnaam	Slatman IT
In samenwerking met	Distribute

Inleiding
De ontwikkelingen op het gebied van slimme apparatuur gaan snel. Steeds meer apparaten krijgen naast hun hoofdfunctie de mogelijkheid om verbinding met het internet te maken of anderszins binnen een netwerk te opereren. Apparaten worden zo slimmer en kunnen effectiever of efficiënter ingezet worden dan hun meer analoge voorlopers. Een voorbeeld hiervan is de slimme meter die door energiemaatschappijen ingezet kan worden om het energieverbruik nauwkeuriger en op afstand te kunnen meten en tegelijkertijd de eindgebruiker meer inzicht kan geven in zijn eigen gebruik.

Deze verbonden apparaten brengen veel voordelen met zich mee, maar er is ook een keerzijde. De allegaar aan apparatuur, veelal zo goedkoop mogelijk geproduceerd, zorgt in toenemende mate voor beveiligingsrisico's. Zo blijkt apparatuur niet zelden slecht in elkaar te steken of slecht onderhouden te worden door de producent van de goederen. Daarnaast groeit de interesse van kwaadwillenden om deze apparatuur te misbruiken: het gaat om laaghangend fruit.

Ook binnen de thuisomgeving en het MKB wordt er in toenemende mate gebruik gemaakt van slimme, verbonden apparaten. Binnen deze omgevingen kunnen de risico's van het Internet of Things extra groot zijn, met name omdat er binnen deze domeinen relatief weinig kennis over IT bestaat en beveiliging daarvan geen prioriteit heeft.



Met HOLMES willen wij de risico's van het Internet of Things binnen de thuissfeer en het MKB verkleinen. HOLMES is een veilige thuisrouter die fungeert als een centrale gateway voor alle apparaten op het netwerk. Door het actief monitoren en scannen van netwerkverkeer en actieve apparaten detecteert Holmes beveiligingsrisico's en wordt de gebruiker daarover geïnformeerd door middel van een mobiele applicatie. Holmes blokkeert bekende dreigingen, verhoogt de persoonlijke privacy op het web en verhoogt de mate van security awareness door directe interactie met de gebruiker.

Daarmee verhogen wij de veiligheid van en het vertrouwen in de Nederlandse ICT-infrastructuur en pakken we de structurele problemen aan die het Internet of Things met zich meebrengt.

Haalbaarheidsonderzoek
Dit projectvoorstel omvat de ontwikkeling van hardware en software die compatibel moet zijn met netwerkapparatuur van Internet service providers en een verscheidenheid aan apparaten. Er moet onderzocht worden welke technologie gebruikt kan en moet worden en hoe deze geïntegreerd moet worden tot een voor een gemiddelde gebruiker bruikbaar systeem. Ook hoe het systeem effectief moet communiceren met gebruikers om tot het gewenste resultaat te komen, is op dit moment een open vraag.

Het haalbaarheidsonderzoek bestaat uit het aangaan van intensieve relaties met externe partijen, het opstellen van een realistisch threat model, het uitvoeren van onderzoek naar en het opmaken van een ontwerp gebaseerd op dat model. Vervolgens zal het ontwerp worden omgezet naar een functionele specificatie, resulterend in een werkend, gevalideerd en geverifieerd prototype.

Organisatie
Dit project zal door Slatman IT in nauwe samenwerking met Distribute uitgevoerd worden. In deze samenwerking komt kennis van IT, informatiebeveiliging en gedistribueerde systemen samen. Daarnaast zullen er, zoals beschreven in de vorige sectie, intensieve samenwerkingen met externe partijen zoals internet service providers gevormd worden om het product commercieel inzetbaar te maken.

Figuur 1: Voorbeeld van interface van mobiele applicatie

Contactpersoon

Herman Slatman

Slatman IT
Amstelstraat 37
7523 SR Enschede
info@slatman-it.nl

Website

https://holmes.slatman-it.nl

SB1CS17010

Projecttitel	CyberSniffer
SBIR-projectnummer	SB1CS17010
Bedrijfsnaam	Delft Dynamics B.V.
In samenwerking met	-

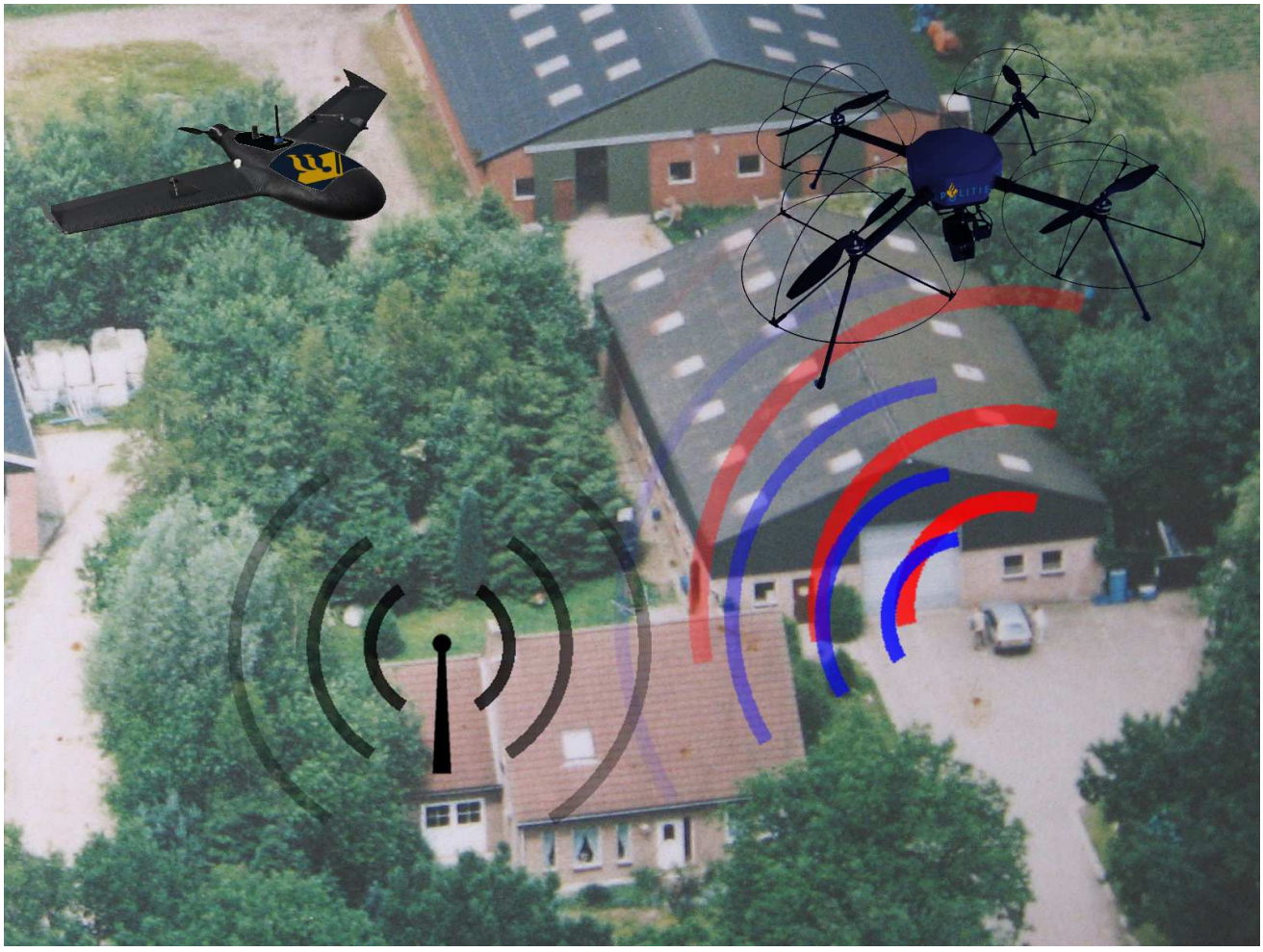
Projectsamenvatting

Delft Dynamics verwacht vanuit haar positie als innovatief Nederlands MKB bedrijf een sterke bijdrage te kunnen leveren aan het vergroten van de cyber security, door in nauwe samenwerking met o.a. de Landelijke Politie onbemande vliegende systemen uit te rusten met

hightech sensoren, waarmee het mogelijk zal zijn om gezochte personen op te sporen aan de hand van digitale profielkenmerken. Met behulp van deze zogeheten CyberSniffer systemen zal het mogelijk zijn om vanuit de lucht signalen op te vangen van WiFi, Bluetooth, GSM, enz., zodat personen gelokaliseerd en geïdentificeerd kunnen worden.

Het haalbaarheidsonderzoek is nodig om een goed beeld te krijgen, welke huidige en toekomstige sensoren gebruikt kunnen worden en hoe deze sensoren in de voor de operationele inzet geschikte onbemande vliegende systemen gebruikt kunnen worden. Hierbij zal dan vooral gekeken worden naar de eisen aan de operationele inzet met betrekking tot geluid, vliegduur, eigenschappen van de sensoren, juridische eisen en eventuele andere eisen, die tijdens gesprekken met de beoogde gebruikers naar voren komen. Ook zal er in de haalbaarheidsstudie bekeken worden of er nog andere partijen aan het project toegevoegd moeten worden voor een goede uitvoering van de onderzoeks- en ontwikkelingsfase.

Delft Dynamics is in februari 2006 opgericht en heeft zich gespecialiseerd in het bouwen van robothelikopters: kleine onbemande helikopters, die door het slim samenvoegen van computer- en sensorapparatuur, gebruikt kunnen worden als stabiele en makkelijk te besturen sensorplatformen. Door de focus op de markt voor Defensie en Veiligheid, is geruime ervaring opgedaan in het ontwikkelen van robuuste hardware en software, die tezamen een robuust product vormen waarmee een hoge inzetbaarheid gewaarborgd is.



Contactpersoon (+eventueel contactgegevens) en website

Ir. A.J. (Arnout) de Jong
info@delftdynamics.nl
www.delftdynamics.nl

SB1CS17011

Projecttitel	Crayonic
SBIR-projectnummer	SB1CS17011
Bedrijfsnaam	Crayonic B.V.
In samenwerking met	Amico Finance, EY en Brightsight.

Projectsamenvatting

Traditioneel wordt een contract ondertekend op papier met een pen, maar deze ceremonie kan worden vervangen door een elektronische ondertekening (‘eSignature’). Hiervoor heeft Crayonic een product ontwikkeld dat bestaat uit twee afzonderlijke delen: Crayonic Paper en Crayonic Pen. Om een tijdwaarmerk (‘timestamp’) toe te kunnen voegen, ook wanneer er geen internetverbinding beschikbaar is, zal er in het project een innovatieve en veilige Real-Time Clock (‘RTC’) worden ontwikkeld die een onderdeel zal gaan vormen van de Crayonic Pen.

De belangrijkste activiteit van de haalbaarheidsstudie is het onderzoek naar de overeenstemming met de ETSI-standaarden van de hard- en software. Om een timestamp uit te kunnen geven moet de Crayonic Pen worden uitgerust met RTC-hardware. De RTC in deze omgeving mag alleen toegang bieden aan vertrouwde entiteiten.

Er zal daarom onderzoek worden gedaan naar zowel de integratie van RTC in het bestaande systeem van Crayonic als naar de potentiele beveiligingsproblemen. De integratie zelf leidt tot twee belangrijke obstakels op de gebieden van: compliancy en beveiliging. In samenwerking met EY zal voor het eerste onderdeel en met Brightsight voor het tweede onderdeel een casestudy worden uitgevoerd.

Crayonic is opgericht in Slowakije in 2015, maar heeft haar hoofdkantoor sinds 2017 in Nederland. Het bedrijf is gestart door zwaargewichten uit de eSignature, beveiliging, cryptografie en biometrie: Michal Varchola (CTO/medeoprichter Crayonic) en Peter Kolarov (CEO/oprichter Crayonic).

Op dit moment neemt Crayonic deel aan het HighTechXL Accelerator-programma. Tijdens het programma wordt Crayonic onder andere begeleid door een groep van mentoren, investeerders en partners met als doel om het product te lanceren in de markt.

Contactpersoon (+eventueel contactgegevens) en website

Contactpersoon: Michal Varchola
Contactgegevens: 00421903582477
mvarchola@crayonic.com
Website: http://www.crayonic.com/

SB1CS17012

n.n.b.

SB1CS17014

Projecttitel	Cell Recovery Management Platform (CRMP)
SBIR-projectnummer	SB1CS17014
Bedrijfsnaam	Group 2000 Nederland BV
In samenwerking met	-

Projectsamenvatting

Inleiding:

- Group 2000 zal binnen dit haalbaarheidsonderzoek de haalbaarheid van het Cell Recovery Management Platform (CRMP) onderzoeken. CRMP beschermt zendmasten voor mobiele technologie tegen overbelasting en maakt het mogelijk om zendmasten nadat zij overbelast zijn sneller beschikbaar te maken door dynamisch de capaciteit van zendmasten aan te passen. Deze overbelasting kan zowel ongericht door calamiteiten optreden, als gericht door cyberattacks. Wegens de omvang van de ontwikkelingen en de verwachte technische, juridische en commerciële onzekerheid is een haalbaarheidsonderzoek wenselijk voordat de ontwikkeling aan het Cell Recovery Management Platform wordt gestart.

Beschrijving van het haalbaarheidsonderzoek:

- Is het mogelijk om binnen het Cell Recovery Management Platform een geconsolideerde oplossing te bieden om de capaciteit van zendmasten op te schalen en af te schalen om zo de uptime te vergroten?
- In hoeverre is het mogelijk om de capaciteit te managen middels het aanpassen van power levels of middels uitsluiten? En welke mogelijkheden bieden zendmasten verder om te kunnen sturen op capaciteit?
- Is het mogelijk om technisch de capaciteit van subdomeinen, zoals machine-to-machine, voice en data, te kunnen schalen en welke voordelen biedt het maken van een dergelijk onderscheid?
- Wat is de impact van de aanwezigheid van small cells op de stabiliteit bij opstarten en welke implicaties heeft dit op CRMP?

illustratie van het project:

- In 2012, teisterde de orkaan Sandy de oost kust van Amerika. De storm bracht ernstige beschadiging aan de mobiele netwerk infrastructuur aan tussen veel cell masten. Tengevolge van de verminderde capaciteit van het draadloze netwerk en de miljoenen klanten wie trachten tegelijk een call op te zetten waren de overblijvende cell masten te snel overbelast. Dit had niet alleen impact op het publieke deel, maar had echter ook impact op de verschillende hulpdiensten om hun activiteiten goed te kunnen uitvoeren.

Met de "Cell Recovery Management Platform", onze CRMP oplossing, zal veel sneller het herstel van het netwerk voor de hulpverleners en het publieke deel weer in de lucht worden gebracht. De mobile netwerk operator zal in het getroffen gebied de capaciteit van elke overblijvende cell mast preventief gaan verminderen, met als resultaat dat de communicatie tussen de hulpverleners en het publieke deel mogelijk blijft.

Beschrijving van de organisatie:

- Group 2000 is gevestigd in Almelo en is opgericht in 1979. Momenteel heeft Group 2000 49 medewerkers.
- Group 2000 is gespecialiseerd in het ontwikkelen van intelligente softwareoplossingen op het gebied van IT en cyber protection. Deze oplossingen maken de maatschappij veiliger en verhogen de weerbaarheid. Het ontwikkelen van oplossingen voor IT en cyber protection is de kernactiviteit van Group 2000. Dit vertaalt zich in de praktijk naar het ontwerpen van designs en architecturen van software, programmeren van deze software, testen hiervan en het installeren van de software in telecommunicatie netwerken waar dan ook ter wereld. In het verlengde hiervan richt Group 2000 zich op het beheer en het onderhoud van de eigen oplossingen
- Group 2000 is gespecialiseerd in het ontwikkelen van software voor het legaal tappen

(intercepten) van telecommunicatie en internetverkeer (b.v. door politie en inlichtingendiensten), het automatiseren van processen in telecomnetwerken en het meten van gedrag alsmede netwerk coverage. In haar 37-jarige geschiedenis heeft Group 2000 zich bewezen in deze industrie en heeft serieuze potentie om een leidende rol te vervullen binnen haar specifieke domeinen. Deze expertrol komt voort uit de missie en visie van Group 2000

Contactpersoon (+eventueel contactgegevens) en website

Bert Beerling
Innovation Counselor
Bert.beerling@group2000.com
Mobiel: 06 20 436 305
www.group2000.com

SB1CS17016

Projecttitel	Security Awareness Beacon Methode (SABM)
SBIR-projectnummer	SB1CS17016
Bedrijfsnaam	Insite Security BV
In samenwerking met	Universiteit Twente, HKU, ABN AMRO

Projectsamenvatting

Een inleiding
De menselijke factor is een van de belangrijkste uitdagingen voor security managers. Processen en techniek zijn concreet en beheersbaar, maar de menselijke factor is minder grijpbaar. Medewerkers worden vaak aangeduid als 'zwakste schakel'. Organisaties zijn voortdurend op zoek naar een nieuwe methodes om kennis, houding en gedrag van medewerkers op een effectieve manier aan te passen.

Bestaande methoden schieten te kort of leveren niet het beoogde resultaat. Insite Security wil met dit haalbaarheidsonderzoek een nieuwe innovatieve trainingsmethode onderzoeken die een hogere effectiviteit realiseert en het gedrag van medewerkers ook daadwerkelijk kan aanpassen (borgt) zodat medewerkers de sterkste schakel in de keten worden.

Een beknopte beschrijving van het haalbaarheidsonderzoek
Insite Security wil met het haalbaarheidsonderzoek bepalen of het mogelijk is om een bewustwordingstrainingsprogramma te ontwikkelen wat direct verbonden is met real life gedragsmetingen en interventies op de werkplek. We noemen dit de "security awareness beacon methode" (SABM).

Een beknopte feitelijke beschrijving van de organisatie
Insite Security B.V., opgericht in 2009 heeft kantoren in Groningen en Haarlem. De organisatie bestaat op het moment van schrijven uit 60 professionals. Onze belangrijkste markten zijn organisaties uit de vitale infrastructuur , in het bijzonder gezondheidszorg, financiële sector, lokale overheid en ICT organisaties. Insite Security verbindt de menselijke, organisatorische en

technische kant van privacy en informatiebeveiliging.

Contactpersoon (+eventueel contactgegevens) en website
ing. Wilbert Pijnenburg CISA CISSP
wpijnenburg@insitesecurity.nl

Insite Security BV
www.insitesecurity.nl
Sylviuslaan 2
9728 NS Groningen
050 820 02 25

SB1CS17017

Projecttitel	Secure Data Storage Beyond Crypto
SBIR-projectnummer	SB1CS17017
Bedrijfsnaam	Storro BV
In samenwerking met	Radboudumc REshape Center, VUmc

Projectsamenvatting

Inleiding
Veel data moet langere tijd (tot vele jaren) bewaard worden, waarbij de waarde van deze informatie niet/nauwelijks afneemt met de tijd (bijv. gevoelige medische gegevens, i.t.t. oude financiële gegevens). Voor veilige opslag wordt vaak op cryptografie vertrouwd.
Verscheidene lekken in encryptie in de afgelopen jaren en de opkomst van kwantumcomputers tonen aan dat cryptografie niet eeuwig houdbaar is. Daarentegen vertrouwen veel partijen voor de beveiliging van hun gegevens toch puur op cryptografie.
Wij willen Secure Data Storage Beyond Crypto (SDSBC) ontwikkelen: een product dat voor haar veiligheid op méér dan enkel cryptografie vertrouwt.

Beknopte beschrijving van het haalbaarheidsonderzoek
Anders dan bij huidige oplossingen, willen we een versleuteld bestand opknippen in verschillende stukken en opslaan op meerdere zelf gekozen cloudproviders of servers, die elk slechts delen van een bestand hebben. Geen enkele opslaglocatie zal ooit elk stukje van een bestand mogen hebben gehad. Hierdoor kan nooit een volledig (versleuteld) bestand worden verkregen bij één hostingpartij (door een inbraak, werknemer of scan van data). Dit betekent dat, zelfs als de cryptografie waarop werd vertrouwd wordt gebroken, informatie verkregen bij één partij nooit kan leiden tot een reconstructie van de gehele informatie.
Doel van dit voorstel is om de technische en economische haalbaarheid te onderzoeken van SDSBC, waarbij bestanden worden versleuteld, opgeknipt en over verschillende locaties worden verdeeld.

Technische haalbaarheid
Om tot Secure Data Storage Beyond Crypto (SDSBC) –een nieuwe dienst– te kunnen komen dient innovatie plaats te vinden op het compartimenteren en verdeeld opslaan van data. De voornaamste innovatie is het waarborgen/afdwingen dat alleen een deel van de gecompartimenteerde data (de 'data chunks') op een specifieke locatie terecht komt.

Economische haalbaarheid
SDSBC is interessant voor bedrijven (zowel MKB als grootbedrijf) die werken met grote hoeveelheden gevoelige informatie zoals klantgegevens, financiële data, medische dossiers en bedrijfsgeheimen. Daarmee is SDSBC breed toepasbaar, zeker in het licht van nationale (Wbp) en Europese (Avg) wetgeving. Strengere regelgeving werkt de behoefte aan SDSBC juist in de hand.

Bij uitstek is SDSBC geschikt voor partijen de gevoelige data hebben met een lange retentiewaarde; data die ook na vijf jaar bewaren nog steeds (zeer) gevoelig is, zoals bij medische data. Een succesvolle introductie tot de markt wordt vergemakkelijkt door al vroegtijdig met partners samen te werken.

SDSBC stelt bedrijven in staat de voordelen van Cloudopslag aan te wenden, zónder bloot te staan aan de risico's hiervan m.b.t. veiligheid en privacy van gevoelige data. We zullen onderzoeken met welk verdienmodel SDSBC het beste vermarkt kan worden, met als start-/ijkpunt het veelgebruikte abonnementsmodel. Naast de betaalbereidheid willen wij de juridische kansen onderzoeken.

Bedrijf en partners
Storro B.V. stelt zich ten doel bij te dragen aan veiligere samenleving door communicatie die veilig, privé en niet-manipuleerbaar is mogelijk te maken. Onze gelijknamige software heeft verschillende (internationale) onderscheidingen ontvangen.

Partners:
Het VUmc is een academisch ziekenhuis en medische faculteit in Amsterdam, verbonden aan de Vrije Universiteit Amsterdam.

Het Radboudumc REshape Center is een academisch ziekenhuis in Nijmegen dat samenwerkt met de Radboud Universiteit Nijmegen. Nictiz is het Nederlandse kenniscentrum voor landelijke toepassingen van ICT in de zorg.

Contactpersoon en website
Voor interesse kunt u zich richten tot Yori Kamphuis; +31 20 308 02 18 of onze website https://storro.com in de gaten houden.

SB1CS17018

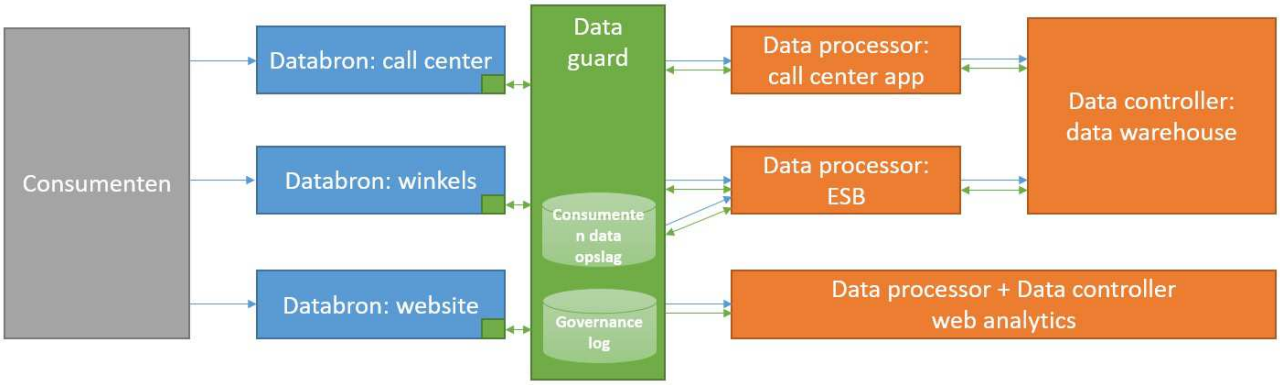
Projecttitel	Data Guard
SBIR-projectnummer	SB1CS17018
Bedrijfsnaam	Adversitement B.V.
In samenwerking met	-

Projectsamenvatting

Gedurende het project zal er datastream management software worden ontwikkeld die wordt aangeboden als dienst (software-as-a-service, 'Saas'). De nieuwe software ('Data Guard') slaat een brug tussen websitegebruik, dataverwerking en de bron (user) door expliciet te vermelden

welke data worden verzameld en met welk doel. Maar de software gaat nog een stuk verder. Het wordt mogelijk om, op individueel niveau, de opgeslagen persoonsgegevens te verwijderen ('Right to be Forgotten').

De belangrijkste kennis die op dit moment nog ontbreekt is de interpretatie van de GDPR-wetgeving en wat dit betekent voor de technische invulling van Data Guard. Er bestaat op dit moment een juridische omschrijving van de verordening, maar er is nog geen enkele jurisprudentie waardoor de interpretatie en de praktische invulling van de wetgeving nog ontbreekt. Dit zal pas veranderen vanaf 25 mei 2018 wanneer de wet ook zal worden gehandhaafd. Tijdens het onderzoek zal de juridische, technische, economische en organisatorische haalbaarheid van Data Guard in kaart worden gebracht.
Adversitement, opgericht in 2002, levert dienstverlening die de gehele keten van het



datamanagement bestrijkt; van de verzameling en verwerking van data tot de weergave van grote datastromen. Het bedrijf, dat opereert vanuit Uden, maakt de afgelopen jaren een snelle ontwikkeling door. Inmiddels is het bedrijf 40 fte groot en is actief als dienstverlener van bedrijven en overheden in binnen- en buitenland. De werkwijzen en zelf ontwikkelde technologieën van Adversitement onderscheiden zich door een sterke nadruk op de privacy van eindgebruikers en een hoge mate van governance mogelijkheden voor de bedrijven.

Contactpersoon (+eventueel contactgegevens) en website

Contactpersoon: Peter Lem
Contactgegevens: peter.lem@O2mc.io
0207606076
Website: https://www.adversitement.com/

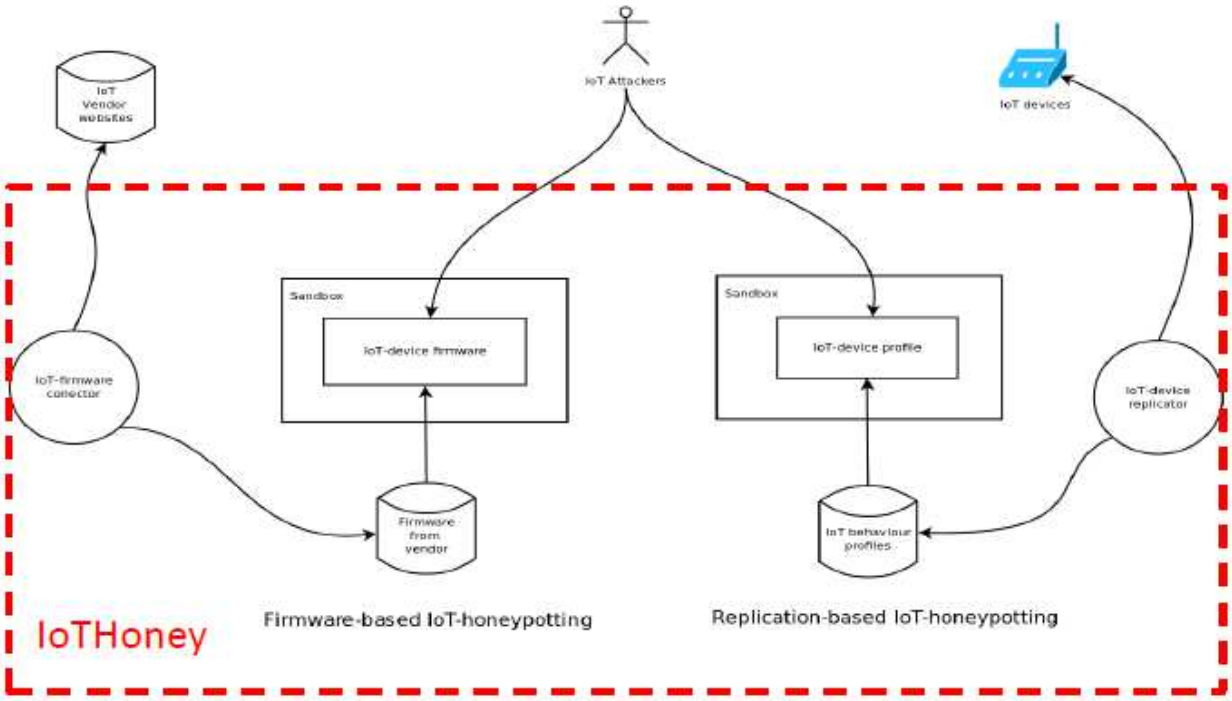
SB1CS17019

Projecttitel	IoT Honeypotting through frimware-emulation and replication (IoTHoney)
SBIR-projectnummer	SB1CS17019
Bedrijfsnaam	Cybersprint B.V.
In samenwerking met	n.v.t.

Projectsamenvatting

Cybersprint wil in dit project honeypot technologie ontwikkelen voor Internet of Things (IoT) apparaten en netwerken om te leren hoe hackers te werk gaan en waar de zwakke schakels zitten in deze apparaten en netwerken. Sinds de DDoS aanval op de systemen van DNS service provider Dyn in oktober 2016 is het besef gegroeid dat IoT apparaten en de netwerken waarin zij opereren gevoelig zijn voor malware. Dns-provider Dyn schat dat ongeveer honderdduizend apparaten van het Mirai-botnet betrokken waren bij de DDoS-aanval en dat de aanval tot 1,2Tbit/s aan verkeer genereerde. Naast de standaardkwetsbaarheden als "default passwords" is er echter nog weinig bekend waar de IoT gevoeligheden precies liggen en hoe malware bescherming verbeterd kan worden.

Het IoTHoney haalbaarheidsonderzoek zal zich richten op de technische haalbaarheid van de IoT honeypotting technologie waar nu onzekerheid zit door het huidige gebrek aan generieke frameworks waarmee (firmware based) honeypots kunnen worden ontwikkeld. Onderzocht moet worden of met bestaande frameworks IoT honeypots zo ontwikkeld kunnen worden dat deze niet als honeypot worden herkend door aanvallers of malware. Hiervoor zal dus ook bestaande malware, het gedrag van hackers en de mogelijkheden tot het simuleren van IoT apparaten en netwerken onderzocht moeten worden. Ook zal onderzocht worden welke essentiële SCADA leveranciers als partners benodigd zijn voor verdere ontwikkeling. Cybersprint wil ook onderzoeken of het mogelijk is om complete interne netwerken van bedrijven, organisaties of installaties te repliceren.



Cybersprint is opgericht in 2015 en bevindt zich momenteel in de scale-up fase: de dienstverlening is bewezen, de innovatieve Cybersprint technologie waarmee websites geanalyseerd kunnen worden om kwetsbaarheden, hacks en malware vroegtijdig te detecteren

werkt. De bestaande dienstverlening is erop gericht websites te analyseren en de resultaten van die analyses te gebruiken om de websites veiliger te maken. Vanwege de hoge

automatiseringsgraad van haar oplossing kan Cybersprint sneller en goedkoper haar diensten aanbieden in vergelijken met haar concurrenten. Inmiddels heeft Cybersprint o.a. grote financiële dienstverleners en overheidsinstellingen zowel in binnenland als buitenland als klant. Cybersprint versnelt deze internationale groei met nieuwe investering van € 700.000 vanuit de Innovation Quarter. In april heeft Cybersprint ook in de categorie Risk, Intelligence & Security de FINTECH awards 2017 gewonnen. Cybersprint is gevestigd in de The Hague Security Delta (HSD Campus), het hart van de Europese cybersecurity.

Contactpersoon (+eventueel contactgegevens) en website

Contactpersoon: Pieter Jansen
Website: https://www.cybersprint.nl/

SB1CS17021

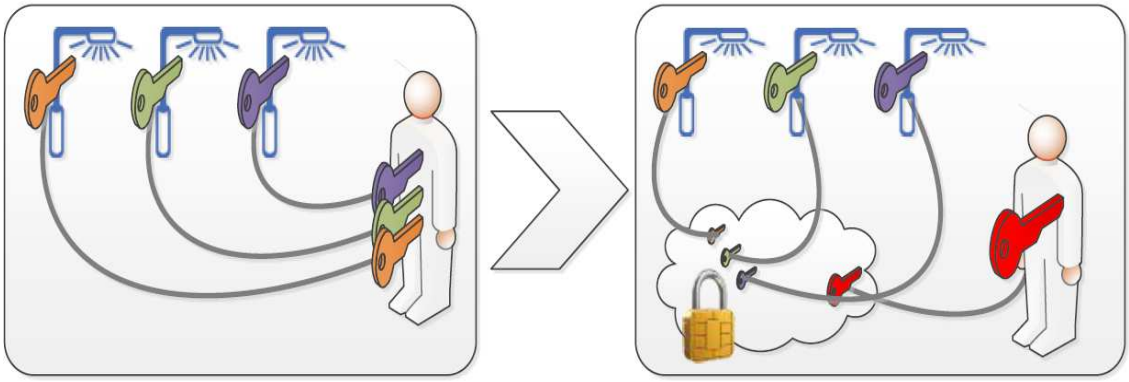
Projecttitel	Security manager for IoT (SEMIO)
SBIR-projectnummer	SB1CS17021
Bedrijfsnaam	Intrinsic ID B.V.
In samenwerking met	Technolution B.V.

Inleiding
Er zijn talloze voorbeelden van machines - verkeerslichten, waterzuiveringsinstallaties, zonnepanelen – die zijn aangesloten op het internet. Dit wordt Internet of Things (IoT) genoemd. Deze apparaten vormen vaak kritieke netwerken zoals stroomvoorziening, verkeersregeling en watervoorziening. Vergaande invoering van IT-technologieën heeft ertoe geleid dat deze infrastructuren niet alleen steeds complexer worden, ook neemt hun kwetsbaarheid voor aanvallen door cybercriminelen toe. Deze toenemende complexiteit maakt het voor netwerkoperators steeds moeilijker het overzicht over hun netwerk te behouden, maar vooral ook om de beveiliging ervan te kunnen garanderen. Een potentieel en reëel gevaar voor de samenleving.

Huidige methoden om deze miljoenen/miljarden apparaten te beveiligen zijn terug te brengen tot het opslaan van sleutels in OTP (eenmalig programmeerbare geheugens) of EEPROM / Flash (herprogrammeerbaar maar eenvoudig uitleesbaar). Hoe dan ook, beide 'opties' bieden schijnveiligheid, zijn veelal duur en niet of nauwelijks schaalbaar voor toepassing in miljarden apparaten.

Haalbaarheidsonderzoek
Om tot een beveiligingsoplossing te komen die wel schaalbaar is naar de miljarden apparaten van het IoT starten Intrinsic ID en Technolution samen een haalbaarheidsonderzoek. Intrinsic ID is een spin-off van Philips Electronics en maakt elektronische producten fysiek onkopieerbaar op basis van de door hen gepatenteerde SRAM PUF technologie. De door Intrinsic ID gepatenteerde SRAM PUF technologie gaat uit van het betrouwbaar uitlezen van unieke chipkenmerken. Deze technologie biedt de meest veilige bescherming voor hardware gebaseerde versleuteling en opslag. Technolution is een technology-integrator en biedt oplossingen voor complexe integratievraagstukken waarbij verschillende systemen tot een goed werkend geheel worden samengevoegd. Systemen die veelal bestaan uit een combinatie van elektronica,

programmeerbare logica en software. Daar komt bovenop dat Technolution niet alleen ervaring heeft met kritieke infrastructuren, maar ook beschikt over de voorzieningen om deze te hosten.



Figuur 1 - Sleutelbeheer in de cloud van 1 sleutel per device naar 1 sleutel om alle devices te gebruiken

Het haalbaarheidsonderzoek draait om een platform voor IoT-oplossingen waarbij, op basis van authenticatie en beveiliging van IoT apparaten middels SRAM PUF technologie, het grootste deel van het beveiligingssysteem kan worden overgebracht van het apparaat naar een cloud platform. Hierdoor wordt het makkelijker om veilig te communiceren, om bedreigingen te monitoren en om actie te ondernemen bij beveiligingsissues. Tevens wordt het beheer van cryptografische sleutels eenvoudiger, zoals te zien is in figuur 1.
Het haalbaarheidsonderzoek moet antwoord geven op de vraag of het beoogde platform de beveiliging van kritieke IoT-infrastructuren volledig kan overnemen. Waar voorheen beveiliging ín het apparaat werd gestopt, wordt het hier als beveiligingsdienst (Security as a Service ofwel SECaaS) aangeboden. Om dit mogelijk te maken moet ook de vraag worden beantwoord of SRAM PUF technologie toegepast kan worden op low-end chips van IoT apparatuur. Vanuit economisch perspectief vormen het markpotentieel, positionering, business model en prijsstelling onderwerp van onderzoek.

Intrinsic ID
Intrinsic ID is marktleider op het gebied van security IP cores en applicaties gebaseerd op gepatenteerde SRAM PUF technologie. Vanuit zijn herkomst uit Philips Research heeft Intrinsic ID veel kennis en expertise opgebouwd omtrent sterke security oplossingen. Als security bedrijf, heeft het een duidelijke focus op het ontwikkelen van oplossingen voor wereldwijde digitale security problemen. Intrinsic ID's hoofdkantoor ligt in Sunnyvale (Californië), met een R&D vestiging in Eindhoven en vertegenwoordigers in Tokyo en Seoel.

Technolution
Technolution uit Gouda is een technology-integrator en biedt oplossingen voor complexe integratievraagstukken waarbij verschillende systemen tot een goed werkend geheel worden gemaakt. Systemen die veelal bestaan uit een combinatie van elektronica, programmeerbare logica en software. Belangrijke markten voor Technolution zijn Mobiliteit, Energie, Industrie en Public Safety & Security. Technolution en Intrinsic ID vullen elkaar niet alleen in kennis en kunde aan, maar ook in marktsegment en contacten.

Contact
Intrinsic
High Tech Campus 9
5656AE Eindhoven
+31 (0)40 851 9020
www.*intrinsic-id*.com

ID Dr. Georgios Selimis
Senior Security Engineer
georgios.selimis@intrinsic-id.com
+31 (0)40 851 9027

SB1CS17023

n.n.b.

SB1CS17028

Projecttitel	Veilig delen van INformatie binnen de vitale seCtoren ter bescherming van kritieke Infrastructuren (VINCI)
SBIR-projectnummer	SB1CS17028
Bedrijfsnaam	Thales Nederland B.V.
In samenwerking met	-

Projectsamenvatting

Introductie
De vitale sectoren zijn, in het kader van nationale veiligheid, gebaat bij een efficiënte digitale transformatie. Aangezien er verschillende stakeholders binnen dit domein met elkaar moeten samenwerken, zal de informatieketen op een beveiligde manier ingericht dienen te worden. In onze oplossing zullen we met name naar de toegang en integriteit van informatie kijken. Cybersecurity, interoperabiliteit en informatie management gaan hierbij hand in hand. Ongeveer tachtig procent van de vitale infrastructuur is in handen van bedrijven en twintig procent in handen van de overheid. Een nauwe samenwerking van overheid en bedrijfsleven bij het vraagstuk van de nationale veiligheid is daarom noodzakelijk. Centraal hierin staat dat men een gezamenlijk beeld heeft van de status van de vitale infrastructuren die men beheert. Men zal dus informatie met elkaar moeten uitwisselen. Digitalisering van vitale netwerken betekent echter wel dat de 'cyber-kwetsbaarheid' steeds groter zal worden. Doorgaans staat een hogere

mate van beveiliging van systemen een efficiënte samenwerking in de weg. De vraag is dan ook hoe organisaties binnen de vitale informatieketens efficiënter en veiliger kunnen samenwerken d.m.v. informatie-uitwisseling.

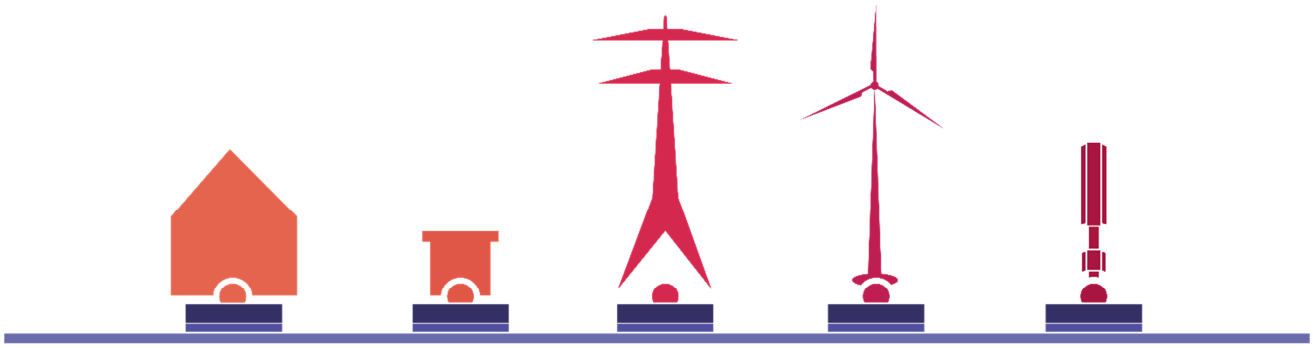
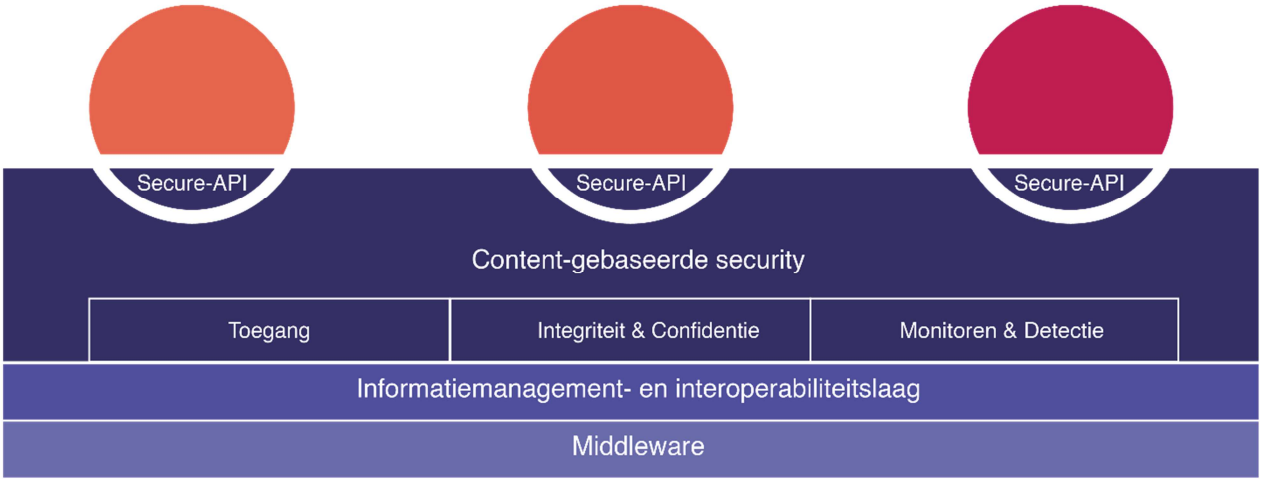


Figure 1 Cybersecure informatieuitwisseling tussen vitale sectoren



Figuur 2 VINCI platform

Haalbaarheidsonderzoek

Voor verbeterde beveiligde informatie-uitwisseling tussen organisaties binnen de vitale sectoren, is een haalbaarheidsonderzoek betreffende een cybersecure informatie-uitwisselingsplatform, VINCI, benodigd. Hierop kan men informatie met elkaar delen waarvan de toegang en integriteit gewaarborgd is. Deze oplossing leggen we als een multi-laags security-schil over de bestaande (digitale) infrastructuur heen, met robuuste en flexibele access control- en interoperabiliteitsmechanismen (Figuur 2). Binnen het haalbaarheidsonderzoek staan een aantal vragen centraal, zoals: (i) Wat zijn de huidige en gewenste behoeften vanuit de verschillende organisaties binnen de vitale sectoren t.b.v. informatie-uitwisseling en welke veiligheidsaspecten hangen hiermee samen? (ii) In hoeverre zijn bestaande systemen gereed om data te delen met andere systemen en wat moet er gebeuren om dit op een cybersecure manier te realiseren? Deze vragen en andere zal kennis leveren omtrent de (on)mogelijkheden van het delen van informatie tussen verschillende systemen binnen de vitale sectoren en daarnaast inzicht geven over de samenhangende cyber veiligheidsaspecten.

Project

We beogen uiteindelijk een generiek platform te ontwikkelen, dat gebruikt kan worden om op een veilige manier verschillende systemen binnen de vitale sectoren met elkaar te verbinden. Deze oplossing is een beveiligings- en interoperabiliteitsschil die we over bestaande infrastructuren en legacy-systemen heen kunnen leggen. Het uitvoeren van het haalbaarheidsonderzoek evenals de ontwikkeling van het platform, VINCI, zal iteratief gebeuren in co-creatie met verschillende eindgebruikers (zoals kritieke infrastructuurbeheerders energie, ICT, OOV, etc.), om zo de interoperabiliteitseisen en samenhangende veiligheidsrisico's in kaart te brengen en af te dekken. Security-by-design vormt hierbij het uitgangspunt. Vragen die centraal staan bij dit project, hebben betrekking op veiligheidsrisico's, het managen van identiteit, privacy en vertrouwen, en het managen van de integriteit van de informatie, beleid en de gecontroleerde toegankelijkheid ervan.

Organisatie

Thales Nederland B.V. behoort tot de Thales Group, een leidende onderneming op gebied van ontwikkeling, productie en levering van missie kritische informatiesystemen en elektronica. De groep heeft 62.000 medewerkers en is wereldwijd actief. De drijvende kracht van de groep zijn haar kennis en vaardigheden op gebied van Aeronautics, Space, Ground Transportation, Defence & Security. Ongeveer de helft van de omzet is defensie-gerelateerd, de andere helft komt uit civiele markten.

Thales Research en Technology Delft (TRT-Delft) telt 17 medewerkers en is onderdeel van Thales Nederland BV. TRT-Delft richt zich sinds de oprichting in 2002 exclusief op de ontwikkeling van oplossingen omtrent het delen van informatie tussen verschillende organisaties en/of verschillende belanghebbenden binnen organisaties. Oplossingen en concepten zijn en worden ontwikkeld en beproefd in publieke, civiele en militaire veiligheidsdomeinen. Thales Nederland BV bouwt missie-kritische systemen voor transport, defensie en veiligheid met ongeveer 2000 medewerkers. Het mission statement van de Thales Nederland B.V. is "Wherever safety and security are critical, Thales delivers. Together, we innovate with our customers to build smarter solutions. Everywhere."

Contact

Dr. Patrick de Oude
Thales Nederland B.V.
Thales Research & Technology Netherlands
Delftechpark 24
2628 XH DELFT

Mob. +31 6 12053442
patrick.deoude@nl.thalesgroup.com
www.thalesgroup.com/nl

SB1CS17030

Projecttitel	Privacy by Design Monitor
SBIR-projectnummer	SB1CS17030
Bedrijfsnaam	Software Improvement Group B.V.
In samenwerking met	Radboud Universiteit Nijmegen

Projectsamenvatting
Door de toenemende digitalisering worden steeds meer persoonsgegevens verzameld en verwerkt door software. Fouten in software zijn daarom toenemend de achterliggende oorzaak bij datalekken. De aanpak hiervan middels Privacy by Design moet zich richten op het verkleinen van zowel waarschijnlijkheid als impact van datalekken door softwarefouten te minimaliseren. Het belang hiervan wordt benadrukt in de nieuwe privacywetgeving.

Het regelmatig vaststellen van Privacy by Design wordt steeds belangrijker naarmate softwareontwikkeling meer plaatsvindt op een agile manier: frequente oplevering van software die kan worden uitgerold. Er is bij softwareontwikkelaars geen tijd en geen budget om elke keer een onderzoek te doen en de kennis van privacy is onder software engineers uiterst beperkt. De Cyber Security Raad (CSR) heeft bovendien gesignaleerd dat een groot tekort aan cybersecurityprofessionals dreigt. Automatiseren van dergelijke evaluaties is daarom essentieel.

Software Improvement Group BV (SIG) beoogt de ontwikkeling van een "Privacy by Design Monitor", waarin een tool-ondersteunde evaluatiemethode wordt aangeboden als continue dienstverlening om inzicht te krijgen en te houden in het niveau van Privacy by Design en welke zaken moeten worden verbeterd. De doelstelling van dit SBIR voorstel is het ontwikkelen van een prototype van de Privacy by Design tooling voor maatwerksoftware bij organisaties en bedrijven.

In dit haalbaarheidsonderzoek wordt middels literatuuronderzoek, interviews en experimentatie onderzoek gedaan naar de identificatie, meting en validatie van de meest kritische fouten en hoe dit uit de broncode is af te leiden, en naar (de kwaliteit en mogelijkheden van) bestaande tools en technieken. Verder wordt een ontwerp van tooling voor de Privacy by Design monitor gemaakt en worden 3-5 case studies uitgevoerd om dit te valideren en het marktpotentieel te onderbouwen, ten einde het Proof of Principle aan te tonen.

SIG is een spin-off van het Centrum voor Wiskunde en Informatica (CWI) in 2000. Door continu te investeren in onderzoek en ontwikkeling en door het analyseren van duizenden softwaresystemen is SIG uitgegroeid tot autoriteit op het gebied van onafhankelijke Tool Based Consultancy voor softwarekwaliteit. SIG heeft nu zo'n 100 werknemers in 7 landen met een jaaromzet van ongeveer 13 miljoen euro.

Contactpersoon (+eventueel contactgegevens) en website
ir. Rob van der Veer
r.vanderveer@sig.eu
+31 20 314 09 50

https://www.sig.eu/security

SB1CS17032

Projecttitel	Haalbaarheidsonderzoek valorisatie SamSam-techniek
SBIR-projectnummer	SB1CS17032
Bedrijfsnaam	Delta Pi
In samenwerking met	Universiteit Twente

Projectsamenvatting

Vitale infrastructuur moet in Nederland aan hoge veiligheidseisen én beschikbaarheidseisen voldoen: storingen van waterkeringen, bruggen, tunnels of spoorwegen levert maatschappelijke schade op of kan leiden tot doden. Daarom is goed risicomanagement, waar maatregelen genomen worden om ongelukken te voorkomen, bij de Maatschappelijk Vitale Organisaties (MVO's) die deze infrastructuren beheren van essentieel belang.

Traditioneel richt het risicomanagement binnen MVO's zich op *Safety* (veiligheidsrisico's) en *Availablity* (bijvoorbeeld doorstroming verkeer). Met de oprukkende automatisering worden cybersecurity-risico's steeds belangrijker: er zijn steeds meer incidenten waarbij cybercriminelen doordringen tot vitale infrastructuur. Cybersecurityrisico's kunnen door het nemen van de juiste maatregelen sterk worden verminderd. Uitdaging hierbij is dat maatregelen om cyberrisico's te verminderen op gespannen voet staan met *Safety*: firewalls houden hackers tegen, maar kunnen ook onterecht een sluiting van een waterkering tegenhouden.

Door deze tegenstelling tussen *Safety*/*Availability* en *Security* ontstaat een impasse. Alleen als securitymaatregelen in een expliciete netto verbetering van *Availability* en *Safety* resulteren, mogen deze geïmplementeerd worden. De huidige methoden van risicoanalyse zijn niet in staat deze impasse te doorbreken: men is niet in staat het belang van cybersecurity te positioneren in een wereldbeeld dat gedomineerd wordt door kwantitatieve *Safety* en *Availability* analyses.

Deze impasse wordt ook ondervonden in de praktijk. Marktonderzoek van Delta Pi heeft laten zien dat security officers van MVO's deze impasse dagelijks ondervinden en op zoek zijn naar methodes om deze te doorbreken. Er is een sterke behoefte om securityrisico's in termen van potentiële *Safety* en/of *Availability* impact te kunnen uitdrukken, om daarmee het belang van (het wel of juist niet nemen van cybersecurity) maatregelen te kunnen aantonen naar de organisatie.

Om deze impasse te doorbreken hebben Delta Pi en de Universiteit Twente gefinancierd samen de SamSam-techniek ontwikkeld [1], die het mogelijk maakt om cyberrisico's te modelleren en te kwantificeren in termen van *Safety* en *Availability* impact. Om deze techniek praktisch toepasbaar te maken (te valoriseren) is het essentieel om deze te vertalen naar een toepasbare methode en die te integreren is met bestaande *Safety* en *Availability* analysemethoden. Voor Delta Pi is een praktisch toepasbare methode die bewezen aansluit bij de dagelijkse praktijk van de MVO's het einddoel van het totale SBIR-project.

Het haalbaarheidsonderzoek richt zich op het herijken of de geconstateerde impasse nog steeds

[1] Zie https://www.utwente.nl/ctit/research/research_projects/national/nwo/nwo-ippsi-kiem/samsam.html

aanwezig is, welke vorm de (in de 2e SBIR-fase) te ontwikkelen methode moet aannemen om te passen in de dagelijkse praktijk van de MVO's en aan welke (commerciële) randvoorwaarden deze methode dient te voldoen. Tevens wordt een eerste specificatie van de methode opgesteld.

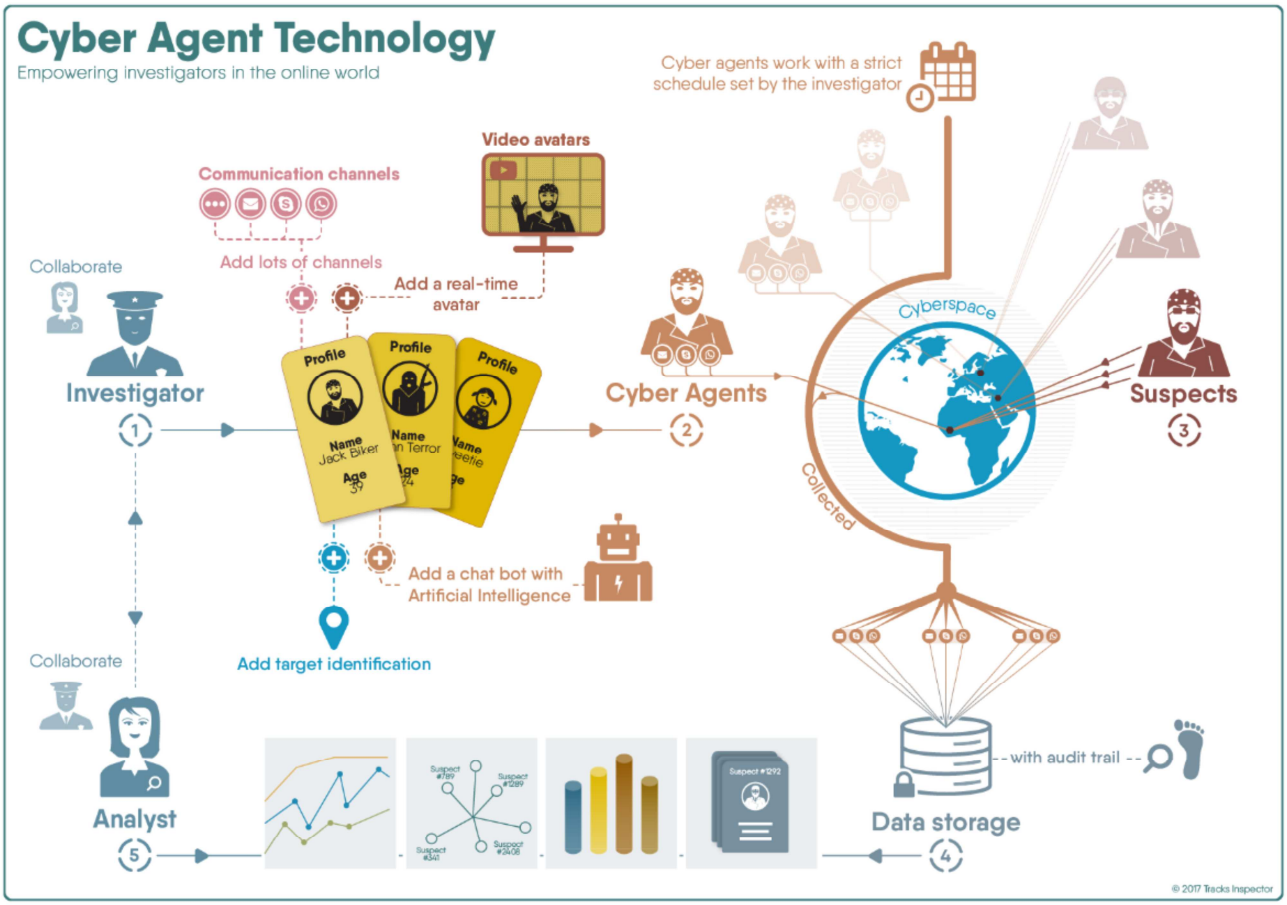
Contactpersoon (+eventueel contactgegevens) en website
Contactpersoon: J.vanEkris@Delta-Pi.nl, website: www.delta-pi.nl

---

SB1CS17033

Projecttitel	Cyber Agent Technology
SBIR-projectnummer	SB1CS17033
Bedrijfsnaam	Tracks Inspector
In samenwerking met	-

Projectsamenvatting
Tracks Inspector heeft voor Terre des Hommes in het kader van project Sweetie 2.0 een innovatieve softwareoplossing gemaakt om kindermisbruikers op internet in chatrooms op te sporen met behulp van chatbots. Deze software is gebaseerd op de Cyber Agent Technology die door Tracks Inspector is ontwikkeld. Tracks Inspector wil onderzoeken of Cyber Agent Technology ook bruikbaar is voor medewerkers van opsporings-, inlichtingen- en veiligheidsdiensten die zich bezighouden met het werken onder dekmantel op internetomgevingen bij vermoeden van, bijvoorbeeld, cybercrime, (cyber)terrorisme, radicalisering, kinderpornografie/kindersekstoerisme, cyberoorlog en bij de opsporing van georganiseerde criminaliteit.



Het werken onder dekmantel op internet is complex en foutgevoelig. Medewerkers communiceren online met targets, registreren de gesprekken, voeren analyses uit en houden de details over hun verschillende identiteiten handmatig bij. Dit gaat ten koste van de productiviteit, veiligheid en bemoeilijkt het trainen nieuwe onderzoekers. Met Cyber Agent Technology krijgen organisaties een omgeving die bovenstaande taken automatiseert zodat onderzoekers zich meer kunnen richten op het vergaren van informatie en waarmee ze met elkaar kunnen samenwerken. Naast vele praktische innovaties zoals de geautomatiseerde koppeling met uiteenlopende communicatieplatformen is de meest aansprekende innovatie de inzet van kunstmatig intelligente chatbots die zelfstandig inlichtingen kunnen verzamelen.

Het haalbaarheidsonderzoek
Tracks Inspector voert een haalbaarheidsonderzoek uit om inzicht te krijgen in de potentiële klanten, concurrenten en mogelijke (strategische) partners in de Nederlandse markt. Daarnaast wordt geïnventariseerd welke functionaliteit nog ontbreekt aan de huidige versie en in hoeverre er juridische en of ethische beperkingen zijn en hoe deze eventueel ondervangen kunnen worden. Indien uit deze inventarisatie blijkt dat er interesse is in de software en er daadwerkelijk een markt voor is, dan wil Tracks Inspector samen met een Nederlandse overheidsorganisatie een proof of concept realiseren. In dat geval onderzoekt Tracks Inspector ook welke mogelijkheden er zijn om de methode (software en of werkwijze) te patenteren ter bescherming van het intellectueel eigendom.

Tracks Inspector
Tracks Inspector is opgericht in 2014 en gevestigd op de campus van The Hague Security Delta.

Tracks Inspector ontwikkelt innovatieve software die gebruikers in staat stelt om samen te werken bij het verzamelen, beheren en onderzoeken van grote hoeveelheden digitaal bewijs. Medewerkers van Tracks Inspector hebben jarenlange ervaring met digitaal onderzoek voor zowel overheid als bedrijfsleven. De belangrijkste markt voor Tracks Inspector is die van opsporings-, inlichtingen- en veiligheidsdiensten. De huidige producten worden wereldwijd verkocht via wederverkopers.

Contactpersoon (+eventueel contactgegevens) en website
Hans Henseler
Tel: 06 24822200
Email: henseler@tracksinspector.com

HSD Campus
Wilhelmina van Pruisenweg 104
2595 AN Den Haag
www.tracksinspector.com

SB1CS17035

Projecttitel	LoRa End-to-End Security for Things-networks
SBIR-projectnummer	SB1SC17035
Bedrijfsnaam	The Things Industries B.V.
In samenwerking met	TNO

Projectsamenvatting
The Things Industries (TTI) is momenteel wereldwijd de enige aanbieder van open source Internet of Things (IoT) oplossingen in het groeiende segment van long range, low power connectiviteit. In de komende jaren zal IoT steeds groter worden en ook een steeds grotere rol vervullen in de dagelijkse levens van consumenten, bedrijven en overheden. Gegeven de verontrustende toename van het aantal botnet aanvallen op IoT devices, worden veiligheid en privacy steeds belangrijker voor de continuïteit en het vertrouwen in IoT systemen.

Om haar diensten in de opkomende wereld van IoT breed inzetbaar te houden, beoogt TTI op het gebied van Cyber Security twee ontwikkelingen in security op (ultra) low-cost end-devices (sensoren) en op end-to-end security & privacy. Belangrijkste doelstellingen in het project zijn een haalbaarheidsonderzoek en het ontwikkelen van prototypen.

In dit haalbaarheidsonderzoek wordt door middel van literatuuronderzoek en deskstudie onderzoek gedaan naar de ontwikkeling van een generiek encryptiemechanisme voor low-cost devices, en van een verbeterde end-to-end network security component. Van deze security services worden de technische en economische haalbaarheid onderzocht.

De missie van The Things Industries is om een wereldwijde, full-service, last-mile IoT service provider te worden, met de focus op LoRaWAN en Bluetooth. Integraal binnen deze missie is de aandacht voor de kwetsbaarheden van IoT.

Contactpersoon (+eventueel contactgegevens) en website
Alexander Overtoom
alexander@thethingsindustries.com
https://www.thethingsindustries.com/

SB1CS17037

Projecttitel	DroneID
SBIR-projectnummer	SB1CS17037
Bedrijfsnaam	Delft Dynamics B.V.
In samenwerking met	-

Projectsamenvatting

Delft Dynamics verwacht vanuit haar positie als innovatief Nederlands MKB bedrijf een sterke bijdrage te kunnen leveren aan het vergroten van de cyber security, door een systeem te ontwikkelen, waarbij het mogelijk is om op afstand drones te kunnen identificeren. Op dit moment worden er regelmatig drones gespot op plaatsen waar deze niet zijn toegestaan. Het is echter erg lastig gebleken voor handhavers om deze drone te volgen en de eigenaar van de drone te achterhalen. Er zijn wel ontwikkelingen om drones op ongewenste plaatsen uit de lucht te halen, maar dit soort acties zal niet overal toegepast worden omdat het vrij kostbaar is.

Er is een groeiende vraag naar de mogelijkheid om drones te kunnen identificeren, terwijl zij zich in het luchtruim bevinden en te bepalen wie de eigenaar is. In dit haalbaarheidsonderzoek wordt uitgezocht welke mogelijkheden er zijn om een betrouwbare, op afstand uitleesbare identificatie van drones te verkrijgen, die zo goedkoop en lichtgewicht is, dat deze ook voor hobbydrones toegepast kan worden. Extra bijkomend voordeel is dat de drone, net als een mobiele telefoon, teruggevonden kan worden als deze verloren c.q. gestolen wordt. En vergelijkbaar met een nummerbord kan het ontbreken van de DroneID dan strafbaar gemaakt worden. Ook op Europees niveau is deze wens al in *prototype regelgeving* geformuleerd, maar nog niet concreet ingevuld.

Delft Dynamics is in februari 2006 opgericht en heeft zich gespecialiseerd in het bouwen van robothelikopters: kleine onbemande helikopters, die door het slim samenvoegen van computer- en sensorapparatuur, gebruikt kunnen worden als stabiele en makkelijk te besturen sensorplatformen. Door de focus op de markt voor Defensie en Veiligheid, is geruime ervaring opgedaan in het ontwikkelen van robuuste hardware en software, die tezamen een robuust product vormen waarmee een hoge inzetbaarheid gewaarborgd is.

Contactpersoon (+eventueel contactgegevens) en website

Ir. A.J. (Arnout) de Jong
info@delftdynamics.nl
www.delftdynamics.nl

SB1CS17041

Projecttitel	Verhoord App Politie 2.0
SBIR-projectnummer	SB1CS17041
Bedrijfsnaam	Milvum B.V.
In samenwerking met	de Politie, het Ministerie van VenJ en het OM

Projectsamenvatting

In een digitaal tijdperk speelt foto, film en geluidsmateriaal een steeds belangrijkere rol in het opsporings- en strafproces. Een agent dient eenvoudig een geluidsopname te kunnen maken om dit bewijsmateriaal vervolgens veilig op te slaan in een portaal, zodat dit bewijsmateriaal ook daadwerkelijk toegepast kan worden bij een strafrechtelijke vervolging. De veiligheid en authenticiteit moeten voorop blijven staan bij het gebruiken en aanleveren van bewijsmateriaal. Hier is (technologische) vernieuwing voor nodig. Tijdens de appathon georganiseerd door het Ministerie van Veiligheid en Justitie, heeft Milvum deze zaken samengebracht in het winnende concept, de Verhoord app.

In dit haalbaarheidsproject zullen eindgebruikers en andere ketenpartners benaderd worden, om het basisconcept van de Verhoord app te verbeteren en uit te breiden door onderzoek te doen naar het business model, de uitrol en de implementatie. Daarnaast, is dus minstens net zo belangrijk, om onderzoek te doen naar extra innovatieve functionaliteiten. Deze dienen in te spelen op de veiligheid van de data en de overdracht tussen ketenpartners alsmede de bruikbaarheid van het bewijsmateriaal voor alle belanghebbenden. Voor het onderzoek zijn er drie belangrijke partijen geïdentificeerd, namelijk de Politie, het Ministerie van Veiligheid en Justitie en het Openbaar Ministerie. Het eindrapport moet dan ook inzicht geven in de te onderzoeken innovatiekansen die er liggen om de Politie en het Openbaar Ministerie ervoor te laten zorgen dat de Nederlandse veiligheid zowel fysiek als digitaal gewaarborgd blijft.

Omschrijving Haalbaarheidsonderzoek

Het haalbaarheidsonderzoek behelst twee verschillende hoofddoelen. Het eerst doel is het verkennen van de markt, waarbij het van belang zal zijn om de behoeften en eisen van de eindgebruikers en ketenpartners vast te stellen en om hier tevens zorg te dragen voor een goede implementatie. Het tweede doel richt zich op de technische mogelijkheden, de implementatie hiervan en het aansluiten van de ketenpartners. Voor het innovatie onderzoek hebben we vooralsnog al vijf verschillende kansen voor nieuwe technologieën geïdentificeerd, die om zowel uitgebreide research vanuit de klant alsmede het technologisch perspectief vragen.

Het marktonderzoek

In het begin van het haalbaarheidsonderzoek zal er een oriënterende fase uitgevoerd worden om de afzetmarkt in kaart te brengen. Het is hierbij van belang om alle ketenpartners en stakeholders vast te stellen om vervolgens concrete stappen te zetten naar gesprekken en workshops. Hierbij zullen de behoeften en eisen van de partijen worden gedefinieerd. Tevens dient het verdienmodel uitgewerkt te worden en gaan we onderzoek doen naar de volgende vragen: Welke markten kunnen bediend worden met het product en hoe zorgen we ervoor dat het idee schaalbaar zal zijn.

Innovatie onderzoek

Het belangrijkste onderdeel in dit haalbaarheidsonderzoek is gericht op het verkennen van de

vooropgestelde functionaliteiten (Blockchain (secure by design), machine learning, speech-to-text (audio en video), stemherkenning, stem separatie) en eventuele nieuwe functionaliteiten opstellen en hun waarde voor de ketenpartners beramen. Via de workshops willen we in samenwerking met de ketenpartners en stakeholders de huidige situatie beter begrijpen, functionaliteiten voorleggen en wellicht nieuwe functionaliteiten bedenken. Het doel is om de ideeën omtrent de Verhoord app uit te breiden en zodanig concreet te maken dat een ontwikkelingstraject in samenwerking met de stakeholders reëel is voor fase 2.

Organisatie
Milvum is opgericht in 2012 en gevestigd in Den Haag. Er werken momenteel 20 man aan allerlei innovatieve projecten. Zo heeft Milvum voor de overheid o.a. de KopieID app ontwikkeld en werkt het voor grote partijen als ING, ABN-AMRO, Radartv (AVROTROS), Deloitte en BZK. Naast een innovatieve mindset, waarbij de focus van Milvum ligt in het bedenken van nieuwe IT-toepassingen voor uitdagingen en kansen, beschikt het bedrijf ook over een ontwikkelingsteam met kennis van de nieuwste technologieën. Zo is Milvum in staat om ook de concrete oplossingen te ontwikkelen in de vorm van applicaties. Tot dusver heeft Milvum al 6 hackathons weten te winnen van o.a. BZK, VenJ en het UWV. Hierdoor blijft Milvum continu in beweging en is zij klaar voor de toekomst.

Contactpersoon (+eventueel contactgegevens) en website
Salim Hadri
Telnr.: 06-81473736
E-mail: salim@milvum.com
Website: www.milvum.com