Self-supporting Blus Unit

Het IFV ontwikkelt, samen met een aantal marktpartijen, de Selfsupporting Blus Unit (SBU). De SBU is een rijdend voertuig dat zelf kan navigeren naar de brand en vervolgens kan bepalen hoe het incident het beste bestreden wordt. Dit doet de SBU door het gebruik van camera's, sensoren, een brainbox waar alle informatie samen komt, straalmotoren voor de verplaatsing, en de SBU is ook voorzien van micro CAFS (Compressed Air Foam System) als blusmiddel. Het is de verwachting dat door het gebruik van de SBU incidenten beter en sneller kunnen worden bestreden. Daarnaast zal ook het risico voor het personeel worden verminderd omdat zij zelf verder van het incident kunnen blijven. Het is uiteraard wel van belang dat de SBU wordt bestuurd door personeel van Brandweer Nederland die de Blus Unit onder controle hebben. Tijdens het project zal een prototype ontwikkeld worden.

Delta-R

Het project ontwikkelt en test een nieuwe detectietechniek, optimaliseert deze ten behoeve van het douane proces op Schiphol en Distributiecentra om pakketpost en bagage te analyseren op aanwezigheid van narcotica en/of explosieven. De techniek detecteert oppervlaktesporen op bagage en pakketpost middels uv-licht reflectie en spectrografie. Het project levert een demonstrator met automatische stand-off trace detectie van narcotica (cocaïne). Dit naast de initiële capaciteit voor detectie van explosieven. Tevens worden de operationele mogelijkheden en beperkingen binnen het douaneproces vastgesteld.

HARVEST

In opdracht van en in samenwerking met de Koninklijke Marechaussee is TNO samen met Qubit-Visual Intelligence (QVI) BV, gestart met het ontwikkelen van innovatieve kennis en techniek om via camerabeelden opvallend of afwijkend gedrag geautomatiseerd te kunnen herkennen. De Koninklijke Marechaussee verwacht dat geautomatiseerde gedragsherkenning in de toekomst een waardevolle ondersteuning voor de taakuitvoering kan bieden.

Het gaat om gedragingen die vaak voorkomen bij diefstal van bagage, het herkennen van onbeheerd achtergelaten bagage, en om situaties die voorkomen als mensen onwel worden. Dit zijn situaties die voor de taakuitvoering van de Koninklijke Marechaussee relevant zijn. De herkenning richt zich niet op gezichten maar op het gedrag van personen, bijvoorbeeld aan de hand van bewegingspatronen. De software zal worden ontwikkeld om te worden toegepast op de bestaande beveiligingscamera's op de luchthaven Schiphol.

De software helpt alleen bij de detectie van objecten en gedragingen, en verandert niets aan de werkwijze, taken of bevoegdheden van de beveiligingsprofessionals. De operator in de toezichtruimte wordt bij het bekijken van de vele cameraposities waar mogelijk automatisch geattendeerd op camerabeelden van incidenten. Dit kan er onder meer voor zorgen dat hulpdiensten sneller kunnen acteren. Dit verhoogt de capaciteit om mensenlevens te redden en criminaliteit tegen te gaan.

SecureHub

De verantwoordelijkheid voor de beveiliging van internetverbindingen ligt traditioneel op toepassingsniveau: ieder stuk software neemt in principe zijn eigen code hiervoor mee. Daarmee is de fundamentele veiligheid en vertrouwelijkheid van verbindingen aan zowel kwaliteitsverschillen als aan veroudering onderhevig: de ontwikkelaars van ieder softwarepakket zijn verantwoordelijk voor de kwaliteit, interoperabiliteit en onderhoud van de betreffende onderdelen van hun software. Het feitelijk gerealiseerde beveiligingsniveau van internetverkeer is ondanks gedeelde technische standaarden per applicatie verschillend, en bovendien weinig transparant.

SecureHub pakt het probleem structureel aan door de beveiliging van verbindingen los te koppelen van de software die de verbinding wil opzetten. SecureHub kanaliseert beveiligde verbindingen op de transportlaag, analoog aan wat een firewall doet voor netwerkverbindingen. De gebruiker kan via SecureHub de regie overnemen volgens een (vooraf gedefinieerd en centraal te beheren) security-profiel. Beveiliging van verbindingen wordt daarmee beter, transparanter en wendbaarder: gebruikers profiteren van sterke cryptografische algoritmes en de nieuwste en sterkste methodes voor authenticatie en privacy, en up-to-date beveiliging kan centraal worden gemonitord en afgedwongen. Omdat er sprake is van een enkel goed toegankelijk koppelpunt voor alle beveiliging op de transportlaag, is SecureHub makkelijk te integreren met additionele hoogwaardige beveiligingsinfrastructuur.

Brede inzetbaarheid beeldverbeteringstechnologie

Binnen het veiligheidsdomein wordt vaak gebruik gemaakt van statische camera-observatie. Weersomstandigheden en het dag-nacht-ritme hebben veel invloed op de beeldkwaliteit die een camera kan leveren. Door het dag-nacht-ritme is vaak een gedeelte van het beeld niet goed zichtbaar door schaduwwerking van objecten. Daarnaast ontstaan er door opwarming, op een zonnige dag, trillingen in de lucht, ook wel turbulentie genoemd.

TNO heeft voor het ministerie van Defensie in de afgelopen jaren een systeem ontwikkeld waarin technologie wordt gebruikt die de beeldkwaliteit verbetert ondanks de weersomstandigheden en het dag-nacht-ritme. Dit is een stand-alone systeem, waarbij gebruik wordt gemaakt van een hoge kwaliteit camera en een speciale computer. Deze computer is geoptimaliseerd om de beeldverbeteringsalgoritme te kunnen gebruiken. Ook is er een speciale videocamera gekozen en is de bandbreedte tussen de camera en de computer groot. Hierdoor is de hele keten van beeldopname tot verwerking volledig geoptimaliseerd. Bij statische camera-observatie is dat niet het geval. Daarom moet de technologie worden hiervoor worden aangepast.

De doelstellingen van dit project zijn: het intelligenter maken van de turbulentiecorrectie, het mogelijk maken van verbetering van gecomprimeerde video, het vereenvoudigen van de inzet van verschillende camera’s en zorgen dat de technologie makkelijk integreerbaar wordt in andere systemen.

Colour the Night

TNO beschikt over technologie (software genaamd *Colour the Night* of CtN) voor het fuseren en in realistische kleuren weergeven van verschillende typen nachtzicht camerabeelden. Met deze technologie kan bij nacht een *situational awareness* worden bereikt die lijkt op die bij daglicht waardoor de efficiency en effectiviteit van een missie substantieel worden verbeterd. Deze technologie is alleen offline en nog niet real-time gedemonstreerd in een scenario (land-land waarneming).Ondanks dat alle offline experimenten erop wijzen dat CtN een meerwaarde heeft bij nachtelijke waarneming is live toepassing binnen het beoogde primaire scenario (lucht-land waarneming) nog niet gedaan.

Het bedrijf ITS bv. ontwerpt, produceert, integreert en verkoopt high-end nachtzichtcamera-systemen, gebaseerd op helderheidversterkers en warmtebeeld sensoren.
Het doel van dit project is om de CtN-beeldfusie technologie zo aan te passen dat deze breed inzetbaar wordt. Getracht zal worden deze technologie inzetbaar te maken en voor meer organisaties om zo een significante verbetering van de *situational awareness* bij nacht te behalen met zo min mogelijk gebruikersinteractie. De combinatie van TNO's software (CtN) en de camera kennis en reeds ontwikkelde techniek van ITS bv zorgen voor een uitstekend fundament om relatief snel te komen tot een systeem waarmee de (op basis van tests in laboratoriumsituaties) te verwachten operationele meerwaarde kan worden bevestigd.

Deep Firmware Inspection Tool

In de meeste apparaten zit her en der zogenaamde firmware, ingebakken software in componenten die op een lager niveau verantwoordelijk zijn voor functionaliteit. De firmware is vaak oorspronkelijk niet ontworpen met het idee dat het aan een netwerkverbinding (laat staan het publieke internet) is gekoppeld. Apparatuur kan daardoor kwetsbaar zijn (of worden) voor ernstig misbruik. Het analyseren van (enkel in binaire vorm beschikbare) firmware is technisch hoogwaardig en bovendien zeer arbeidsintensief werk dat niet weggelegd is voor de meeste organisaties. Daardoor wordt in de praktijk vrijwel nergens structureel actief toezicht gehouden op de hardware-inventaris, en wordt er ook geen preventief onderhoud gepleegd. De meeste apparatuur blijft net zolang in gebruik tot het betreffende apparaat het fysiek heeft begeven. Dit kan leiden tot grootschalige kwetsbaarheid en onmerkbaar misbruik van apparaten en netwerkinfrastructuur door derde partijen.

Deep Firmware Inspection Tool is een open source tool om voor een deel geautomatiseerd beveiligingsscans te kunnen doen. Daardoor kan firmware gelinkt worden met elders bekende kwetsbaarheden. Door de firmware van apparatuur te fingerprinten op aanwezige software-onderdelen, kunnen ze vervolgens ook in de gaten gehouden worden. Door als klant zelf op de hoogte te zijn van latent aanwezige securityproblemen, kunnen leveranciers direct op hun verantwoordelijkheden worden aangesproken.

Normalware

Overheidsinstanties willen beter kunnen vaststellen of zakelijke mobiele telefoons of tablets zijn geïnfecteerd met schadelijke software (malware). Binnen het *normalware* project wordt programmatuur ontwikkeld voor detectie van mogelijke malware op mobiele apparatuur binnen bedrijfs- of overheidsomgevingen. Deze tool is vooral gericht op detectie van malware die nog niet door commerciële malware scanners wordt gevonden. Als eerste wordt binnen een aantal overheidsinstellingen geïnventariseerd op welke manier mobiele apparatuur wordt uitgegeven en beheerd. Daarna wordt een vergelijkingsmethode ontwikkeld om alle apparaatgegevens te voorzien van een waarschijnlijkheidsscore (*malware risk index*). Naast de kans op infectie met malware kunnen deze scores ook dienen als input voor aanvullend onderzoek aan specifieke, hoog scorende, bestanden uit het onderzochte apparaat.

Aanpak cybercrime via hostingbedrijven

Criminelen maken gebruik van commerciële hostingbedrijven om grote hoeveelheden data op te slaan en hun criminele activiteiten uit te voeren. Dit project ontwikkelt software voor het geautomatiseerd intelligent onderzoeken van computersystemen van criminelen. Dit project ontwikkelt 3 modules waarmee:

1. Verdachte data in samenspraak met hostingbedrijven op afstand op forensisch verantwoord veiliggesteld kan worden door de politie;
2. De data slim doorzocht kan worden op sporen die leiden naar de verdachte en een indicatie gegeven wordt van de kansrijkheid van een opsporingsonderzoek naar de dader;
3. De botnetdata zo gefilterd wordt dat de slachtoffers geïnformeerd kunnen worden, trends in cybercrime gesignaleerd kunnen worden en daderbeelden geschetst kunnen worden.

Gefunctionaliseerde Nanodeeltjes voor het Zichtbaar Maken van Vingersporen

Projectvoorstel ingediend door NFI

Het belang van vingersporen in een gerechtelijk onderzoek is nog steeds ongekend groot. Recente ontwikkelingen op het gebied van het zichtbaar maken van latente vingersporen hebben laten zien dat een selectieve visualisatie van vingersporen mogelijk is. Het ontwikkelen van reagentia voor deze selectieve visualisatie is complex door een groot scala aan parameters. In het project 'Gefunctionaliseerde Nanodeeltjes voor het Zichtbaar Maken van Vingersporen' wordt onderzocht wat de mogelijkheden zijn om selectieve reagentia te maken via een snel synthetisch proces. Het uiteindelijke doel van het project is het ontwikkelen van methode voor het synthetiseren van reagentia waarmee selectief vingersporen zichtbaar gemaakt kunnen worden en de werking op een toepassing aan te tonen.