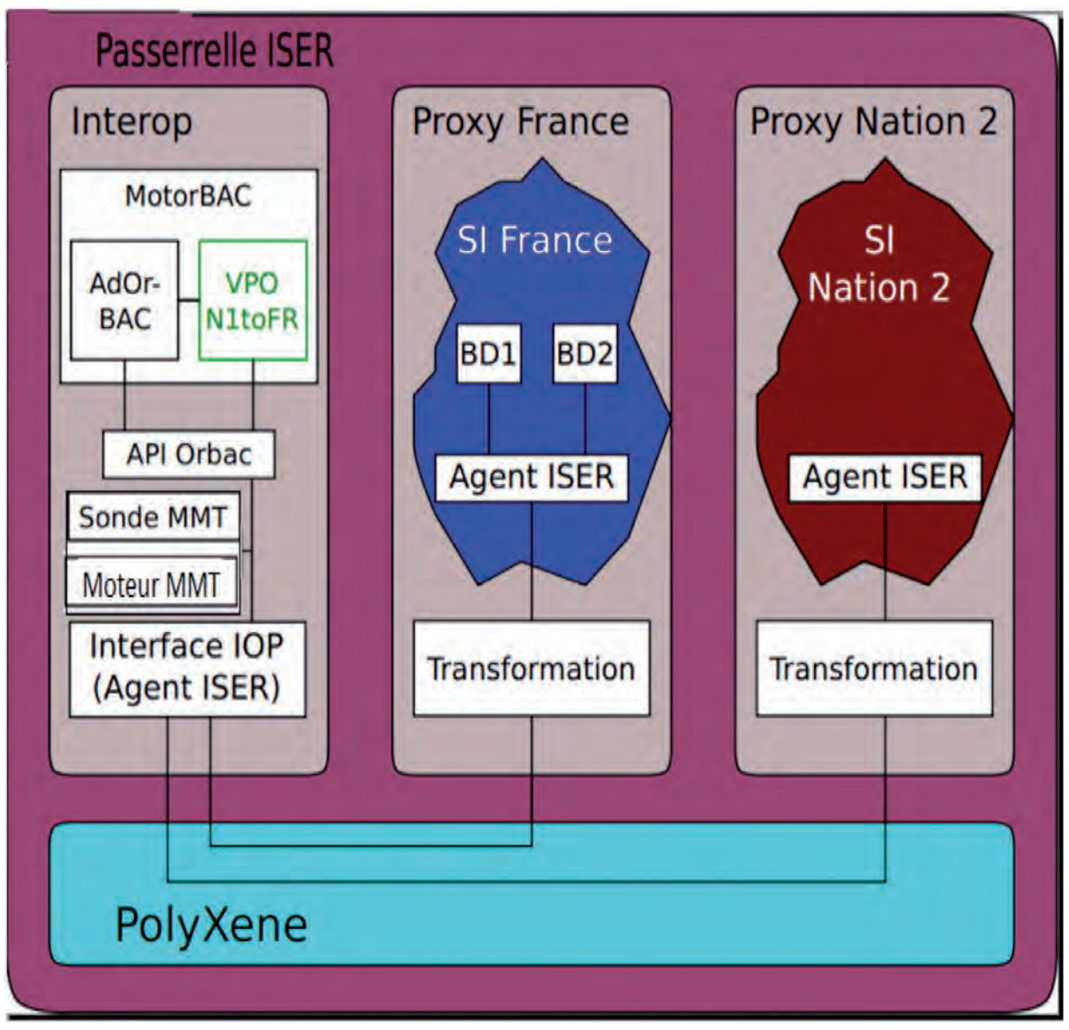
ISER - INTEROPÉRABILITÉ SÉCURISÉE DES SYSTÈMES DE RENSEIGNEMENT MULTI-SOURCES



ISER Architecture

OBJECTIFS TECHNOLOGIQUES DU PROJET

- Définition de mécanismes pour la négociation et la délégation de droits préservant la confidentialité au regard de la politique d'interopérabilité
- Mécanismes de déploiement de politiques
- Définition de mécanisme de protection de la plateforme
- Test et supervision des politiques déployées pour la détection et la prévention d'intrusion

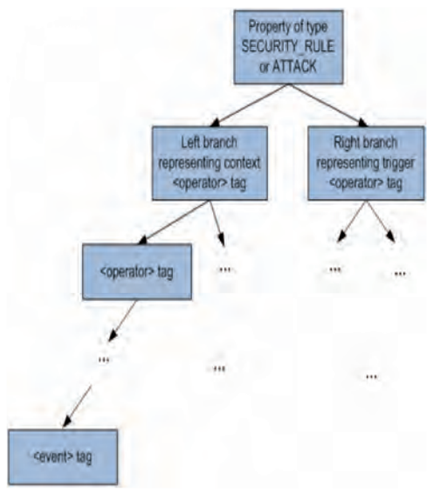
ARCHITECTURE ISER

- MotOrBAC :
  - Outil de définition et implémentation de politiques de sécurité suivant le modèle de contrôle d'accès OrBAC ;
  - Permet l'identification et la détection des conflits dans les politiques permettant ainsi une aide à leur définition.

- PolyXene :
  - L'OS PolyXene est un hyperviseur de haute sécurité qui permet l'accès et la connexion d'une machine unique vers différents réseaux et des systèmes d'information ayant des niveaux de sécurité différents ;
  - Certifié EAL 5+ par l'ANSSI.

- MMT :
  - Outil de supervision qui permet la capture et l'analyse de trafic réseaux et/ou d'événements de sécurité ;
  - Vérifie la bonne mise en application des politiques et détecte les tentatives d'intrusions.

ISER Demonstrator



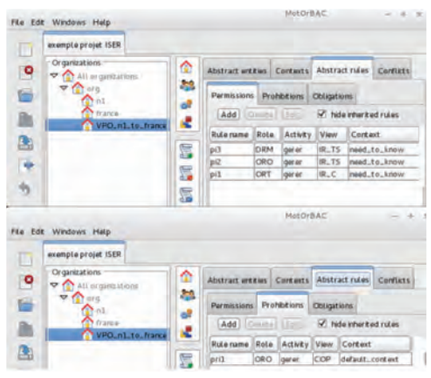
```
<!-- security property 9 -->

<property value="THEN" property_id="2"  delay_max="0"
          type_property="SECURITY_RULE"
          description="Un ORT a le droit de lire les
          informations de renseignement si ces
          informations sont de niveau de sécurité
          inferieur ou égale au niveau Confidentiel.">

      <event value="COMPUTE" event_id="3"
         description="reception d'une requête envoyée
         d'un ORT d'une organisation autorisée pour
         lire des informations"
         boolean_expression="((ISER.ROLE == 'ORT')
         &amp;amp;&amp;amp;(ISER.ROLE_ORG == 'VPO_n1_to_france))" />

      <event value="COMPUTE" event_id="4"
         description="demande autorisée seulement si le niveau
         des fichier et inferieur au niveau confidentiel."
         boolean_expression="(((ISER.ANSWER == 1)&amp;amp;&amp;amp;
         ((ISER.VIEW == 'IR_NC')||(ISER.VIEW == 'IR_R')
         ||(ISER.VIEW == 'IR_C')))
         || ((ISER.ANSWER == 0)&amp;amp;&amp;amp;
         ((ISER.VIEW == 'IR_S')||(ISER.VIEW == 'IR_TS'))) )"/>
</property>
```

Régles de sécurité MM



Édition de politiques d'interopérabilité

Security rules summary results

Id	Description		
1	SECURITY RULE:	0	0
2	SECURITY RULE: Un ORT a le droit de lire les informations de renseignement si ces informations sont de niveau de sécurité inferieur ou égale au niveau Confidentiel.	17	13
3	SECURITY RULE: Un ORO du système a le droit de lire les informations de renseignement si ces informations sont de niveau de sécurité inferieur ou égale au niveau Secret.	10	0
4	SECURITY RULE: Un DRM a le droit de lire les informations de renseignement si ces informations sont de niveau de sécurité inferieur ou égale au niveau Très Secret.	0	0

Résultat d'évaluation de règles de sécurité

CONTACT
Sammy HADDAD • sammy.haddad@oppida.fr
http://www.iser.fr

DURÉE DES TRAVAUX
36 mois

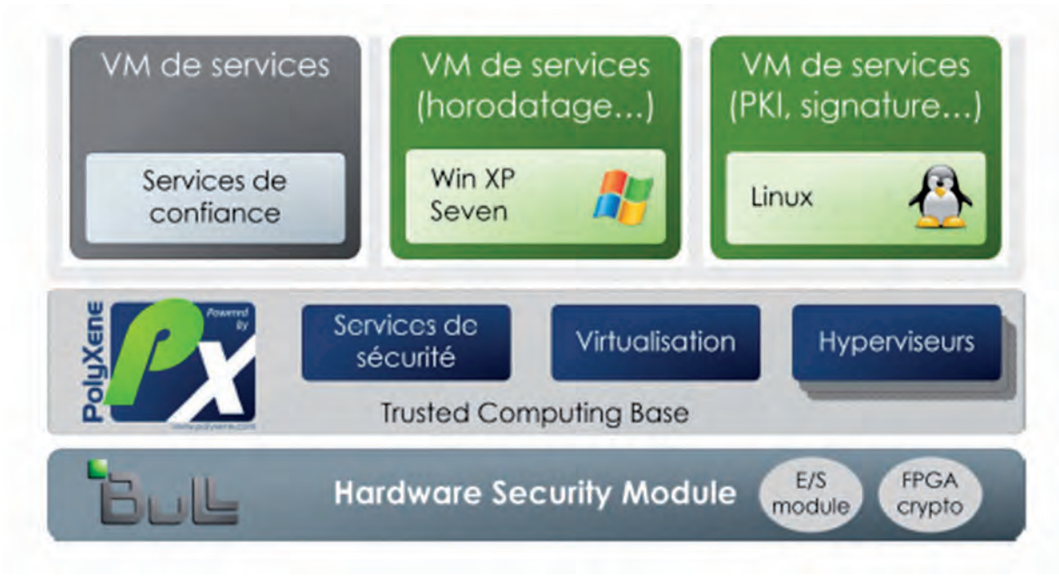
PARTENAIRES
Institut Mines-Telecom
OPPIDA, BERTIN technologies

PISCO

PLATEFORME D'INTÉGRATION DE SERVICES DE CONFIANCE

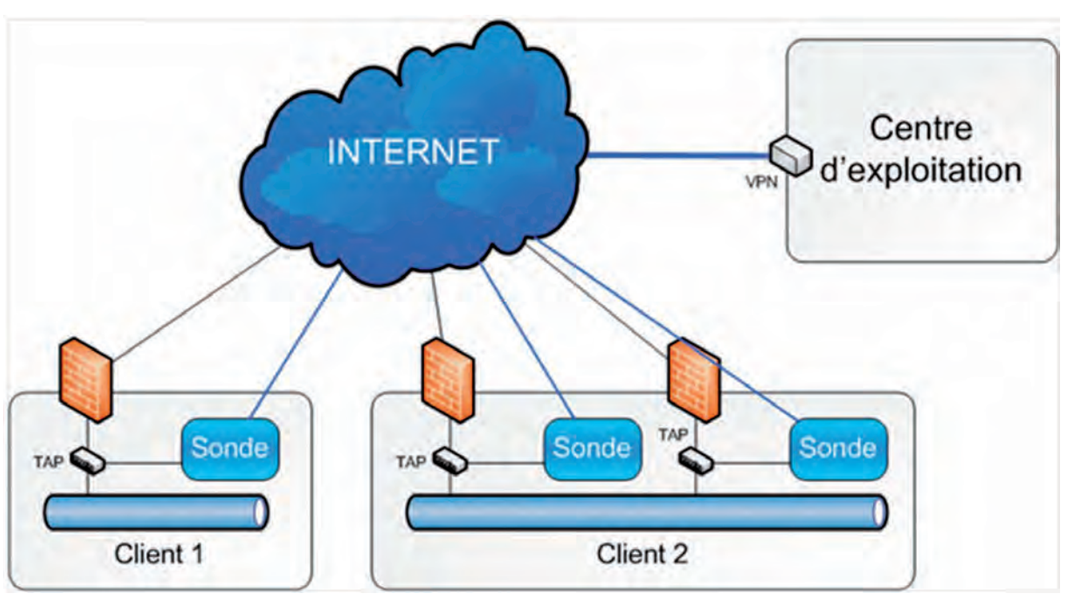
FUI

Plateforme matérielle



Intégration de PolyXene dans la plateforme matérielle

Appliance multi-services de confiance TrustyBox



Protection de sondes de collecte d'information

OBJECTIFS SCIENTIFIQUES DES TRAVAUX

- Réalisation d'une plateforme matérielle générique à très forte sécurité, destinée à être intégrée dans des solutions de sécurité multifonctions (appliance OEM).
- Développement d'outils destinés à faciliter l'intégration des applications et à assurer leur authenticité et leur intégrité.
- Vérification des propriétés de sécurité de la plateforme à l'aide d'outils d'analyse et vérification de code, méthodes d'attaque en fautes et protection face à ce type d'attaque.
- Certification CSPN de la plateforme.

APPROCHE SCIENTIFIQUE

- Analyse des besoins (exigences de sécurité pour la plateforme, définition des objectifs d'analyse et de vérification de la sécurité).
- Implémentation et analyse sécurité (portage de PolyXene et des services de confiance, analyse de sécurité des services offerts par la plateforme aux différentes applications hébergées, vérification des codes source).
- Préparation à la certification (analyse de la problématique de composition, rédaction d'une Cible de sécurité CSPN et d'une Cible de sécurité composite).
- Réalisation des démonstrateurs.

PRINCIPAUX RÉSULTATS OBTENUS ET FAITS MARQUANTS

- PolyXene intégré dans la plateforme matérielle avec succès
- Démonstrateurs fonctionnels :
  - Appliance service d'horodatage TrustyTime (C-S).
  - Protection de sondes de collecte d'information (Airbus).
  - Appliance service d'horodatage Eternity (Cryptolog).
  - Protection des communications HF (Serpikom).
- Travail sur le standard PKCS#11 : règles d'utilisation, moyens de test.

PERSPECTIVES ENVISAGÉES

- Constitution de partenariats technologiques et/ou commerciaux avec les éditeurs logiciels, du monde de la PKI, signature électronique, horodatage, dématérialisation de factures, en France et à l'export.
- Les résultats obtenus seront utilisés par un nouveau projet, sélectionné dans le cadre de l'AAP du FUI17 : IGDCI.

CONTACT
Liliana CABALANTTI • liliana.cabalantti@bull.net • Site web : http://www.projet-pisco.fr

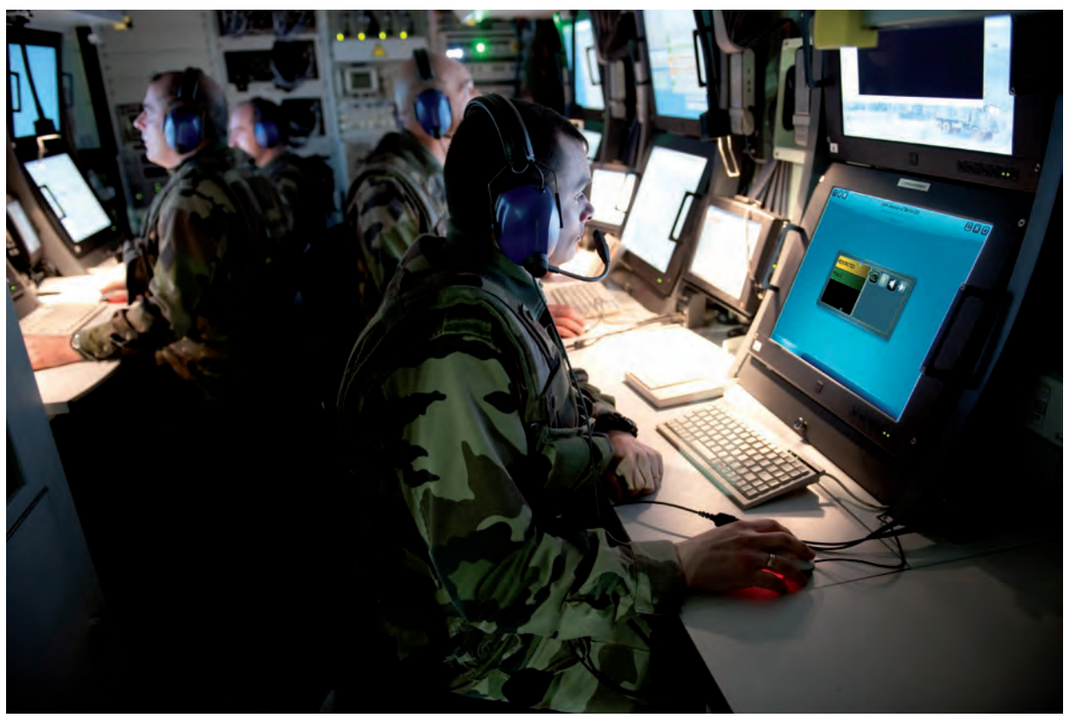
DURÉE DES TRAVAUX
24 mois

PARTENAIRES
BULL SAS, BERTIN TECHNOLOGIES, CASSIDIAN CYBER SECURITY, CS COMMUNICATIONS ET SYSTEMES, CRYPTOLOG INTERNATIONAL, SARL SERPIKOM, SAFERIVER, OPPIDA, CEA LIST, TELECOM PARISTECH, INRIA

SINAPSE - SOLUTION INFORMATIQUE À NOYAU AVANCÉ POUR UNE SÛRETÉ ÉLEVÉE

Toutes vos données et applications sur un même poste de travail, quelle que soit leur sensibilité

PEA



OBJECTIFS TECHNOLOGIQUES DU PROJET

Démontrer la faisabilité d'une couche logicielle de virtualisation à haut niveau de sécurité permettant la cohabitation étanche de différents environnements informatiques sur un même poste de travail.

CONTRAINTES

La solution logicielle doit être capable de satisfaire des exigences de sécurité élevées, compte tenu de la sensibilité des données et applications exploitées, et de maintenir l'intégrité des systèmes mis en œuvre.

CARACTÈRE INNOVANT DU PROJET

Dans les SI de Défense, le cloisonnement des informations selon leur classification est assuré par l'isolation physique des réseaux. Si cet air gap limite effectivement le risque de fuites, il s'avère contraignant (échange de données par supports amovibles, temps de latence de la transmission d'information, ergonomie défaillante, …) et coûteux (possession/exploitation).

Le PEA SINAPSE vise la réalisation d'une solution logicielle qui permette de s'affranchir de ces contraintes, en répondant aux exigences de sécurité, d'efficacité et d'optimisation des ressources.

ÉTAPES FRANCHIES

- Faisabilité démontrée et version préliminaire d'une plateforme logicielle multiniveau
- Déclinaison d'une version pour nos partenaires de l'OTAN
- Déploiement expérimental d'un démonstrateur à l'EMA
- Contrat MCO–MCS avec démonstrateurs, serveurs et postes tactiques
- Utilisation dans un programme d'industrialisation d'une passerelle

RÉSULTATS OBTENUS

- Intégration de la solution dans une passerelle multiniveau (ISIRWAY) éprouvée en conditions opérationnelles
- Certification EAL 5 en 2009 ; certification EAL 5+ en cours
- Création d'une solution packagée sous la marque PolyXene®
- 3 participations au CWIX

APPLICATIONS

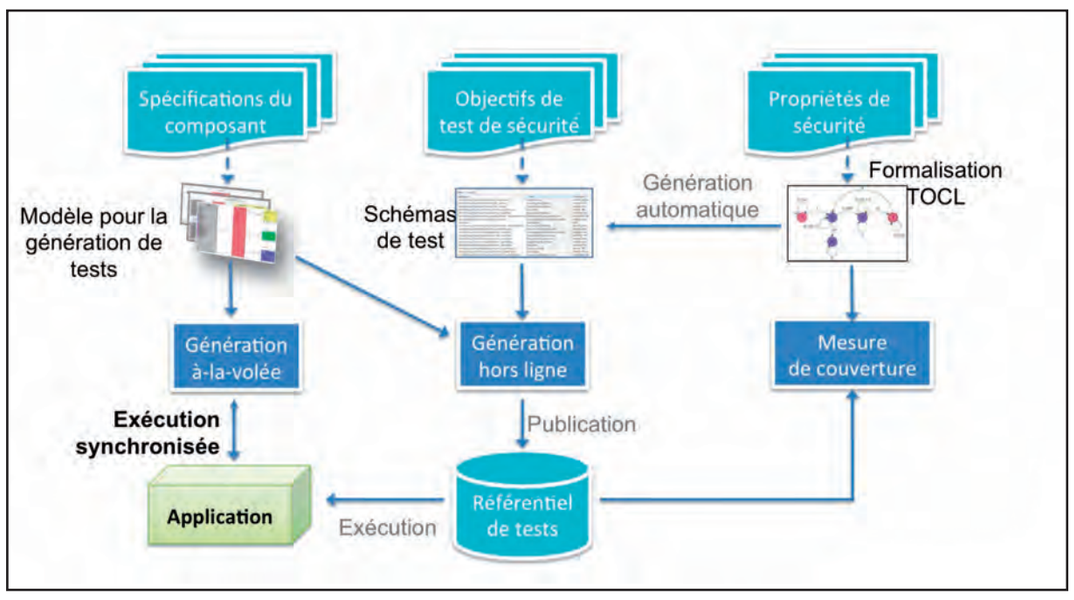
- Protection en confidentialité et en intégrité des SI sensibles
- Accès simultané à des données et applications de sensibilités différentes sur un poste multiniveau
- Interopérabilité sécurisée en environnement interallié

CONTACT
David BOUCHER • Responsable de la BU Sécurité des systèmes d'information / Bertin IT
david.boucher@bertin.fr

DURÉE DES TRAVAUX
SINAPSE 1 : 2004 – 2009 (60 mois)
SINAPSE 2 : 2009 – en cours

MBT_Sec

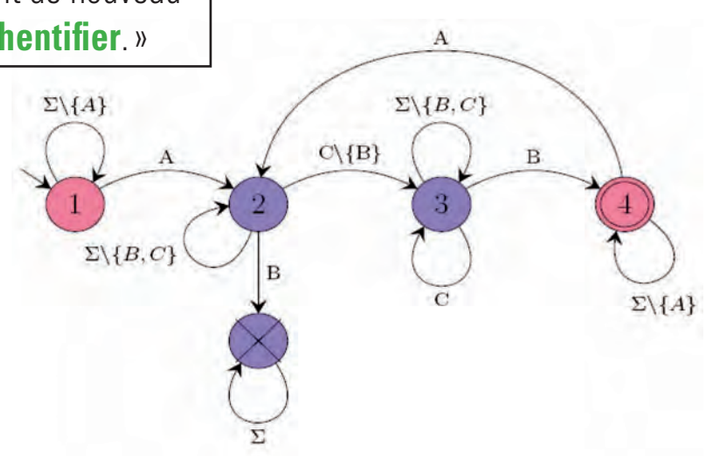
GÉNÉRATION AUTOMATIQUE DE TESTS POUR COMPOSANTS DE SÉCURITÉ



Processus MBT_Sec

« Lorsque l'équipement subit un **arrêt/démarrage**, les opérateurs qui souhaitent **administrer l'équipement** doivent de nouveau **s'identifier et s'authentifier**. »

Between reinit and adminOK eventually connexionOK



A = **reinit**
B = **adminOK**
C = **connexionOK**

Formalisation TOCL

OBJECTIFS SCIENTIFIQUES DES TRAVAUX

- Concevoir des techniques de génération automatique de tests, utilisant des méthodes formelles, adaptées pour les composants de sécurité.
- Piloter la génération des tests par des propriétés de sécurité et par des patterns de test, s'appuyant sur une formalisation UML/OCL des comportements applicatifs.

APPROCHE SCIENTIFIQUE

- Exploiter des techniques symboliques pour le calcul des tests et la formalisation des propriétés de sécurité.
- Optimiser des algorithmes de génération automatique de tests.
- Expérimenter sur des composants de sécurité matériels et logiciels en vraie grandeur.

PRINCIPAUX RÉSULTATS ET FAITS MARQUANTS

- La technologie de génération de tests améliore la détection des failles de sécurité.
- Le couplage de plusieurs stratégies de génération assure une forte couverture des besoins de test et des propriétés de sécurité.
- La technologie MBT_Sec via la formalisation TOCL (Temporal OCL) accroît la couverture des tests de sécurité, leur précision et pertinence.

PERSPECTIVES ENVISAGÉES

- Appliquer la démarche à d'autres systèmes sensibles en termes de Cybersécurité.
- Contribuer à la certification des composants par la maîtrise de la couverture des propriétés de sécurité.
- Réaliser une bibliothèque de patterns qui permettra de capitaliser sur des patterns de test de sécurité / vulnérabilité pour capter le savoir métier.

CONTACTS
Smartesting • Bruno LEGEARD • bruno.legeard@smartesting.com
Université de Franche-Comté/FEMTO-ST • Frédéric DADEAU • frederic.dadeau@femto-st.fr

DURÉE DES TRAVAUX
24 mois

PARTENAIRES
Smartesting,
Université de Franche-Comté/FEMTO-ST

BRES - BRIQUE ÉLÉMENTAIRE DE SÉCURITÉ

Oreillette chiffrante
Transmettre la voix en toute confidentialité quel que soit son téléphone

PEA

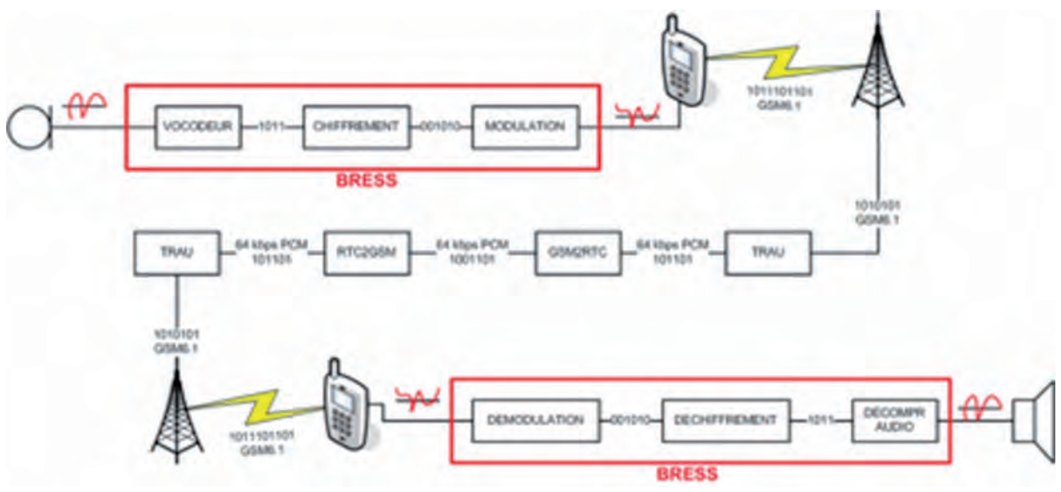


Figure 1 : Description technique de l'oreillette chiffrante

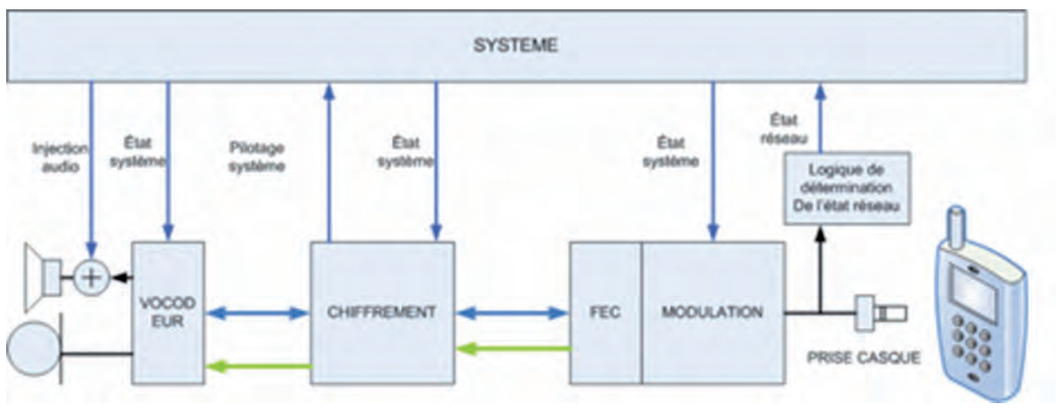


Figure 2 : Architecture de l'oreillette chiffrante

OBJECTIFS SCIENTIFIQUES DES TRAVAUX

Le PEA BRES propose de conduire l'étude et le développement d'un système de chiffrement point à point des communications audio téléphoniques pour les supports de téléphonie courants : GSM, VoIP ou RTC

APPROCHE SCIENTIFIQUE

L'approche générale de ce système est d'utiliser le canal audio comme support d'une modulation numérique, qui elle-même transporte de la phonie numérisée et chiffrée. Cette technologie permet de réaliser une communication chiffrée de point à point indépendamment du téléphone. Le principe d'architecture retenu offre une solution de sécurisation des communications téléphoniques pour les appareils standard du marché.
En plus des aspects chiffrement et implémentation, le transport de la modulation sur le canal audio reste la contrainte majeure : le modem doit inclure un système de variation lente d'amplitude des signaux émis afin de tromper les systèmes de VAD (Voice Activity Detection) des réseaux téléphoniques. Il doit aussi être compatible des dispositifs de contrôle automatique de gain situés sur l'entrée microphone, et sur la sortie haut-parleur des terminaux standards.

PRINCIPAUX RÉSULTATS OBTENUS ET FAITS MARQUANTS

Réalisation d'un démonstrateur logiciel à partir de modules développés et intégrés par Bull TrustWay et Amesys sur une plateforme linux.
La modulation/démodulation se déroule correctement lors de communications :

- mobiles utilisant les codecs EFR, FR, HR, AMR-12.2, AMR-10.2, AMR-7.95, AMR-7.40, AMR-6.70 et AMR-5.90 ;
- VOIP : codec G711µ, G711A et G729 ;
- RTC.

La capacité d'envoyer des données quelconques (voix ou messages texte chiffrés) sur un réseau mobile, RTC ou VOIP est démontrée.
Un flux de paroles traversant toute la chaîne de communication avec ou sans chiffrement reste compréhensible.

PERSPECTIVES ENVISAGÉES

Développement d'un produit pour la protection des communications sur les réseaux téléphoniques.

CONTACT
BULL SAS • René MARTIN • Directeur UO TrustWay

DURÉE DES TRAVAUX
20 mois + 16 mois

PARTENAIRES
BULL/TrustWay, AMESYS

ELVIS - VISUALISATION D'ÉVÈNEMENTS DE SÉCURITÉ

Des informations de renseignement sur-mesure

Thèse

OBJECTIFS SCIENTIFIQUES

Il est aujourd'hui difficile de tirer partie des grandes quantités de données générées dans le cadre de la surveillance défensive des systèmes d'information. Bien que versatiles, les solutions manuelles telles que grep ou wireshark par exemple requièrent un haut niveau d'expertise et sont limitées par la vitesse d'analyse de l'utilisateur. À l'inverse, les solutions totalement automatiques (détection d'intrusion et corrélation d'alertes par exemple) peuvent traiter rapidement de grandes masses de données mais génèrent souvent trop de faux positifs ou laissent passer des attaques. Pire, elles s'adaptent souvent très mal aux situations nouvelles. La visualisation est une approche prometteuse pour reprendre le contrôle des données dans le contexte de la surveillance défensive des systèmes.

APPROCHE SCIENTIFIQUE

Étant donnée la très grande variété des sources de données disponibles, l'approche suivie dans ELVis (Extensible Log Visualization) consiste à pouvoir importer de nombreux types de fichiers de logs et à proposer automatiquement des représentations adéquates en fonction des types des données (ordinales, cardinales, catégorielles, géographiques) des champs que l'utilisateur souhaite voir représenter.

APPLICATIONS

Dans ses missions de surveillance défensive de ses systèmes d'information, la Défense Française collecte automatiquement des quantités importantes de données sur les évènements se déroulant sur ceux-ci. Ces informations portent sur des systèmes très différents les uns des autres et sont donc très diverses en terme de sémantique et de formats. De plus, de nouveaux outils de collecte de données doivent pouvoir être ajoutés de manière opportuniste en fonction des besoins. Pour autant, les informations qu'ils fournissent doivent être facilement exploitables. ELVis permet d'importer des données soumises sous de nombreux formats. Il peut aussi être facilement étendu pour en accepter de nouveaux. Le choix automatique de représentations en fonctions des données que l'utilisteur souhaite analyser lui permet de se focaliser sur sa tâche et son expertise en sécurité des systèmes d'information.

RÉSULTATS

Une implémentation d'ELVis se basant sur les technologies web a été réalisée. Les tests utilisateurs ont montré la validité de l'approche : les représentations automatiquement proposées par ELVis sont pertinentes et permettent aux analystes de détecter rapidement des évènements anormaux symptomatiques d'attaques. Les travaux s'orientent désormais sur des représentations synchronisées d'informations provenant de plusieurs sources de données. Les sources de données partageant certains types d'informations (adresses IP, dates/heures, etc.), il s'agit désormais de permettre à l'analyste de se servir des informations découvertes dans une des sources de données pour explorer plus facilement les autres.

CONTACT

DOCTORANT : Christopher Humphries • christopher.humphries@supelec.fr
Tuteurs : Christophe BIDAN • christophe.bidan@supelec.fr
Frédéric MAJORCZYK • frederic.majorczyk@intradef.gouv.fr, DGA-MI
Nicolas PRIGENT • nicolas.prigent@supelec.fr

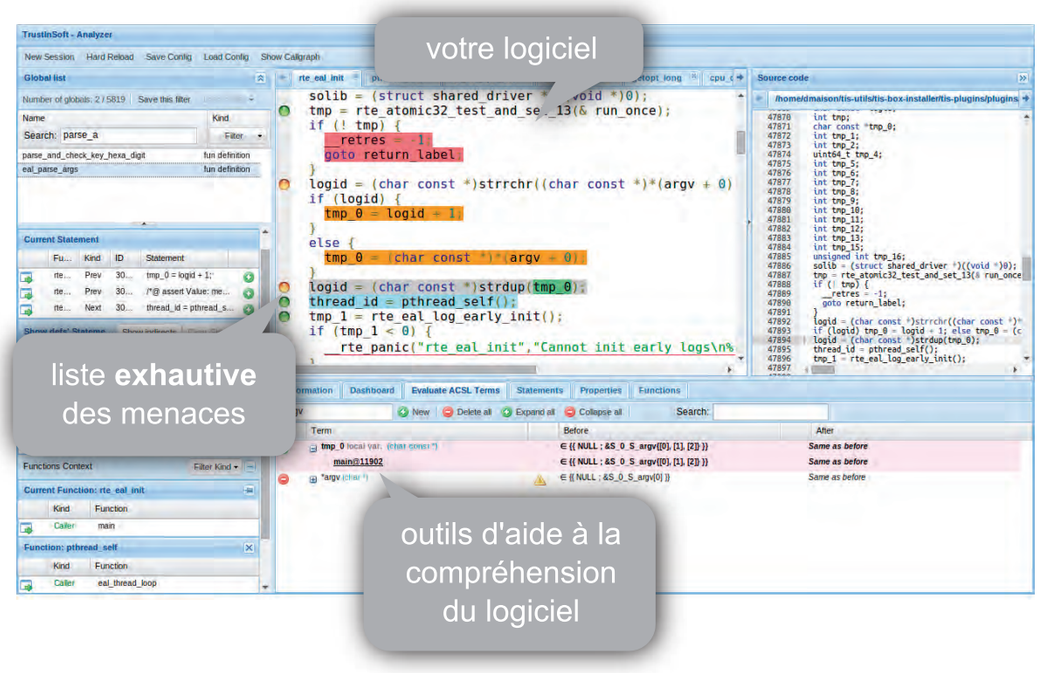
PARTENAIRES

Inria/Université de Rennes 1/CNRS/
Supélec CIDre

Inria
INVENTEURS DU MONDE NUMÉRIQUE

AUROCHS

Sécurité logicielle mathématiquement garantie



Copie d'écran de la technologie développée dans le cadre du projet

OBJECTIFS SCIENTIFIQUES DES TRAVAUX

AUROCHS propose des outils d'analyse de logiciel qui répondent aux attentes du monde de la défense concernant la robustesse des systèmes d'information et leur cyber-défense.

APPROCHE SCIENTIFIQUE

Dans le cadre du projet AUROCHS, des outils mathématiques logiciel d'analyse de logiciel sont développés et testés sur des composants sensibles : ces outils apportent des garanties de fiabilité et d'absence de failles de sécurité.
La technologie repose sur une collaboration efficace de méthodes mathématiques ayant déjà fait leurs preuves : l'interprétation abstraite et le calcul de plus faible préconditions.

PRINCIPAUX RÉSULTATS ET FAITS MARQUANTS

Les outils développés dans AUROCHS permettent de garantir mathématiquement que les systèmes analysés sont immunisés contre les familles de cyber-attaques les plus fréquentes.

PERSPECTIVES ENVISAGÉES

Les technologies développées dans le cadre du projet ont une portée duale, les attaques logicielles concernant aussi bien le domaine militaire que le domaine civil. Les principaux secteurs concernés sont l'aéronautique, les télécommunications, le nucléaire, le ferroviaire, la banque, la santé, le spatial.
Les technologies d'AUROCHS sont déjà déployées dans plusieurs de ces secteurs.

CONTACT
TrustInSoft • Fabrice DEREPAS • fabrice.derepas@trust-in-soft.com • Tél. +33 (0) 6 51 70 36 77

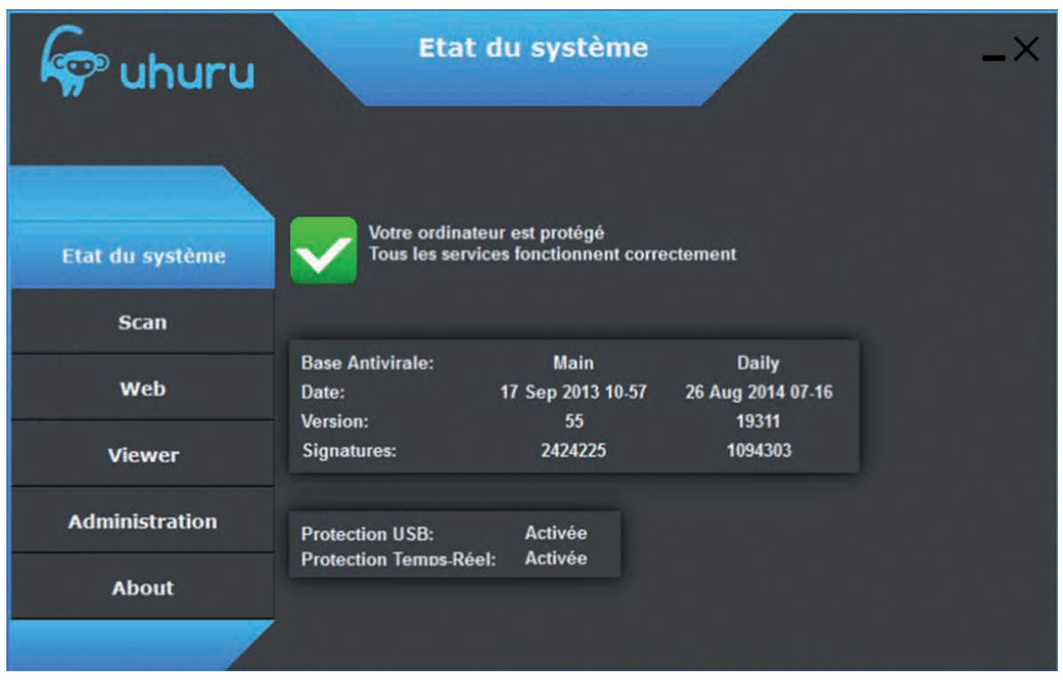
DURÉE DES TRAVAUX
30 mois

PARTENAIRES
CEA List, TrustInSoft

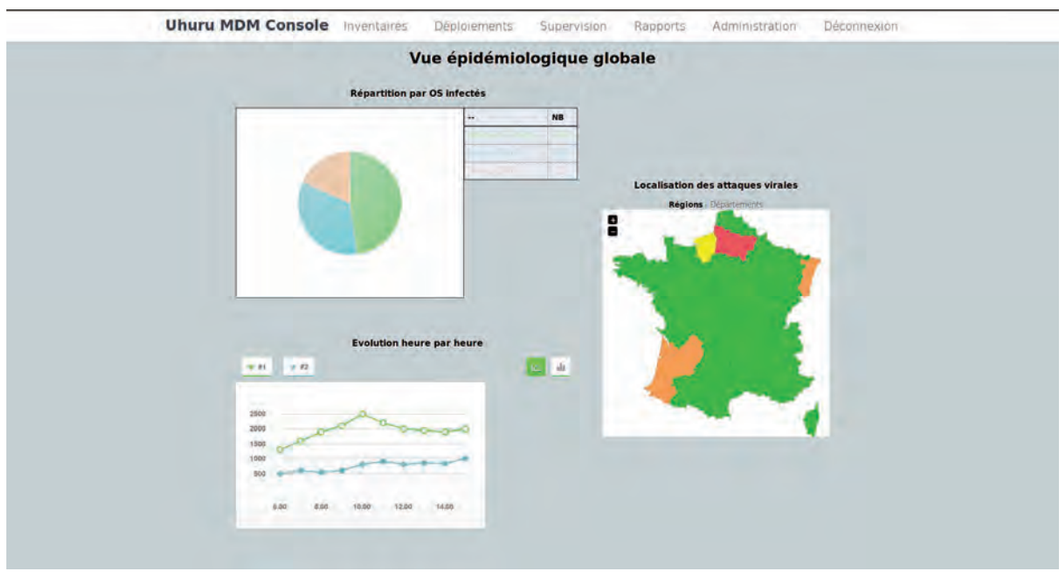
DAVFI - UHURU

Antivirus de nouvelle génération et solution mobile sécurisée

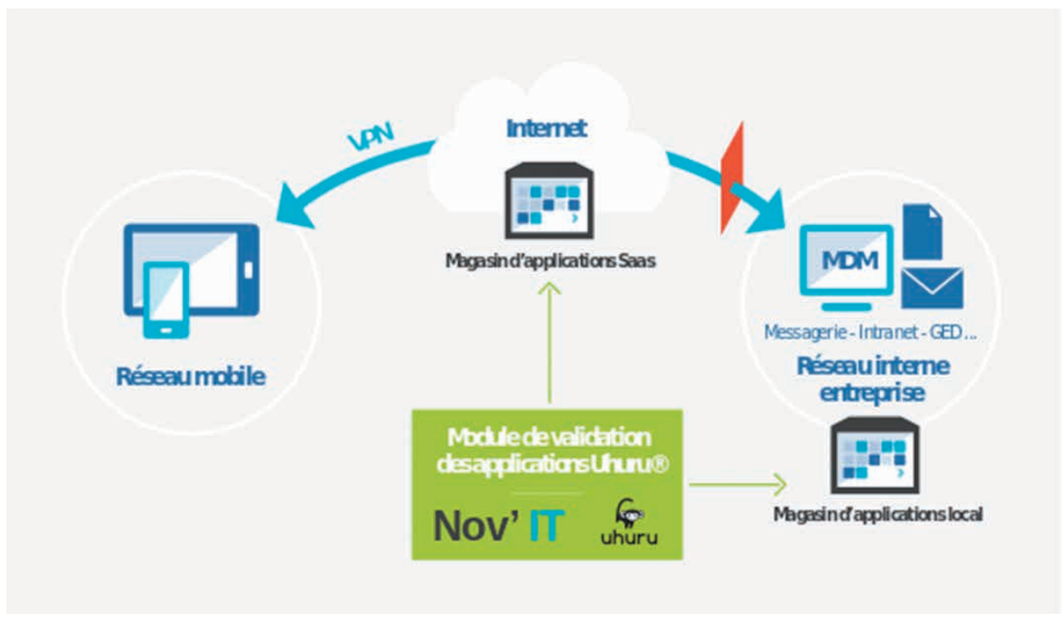
PIA



Copie d'écran du logiciel antivirus



Console centrale



Architecture Uhuru Mobile

OBJECTIFS SCIENTIFIQUES DES TRAVAUX

DAVFI / Uhuru a pour objectif de proposer une approche scientifique et technique nouvelle dans la lutte contre les codes malveillants (virus) et d'apporter des réponses innovantes et de confiance pour la mobilité sécurisée.

Partie antivirus

DAVFI / Uhuru Antivirus permet de lutter contre les codes malveillants, et en particulier les codes inconnus.

Partie mobilité sécurisée

DAVFI / Uhuru Mobile apporte une solution complète intégrant :

- un système d'exploitation durci (base Android) pour les derniers téléphones/tablettes du marché offrant une protection contre les attaques physiques et logiques ;
- un magasin d'applications privé par entité (administration ou entreprise) ;
- des outils de validation d'applications ;
- une console centrale pour le management (MDM) ;
- des applications de chiffrement de la voix, des données et des SMS.

APPROCHE SCIENTIFIQUE

Les principales contraintes ont été respectées :

- la détection de codes d'attaque inconnus ;
- la résistance à des attaques visant à réprimer les outils ;
- la performance quant à la rapidité de traitement et d'analyse.

PRINCIPAUX RÉSULTATS ET FAITS MARQUANTS

Partie Antivirus

Un taux de détection des codes inconnus supérieur à 98 % et une rapidité de traitement et d'analyse bien au delà des résultats des solutions actuelles.

Partie mobilité sécurisée

Une solution complète prête à être commercialisée avant la fin du projet de R&D (démonstrateur livré avec une année d'avance).

PERSPECTIVES ENVISAGÉES

Partie Antivirus

- Sécurisation des postes de travail et des serveurs des administrations et des entreprises
- Déploiement clé dans une Administration française

Partie mobilité sécurisée

- Réponse en direct à des besoins interministériels
- Fourniture du socle technique pour des partenaires souhaitant intégrer leurs propres développements applicatifs dans un environnement sécurisé (accords OEM)

CONTACT

Nov'IT • Jérôme NOTIN • j.notin@nov-it.fr • Tél. : +33 (0) 7 77 83 75 41

Nov'IT uhuru

DURÉE DES TRAVAUX

24 mois

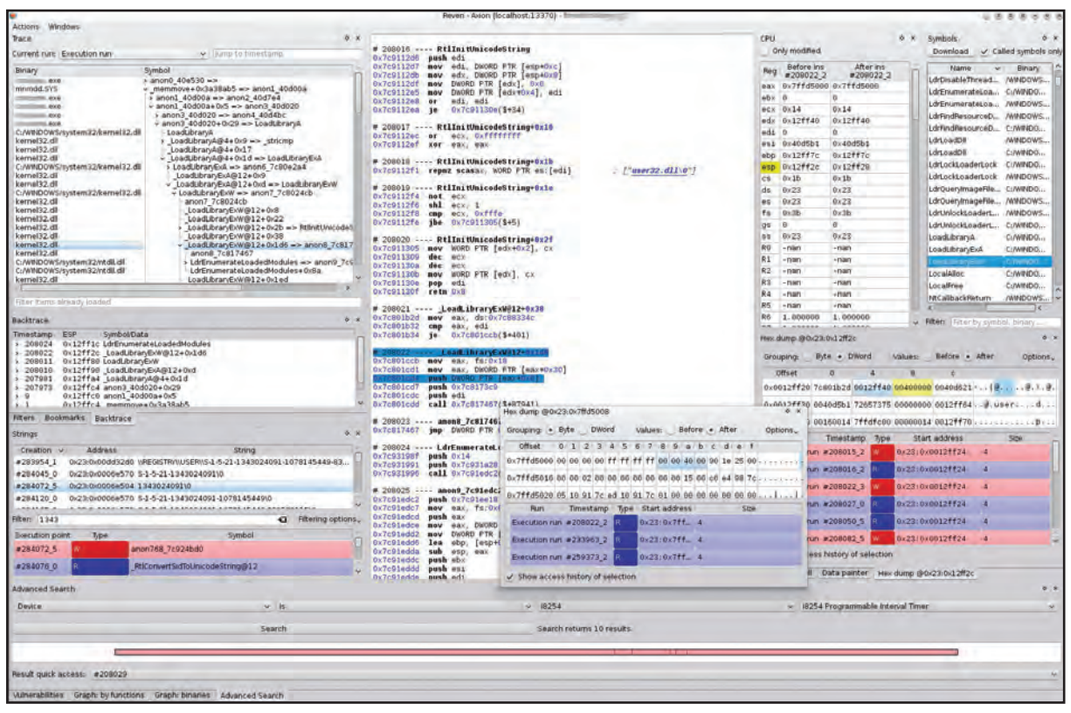
De octobre 2012 à octobre 2014

PARTENAIRES

ESIEA, Qosmos, Teclib', Nov'IT (Chef de file)

REPER - EVEN PERFORMANCES

Tester la vulnérabilité de tout logiciel



Interface Reven axion

Interface Reven report

OBJECTIFS TECHNOLOGIQUES DU PROJET

- Augmenter significativement la vitesse de traitement du moteur REVEN pour analyser des systèmes logiciels complets (OS + Drivers + Middleware + Applications) en un temps opérationnel.
- Parallélisation du CPU Symbolique REVEN en vue de son utilisation sur une ferme de serveurs.

Le moteur d'analyse REVEN est un CPU symbolique qui simule un CPU numérique physique (type x86 actuellement). Il analyse des logiciels de manière statique, dynamique ou hybride, apportant une vision très précise de ce que ferait réellement le CPU numérique s'il exécutait ces logiciels (Reverse-Engineering).
Il détecte des bugs/failles 'nano-level', liées à l'utilisation de ressources matérielles/logicielles critiques.
L'analyse peut être pilotée par des algorithmes automatisés et des ingénieurs, en mode collaboratif et distribué. REVEN dispose d'une API Python/C++ pour l'étendre via des plugins (nouveaux widgets et algorithmes).

INNOVATIONS DÉVELOPPÉES PAR LE PROJET ET RÉSULTATS OBTENUS

- Multiplication par 40 sur la vitesse brute d'un CPU REVEN (08/2014 vs 01/2014).
- Création d'un nouveau procédé de parallélisation d'analyse (brevet déposé).

EN COURS :

- Implémentation du framework de parallélisation de l'analyse par REVEN pour distribution de l'analyse sur une ferme de serveurs.

APPLICATIONS MARCHÉS

De manière générale, toute analyse de logiciel dont on ne dispose pas des codes sources, ou dont on voudrait chercher les vulnérabilités de manière préventive avec les mêmes armes qu'un attaquant potentiel.

Applications marché défense

- *Reverse-engineering* approfondi de logiciels malveillants.
- Amélioration de la qualité des développements internes (fiabilité, résistance aux outils de *reverse-engineering* traditionnels).
- Validation qualité/fiabilité/sécurité des développements tiers (achats sur étagère ou sous-traitance).

Applications marché civil

- Réduction des coûts et augmentation du niveau de QA sur développements de logiciels critiques.
- Validation qualité des développements tiers (achats sur étagère ou sous-traitance).
- Sûreté de fonctionnement.
- Certifications, audits, etc.

CONTACT
Frédéric MARMOND • Président / Directeur R&D • fmarmond@tetrane.com • Tél. +33 (0)3 39 25 00 45

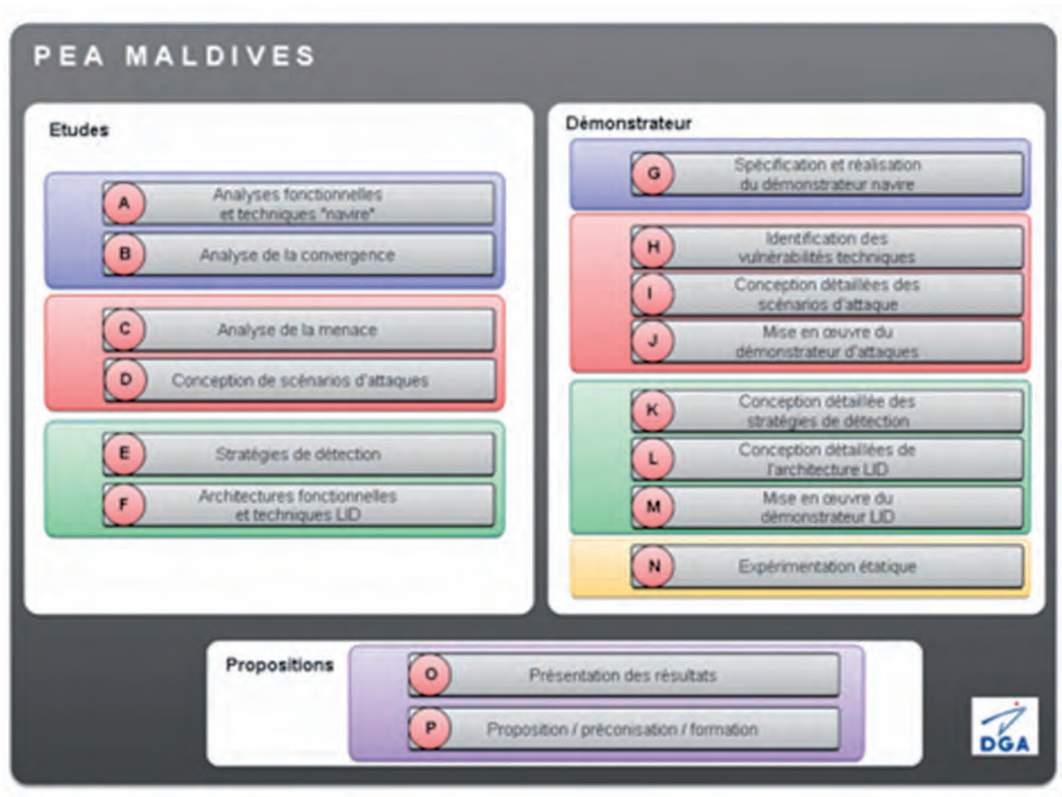
DURÉE DES TRAVAUX
18 mois
De septembre 2013 à mars 2015

MALDIVES - MENACES, ANALYSE ET DÉTECTION D'INTRUSION POUR LES NAVIRES

Étude et proposition de mise en œuvre de capacités de lutte informatique défensive à bord des navires

PEA

Frégate FREMM et environnement naval



Structuration du PEA MALDIVES

OBJECTIFS SCIENTIFIQUES DES TRAVAUX

Après une analyse de risque Cyber des navires militaires, l'objectif consiste à définir les différentes stratégies de détection possibles et les architectures techniques et fonctionnelles nécessaires et adaptées pour la lutte informatique défensive (LID).

Le projet se décompose en trois phases :

- Études Cyber (analyse de la menace, stratégie de détection).
- Réalisation et exploitation des solutions de LID sur le démonstrateur navire via des Cyberattaques issues de la phase étude.
- Proposition de solutions LID pour navires de la Marine Nationale.

APPROCHE SCIENTIFIQUE

←Le PEA MALDIVES est basé sur les activités « structuration » décrites ci-contre.:

PRINCIPAUX RÉSULTATS OBTENUS ET FAITS MARQUANTS

Travaux en cours et classifiés, T0= Mars 2014

J1 : Aout 2014 : Analyse fonctionnelle et technique du navire armé

PERSPECTIVES ENVISAGÉES

À l'issue du PEA, un modèle de solution de lutte informatique défensive aura été évalué sur un démonstrateur navire.
Sur cette base, des principes de développement seront proposés afin d'intégrer la LID à bord des navires.

CONTACTS

DGA • Marie-Thérèse ANDRE - Responsable Laboratoire LID • David GOUYA - Expert CyberDéfense
DCNS • Laurent COMTE - Responsable du service SSI • laurent.comte@dcnsgroup.com

DURÉE DES TRAVAUX

24 mois

PARTENAIRES

Maître d'œuvre : DCNS
Relations avec la chaire de Cyberdéfense des systèmes navals de l'Ecole Naval