Equipe « Sécurité, Fiabilité, Intégrité, de l'Information et des Systèmes »

LUSSI

et

CNRS (Lab - STICC)

Equipe SFIIS – Les membres

Nora Cuppens

Frederic Cuppens

Caroline Fontaine

Jean-Marc Le Caillec

Didier Gueriot

Basel Solaiman

Ingénieurs de Recherche

Fabien Autrel
Sabir Idrees
Pierre Konopacki
Samiha Ayed
Benjamin Justus
Said Oulmakhzoune

Chercheurs associés

Johan Barbier
Eloi Bosse
Florence Dupuis
Benoît Zerr
Riadh Abdelfattah
Luc Pigeon
Sylvie Daniel
Karim Ettabaa
Ali Hamie

33 Doctorants

Contact : Frederic.cuppens@telecom-bretagne.eu

TELECOM Bretagne

Problématique

Administration

Politique de Sécurité

Gestion Conflits

Analyse de Risques

Réaction Réflexe

Détection d'Intrusions

Déploiement

Gestion Anomalies

Architecture de Sécurité

Le Système

Anomalies

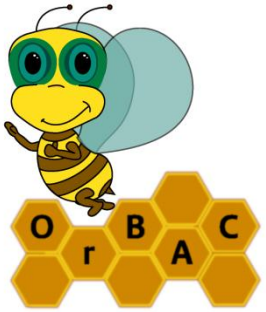
MAJ

Attaques

Contenu technique

- **Exigences de sécurité**
  - Confidentialité, Intégrité, Disponibilité
  - Authentification
  - Droit d'Auteur, Traçabilité
- **Expression de politiques de sécurité**
  - Gestion des identités
  - Contrôle d'accès et d'usage (OrBAC)
  - Contrôle de flux
  - Interopérabilité et négociation
  - Gestion de la confiance
- **Déploiement et configuration**
  - Réseau (Ipv6, ad-hoc, capteur, …)
  - Système (SE-Linux, SGBD, XML, …)
  - Service (Service webs, workflow, …)
- **Supervision**
  - Détection et corrélation
  - Diagnostic et évaluation d'impact
  - Réaction et contre-mesures
- **Test, validation et preuve**
  - Model-checking
  - Machines B
  - Logique modale
- **Prototypes**
  - MotOrBAC (Policy Management)
  - Protekto (IAM)
  - XENA (Interoperability and négotiation)
  - fQuery (Security by query transformation)
  - MIRAGE (Misconfig. Management)
  - CRIM (Correlation)
  - Artemis (Zero-Day Detection)

Autorisation / Obligation



- **OrBAC**
  - Organization Based Access Control
  - www.orbac.org
- **Implantation du prototype MotOrBAC**
  - Version open source sur sourceforge.net
  - Spécification, analyse, simulation, administration et déploiement de politiques de sécurité
- **Travaux en cours**
  - Obligations avec délai (gestion des conflits potentiels)
  - Intéropérabilité et négociation de politiques (O2O)
  - Contrôle a posteriori
  - Policy mining

Vie privée et protection des données externalisées

- **Sécurité par réécriture de requêtes**
  - fQuery : réécriture de requêtes SPARQL (consultation et mise à jour)
  - Application à un médiateur de requêtes
- **Amélioration des techniques de searchable encryption**
  - Recherche optimisée de mots-clés dans des documents chiffrés
  - Recherche d'expression booléenne
  - Evaluation de requêtes booléennes
- **Fragmentation et tatouage de bases de données**
  - Protection des associations sensibles
  - Traçabilité des données
- **Applications**
  - Cloud computing
  - Big Data

Identity and Access Management

- **Gestion d'identité globale basée sur SSO**
- **Authentification dynamique**
  - Authentification dynamique SAML / OpenID
  - Serveur d'identités DINEPO
- **Profil OrBAC de XACML**
- **Réalisations**
  - Serveur d'identités DINEPO
  - Plateforme d'IAM PROTEKTO

Déploiement de politiques de sécurité

- **Processus de raffinement/configuration**
  - Configuration des composants d'une architecture de sécurité mise en place par les RSSI.
- **Intégration de la sécurité dans des applications existantes**
  - Tissage d'aspects (Aspect Oriented Programming)
- **Détection des anomalies intra et inter composants**
  - Firewall stateless et stateful, VPN, Détection d'intrusion
- **Applications**
  - Web services
  - Filtrage réseau
  - Réseaux ad-hoc, réseaux de capteurs

Supervision et détection d'intrusion

- **Nouvelle approche pour la corrélation d'alertes**
  - Corrélation semi-explicite
  - Reconnaissance de nouveaux scénarios d'attaques
  - Diagnostic et reconnaissance d'intention
- **Basée sur une modélisation logique des attaques**
  - Langage LAMBDA
- **Fonctionnalités implantée dans CRIM**
  - Corrélation et Reconnaissance d'Intentions Malveillantes
- **Réaction automatique**
  - Anti-corrélation pour bloquer l'attaquant
  - Analyse de dépendances et mesure d'impact pour déterminer la réaction adéquate
- **Attaques complexes et planification des réactions**

CRIM
Cooperation and Recognition of Malevolent Intentions

Equipe SFIIS – Principaux projets

Projet Européen
FP7 DEMONS

Objet : Détection et réaction à des attaques distribuées et coordonnées
Contribution : négociation de la confiance et protection de la vie privée
Principaux partenaires : Telefonica, NEC, Hitachi, France Telecom, Deutsche Telekom, ETH Zürich, Telecom AG.

Projet Européen FP7
INTER-TRUST

Objet : Infrastructure interopérable de confiance
Contribution : Modélisation et déploiement de politiques de sécurité d'interopérabilité
Principaux partenaires : Softeco, Montimage, SCYTL, INDRA, Search-Lab, Universités de Reading, Malaga, Tarragone et Murcia

---

Projet Européen
ITEA2 Predykot

Objet : Maintien d'un système en condition de sécurité
Contribution : Langage de raisonnement pour le redéploiement contextuel de politiques de sécurité
Principaux partenaires : Evidian, Cassidian, Thales, Gémalto, C2Tech, Nextel, Intelligence Power, VTT, Universités Paul Sabatier, de Créteil et d'Oulou.

Projet Européen
ITEA2 ADAX

Objet : Détection d'attaques et simulation de contre-mesures
Contribution : Combinaison d'attaques et contre-mesures coordonnées
Principaux partenaires : Cassidian, Netasq, 6cure,. RTCO, AVEA, Bogazici

---

Projet ANR
PAIRSE

Objet : Préservation des confidentialités dans les Services Web
Contribution : réécriture de requêtes d'accès pour préserver la vie privée
Partenaires : LIRIS, IRIT, SWID, SEMSOFT, Lyon 1, MTIC