Notice des titres et travaux scientitiques

Thibault CHOLEZ

Septembre 2016

Sommaire

1 Curriculum Vitae

Docteur et Ingénieur en informatique

Sujet de recherche : Supervision et Analyse des réseaux informatiques

1.1 Informations pratiques

État civil

Thibault CHOLEZ
Né le 15 septembre 1984
Nationalité française
Marié

Emploi

Maître de Conférences à l'Université de Lorraine
Laboratoire : LORIA (UMR 7503 : UL, CNRS, INRIA)
Composante d'enseignement : TELECOM Nancy
NUMEN : 12S1300904FKR

Coordonnées professionnelles

LORIA / INRIA Nancy-Grand Est
615 Rue du Jardin Botanique
54600 Villers-lès-Nancy, FRANCE
Bureau B136 (03 83 59 20 53)

TELECOM Nancy
193 Avenue Paul Muller
54602 Villers-lès-Nancy, FRANCE
Bureau 2.7 (03 83 68 26 70)

Courriel : thibault.cholez@loria.fr
Site web : http://thibault.cholez.free.fr

1.2 Études supérieures

Juin 2011 : Diplôme de Doctorat en informatique de l'Université Henri Poincaré (Nancy1), *"Supervision des réseaux pair à pair structurés appliquée à la sécurité des contenus"*, Laboratoire LORIA (UMR 7503), Nancy, France

Composition du jury

- Président : Claude Godart, Professeur à l'ESSTIN, Université Henri Poincaré
- Rapporteurs :
  - Matthieu Latapy, Directeur de recherche CNRS au LIP6
  - Ludovic Mé, Professeur à Supélec-Rennes
- Examinateurs :
  - Ernst Biersack, Professeur à EURECOM
  - Isabelle Chrisment, Professeur à l'ESIAL, Université Henri Poincaré
  - Olivier Festor, Directeur de recherche à l'INRIA Nancy-Grand Est
- Invité : Guillaume Doyen, Maître de conférences à l'UTT

Juin 2007 : Diplôme de Master recherche en informatique de l'Université Henri Poincaré, spécialité SDRC (Services Distribués et Réseaux de Communication), Nancy, France

- Connaissances avancées en réseaux et systèmes distribués (routage, sécurité, cohérence et réplication des données, services web, etc.)
- Sujet de stage : Conception de mécanismes de révocation dans les réseaux dynamiques

Juin 2007 : Diplôme d'Ingénieur ESIAL (devenu **TELECOM Nancy**), spécialité TRS (Télécom, Réseaux et Systèmes), Nancy, France

- École publique habilitée par la Commission des Titres d'Ingénieur et spécialisée en informatique
- Projet Industriel avec Orange Labs : Conception et implantation d'une architecture sécurisée et évolutive de honeypots distribués pour la capture de malwares

1.3 Expérience professionnelle

Depuis Septembre 2013 : Maître de Conférences à l'Université de Lorraine, Nancy, France.

- Activités d'enseignement réalisées à TELECOM Nancy, école d'ingénieur en informatique affiliée à l'Institut Mines-Télécom et au collégium Lorraine INP.
- Activités de recherche réalisées dans l'EPC (équipe projet commune) MADYNES du laboratoire LORIA (Laboratoire lorrain de Recherche en Informatique et ses Applications, UMR 7503 (UL, CNRS, INRIA)).

Septembre 2011 - Septembre 2013 : Chercheur Post-doctorant au centre de recherche SnT (Interdisciplinary Centre for Security, Reliability and Trust) de l'Université du Luxembourg, Ville de Luxembourg, Luxembourg.
Sujet : Supervision et sécurité des réseaux (Content-Centric Networking, P2P, IPv6) dans le cadre de l'Internet des Objets. Impliqué dans deux projets de R&D européens (BUTLER et IoT6) du FP7 ; participation aux enseignements de l'Université.

Janvier 2011 - Août 2011 : Chercheur Post-doctorant à l'UTT (Université de Technologie de Troyes), équipe ERA (Environnement de Réseaux Autonomes), Troyes, France.
Sujet : Détection des nœuds malveillants pour la sécurité des systèmes distribués. Impliqué dans le projet de recherche CNRS-GIS ACDAP2P ; participation aux enseignements de l'Université.

Octobre 2007 - Décembre 2010 : Doctorant financé par l'INRIA (Institut National de Recherche en Informatique et Automatique), équipe MADYNES (Management of Dynamic Networks and Services), LORIA, Nancy, France
Sujet : Supervision des Réseaux Pair à Pair Structurés Appliquée à la Sécurité des Contenus. Impliqué dans le projet de recherche ANR MAPE.

2 Activités de recherche et d'enseignement

2.1 Activités d'enseignement

2.1.1 Résumé des services d'enseignement à TELECOM Nancy

Maître de conférences depuis septembre 2013, je réalise chaque année un service d'enseignement à TELECOM Nancy et m'implique dans les activités pédagogiques nécessaires au bon fonctionnement de cette formation d'ingénieur. Le Tableau 1 ci-dessous liste les heures d'enseignement (en équivalent TD) que j'ai dispensées à TELECOM Nancy dans les différents modules où je suis intervenu.

Module	Rôle	Niveau	13-14	14-15	15-16
TOP	R[1]	1A[2]	54H	44H	44H
RSI	R	1A	26H	71H	22H
CSH	R	1A	22H	41H	43H
PFSI	I	1A	16H	-	-
POO	I	1A	34H	27H	35H
BDD	I	1A	54H	30H	-
OCI	R	2A	10H	32H	8H
ASR	R	2A	-	8H	-
AMIO	R	3A	-	23H	44H
Encadrement	-	-	42H	72H	106H
Service	-	-	258H	348H	302H

TABLE 1 – Services d'enseignement à TELECOM Nancy

Modules enseignés

- TOP : Techniques et Outils pour Programmer (complexité algorithmique, preuves d'algorithmes, récursivité, dérécursivation, backtracking, couverture de tests, etc.) ;
- RSI : Réseaux et Services Internet (modèle OSI, architectures réseau, fonctionnement des principaux protocoles (ethernet, IP, TCP, ICMP, HTTP, DNS), contrôle de congestion TCP, programmation socket C, etc.) ;
- CSH : Langage C (syntaxe, pointeurs, structures, gestion mémoire, makefile, gdb, valgrind, etc.) et Shell (langage bash, principales commandes et gestions des droits UNIX, expressions rationnelles (grep, sed), etc.) ;
- PFSI : Principes Fondamentaux des Systèmes Informatiques (modes d'adressages, structure d'un programme en mémoire, programmation assembleur, etc.) ;
- POO : Programmation Orientée Objet (langage JAVA, modélisation objet, héritage, liaison dynamique, gestion des exceptions, etc.) ;
- BDD : Bases de données (conception, modèle entité-association, modèle relationnel, algèbre relationnel, formes normales, SQL, PL/SQL, etc.) ;
- OCI : Objets Connectés Intelligents (langage C++, multitâche coopératif, programmation de capteurs sans fil (contiki OS), etc.) ;
- ASR : Administration Réseau et Système (configuration et outils réseau sous GNU-Linux, installation et configuration de serveurs web, mail, DNS, SSH) ;

1. R : Responsable du module ; I : Intervenant
2. 1A : 1ère année (niveau L3) ; 2A : 2ème année (niveau M1) ; 3A : 3ème année (niveau M2)

— AMIO : Applications Mobiles et Internet des Objets (programmation Android, programmation de capteurs sans fil (contiki OS), protocoles de l'IoT (802.15.4, 6lowpan, COAP), etc.).

Une description plus précise du contenu de chaque module est disponible dans les livrets de l'élève de TELECOM Nancy, détaillant le programme pédagogique de l'école pour la formation initiale et la formation par apprentissage.

Activités d'encadrement

Les heures d'encadrement indiquées à la fin du Tableau 1 correspondent aux activités suivantes :

— Suivi académique d'apprentis ingénieurs sur les trois années ;
— Suivi de stages de deuxième et de troisième année ;
— Suivi de projets industriels de troisième année ;
— Encadrement de projets d'initiation à la recherche.

2.1.2 Implication dans la vie de l'école

Outre mes activités d'enseignement et d'encadrement à TELECOM Nancy, j'exerce des responsabilités collectives au sein de l'école et suis impliqué dans des activités d'innovation en lien avec les enseignements que je dispense.

Activités d'innovation

Mise en place de plate-formes pédagogiques pour l'expérimentation et l'innovation au sein de l'école :

— Plate-forme **TELECOM Nancy Sensor Living Lab** sur le thème des réseaux de capteurs sans fil et de l'Internet des Objets : déploiement d'un réseau de 30 capteurs TelosB dans le bâtiment de l'école et exposant les informations relevées (température, humidité, luminosité, énergie, topologie réseau) via une API ouverte aux étudiants.
— Plate-forme **Sencity** sur le thème des voitures connectées et de la ville intelligente : voiture électrique instrumentée par divers capteurs (caméras, télédétection par laser, GPS, antenne wifi, port OBD, capteurs de qualité de l'air, IMU, etc.) acquis en temps réels via ROS et pouvant effectuer des mesures à l'échelle de la ville. Cette plateforme est intégrée au projet « Lorraine Smart Cities Living Lab ».

Réalisation de projets d'innovation en lien avec les partenaires de l'école :

— En partenariat avec l'**École nationale supérieure d'architecture de Nancy** (Ensan), dans le cadre du projet AALUM (Animations participatives des Architectures de la LUMière) du CityLedLab : conception et réalisation d'une application web pour smartphone ainsi que d'une infrastructure de commande de LEDs (via le protocole DMX) permettant de contrôler en temps réel et de manière collaborative une infrastructure l'illumination d'un bâtiment.
— En partenariat avec l'Office d'Hygiène Sociale (OHS) et l'Institut Mines-Telecom : conception, réalisation et déploiement de la **plate-forme Info-Autonomie**, constituée d'un réseau de capteurs sans fil et d'une application graphique, et permettant d'observer dans le temps le niveau d'autonomie de personnes handicapées hébergées dans un appartement instrumenté de l'EVA (École de la Vie Autonome).

Responsabilités collectives

— Membre du conseil pédagogique de la filière par apprentissage ;
— Membre du jury de recrutement de la filière par apprentissage ;

— Rédacteur pour le concours Mines-Télécom, épreuve d'aptitude aux sciences du numérique ;
— Examinateur aux oraux de recrutement ;
— Responsable du stand R&D aux journées porte ouverte (présentation des activités de R&D à travers les projets, les plateformes et les laboratoires de recherche partenaires de l'école) ;
— Président de jury de BAC (2014) et BTS (2015).

2.1.3 Autres activités d'enseignement

Cours invités

J'ai été invité à donner quelques heures de cours en dehors de l'Université de Lorraine sur des sujets très spécifiques qui sont directement en lien avec mes travaux de recherche, à savoir :

— Un cours donné annuellement à l'**Université de Technologie de Troyes** sur les méthodes de supervision des réseaux P2P, à l'attention des gendarmes de la Licence Professionnelle « Enquêteur Technologies Numériques » (2h CM et 2h TP).
— Un cours donné à l'**École polytechnique fédérale de Zurich** sur la sécurité des réseaux P2P pour des étudiants de Master 2 du département informatique (3h CM en 2013).

Précédentes vacations

J'ai réalisé plusieurs vacations afin de participer aux enseignements des universités m'ayant accueillies lors de mes postdoctorats, à savoir :

— Module **Sécurité des réseaux et des systèmes** (20h par an, années 2011/2012 et 2012/2013) pour les élèves en L3 Telecom à l'Université du Luxembourg : cours sur les politiques de sécurité et les pare-feux, network forensic (analyse de traces d'attaques et découverte de preuves), configuration de pare-feu sous GNU Linux (iptables), sécurité des protocoles de VOIP (SIP, RTP) par analyse d'attaques.
— Module **Services réseau** (34h, année 2010/2011) pour des élèves ingénieurs (niveau M1-M2) à l'UTT : configuration de réseaux (routeur, switch, VLAN et postes terminaux) et mise en œuvre de services réseau (SSH, résolution de noms (DNS), service d'annuaire (LDAP), supervision d'équipements (SNMP), virtualisation (Xen) et cloud computing (Hadoop)).

2.2 Activités de recherche

2.2.1 Travaux en cours

Contexte et problématiques

Les récents développements d'internet ont conduit à l'émergence de plusieurs tendances de fond qui sont à l'origine de nouveaux défis quant à la supervision, la sécurité et les performances des réseaux informatiques. Mes travaux de recherche visent à répondre à ces différents défis.

Tout d'abord, **le chiffrement des communications** a récemment connu une croissance sans précédent, passant de 5% du trafic en 2012 à plus de 50 % en 2015 [3]. Ce recours massif au chiffrement rend caduque les techniques de supervision précises des communications (Deep Packet Inspection), faisant perdre aux opérateurs et aux administrateurs de réseaux la connaissance des informations transitant. Alors que certaines méthodes déchiffrent le trafic (proxy HTTPS), violant ainsi la vie privée des utilisateurs, je travaille sur l'élaboration de solutions de supervision respectant la vie privée tout en offrant un niveau d'information permettant l'analyse.

Ensuite, le principal usage d'internet a évolué vers la **diffusion massive de contenus** (vidéos en streaming, etc.). Initialement conçus pour envoyer des tâches sur des serveurs distants, les principaux protocoles d'internet sont aujourd'hui inadaptés à sa principale utilisation, ce qui pose des problèmes de performances partiellement compensés par le recours aux Content-Delivery Networks. Pour pallier ce problème, de nouvelles architectures de réseaux centrés sur les contenus (Information-Centric Networking) proposent un changement de paradigme en adressant les contenus plutôt que les machines à l'échelle d'internet afin d'optimiser la diffusion de l'information, et visent à long terme à offrir une alternative à TCP/IP. Certaines solutions comme Named-Data Networking, qui fédère la majorité des recherches académiques sur ce sujet, deviennent progressivement fonctionnelles. Dans ce contexte, je m'intéresse aux verrous technologiques empêchant le déploiement de tels protocoles, en particulier en étudiant leurs performances, leur sécurité, leur interconnexion avec les protocoles actuels et les stratégies de déploiement possibles, notamment en ayant recours à la virtualisation de fonctions réseau (Network Function Virtualization).

Enfin, **la multiplication des acteurs** fait qu'il est de plus en plus difficile d'identifier ceux responsables d'une dégradation de la QoS ou de la QoE des services réseau. En effet, les sites web modernes sollicitent l'accès à de multiples contenus tiers au sein d'une même page, notamment pour diffuser de la publicité. Je m'intéresse ainsi à la mesure de l'impact de la publicité sur la QoS lors de la navigation sur le web.

Supervision du trafic web chiffré (HTTPS)

- Contexte : co-encadrement de la thèse de de M. Wazen Shbair
- Projet CNRS PEPS NEFAE
- Publications : [4–6]
- Constatant qu'une nouvelle technique de filtrage du trafic HTTPS basée sur l'observation du champ SNI de TLS a récemment été implantée dans de nombreux logiciels de type pare-feu, nous avons évalué cette technique est montré que celle-ci n'est pas fiable. Deux failles, l'une basée sur la rétrocompatibilité de TLS, l'autre sur les certificats partagés entre domaines permettent de contourner facilement cette détection [6]. Nous avons ainsi réalisé un logiciel, Escape, démontrant ces faiblesses et évalué que 92% [4] des sites web HTTPS sont accessibles tout en

3. Rapport 2015-0832 de l'ARCEP : www.arcep.fr/uploads/tx_gsavis/15-0832.pdf

permettant d'échapper à cette supervision. Nous avons également proposé une méthode permettant de détecter les tentatives de contournement grâce à un service DNS de confiance. D'un autre côté, les techniques classiques de supervision des flux chiffrés offrent une granularité soit trop grossière (identification du protocole : HTTPS, SSH, etc.), soit trop précise (identification d'une page web parmi un site). Nous avons alors conçu une nouvelle méthode capable d'identifier les services accédés par HTTPS tout en respectant la vie privée des utilisateurs (aucun déchiffrement). Celle-ci ne repose pas sur des champs spécifiques mais sur les caractéristiques du trafic qui sont analysés par un processus d'apprentissage supervisé à plusieurs niveaux et permet l'identification des services avec une précision élevée [5]. Nous travaillons actuellement dans le cadre du projet CNRS NEFAE pour permettre ce traitement en temps réel.

Virtualisation réseau pour le déploiement de l'architecture Named-Data Networking

- Contexte : co-encadrement de la thèse de M. Xavier Marchal
- Projet ANR DOCTOR
- Publications : [3, 7, 21, 22]
- Les ICN sont des architectures réseau prometteuses pour le futur d'internet mais leur déploiement à grande échelle fait face à de nombreux verrous technologiques et économiques. Dans le cadre du projet ANR DOCTOR, nous travaillons à l'élaboration d'une infrastructure virtualisée permettant un déploiement progressif du protocole NDN [7] tout en répondant aux critères de sécurité, de performances, de gestion du réseau et d'interconnexion avec les protocoles actuels. Nous avons ainsi identifié une vulnérabilité critique dans les spécifications du protocole permettant de réaliser facilement des attaques DoS [21], et nous avons proposé des corrections. Concernant les performances, nous avons créé un outil de mesure similaire à Iperf, Ndnperf [3], et identifié les facteurs limitant le débit des services temps-réel (live streaming, VOIP, etc.). Nous avons également conçu et réalisé une passerelle HTTP/NDN permettant de faire transiter des contenus web sur un réseau NDN, bénéficiant ainsi de l'agrégation des requêtes et du cache, le tout de manière transparente pour le client et le serveur [22]. Ces trois contributions furent publiées et présentées dans la conférence de référence du domaine : ACM ICN. La suite de ces travaux concernera la supervision et l'orchestration du réseau NDN virtualisé.

Identification des problèmes de QoS/QoE sur le web

- Projet ANR BottleNet
- La réalisation de services dépendant du réseau fait intervenir de nombreux acteurs, ce qui rend difficile l'identification des causes à l'origine d'une dégradation de qualité de service ou d'expérience. Grâce à l'instrumentation d'un navigateur web et l'utilisation de divers bloqueurs de publicité, nous réalisons actuellement des campagnes de mesure visant à évaluer l'impact des contenus tiers, et notamment de la publicité, sur la QoS.

2.2.2 Résumé des précédentes activités de recherche

Supervision et détection des attaques IPv6

- Contexte : Stage M1 (2006), équipe MADYNES, INRIA, Nancy, France
- Encadrants : Frédéric Beck, Olivier Festor
- Publications : [20, 28]

— Après avoir étudié ARPWatch pour IPv4 ainsi que l'état de l'art des attaques exploitant ICMPv6, j'ai conçu et développé un programme de supervision du protocole Neighbor Discovery d'IPv6, appelé NDPMon, qui peut détecter les changements, les mauvaises configurations et les attaques d'un réseau IPv6 et en avertir l'administrateur. **NDPMon est aujourd'hui devenu un outil de référence pour la supervision des réseaux IPv6** dont il permet de limiter les problèmes de sécurité : http://ndpmon.sourceforge.net/.

Mécanismes de révocation dans les réseaux dynamiques

— Contexte : Stage de Master Recherche (2007), équipe MADYNES, LORIA, Nancy, France
— Encadrant : Isabelle Chrisment
— Publications : [19, 26]
— J'ai conçu un mécanisme de révocation pour les réseaux P2P où la réputation globale de chaque pair est accessible aux autres à travers un compte public stocké dans la DHT. La réputation est ensuite vérifiée préalablement à tout service échangé entre pairs. Certains services peuvent ainsi être bloqués, réalisant une révocation distribuée et adaptative des nœuds déviants. J'ai appliqué ce mécanisme pour combattre les pairs égoïstes en prenant en compte la contribution de chacun aux ressources du réseau. Bien que récompensés par deux publications dont l'obtention d'un **titre de meilleur papier**, ces travaux furent limités dans leur application en raison de l'attaque Sybil permettant de prendre le contrôle des données stockées dans une DHT.

Supervision et protection des réseaux P2P

— Contexte : Doctorat (2007-2010), équipe MADYNES, LORIA, Nancy, France
— Encadrants : Isabelle Chrisment, Olivier Festor
— Projet ANR MAPE, Collaboration avec le Laboratoire d'Informatique de Paris 6
— Publications : [1, 14–18, 25, 29]
— Les réseaux pair à pair sont des systèmes d'information majeurs comptant des dizaines de millions d'utilisateurs et l'un des principaux usages d'internet. Ils souffrent cependant de plusieurs problèmes de sécurité affectant les contenus stockés. D'une part, l'indexation par des tables de hachage distribuées (DHT) présente des vulnérabilités permettant l'insertion massive de nœuds (attaque Sybil) pouvant réaliser plusieurs actions malveillantes (pollution, suppression de données, déni de service, etc.). D'autre part, ces réseaux sont utilisés pour diffuser des contenus illégaux (contenus à caractère pédophile, virus, etc.) ou hautement indésirables. Ma thèse avait pour objectif de concevoir et d'appliquer des méthodes de supervision capables d'appréhender les problèmes de sécurité affectant les réseaux P2P, en particulier la diffusion de contenus malveillants. Dans un premier temps, j'ai proposé une nouvelle **méthode de supervision des contenus** capable d'observer l'ensemble des requêtes émises par un pair pour un contenu donné afin d'identifier précisément les accès. Celle-ci qui fut appliquée à la **quantification des contenus pédophiles**. Dans un second temps, j'ai **amélioré la sécurité des données indexées dans une DHT** en proposant des algorithmes de détection des attaques Sybil ciblées, basés sur des tests statistiques prenant en compte la distribution des identifiants des pairs proches d'un contenu. Ces algorithmes et les contre-mesures associées ont été **implantés et évalués dans plusieurs réseaux P2P**, notamment KAD, BitTorrent et Gnutella et constituent à ce jour la seule solution performante et directement applicable contre ces attaques.

Détection et quantification des attaques dans les réseaux P2P

- Contexte : Postdoctorat (2011), équipe ERA, UTT, Troyes, France
- Projet CNRS-GIS ACDAP2P
- Publications : [2, 13, 24, 27, 30–32]
- Travaillant sur la **détection des nœuds malveillants pour la sécurité des systèmes distribués**, j'ai conçu un explorateur permettant de découvrir l'ensemble des pairs de KAD et un algorithme capable de **quantifier les attaques Sybil en cours** sur une DHT. J'ai ensuite conçu une métrique basée sur l'analyse des dis-similarités entre les différents noms de fichiers associés à un même contenu et permettant de **détecter une nouvelle forme de pollution** particulièrement néfaste sur les réseaux P2P. Par des mesures à grande échelle, j'ai estimé l'étendue de celle-ci à 2/3 des fichiers populaires du réseau KAD. J'ai finalement appliqué à BitTorrent l'ensemble des travaux de sécurisation menés sur KAD.

Supervision et sécurité de l'architecture Content-Centric Networking

- Contexte : Postdoctorat (2011-2013), Centre SnT, Université du Luxembourg
- Projets EU FP7 BUTLER et IoT6, Collaboration avec l'Université Polytechnique de Turin
- Publications : [9–12]
- Comme toutes les architectures réseau de type Information-Centric Networking, CCN pose de nouvelles questions en terme de gestion et de sécurité. J'ai ainsi proposé une première approche de supervision [12] couplée à un mécanisme détectant certains dysfonctionnements possibles. J'ai ensuite conçu un **pare-feu spécifique** permettant l'application de règles de sécurité ainsi qu'un **schéma de gestion des clés** plus adapté à cette architecture [10, 11]. CCN doit également pouvoir véhiculer efficacement le trafic généré en périphérie du réseau par des capteurs ou objets connectés. Dans ce but, j'ai proposé une optimisation de l'architecture CCN [9] visant à mieux traiter ce type de trafic.

2.2.3 Activités d'encadrement

Encadrement de thèses de doctorat :

- thèse de M. Wazen Shbair (50 % avec Isabelle Chrisment) portant sur la supervision du trafic web chiffré (HTTPS) [4–6] (soutenance prévue Q1 2017) ;
- thèse de M. Xavier Marchal (prévu à 50 % avec Olivier Festor) portant sur l'utilisation de la virtualisation de fonctions réseau (NFV) pour le déploiement de l'architecture NDN [3, 21, 22].

Encadrement de stages de niveau Master 2 (6 mois) :

- stage de M. Xavier Marchal (2015) portant sur l'évaluation des solutions de virtualisation existantes pour le déploiement de fonctions réseau virtualisées ;
- stage de M. Cédric Enclos (2015) portant sur l'amélioration de l'élasticité et de la robustesse d'une fonction de routage NDN virtualisée ;
- stage de M. Guillaume Montassier (2011, 90% avec Guillaume Doyen) portant sur la détection et l'évaluation de la pollution dans un réseau P2P [13] ;
- stage de M. Juan-Pablo Timpanaro (2009, 75% avec Isabelle Chrisment) portant sur le passage à l'échelle d'une architecture de supervision pour les réseaux P2P.

Encadrement de stages de niveau Master 1 (2 à 3 mois) :

- stage de M. Paul Andrey (2016) portant sur l'étude de l'impact des logiciels antipub sur la QoS des sites web d'information en ligne ;

— stage de M. Quentin Rouy (2016) portant sur la réalisation d'une plateforme de mesure de la QoS lors du chargement des sites web ;
— stage de M. Florian Dehau (2015) portant sur la conception et réalisation de composants logiciels servant au pilotage en temps réel d'un réseau de LEDs depuis un smartphone ;
— stage de M. Xavier Wirth (2015) portant sur l'intégration de capteurs hétérogènes sur une voiture électrique et la collecte des données ;
— stage de M. Nicolas Schnepf (2015) portant sur l'étude de l'impact des téléchargements en streaming sur l'infrastructure de Bittorrent ;
— stage de M. Antoine Goichot (2014) portant sur la réalisation démonstrateur permettant de contourner des règles de filtrage appliquées au protocole HTTPS par certains pare-feu [6] ;
— stage de M. Anthony Deroche (2014) portant sur la mise en place d'un service de géolocalisation au sein d'une plateforme d'exploitation d'un réseau de capteurs sans fil ;
— stage de M. Christopher Hénard (2010) portant sur le développement d'un outil réalisant l'exploration exhaustive des nœuds d'un réseau P2P et sur l'analyse des données collectées [24].

Encadrement de doctorants étrangers en visite :

— stage de M. Sarmad Ullah Khan de l'Université Polytechnique de Turin (2012, 4 mois) portant sur la conception d'un schéma de gestion des clés pour l'architecture CCN [11] ;
— stage de M. Juan Caubet de l'Université Polytechnique de Catalogne (2013, 3 mois) portant sur l'amélioration d'un système de gestion des clés pour les réseaux ICN.

2.3 Animation scientifique et responsabilités collectives

2.3.1 Réalisation de démonstrations et tutoriaux

J'ai réalisé un tutoriel et des démonstrations dans le cadre de conférences internationales, permettant ainsi de valoriser les savoir-faire techniques acquis :

— deux démonstrations à la conférence ACM ICN 2016, l'une portant sur l'exploitation d'une vulnérabilité, l'autre sur une passerelle permettant d'acheminer du trafic HTTP sur ICN [**?**, **?**] ;
— un tutoriel d'une demi-journée à la conférence AIMS 2012 présentant l'architecture *Content-Centric Networking* et son implantation de référence (CCNx) [23].

2.3.2 Diffusion de l'information scientifique (communications sans actes)

J'ai été invité à donner des discours en lien avec mes travaux dans le cadre d'ateliers nationaux :

— présentation à RESSI 2016 des limites des pare-feu dans leur traitement des flux HTTPS [35] ;
— présentation à l'école d'été du CNRS, RESCOM 2013, des problématiques de management réseau soulevées par les architectures ICN [38].

J'ai également participé à la diffusion de mes travaux dans le cadre de manifestations sans actes :

— dans le cadre d'organismes de normalisation, à l'Internet Research Task Force : [36, 37] ;
— dans des ateliers internationaux : [33, 34, 39–41].

2.3.3 Participation à des projets de recherche

J'ai été impliqué dans plusieurs projets de recherche avec un niveau de responsabilité croissant, allant de la rédaction de livrables à la rédaction de la proposition ou la direction de Work Packages :

— Projet CNRS PEPS-INS2I NEFAE (Sécurité Informatique et des Systèmes Cyber-physiques, Next-Generation Firewall for Analysing Encrypted Traffic) 2016 ;

— Projet ANR BottleNet (Understanding and Diagnosing End-to-end Communication Bottlenecks of the Internet) 2015-2018 ;
— Projet ANR DOCTOR (DeplOyment and seCurisaTion of new functiOnalities in virtualized networking enviRonnements) 2014-2018 ;
— Projet Européen FP7 BUTLER (uBiquitous, secUre inTernet-of-things with Location and contExawaReness) 2011-2013 ;
— Projet Européen FP7 IoT6 (Universal Integration of the Internet of Things through an IPv6-based Service Oriented Architecture enabling interoperability) 2012-2013 ;
— Projet CNRS GIS-3SGS ACDAP2P (Grouprement d'Intérêt Scientifique pour la Surveillance, la Sûreté et la Sécurité des Grands Systèmes) 2010-2011 ;
— Projet ANR MAPE (Measurement and Analysis of Peer-to-peer Exchanges for pedocriminality fighting and traffic profiling) 2007-2010.

2.3.4 Expertise scientifique

Je participe régulièrement au processus d'évaluation par les pairs garantissant la qualité de la recherche scientifique. J'ai ainsi été sollicité en tant qu'expert par les journaux et conférences suivants :

— journal IEEE Transactions on Network and Service Management (TNSM) ;
— journal IEEE Transactions on Information Forensics and Security (TIFS) ;
— journal IEEE Transactions on Parallel and Distributed Systems (TPDS) ;
— journal IEEE Transactions on Computers (TC) ;
— journal IEEE Communications and Networks (JCN) ;
— journal IEEE Communications Letters ;
— journal Elsevier Computer Communications ;
— journal Elsevier Computer Networks ;
— journal Elsevier Computers & Security ;
— International Journal of Network Management (Wiley, IJNM) ;
— conférence IEEE International Conference on Network and Service Management (CNSM) ;
— conférence IFIP/IEEE International Symposium on Integrated Network Management (IM) ;
— conférence IFIP/IEEE Network Operations and Management Symposium (NOMS) ;
— conférence IEEE International Conference on Communications (ICC) ;
— conférence IEEE Global Communications Conference (Globecom) ;
— conférence IEEE Symposium on Computers and Communications (ISCC) ;
— conférence on Autonomous Infrastructure, Management and Security (AIMS) ;
— conférence International Teletraffic Congress (ITC).

J'ai également été membre du comité technique (TPC) des conférences suivantes :

— 7th IEEE International Workshop on Network Science for Communication (NetSciCom 2015, IEEE INFOCOM Workshop) ;
— 9th International Conference on Autonomous Infrastructure, Management and Security (AIMS 2015 PhD Workshop) ;
— 2nd IEEE International Workshop on Security Testing and Monitoring (STAM 2016, IEEE ICDCS Workshop).

Enfin, j'ai été invité par l'entreprise Thales pour évaluer les conclusions du réseau d'excellence européen ICT-FP7 CAPITAL dont l'objectif est de définir un programme de recherche en Cybersécurité pour la Commission Européenne.

3 Publications

3.1 Revues internationales

[1] R. Fournier, T. Cholez, M. Latapy, I. Chrisment, C. Magnien, O. Festor, and I. Daniloff, "Comparing Pedophile Activity in Different P2P Systems," *Social Sciences*, vol. 3, no. 3, pp. 314–325, Jul. 2014. [Online]. Available : https://hal.inria.fr/hal-01052773

[2] T. Cholez, I. Chrisment, O. Festor, and G. Doyen, "Detection and mitigation of localized attacks in a widely deployed P2P network," *Peer-to-Peer Networking and Applications*, vol. 6, no. 2, pp. 155–174, May 2012. [Online]. Available : https://hal.inria.fr/hal-00786438

3.2 Conférences internationales sélectives

[3] X. Marchal, T. Cholez, and O. Festor, "Server-side performance evaluation of NDN," in *3rd ACM Conference on Information-Centric Networking (ACM-ICN'16)*, ACM SIGCOMM. Kyoto, Japan : ACM, Sep. 2016, pp. 148 – 153. [Online]. Available : https://hal.inria.fr/hal-01386777

[4] W. M. Shbair, T. Cholez, J. François, and I. Chrisment, "Improving SNI-based HTTPS Security Monitoring," in *2nd IEEE International Workshop on Security Testing and Monitoring*, ser. Workshops of the 36th IEEE International Conference on Distributed Computing Systems (ICDCS Worshops). Nara, Japan : IEEE, Jun. 2016, p. 6. [Online]. Available : https://hal.inria.fr/hal-01349710

[5] ——, "A Multi-Level Framework to Identify HTTPS Services," in *IFIP/IEEE Network Operations and Management Symposium (NOMS 2016)*, IFIP/IEEE. Istanbul, Turkey : IEEE, Apr. 2016, pp. p240–248. [Online]. Available : https://hal.inria.fr/hal-01273160

[6] W. M. Shbair, T. Cholez, A. Goichot, and I. Chrisment, "Efficiently Bypassing SNI-based HTTPS Filtering," in *IFIP/IEEE International Symposium on Integrated Network Management (IM 2015)*. Ottawa, Canada : IFIP/IEEE, May 2015, pp. 990–995. [Online]. Available : https://hal.inria.fr/hal-01202712

[7] M. Bertrand, G. Doyen, W. Mallouli, T. Silverston, O. Bettan, F.-X. Aguessy, T. Cholez, A. Lahmadi, P. Truong, and E. Montes de Oca, "Monitoring and Securing New Functions Deployed in a Virtualized Networking Environment," in *1st International Workshop on Security Testing and Monitoring*, ser. Workshops of the 10th International Conference on Availability, Reliability and Security (ARES Workshops). Toulouse, France : IEEE, Aug. 2015, pp. 741 – 748. [Online]. Available : https://hal.inria.fr/hal-01238048

[8] J. P. Timpanaro, T. Cholez, I. Chrisment, and O. Festor, "Evaluation of the Anonymous I2P Network's Design Choices Against Performance and Security," in *1st International Conference on Information Systems Security and Privacy (ICISSP 2015)*. Angers, France : SciTePress, Feb. 2015, pp. 46–55. [Online]. Available : https://hal.inria.fr/hal-01238453

[9] J. François, T. Cholez, and T. Engel, "CCN Traffic Optimization for IoT," in *The 4th International Conference on Network of the Future (NoF 2013)*, IFIP/IEEE. Pohang, South Korea : IEEE, Oct. 2013. [Online]. Available : https://hal.inria.fr/hal-00922728

[10] D. Goergen, T. Cholez, J. François, and T. Engel, "A Semantic Firewall for Content-Centric Networking," in *the 13th IFIP/IEEE International Symposium on Integrated Network Management (IM 2013) : Mini-Conference*, IFIP/IEEE. Ghent, Belgium : IEEE, May 2013, pp. 478–484. [Online]. Available : https://hal.archives-ouvertes.fr/hal-00829615

[11] S. U. Khan, T. Cholez, T. Engel, and L. Lavagno, "A Key Management Scheme for Content Centric Networking," in *the 13th IFIP/IEEE International Symposium on Integrated Network Management (IM 2013)*, IFIP/IEEE. Ghent, Belgium : IEEE, May 2013, pp. 828–831. [Online]. Available : https://hal.inria.fr/hal-00922486

[12] D. Goergen, T. Cholez, J. François, and T. Engel, "Security Monitoring for Content-Centric Networking," in *5th SETOP International Workshop on Autonomous and Spontaneous Security*, vol. 7731, Workshop of the 17th European Symposium on Research in Computer Security (ESORICS Workshops). Pisa, Italy : Springer-Verlag, Sep. 2012, pp. 274–286. [Online]. Available : https://hal.inria.fr/hal-00785254

[13] G. Montassier, T. Cholez, G. Doyen, R. Khatoun, I. Chrisment, and O. Festor, "Content Pollution Quantification in Large P2P networks : a Measurement Study on KAD," in *11th IEEE International Conference on Peer-to-Peer Computing (IEEE P2P'11)*. Kyoto, Japan : IEEE Communications Society, Aug. 2011, pp. 30–33. [Online]. Available : https://hal.inria.fr/inria-00619965

[14] J. P. Timpanaro, T. Cholez, I. Chrisment, and O. Festor, "When KAD meets BitTorrent - Building a Stronger P2P Network," in *Eighth International Workshop on Hot Topics in Peer-to-Peer Systems (HotP2P 2011)*. Anchorage, ALASKA, USA : IEEE International Parallel & Distributed Processing Symposium (IPDPS Workshops), May 2011. [Online]. Available : https://hal.inria.fr/inria-00595086

[15] ——, "BitTorrent's Mainline DHT Security Assessment," in *4th IFIP International Conference on New Technologies, Mobility and Security (NTMS 2011)*. Paris, France : IEEE, Feb. 2011, iSBN : 978-1-4244-8704-2. [Online]. Available : https://hal.inria.fr/inria-00577043

[16] T. Cholez, I. Chrisment, and O. Festor, "Monitoring and Controlling Content Access in KAD," in *IEEE International Conference on Communications (IEE ICC 2010)*. Capetown, South Africa : IEEE, May 2010. [Online]. Available : https://hal.inria.fr/inria-00490347

[17] ——, "Efficient DHT attack mitigation through peers' ID distribution," in *Seventh International Workshop on Hot Topics in Peer-to-Peer Systems (HotP2P 2010)*. Atlanta, USA : IEEE International Parallel & Distributed Processing Symposium (IPDPS Workshops), Apr. 2010. [Online]. Available : https://hal.inria.fr/inria-00490509

[18] ——, "Evaluation of Sybil Attacks Protection Schemes in KAD," in *3rd International Conference on Autonomous Infrastructure, Management and Security (AIMS 2009)*, R. Sadre and A. Pras, Eds., vol. 5637, University of Twente. Enschede, Netherlands : Springer, Jun. 2009, pp. 70–82. [Online]. Available : https://hal.inria.fr/inria-00405381

[19] ——, "A Distributed and Adaptive Revocation Mechanism for P2P networks," in *Seventh International Conference on Networking (ICN 2008)*. Cancun, Mexico : IARIA, Apr. 2008, pp. pp. 290–295. [Online]. Available : https://hal.archives-ouvertes.fr/hal-00323990

[20] F. Beck, T. Cholez, O. Festor, and I. Chrisment, "Monitoring the Neighbor Discovery Protocol," in *The Second International Workshop on IPv6 Today - Technology and Deployment (IPv6TD 2007)*, ser. Workshops of the International Multi-Conference on Computing in the Global Information Technology (ICCGI Worshops). Guadeloupe/French Caribbean, Guadeloupe : IARIA, Mar. 2007. [Online]. Available : https://hal.inria.fr/inria-00153558

3.3 Démonstrations et tutoriaux sélectionnés

[21] X. Marchal, T. Cholez, and O. Festor, "PIT matching from unregistered remote Faces : a critical NDN vulnerability," 3rd ACM Conference on Information-Centric Networking (ACM-ICN'16), ACM SIGCOMM, pp. 211 – 212, Sep. 2016, poster. [Online]. Available : https://hal.inria.fr/hal-01386809

[22] X. Marchal, M. El Aoun, B. Mathieu, W. Mallouli, T. Cholez, G. Doyen, P. Truong, A. Ploix, and E. Montes De Oca, "A virtualized and monitored NDN infrastructure featuring a NDN/HTTP gateway," 3rd ACM Conference on Information-Centric Networking (ACM-ICN'16), ACM SIGCOMM, pp. 225 – 226, Sep. 2016, poster. [Online]. Available : https://hal.inria.fr/hal-01386615

[23] T. Cholez, "Introduction to Content-Centric Networking and the CCNx framework," in *6th International Conference on Autonomous Infrastructure, Management and Security (AIMS 2012)*, Luxembourg, Luxembourg, Jun. 2012. [Online]. Available : https://hal.inria.fr/hal-00785298

3.4 Conférences francophones sélectives

[24] T. Cholez, C. Hénard, I. Chrisment, O. Festor, G. Doyen, and R. Khatoun, "Détection de pairs suspects dans le réseau pair à pair KAD," in *6ème Conf. sur la Sécurité des Architectures Réseaux et Systèmes d'Information (SAR-SSI 2011)*. La Rochelle, France : IEEE, May 2011. [Online]. Available : https://hal.inria.fr/inria-00596677

[25] T. Cholez, I. Chrisment, and O. Festor, "Une architecture de honeypots distribués pour superviser le réseau P2P KAD," in *9e Conférence Internationale sur Les NOuvelles TEchnologies de la REpartition (NOTERE 2009)*, A. Obaïd, Ed., Montréal, Canada, Jun. 2009, pp. 76–82. [Online]. Available : https://hal.inria.fr/inria-00405771

[26] ——, "Un mécanisme de révocation distribué et adaptatif pour les réseaux pair-à-pair," in *9ème journees Doctorales en Informatique et Reseaux (JDIR 2008)*, Villeneuve d'Ascq, France, Jan. 2008, p. 87, prix du meilleur papier. [Online]. Available : https://hal.archives-ouvertes.fr/hal-00323940

3.5 Chapitres de livre

[27] T. Cholez, G. Doyen, I. Chrisment, O. Festor, and R. Khatoun, "Faiblesses de l'identification dans les espaces numériques ouverts de partage de contenus : le cas des réseaux pair-à-pair," in *Enseignement, préservation et diffusion des identités numériques*, ser. Traité des sciences et techniques de l'information, J.-P. Pinte, Ed. Hermès - Lavoisier, May 2014. [Online]. Available : https://hal.inria.fr/hal-01052851

[28] F. Beck, T. Cholez, O. Festor, and I. Chrisment, *Supervision IPv6 - Applications Specifiques - NDPMon*. O'Reilly, 2007, online version of a french reference book on IPv6. [Online]. Available : http://livre.g6.asso.fr/index.php/Les_applications_sp%C3%A9cifiques

3.6 Thèse

[29] T. Cholez, "Supervision des réseaux pair à pair structurés appliquée à la sécurité des contenus," Theses, Université Henri Poincaré - Nancy I, Jun. 2011. [Online]. Available : https://tel.archives-ouvertes.fr/tel-00608907

3.7 Rapports de recherches

[30] T. Cholez, G. Montassier, G. Doyen, R. Khatoun, I. Chrisment, and O. Festor, "Détection et quantification de la pollution dans le réseau P2P KAD," UTT-LORIA, Research Report, Sep. 2011. [Online]. Available : https://hal.inria.fr/hal-00644174

[31] T. Cholez, J. P. Timpanaro, G. Doyen, I. Chrisment, O. Festor, and R. Khatoun, "Vulnérabilités de la DHT de BitTorrent & Identification des comportements malveillants dans KAD," UTT-LORIA, Research Report, Aug. 2011. [Online]. Available : https://hal.inria.fr/hal-00644151

[32] T. Cholez, I. Chrisment, G. Doyen, J. Dromard, F. Olivier, and R. Khatoun, "Etat de l'art : Réseaux pair à pair, supervision, sécurité et approches collaboratives," UTT-LORIA, Research Report, Oct. 2010. [Online]. Available : https://hal.inria.fr/inria-00533385

3.8 Affiches

[33] T. Cholez, I. Chrisment, and O. Festor, "Fighting against paedophile activities in the KAD P2P network," Advances in the Analysis of Online Paedophile Activity, Laboratoire d'Informatique de Paris 6, Jun. 2009, poster. [Online]. Available : https://hal.inria.fr/inria-00405636

[34] ——, "Un mécanisme de révocation orienté services pour les réseaux P2P," RESCOM 2008, CNRS, Jun. 2008, poster. [Online]. Available : https://hal.inria.fr/inria-00338389

3.9 Autres communications (sans actes)

[35] W. M. Shbair, T. Cholez, A. Goichot, and I. Chrisment, "Efficiently Bypassing SNI-based HTTPS Filtering," Rendez-Vous de la Recherche et de l'Enseignement de la Sécurité des Systemes d'Information (RESSI 2016), Toulouse, France, 2016.

[36] M. Bertrand, G. Doyen, W. Mallouli, T. Silverston, O. Bettan, F.-X. Aguessy, T. Cholez, A. Lahmadi, P. Truong, and E. Montes de Oca, "Challenges and directions for the security management of ICN services," Information-Centric Networking Research Group (IRTF ICNRG), Paris, France, 2016.

[37] W. M. Shbair, T. Cholez, J. François, and I. Chrisment, "HTTPS Traffic Classification," Network Machine Learning Research Group (IRTF NMLRG), Buenos Aires, Argentina, 2016.

[38] T. Cholez, "Management of Content-Centric Networking," ResCom 2013 : Les réseaux centrés sur les contenus, Évolution ou révolution de l'Internet ?, CNRS, May 2013. [Online]. Available : https://hal.inria.fr/hal-00924363

[39] T. Cholez, I. Chrisment, and O. Festor, "Efficient DHT Attack Mitigation through Peers' ID Distribution," Grande Region Security and Reliability Day (GRSRD 2011), Trier, Germany, 2011.

[40] ——, "Exploiting KAD Vulnerabilities to Build an Efficient Honeypot Architecture," 2nd EMANICS Workshop on Peer-to-Peer Management, University College London, London, United Kingdom, 2009.

[41] ——, "A Distributed and Adaptive Revocation Mechanism for P2P Networks," 1st EMANICS Workshop on Peer-to-Peer Management, ETH Zurich, Zurich, Switzerland, 2008.