Une troisième subvention ERC en trois ans pour EURECOM

Davide Balzarotti
Professeur au Département
Systèmes de Communication

Obtenir une subvention du Conseil européen de la Recherche (ERC) n'est pas chose simple. Pourtant Davide Balzarotti, Professeur au Département Sécurité y est parvenu. Il est le troisième professeur d'EURECOM à obtenir une telle bourse en trois ans.

Davide, vous venez de décrocher une bourse Consolidator Grant, l'une des plus prestigieuses en Europe. Quelle est votre réaction ?

Tout le monde sait qu'il s'agit de l'une des bourses les plus sélectives en Europe ; j'en suis donc particulièrement fier. C'est de toute évidence une étape majeure dans ma carrière. C'est la reconnaissante de mon travail pour décrocher cette bourse et de la pertinence du projet présenté. J'ai appris que seuls 329 chercheurs en Europe – et 38 en France – l'avaient reçue cette année. Je me sens donc très honoré de compter parmi eux. Je suis également très heureux pour EURECOM qui en est à sa troisième bourse depuis trois ans. Etant donné que nous ne sommes que 23 professeurs, c'est un véritable succès !

Cette subvention va-t-elle changer votre quotidien en tant que chercheur à EURECOM ?

Bien sûr ! Et de plusieurs façons. D'abord, je ne vais plus avoir besoin de chercher des fonds pendant deux ans puisque la Consolidator Grant représente deux millions d'euros sur cinq ans. En plus d'être généreuse, elle offre reconnaissance et visibilité. D'ailleurs, les deux précédents récipiendaires d'un ERC à EURECOM, David Gesbert et Petros Elia, m'ont expliqué que je serai certainement plus sollicité par la communauté de chercheurs. Cette bourse va également me donner beaucoup d'indépendance et de liberté de création pour mener mon projet : BITCRUMBS - Towards a Reliable and Automated Analysis of Compromised Systems. Je vais y consacrer 70 % de mon temps, mais avec une liberté totale dans la façon de le gérer avec mes collaborateurs. Je dois engager une équipe de sept chercheurs, cinq doctorants et deux post-doctorants, et un ingénieur. Je vais aussi participer au comité ERC d'EURECOM, qui entend faire profiter les chercheurs de l'expérience de ceux qui ont déjà reçu cette subvention. Ce comité m'a beaucoup aidé dans la rédaction de ma proposition ; c'est donc avec plaisir que j'aiderai à mon tour mes collègues.

BITCRUMBS semble être un projet novateur dans le domaine informatique. Pouvez-vous nous expliquer son objectif ?

BITCRUMBS est en fait une toute nouvelle façon d'appréhender les questions de sécurité informatique. La bourse ERC va m'aider à poursuivre des objectifs de recherche très ambitieux, qui couvrent une large palette de problématiques de sécurité numérique, et j'espère que nos résultats changeront la façon dont elle sera gérée dans l'avenir. L'objectif premier de BITCRUMBS est de repenser le concept de « réponse aux incidents ». Il est évident que la recherche menée sur la prévention et la détection contribue à mieux sécuriser les appareils, mais puisqu'un système sûr à 100 % n'existe pas, améliorer la réponse aux incidents peut aussi être très utile. Ce concept englobe tout ce qui se passe après une faille de sécurité qui, si elle n'est pas gérée correctement, peut aboutir à une violation des données ou à un crash du système. Nous savons que les risques d'atteinte à la sécurité sont aujourd'hui maximaux. Les pirates s'introduisent dans les réseaux d'entreprise, les services de l'État, et même les infrastructures critiques. Presque la moitié des ordinateurs dans le monde sont infectés par un logiciel malveillant. Une machine à voter peut être altérée pour manipuler les résultats d'une élection, un véhicule connecté être piraté ou une caméra de sécurité être contrôlée pour espionner notre maison et notre famille. Le problème est que nous n'avons pas les outils pour analyser ces attaques et en comprendre les causes ! Tout cela doit changer.

Mon but, avec BITCRUMBS, est de donner aux enquêteurs la possibilité de vérifier rapidement l'état des systèmes compromis et d'aider les citoyens à faire confiance aux résultats des investigations informatiques. Je pense que, dans l'avenir, la conception des systèmes numériques devrait suivre le même protocole que celui appliqué à l'aéronautique : sécuriser les systèmes contre les crashs et les équiper de boîtes noires qui recueillent les données nécessaires à une recherche d'incident.

Quelle démarche allez-vous suivre pour atteindre votre but ?

Pour analyser les systèmes compromis, je souhaite proposer une méthodologie plus scientifique et globale selon trois étapes. La première partie du projet s'attachera à mesurer l'efficacité et l'exactitude des techniques qui sont actuellement utilisées pour analyser les systèmes compromis et à évaluer la fiabilité de leurs sources de données. Cela permettra d'élargir les fondements théoriques et scientifiques des techniques de réponse aux incidents. Dans un deuxième temps, nous mettrons en œuvre de nouvelles techniques automatisées d'analyse capables de gérer des menaces sophistiquées et l'analyse des appareils connectés à l'Internet des Objets. Ces techniques devront être robustes, évolutives et génériques, capables de fonctionner avec différentes catégories de dispositif. Bien sûr, les résultats générés par ces techniques seront fiables et fondés sur une solide base théorique. La dernière étape consistera à introduire une nouvelle méthodologie d'analyse forensique. Mon but est d'apporter de nouvelles lignes directrices pour la conception des prochains systèmes et logiciels, mais aussi d'aider les développeurs à fournir les informations nécessaires à l'analyse des systèmes compromis.

Qu'en est-il des impacts scientifiques et technologiques ?

J'espère que les travaux menés dans le cadre de BITCRUMBS auront un impact durable, et pas seulement scientifique, dans le domaine de la réponse aux incidents ainsi que sur la façon dont nous analysons les systèmes compromis. BITCRUMBS nous donnera une base scientifique fondée sur des expériences reproductibles et des mesures précises de la fiabilité des données et des techniques utilisées dans les investigations actuelles. Il aura également un impact concret puisque le projet produira des outils open source et améliorera les logiciels qui ont utilisés par les entreprises et les forces de l'ordre pour traiter les attaques informatiques. Dernier point, mais non des moindres, BITCRUMBS aura un impact sur notre société. L'amélioration du processus de réponse aux incidents renforcera la confiance des citoyens dans les résultats des investigations forensiques. Pour montrer l'impact de BITCRUMBS dans différents domaines et scénarios, nous utiliserons des études de cas réelles empruntées à des logiciels traditionnels et des systèmes embarqués.

Quels seront les principaux défis de BITCRUMBS ?

Comme pour tout projet majeur, le succès de BITCRUMBS dépend de multiples facteurs. D'un point de vue scientifique, il s'agit d'une association de compétences en recherche très diverses, qui couvrent l'analyse de la mémoire volatile, la sécurité des systèmes embarqués, les logiciels malveillants et l'analyse binaire ainsi que la conception et la protection des systèmes distribués et des systèmes d'exploitation. J'ai une vaste expérience dans chacun de ces domaines de recherche mais, pour réduire les risques, j'ai déjà établi des collaborations stratégiques avec des universités de renom. Cela va me permettre de trouver des partenaires issus de différents milieux de recherche. L'autre risque potentiel est l'éventuel échec pour développer certaines des techniques envisagées. Il s'agit d'un risque classique dans les projets de recherche qui introduisent des solutions novatrices. Aussi, pour chaque approche en rupture que je souhaite développer, j'ai déjà réfléchi à des techniques moins risquées que je connais bien et avec lesquelles j'ai déjà mené des recherches pour évaluer la faisabilité de certaines idées. Mais surtout, l'un des principaux défis consistera à trouver des post-doctorants motivés par la sécurité numérique et qui souhaitent travailler en Europe. La plupart d'entre eux partent aux États-Unis une fois leur thèse dans la poche ou sont embauchés par des entreprises de sécurité qui leur offrent d'excellentes conditions de travail et des débouchés intéressants. J'espère que les défis de BITCRUMBS et les résultats potentiels seront des facteurs d'attractivité.

Subventions ERC : Faits et chiffres

- Le budget global alloué à l'ERC pour 2014-2020 s'élève à 13,1 milliards d'euros, soit 17 % du budget global d'Horizon 2020. Il offre aux meilleurs chercheurs la possibilité d'avoir un impact scientifique majeur.
- Les récipiendaires des bourses ERC ont aussi remporté des prix prestigieux : six ont reçu le Prix Nobel, quatre la Médaille Fields et cinq le Prix Wolf.
- Il existe trois types de bourse ERC (selon l'expérience du candidat) : Starting Grants, Consolidator Grants et Advanced Grants.
- Consolidator Grants : Type de bourse octroyé à Davide en 2017. Budget global de 630 millions d'euros.
- Les bourses Consolidator Grants sont destinées à de jeunes chercheurs sept à douze ans après l'obtention de leur thèse et dont les travaux sont très prometteurs.
- Seuls 38 chercheurs travaillant en France ont reçu cette bourse cette année, ce qui place la France au troisième rang des pays récipiendaires de subventions ERC, derrière le Royaume-Uni et l'Allemagne.
- Parmi les 2 538 propositions évaluées, 13 % ont obtenu un financement.
- La durée de la bourse (dont le plafond est de 2 millions d'euros) est de cinq ans; elle couvre essentiellement l'embauche de chercheurs et autres personnels.