ÉDITORIAL

Alors qu'une carte perforée pouvait être dérobée pendant son trajet entre une perforatrice et une tabulatrice, une information d'aujourd'hui, dématérialisée, est soumise à d'innombrables menaces quant à sa sécurité. Les artefacts technologiques sont partout, l'informatique est ubiquitaire, si bien que l'individu n'est plus un simple utilisateur du système d'information, mais il en est un composant à part entière. Comment assurer alors la sécurité d'un système d'information en prenant en compte des technologies omniprésentes, universelles et discrètes, aussi bien que des personnes au comportement parfois irrationnel ?

Ce numéro spécial de la revue *Ingénierie des Systèmes d'Information* propose d'aborder la sécurité des systèmes d'information en la regardant du point de vue des technologies et des personnes. En effet, un système d'information peut être vu comme un ensemble de ressources non seulement numériques, mais aussi humaines, organisées afin de traiter, diffuser et stocker des informations. Différentes normes, modèles d'évaluation et méthodes d'analyse des risques existent pour appréhender la sécurité des systèmes d'information. Néanmoins, la question des connaissances portées par les personnes, aussi bien que la confiance qu'elles accordent au système et que le système leur accorde sont cruciales pour assurer la sécurité des systèmes d'information dans les organisations.

Au début des années 1990, la littérature en sécurité des systèmes d'information statuait déjà qu'il existait « *a gap between the use of modern technology and the understanding of the security implications inherent in its use*[1] » (Loch *et al.*, 1992, p. 173). L'arrivée massive de micro-ordinateurs s'était en effet accompagnée d'interrogations quant à la sécurité de systèmes interconnectés là où l'informatique était auparavant orientée *mainframe*, c'est-à-dire destinée à un ordinateur central. En 2017, le nombre d'artefacts technologiques a explosé et cette augmentation est allée de pair avec l'évolution des usages qui en sont faits (Canohoto *et al.*, 2015) : là où hier un terminal reliait l'utilisateur à l'ordinateur, aujourd'hui les points d'entrée dans le système d'information sont multiples, universels, interconnectés et de plus en plus discrets. L'activité sociale des employés peut être supportée par des réseaux sociaux et leur santé entretenue au travers de montres connectées.

Dans ce numéro, des auteurs de divers domaines (cybersécurité, informatique fondamentale, psychologie) et de profils variés (militaires, universitaires, professionnels) dressent un état des lieux et des connaissances autour de la sécurité des systèmes d'information avec un focus tout particulier sur les technologies et les personnes. En effet, technologies et personnes constituent autant de points d'entrée dans le système qui sont susceptibles de subir des attaques.

1. Traduction : « Un écart entre l'usage des technologies modernes et la compréhension des implications en termes de sécurité inhérentes à leur usage ».

Dans le premier article, Benjamin Coste, Cyril Ray et Gouenou Coatrieux s'intéressent aux sources d'informations dans les systèmes d'information. Ils argumentent que la multiplication des capteurs et des objets communicants a significativement augmenté le nombre de sources d'information, indépendamment de leur contrôle et de leur maîtrise. Ils expliquent notamment qu'un tiers peut prendre le contrôle d'un navire et le détourner en falsifiant les informations de position qui lui sont transmises. Aussi, par un effet d'entraînement, l'augmentation du nombre de sources pouvant être corrompues ou leurrées impacte la confiance accordée aux informations portées par le système. Dans cet article, les auteurs définissent et évaluent la confiance accordée à un système d'information en proposant de modéliser les sources d'information. Deux caractéristiques sont analysées : la compétence et la sincérité. Un jeu de données réelles provenant de l'*Automatic Identification System* d'un bateau de type cargo à proximité de Brest vient illustrer le modèle proposé. Les résultats obtenus valident la pertinence de l'utilisation de la confiance dans un processus de détection de cyberattaque, ce qui constitue une originalité majeure en sécurité des systèmes d'information.

Dans le deuxième article, Gloria Elena Jaramillo, Manuel Munier et Philippe Aniorté regardent l'architecture orientée service (SOA) comme un moyen prometteur de faciliter la coopération commerciale, à ceci près que l'interaction humain y est basée uniquement sur la confiance. Les aspects de contrôle et de sécurité sont présentés comme étant induits par les contrats, c'est pourquoi les auteurs proposent un modèle et une ontologie formalisant la sémantique des contrats de service avec OWL 2 comme syntaxe concrète. La conformité, l'exécution, le respect des engagements et la sécurité sont ainsi évalués au travers d'une plate-forme qui audite les interactions entre clients et fournisseurs, au regard des contrats modélisés.

Dans le troisième article, Wilson Goudalo, Christophe Kolski et Frédéric Vanderhaegen abordent de manière conjointe les problèmes de sécurité, d'utilisabilité et de résilience des systèmes d'information. Ils argumentent qu'au-delà des risques qui sont implicites au système d'information, il y en a qui sont induits par le fonctionnement même du système d'information, de par les applications d'entreprise ou les activités au quotidien des acteurs internes à l'entreprise ou à l'organisation. Prenant appui sur des récentes études d'universités et de cabinets d'audit et de conseil estimant à 8,5 milliards de dollars par an le coût total des attaques informatiques, les auteurs défendent vouloir rendre les services numériques fiables, protégés et sécurisés, faciles d'utilisation et résilients. Des modèles de conception mesurables et concrets sont en effet discutés et illustrés au travers d'une étude de cas, allant dans le sens d'une sécurité ne détériorant pas l'expérience utilisateur.

Avec le quatrième article, Bako Rajaonah propose une vision transdisciplinaire de la recherche sur la confiance dans les systèmes d'information vue sous l'angle de la protection des infrastructures critiques. L'auteure argumente que, bien que la confiance est effectivement reconnue comme importante dans les environnements numériques, peu d'études s'intéressent à la fois à la sécurité des systèmes d'information et à la confiance. Cet article défend que les sciences humaines et

sociales ont beaucoup à apporter pour étudier, comprendre et appréhender la confiance, qu'elle soit interpersonnelle, systémique ou technologique. À l'aide d'une approche holistique de la protection des infrastructures critiques, l'auteure propose de sortir d'une conception de la confiance centrée autour de propriétés répondant à des standards et à des exigences informatiques pour aller vers une vision transdisciplinaire intégrant les personnes en présence.

Le lecteur aura remarqué comme les articles publiés dans ce numéro spécial mettent l'accent sur une spécificité des personnes par rapport aux technologies : la confiance. Cette spécificité est parfois efficace et parfois dommageable en termes de sécurité des systèmes d'information. En effet, dans un monde international et interconnecté, technologies et personnes interagissent au travers de protocoles, de procédures et de fragments de code au comportement connu, raisonnable et maîtrisé. Autrement dit, la cohérence a pris le pas sur la confiance, référentiel que nous utilisons pourtant tous dès lors que nous devenons des individus sociaux en interaction avec le monde qui nous entoure : technologies et personnes. Ces aspects sont abordés dans l'avant-propos de ce numéro, que Charles P. Pfleeger et Shari Lawrence Pfleeger nous ont fait l'honneur de proposer et pour lequel nous les remercions.

Pierre-Emmanuel ARDUIN
PSL, Université Paris-Dauphine
DRM UMR CNRS 7088

Káthia Marçal de OLIVEIRA
Université de Valenciennes et du Hainaut-Cambrésis
LAMIH UMR CNRS 8201