Introduction

Les ordinateurs et les réseaux font partie intégrante de notre vie quotidienne et sont à la base de nos infrastructures économiques, sociales et institutionnelles. Ils sont devenus une nécessité et leur vulnérabilité est un obstacle majeur.

La sécurité informatique ne se limite pas aux questions marchandes de paiement électronique, de commerce électronique (B2C) ou de transactions financières (B2B). Elle englobe également la sécurité des communications, de la messagerie, du partage des connaissances et de la propriété intellectuelle. La sécurité de l'informatique et des télécoms conjugue enfin la liberté et la volonté de protéger les valeurs matérielles ou intangibles et leur image de marque, avec la correction des logiciels, la robustesse des architectures, l'immunité des applications, la résilience des systèmes, l'instillation et le maintien de la confiance dans les édifices numériques.

L'industrie outre-atlantique est combative en sécurité tant en matière de suprématie (cf. Verisign, Microsoft), de solutions (cf. TCPA, passeport sécurisé) que de normes (cf. IETF, carte à puce EMV). Le monde numérique est le reflet de notre société, avec sa violence et ses rapports de force. Celui qui domine la sécurité des systèmes numériques possède un atout décisif dans sa stratégie pour influencer l'avenir. La maîtrise des technologies de sécurité au niveau industriel est fondamentale dans la perspective de la souveraineté des Etats et de l'indépendance économique du monde industriel car la chaîne de la confiance commence par la crédibilité qu'on peut avoir dans les concepteurs des produits.

La sécurité à l'ère numérique offre une photographie de la sécurité informatique dans son aspect multidisciplinaire : la recherche européenne en cryptologie, les perspectives de la cryptographie quantique, le retour sur

LCN, volume 4, n° 3-4/2003, pages 9 à 12

expérience des déploiements des infrastructures de gestion de clés publiques, le bilan sur les techniques de tatouage multimédia, la sécurité du Wi-Fi, la défense de l'individu (CNIL), l'apparition de la preuve numérique dans les enquêtes judiciaires et la sociologie de la confiance en sécurité des systèmes d'information.

En 2004, la cryptologie demeure la discipline scientifique noble de la sécurité et elle restera pour longtemps encore la technique maîtresse pour sécuriser et protéger le transport et le stockage de l'information. L'article de Louis Granboulan dresse un bilan des activités européennes dans ce domaine. Elles vont se poursuivre dans le cadre du 6e PCRD avec le Réseau d'Excellence ECRYPT pour fédérer les efforts des équipes européennes de cryptologie. Pour lever les principaux verrous, la cryptologie moderne doit proposer :

– des mécanismes cryptographiques moins gourmands en ressources notamment en environnement contraint ;

– des mécanismes cryptographiques pour la gestion des droits numériques, *Digital Rights Management* (DRM) ;

– des méthodes de chiffrement par flot, (*stream cipher*), aussi sûres que les méthodes actuelles de chiffrement par blocs mais plus rapides.

L'article de Philippe Grangier *et al.* est une introduction pédagogique à la cryptographie quantique. Les travaux récents de ce domaine émergeant promettent, à moyen terme, le déploiement de réseaux de communication quantique, avec, en particulier, la mise en œuvre de systèmes de distribution de clés pour suppléer, dans certains cas, les infrastructures classiques de gestion de clés (IGC), *Public Key Infrastructure* (PKI).

L'article de Jean-Luc Archimbaud introduit de manière très pragmatique la théorie des IGC, leur implémentation et leur exploitation, au sein d'une organisation, ici le CNRS. Les deux articles descriptifs de déploiement d'IGC constituent une initiation indispensable pour les lecteurs qui s'intéressent aux usages de la sécurité. Ce retour sur expérience est un témoignage concret, vécu par des informaticiens qui résolvent au quotidien les soucis réels des utilisateurs de la sécurité informatique.

Dans les années 1990, une nouvelle discipline, révélée dans les publications en langue anglaise par le terme *watermarking*, et baptisée en français « tatouage » a créé une grande effervescence. L'article de Philippe Nguyen *et al.* sur le tatouage de données audiovisuelles réexamine dans un premier temps les relations entre tatouage, stéganographie et cryptographie. Différentes situations applicatives sont ensuite exposées, ce qui forme une base à partir de laquelle on peut enfin partir plus sûrement vers l'examen

des questions relatives à la sécurité. Le tatouage n'a pas encore réussi à émerger sur le plan industriel, car les standards tardent à s'imposer. Par ailleurs, le monde de l'audiovisuel et du multimédia est très conservateur.

L'article de Pascal Urien présente l'amélioration de la sécurité des réseaux Wi-Fi. C'est un exemple parfait de déploiement rapide d'une technologie avec une cryptographie mal maîtrisée au départ et une vulnérabilité intrinsèque qui se résout peu à peu.

L'article de Stéphane Tijardovic fait le point sur les garanties juridiques que le citoyen est en droit d'exiger face aux évolutions des technologies de l'information et de la communication (TIC). La situation internationale y est exposée tout en mettant l'accent sur la norme européenne omniprésente et la réglementation en vigueur en France, à travers le contrôle exercé par la CNIL.

L'article de Eric Freyssinet présente ce nouveau champ de l'analyse criminelle qu'est la preuve numérique, du point de vue de la gendarmerie en charge des questions délicates de perquisition. Il expose la situation dans toute son ampleur technique, juridique et humaine.

La dimension humaine, ses aspects psychologiques et sociologiques, sa part irrationnelle, est déterminante dans la mise en vigueur de la sécurité et dans son application par les utilisateurs. L'article de Dominique Boullier qui conclut cet ouvrage, montre, suite à des analyses en vraie grandeur sur des mises en œuvre de sécurité, les réactions insolites ou surprenantes mais réelles des utilisateurs sur le terrain.

L'accès généralisé du grand public à internet, à l'univers mobile et en ligne modifie le comportement des utilisateurs et change profondément les risques encourus. L'industrie et la recherche doivent intensifier leur relation pour permettre une dissémination rapide et un déploiement efficace des découvertes du monde scientifique. Les entreprises ont besoin de solutions compétitives relatives aux fonctions de sécurité traditionnelles :

– l'identité d'une personne (par biométrie, par entité de confiance personnelle), d'une application, d'un document, d'une entité informatique (un paquet IP, une connexion, une station de base) ;

– la preuve de l'identité (l'authentification) par l'authenticité d'un titre, d'une étiquette, d'un tatouage ;

– l'audit des faits, l'imputabilité, l'enregistrement de l'histoire du système à partir de capteurs et de sondes, la traçabilité des mouvements des divers sujets et des objets ;

– la preuve d'une communication (non répudiation), d'un consentement avec des signatures numériques de toutes sortes ;

– la protection du transport, du traitement, du stockage, de l'archivage de documents, de bases de données, de transactions et d'actes ;

– la gestion des droits et des devoirs des propriétaires, des auteurs, des distributeurs, des abonnés : protection contre le piratage, la modification, le plagiat, la rediffusion ;

– la restriction d'accès, les autorisations en accord avec des politiques de sécurité, variables avec le temps, l'espace et le contexte ;

– la gestion de la sécurité : administration des outils et dispositifs de sécurité, évaluation globale du niveau d'assurance de sécurité.

La sécurité doit être en phase avec les paradigmes informatiques de son époque. Les aspects nomades des TIC inclinent à prendre en compte à la fois l'environnement réel (l'identité géographique, l'identité d'origine) et virtuel des sujets et des objets et la kyrielle des états de confiance très différents dans lesquels ils baignent. La sécurité du monde intangible doit, de ce fait, concevoir des modèles et des politiques de sécurité qui appréhendent le contexte et la sémantique des applications et des communications. Evoquant la communication numérique avec en arrière-plan les théories de Claude Shannon, Jacques Lacan[1] déplorait déjà en 1955 : « Il s'agit de savoir quelles sont les conditions les plus économiques qui permettent de transmettre des mots que les gens reconnaissent. Le sens, personne ne s'en occupe. » Il aura été visionnaire car les verrous technologiques de la sécurité informatique subsistent justement là où le sens des abstractions fait défaut. La restitution du sens du monde numérique est inéluctable. La clé de la sécurité dans l'intelligence ambiante gît certainement là. C'est dans le dépassement de la césure entre le biologique unique (le corps de l'utilisateur) et le numérique volatile, reproductible et vulnérable (les applications, les données, les prothèses de la personne responsable), et dans la synthèse entre le physique et le logique, le réel et le virtuel que la sécurité informatique triomphera de la crise qu'elle traverse en ce moment, empêtrée qu'elle est dans un assortiment disparate de solutions et dans une construction compliquée, difficilement accessible à un utilisateur normal. La sécurité devra surmonter par une dialectique profonde son obligation d'omniprésence quasi transparente pour simplifier et faciliter son intégration dans les démarches informatiques, et son exigence de disparition quasi inévitable pour affranchir les transactions informatiques d'une intervention humaine toujours hasardeuse et suspecte.

1. Jacques Lacan, *Le Séminaire*, Livre II, 19 janvier 1955, p. 105.