Inria dévoile son ***Livre blanc sur la cybersécurité***

© Inria / illustration Clod

La transformation numérique de la société crée de formidables opportunités mais, avec une connexion permanente à Internet, elle entraîne aussi une exposition accrue de nos systèmes d'information aux attaques. Les données à caractère personnel des citoyens risquent ainsi à tout moment d'être volées, détruites, modifiées ou exposées de manière non contrôlée. Les risques sont également majeurs pour les états, les opérateurs d'importance vitale et plus généralement toutes les organisations. Les dommages causés par une cyberattaque réussie peuvent être significatifs que ce soit par l'impact économique ou par les conséquences sur les personnes concernées. La perte de confiance possible en la société numérique est un autre enjeu. Dans ce contexte, Inria dévoile un nouveau livre blanc dédié à la cybersécurité, à la fois pour faire le point sur les grands défis scientifiques et technologiques et renforcer la prise de conscience par tous que ce sujet doit être un point d'attention de premier ordre.

À propos de ce livre blanc

Ce livre blanc fournit un aperçu des travaux académiques sur différents aspects relatifs à la cybersécurité, avec en particulier une cartographie des activités de recherche menées par les équipes Inria.

La place d'Inria dans le paysage français est significative puisque quasiment 25% de l'activité académique française en cybersécurité est menée dans des équipes-projets Inria communes avec ses partenaires (CNRS, universités et écoles d'ingénieurs). Au sein d'Inria, une trentaine d'équipes ont une activité en cybersécurité, ce qui représente au total près de 200 équivalents temps plein.

Le livre blanc commence par une description des menaces et des modèles d'attaques, que ce soit au niveau matériel, réseau, système d'exploitation, application, ou humain. Face à ces menaces, les "primitives cryptographiques", telles que le chiffrement, constituent une première défense pour garantir la confidentialité et l'intégrité des données. Mais la sécurité de ces primitives doit aussi être continuellement scrutée : c'est le rôle de la cryptanalyse. L'établissement de communications sécurisées, y compris en présence d'attaquants, utilise des protocoles cryptographiques, construits au-dessus des primitives de base. La complexité de ces protocoles rend nécessaire leur validation via des techniques formelles, qui se sont avérées particulièrement efficaces pour la détection de failles ou pour garantir l'absence de certains types d'attaques. Munis de ces primitives et protocoles, l'étape suivante consiste à construire des services de sécurité, par exemple pour l'authentification ou le contrôle d'accès, que ce soit au sein du système d'exploitation ou d'Internet. Cependant, comme rien n'est infaillible, une surveillance de ces systèmes d'informations est aussi nécessaire pour détecter les violations des politiques de sécurité, et des mécanismes automatiques doivent être ajoutés pour pouvoir réagir rapidement en cas d'attaque afin d'en limiter les impacts.

Le respect de la vie privée, aspect essentiel de la cybersécurité, est également complexe, car intégrant aussi des dimensions légales, économiques et sociétales. Plusieurs facettes sont explorées, que ce soit dans la compréhension des principes, dans la construction d'outils, ou dans la mise en évidence des pratiques de captation de données personnelles.

Enfin, différents domaines applicatifs posent de sérieuses questions en matière de cybersécurité, car en devenant connectés, les systèmes numériques ont largement augmenté la surface d'attaque possible et sont devenus potentiellement plus vulnérables.

Quelques succès et des recommandations

Le renforcement de la cybersécurité est un pilier fondamental du développement de la société, même si cela a un coût. Les motivations et compétences des attaquants sont très variables, et la sécurité n'est jamais totalement garantie, d'où la nécessité d'être aussi résilient aux attaques, tout en insistant sur la sensibilisation et la formation pour limiter les risques, car le facteur humain reste trop souvent le maillon faible.

Face à ces constats, la recherche académique française, en particulier chez Inria, peut apporter des éléments de réponse. Les trois domaines suivants ont en particulier connu des avancées majeures :

- **Cryptographie :**

La qualité de la recherche française en cryptographie et cryptanalyse est internationalement reconnue. En plus d'être à la base de nombreux systèmes de chiffrement et de signature numérique, les scientifiques français participent régulièrement aux efforts de standardisation du NIST (l'organisme de standardisation des Etats-Unis, qui joue un rôle clé au niveau mondial), à la fois pour proposer des nouvelles primitives et lors de l'évaluation des candidats. Des équipes Inria maintiennent également plusieurs records de calcul tels que la factorisation de clés RSA permettant de "casser" cette méthode de chiffrement.

- **Méthodes formelles :**

La conception d'assistants de preuve, tels que Coq ou plus récemment F*, et leur utilisation pour la vérification de systèmes critiques sont des forces historiques d'Inria. Appliqués dans le contexte de la cybersécurité, ces outils et plus généralement les méthodes formelles, ont permis de déceler de nombreuses failles dans des protocoles tels que TLS, et de proposer des implémentations de protocoles et primitives cryptographiques dont la sécurité est prouvée de bout en bout, comme la librairie HACL*, aujourd'hui intégrée dans les logiciels de Mozilla.

- **Vote électronique et protection de la vie privée**

Par l'application de nouvelles recherches dans ces domaines, Inria et ses partenaires au sein de la recherche française ont aussi un impact important sur la société.
Par exemple, les travaux sur le vote électronique menés conjointement par Inria et le CNRS ont permis le développement de la plateforme ouverte Belenios, qui utilise des protections cryptographiques pour garantir le secret du vote et l'intégrité de l'élection, sans avoir à faire confiance aux organisateurs de l'élection ni aux serveurs qui la gèrent. Ce travail a indirectement permis de sensibiliser le public aux questions de sécurité liées au vote, qu'il soit électronique ou papier. D'autres travaux de tout premier plan sur le respect de la vie privée, allant des concepts clés aux études de cas, qui héritent de la sensibilité toute particulière de la France sur cette thématique depuis la Loi Informatique et Liberté de 1978, ont réussi à avoir un impact au niveau européen jusque dans sa réglementation sur la protection des données (Règlement Général sur la Protection des données, RGPD).

Les scientifiques français en cybersécurité disposent de connaissances pointues sur un grand nombre de sujets. Ils sont sollicités de manière croissante pour des missions d'expertise. Le besoin de compétences en cybersécurité se fait de plus en plus ressentir dans tous les domaines, et tout particulièrement les systèmes industriels et médicaux ou l'Internet des objets, pour lesquels un transfert d'expertise est nécessaire. De même, la cybersécurité a un besoin pressant de compétences en techniques d'intelligence artificielle. Bien que la France ait une position de premier plan dans de nombreux domaines de la cybersécurité, un déficit existe sur des recherches plus expérimentales comme la sécurité des réseaux et des systèmes qu'il conviendrait de mieux valoriser, tout en facilitant l'accès aux données bien souvent indispensables à ces recherches.

Comme le facteur humain reste souvent le maillon faible, l'éducation et les actions de médiation en cybersécurité sont également incontournables, et ce à destination de tous les acteurs: citoyens, acteurs industriels, enseignants et élèves de tous âges, du primaire à l'enseignement supérieur.

De nombreux rapports récents sur la cybersécurité nous mettent en garde vis-à-vis de possibles attaques massives envers des entreprises ou des pays. La résilience de nos opérateurs d'importance vitale est cruciale et, comme la sécurité, elle ne peut être assurée que si elle est prise en compte dès la conception.

Les défis scientifiques

Tout au long du livre blanc plusieurs défis scientifiques et technologiques sont identifiés, notamment :

- **Penser la cryptographie post-quantique.** Comme l'apparition à moyen terme d'un ordinateur quantique, capable de casser la majorité des systèmes cryptographiques actuels, semble de plus en plus vraisemblable, il faut dès maintenant concevoir des primitives cryptographiques qui résistent à un ordinateur quantique afin que les informations sensibles dans les messages chiffrés aujourd'hui restent indéchiffrables demain.
- **Calculer sur des données chiffrées.** L'apparition du "cloud" et l'externalisation du stockage et du traitement de données ont créé le besoin de réaliser des calculs sur des données chiffrées pour garantir leur confidentialité. L''efficacité des chiffrements homomorphes et fonctionnels qui répondent à ces besoins est actuellement insuffisante pour passer à l'échelle et reste un sujet de recherche essentiel avec un impact économique potentiel considérable.
- **Prouver de bout en bout des protocoles cryptographiques.** Garantir la sécurité de protocoles cryptographiques est extrêmement complexe, que ce soit au niveau des spécifications ou de l'implémentation. Les méthodes formelles et les preuves assistées par ordinateur sont essentielles pour assurer un niveau de confiance suffisant. Il faut donc en généraliser l'utilisation. Il faudrait aussi les étendre pour permettre la certification de propriétés complexes comme l'anonymat.
- **Développer la sécurité de l'Internet des Objets**. Sécuriser les objets connectés de l'Internet des objets est un défi majeur, du fait de la quasi absence de protection de beaucoup d'entre eux, de leur caractère intrusif dans le monde physique, et de l'ampleur des attaques permises.
- **Renforcer la protection de la vie privée des citoyens.** L'accroissement massif du volume et du caractère intrusif des collectes de données personnelles pose de nombreuses questions. Des recherches transversales sont nécessaires afin d'apporter la transparence et de mettre en évidence les pratiques, bonnes ou mauvaises, dans ces environnements complexes sujets à de constantes évolutions technologiques.

La France dispose d'un écosystème de premier plan en cybersécurité, avec notamment des acteurs comme l'ANSSI ou la DGA, plusieurs groupes industriels et des start-up technologiques extrêmement innovantes. Pour renforcer cet écosystème, étant donné les enjeux croissants de la cybersécurité liés à la pénétration du numérique dans tous les pans de la société et de l'économie, la France doit aussi maintenir, voire accroître, son effort de recherche consacré à la cybersécurité, à l'instar de ce que font déjà d'autres pays.

CONTACT PRESSE Inria
Laurence GOUSSU - 06 81 44 17 33
Laurence.goussu@inria.fr