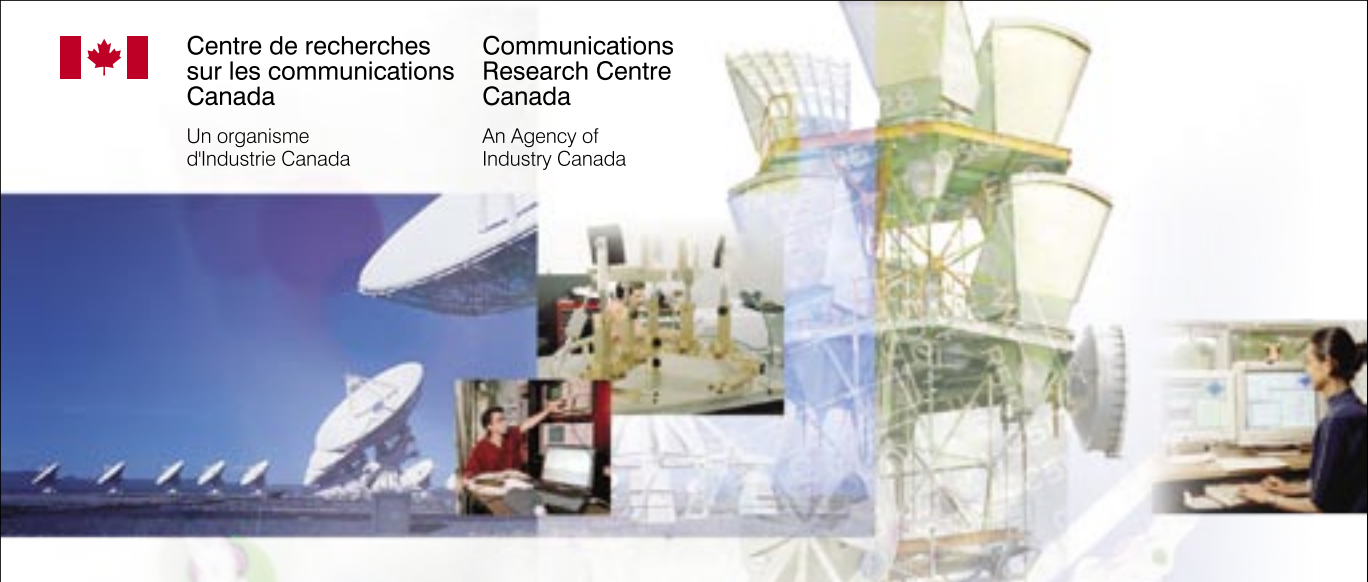
Centre de recherches sur les communications Canada
Un organisme d'Industrie Canada

Communications Research Centre Canada
An Agency of Industry Canada



Activités de recherche fédérales

Le CRC : gardien des réseaux du Canada

Le Centre de recherches sur les communication Canada (CRC) améliore la sécurité des réseaux du Canada et du monde entier. La sécurité des réseaux est un enjeu de portée nationale qui touche tous les secteurs, depuis les communications et les transactions de consommateur aux soins de santé et à la défense nationale. Rien que le coût mondial des attaques contre l'Internet a augmenté régulièrement, passant de 3,3 milliards de dollars américains en 1997 à environ 12 milliards en 2003 (Computer Economics, Carlsbad CA). La sécurité des réseaux constitue une priorité pour le Canada, et le CRC collabore avec son ministère d'attache, Industrie Canada, dans le cadre d'un effort plus vaste pour régler ce problème.

Pourquoi le CRC?

Le CRC est le principal laboratoire de recherche et de développement (R-D) en communications de pointe du gouvernement du Canada. La R-D du CRC, qui se situe entre la recherche industrielle et universitaire, fournit un moyen d'orientation crucial aux dirigeants de l'industrie et aux décideurs du gouvernement. La recherche en sécurité des réseaux s'inscrit à l'appui des besoins d'Industrie Canada en matière de décisions stratégiques et de réglementation publique, tout en permettant des transferts de technologie à l'industrie. Elle répond également aux besoins de communications sécurisées du ministère de la Défense nationale.

La sécurité et la fiabilité des réseaux sont des priorités cruciales du CRC pour les trois à cinq prochaines années. En collaborant avec des partenaires du gouvernement, de l'université et de l'industrie, le CRC est en mesure de réagir rapidement et efficacement à un vaste ensemble de problèmes de sécurité des réseaux.

L'échange sûr et fiable d'information sur tous les réseaux est une priorité-clé de la recherche pour le CRC. À long terme, le CRC examinera de futurs réseaux reposant sur des technologies de pointe utilisées dans les réseaux câblés et sans fil.

L'expertise du CRC comprend la recherche fondamentale, l'élaboration de technologies et de sous-systèmes, des essais de terrain et la démonstration de concepts liés aux systèmes. Les secteurs dans lesquels il mène des projet sont les suivants :

Surveillance des réseaux et détection

L'enjeu : Les intrusions dans les réseaux menacent la sécurité et l'intégrité de l'infrastructure de réseau moderne.

La réaction du CRC : Le CRC effectue des travaux de recherche sur les techniques et les technologies qui sont le fondement des systèmes efficaces de détection d'intrusion. Il est en train de mettre au point des outils et algorithmes de surveillance active et passive afin de parer les attaques actuelles et futures qui exploitent la vulnérabilité des protocoles et la mise en œuvre de protocoles utilisés dans les réseaux IP. Les chercheurs du CRC collaborent avec l'industrie et les usagers afin de déterminer et de mettre en œuvre des approches applicables aux infrastructures de réseau actuelles qui évoluent rapidement. Les méthodes d'attaque devenant plus complexes, il faut élaborer des mécanismes de détection afin de déceler des anomalies qui révèlent les attaques. Le CRC continue d'élaborer des méthodes et des outils qui reconnaissent les catégories d'attaques ainsi que les scénarios d'attaque individuels.

Gestion et sécurité des réseaux

L'enjeu : Un défi que se pose en permanence aux propriétaires et exploitants d'infrastructure est la gestion efficace de mesures et d'instruments de sécurité du réseau qui jouent un rôle de premier plan pour la protection de l'infrastructure essentielle et qui comprennent : les routeurs filtrants, les pare-feu, les réseaux privés virtuels, les systèmes de détection d'intrusion et les systèmes de vérification de la sécurité.

La réaction du CRC : Le CRC tire parti de ses longs antécédents dans l'élaboration de technologies de gestion de réseaux dans le but de développer de nouvelles stratégies et technologies pour les réseaux fondés sur le protocole Internet. De récents travaux ont porté principalement sur la gestion reposant sur des politiques de l'infrastructure de réseau, méthode normalisée d'élaboration de spécifications de configuration et de contrôle pour les services de sécurité et d'autres mécanismes de gestion. La gestion reposant sur des politiques permet aux propriétaires de réseau de décrire les services et applications exploités par le réseau et de configurer des mesures de sécurité efficaces. Le CRC travaille sur un prototype de systèmes de gestion reposant sur des politiques et participe à des essais de terrain nationaux et internationaux avec d'autres organisations.

Les flots d'information à l'intérieur des réseaux

L'enjeu : Des milliers d'applications et de services divers sont acheminés quotidiennement par les réseaux utilisés par les pouvoirs publics, l'industrie et des particuliers. De récentes attaques ont été cachées à l'intérieur de ces flots d'information, sous la forme d'éléments de trafic réseau camouflés de façon à sembler légitimes. Ainsi, les agresseurs peuvent dissimuler une attaque fondée sur un protocole particulier à l'intérieur d'un « flot » inoffensif d'un autre protocole.

CRC

Canada

La réaction du CRC : Le CRC s'efforce de déceler les flots d'information qui camouflent les attaques. La recherche a révélé que les applications et les services communs comportent des caractéristiques semblables à des signatures qui peuvent être décelées. Les différences des signatures peuvent indiquer qu'une attaque est en cours. Les défis qui se posent à la recherche sont, entre autres, la découverte de ces différences dans les liens de réseaux à grande vitesse et à débit élevé, et à l'intérieur d'un protocole dont l'objet est de masquer les détails de l'information qui est transportée.

La sécurité des réseaux mobiles ad hoc (MANET)

L'enjeu : Comment sécuriser un réseau mobile ad hoc (MANET)?

La réaction du CRC : Contrairement aux réseaux cellulaires qui comportent des stations de base ou des points d'accès, des routeurs et des commutateurs qui sont fixes et reliés par câbles, les MANET sont constitués par un groupe de nœuds mobiles connectés les uns aux autres par des liens sans fil. Tout hôte mobile pourrait faire office de routeur ou de relais sans fil si le besoin se faisait sentir. Ces réseaux sont très flexibles, ce qui les rend idéaux pour des applications commerciales et le secteur des normes. Conçus à l'origine pour un usage militaire, leur flexibilité inhérente les rend également attrayants pour diverses applications commerciales ainsi que pour le secteur des normes. L'introduction de Bluetooth, IEEE 802.11 et Hyperlan suscite l'intérêt commercial pour les utilisations de réseaux mobiles ad hoc à l'extérieur du domaine militaire. De nouvelles applications ad hoc de réseau sont élaborées pour les services d'urgence, les plans de secours et la surveillance environnementale. La souplesse inhérente du réseau le rend également attrayant pour des opérations de maintien de l'ordre, les opérations de recherche et de sauvetage et les applications de réseaux de capteurs.

Le réseau mobile ad hoc a besoin d'approches nouvelles et originales de prévention et de détection des intrusions. Au CRC, les chercheurs élaborent des techniques de répartition des clés de chiffrement, des mécanismes d'authentification répartis, des protocoles de routage ad hoc sécurisés et des systèmes de détection d'intrusion permettant de reconnaître et d'isoler les nœuds dont le comportement est suspect. La sécurisation des réseaux mobiles ad hoc est une activité récente au CRC qui s'inspire d'une vaste recherche antérieure sur les diverses formes de réseaux mobiles.

La sécurité des réseaux sans fil

L'enjeu : L'utilisation accrue de réseaux sans fil pour accéder aux réseaux d'entreprise et à d'autres réseaux aggrave les préoccupations au sujet de leur sécurité. Il est difficile de déterminer quelle solution répond le mieux aux besoins des utilisateurs.

La réaction du CRC : Le CRC s'efforce de rendre cette tâche plus facile. Les secteurs-clés de la recherche portant sur des techniques de piratage sans fil comprennent : les empreintes radio et les contre-mesures connexes, les formes d'ondes radio ayant une faible probabilité d'interception et de brouillage, des techniques d'antennes réceptrices adaptives pour contrer les interférences radio, des systèmes vocaux sur Internet sécurisés reposant sur des logiciels et l'authentification de tiers pour les réseaux WI-FI.

Systèmes satellitaires pour les interventions en cas d'urgence/de catastrophe

L'enjeu : L'utilisation de satellites pour la gestion des mesures d'urgence.

La réaction du CRC : Le CRC met son expertise en matière de communication par satellite à la disposition du projet REMSAT (gestion des mesures d'urgence en temps réel par satellite) afin de stimuler une utilisation accrue des technologies satellitaires pour la gestion des mesures d'urgence. Ce projet est une entreprise conjointe de l'Agence spatiale européenne (ASE) et de l'Agence spatiale canadienne (ASC). Parmi les autres partenaires, citons Telesat Canada, le Service des forêts de Colombie-Britannique, l'Université Simon Fraser et le BC Ambulance Service.

Radio réalisée par logiciel (RRL)

L'enjeu : La mise en service d'une nouvelle technologie radio qui aidera la police, les pompiers et d'autre personnel d'urgence à communiquer entre eux en situation de crise.

La réaction du CRC : La RRL est une radio unique pour des services, des normes et des protocoles de communication multiples. Le CRC élabore cette technologie radio unique qui fonctionne en grande partie comme un ordinateur de bureau. Tout comme un ordinateur particulier ou de bureau est en mesure d'effectuer de nombreuses fonctions reposant sur le logiciel qui y a été installé, la RRL permettra à une radio unique de s'adapter à différents milieux et systèmes de communication en choisissant le logiciel qui convient le mieux à la situation. Elle permettrait à des organisations de sécurité publique utilisant des radio différentes de communiquer entre elles lorsqu'elles interviennent dans des situations d'urgence.

L'élément central de la technologie RRL est le cadre de base de l'architecture logicielle (ALC) qui permet la mise en service et la configuration de ce logiciel radio. Le CRC est un expert de renommée mondiale de l'ALC et il élabore à l'heure actuelle différentes applications de cette technologie pour répondre à divers secteurs du marché de la RRL, ainsi que des outils de développement tel que des générateurs de codes, des éditeurs de composants, un outil de développement d'applications et un module administrateur radio. Le CRC fournit également un soutien à l'industrie, aux laboratoires du gouvernement ou aux universités pour l'élaboration de technologies de RRL et de radios reposant sur l'ALC au moyen de cours et de conseils techniques donnés sur place.

Relever les défis futurs

La recherche actuelle du CRC est conçue de façon à répondre à des menaces nouvelles à la sécurité publique, à l'infrastructure et aux services essentiels fournis au moyen de réseaux publics et privés, dans tout le pays. Son programme de R-D intègre expertise et expérience technique pour une réaction rapide et efficace aux manifestations de menaces visant la sécurité des réseaux.

Pour obtenir plus de renseignements et connaître les occasions de collaboration, veuillez visiter le site à l'adresse suivante : **www.crc.ca**.