Communications Research Centre Canada

An Agency of Industry Canada

Centre de recherches sur les communications Canada

Un organisme d'Industrie Canada

Public Research at Work

CRC: Safeguarding Canada's Networks

The Communications Research Centre Canada (CRC) is making networks in Canada – and around the world – more secure. Network security is an issue of national concern, affecting everything from communications and consumer transactions to healthcare and national defence. The worldwide cost of Internet attacks alone has grown steadily from $3.3 billion (U.S.) in 1997 to approximately $12 billion in 2003 (Computer Economics, Carlsbad CA). Network security is a priority for Canada, and the CRC is working with its parent department, Industry Canada, in a larger effort on this issue.

Why CRC?

CRC is the Government of Canada's primary laboratory for research and development (R&D) in advanced communications. Positioned between the research performed by industry and academia, CRC's R&D provides a critical roadmap for industry leaders and government policy makers. Research in network security supports the needs of Industry Canada in public policy decisions and regulations, and also carries out technology transfer to industry. It also supports the Department of National Defence's requirement for secure communications.

Network security and reliability are key priorities for CRC over the next three to five years. Working with partners in government, academia and industry, CRC is able to respond quickly and efficiently to a broad range of network security issues.

Exchanging information across networks in a safe and reliable way is a key research priority for CRC. Over the longer term, CRC will investigate future networks based on leading-edge technologies used in both wired and wireless networks.

CRC's expertise includes basic research, the development of technologies and subsystems, field trials and the demonstration of system concepts. Project areas include:

Network Monitoring and Discovery

The Issue: Network intrusions threaten the security and integrity of modern networking infrastructure.

CRC's Response: CRC conducts research in technologies and techniques that are the foundation of effective intrusion detection systems. Active and passive monitoring tools and algorithms are being developed to counter current and future attacks that exploit vulnerabilities in protocols and implementations of protocols used in IP networks. CRC researchers work with industry and user communities to identify and apply approaches for current and rapidly evolving network infrastructures. As attack methods become more complex, detection mechanisms must be developed to identify anomalies that expose the attacks. CRC continues to develop methods and tools that identify classes of attacks as well as individual attack scenarios.

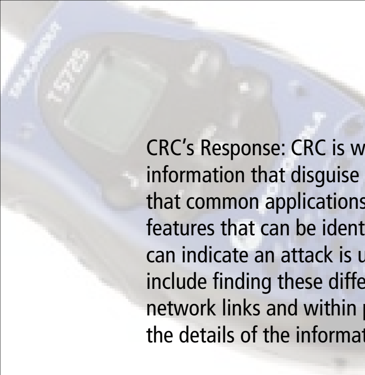
Network Management and Security

The Issue: An ongoing challenge for infrastructure owners and operators is effectively managing network security measures and devices that play a key role in protecting critical infrastructure. These include filtering routers, firewalls, virtual private networks, intrusion detection systems and security auditing systems.

CRC's Response: CRC is building on its long history of developing network management technology with the development of new strategies and technologies for IP-based networks. Recent work has focused on policy-based management of networking infrastructures – a standardized method of developing configuration and control specifications for security services and other management mechanisms. Policy-based management allows network owners to describe the services and applications that are supported by the network, and to configure effective security measures. CRC continues to develop prototype policy-based management systems and participate in field trials with other organizations, both nationally and internationally.

Information Flows in Networks

The Issue: Thousands of diverse applications and services flow daily over networks used by governments, industry, and private users. Recent attacks have been hidden within these information flows by disguising certain network traffic to appear to be legitimate. For example, attackers may "tunnel" an attack based on a specific protocol within a harmless "flow" of another protocol.



CRC's Response: CRC is working to identify flows of information that disguise attacks. Research has shown that common applications and services have signature-like features that can be identified. Differences in the signatures can indicate an attack is underway. Research challenges include finding these differences in high-speed, high-volume network links and within protocols that are intended to screen the details of the information carried.

Security in Mobile Ad Hoc Networks (MANET)

The Issue: How do you secure a Mobile Ad Hoc Network (MANET)?

CRC's Response: Unlike cellular networks, which include base stations or access points, routers and switches that are fixed and wired together, MANETs are formed by a group of mobile nodes interconnected by wireless links. Any mobile host could act as a wireless router or relay if needed. These networks are highly flexible, making them ideal for commercial applications and the standards community. Although originally conceived for military purposes, the inherent flexibility offered by these networks is also appealing to various commercial applications as well as to the standards community. The introduction of Bluetooth, IEEE 802.11 and Hyperlan are driving commercial interest in MANET deployments outside the military domain. New ad hoc networking applications are being developed for emergency services, disaster recovery and environment monitoring. The inherent flexibility of the network also makes it attractive for law enforcement, search-and-rescue operations and sensor network applications.

MANET requires novel approaches to intrusion prevention and detection. At CRC, researchers are developing cryptographic key distribution techniques, distributed authentication mechanisms, secure ad hoc routing protocols, and intrusion detection systems to identify and isolate misbehaving nodes. Securing mobile ad hoc networks is a recent initiative at CRC that builds on extensive previous research into various forms of mobile networks.

Wireless Security

The Issue: The increasing use of wireless networks to access enterprise and other networks is heightening concern about their security. Identifying which solution best meets a user's requirements is a difficult task.

CRC's Response: CRC is working to make this task easier. Key research areas related to wireless hacking techniques include: radio fingerprinting and related counter measures, radio waveforms with low probability of intercept and jamming, adaptive receiving antenna techniques to counter radio interference, software based secure Voice-Over-IP applications and third party authentication for WI-FI networks.

Satellite Systems for Emergency/Disaster Response

The Issue: Using satellites for emergency management.

CRC's Response: CRC is providing its satellite communication expertise to the REMSAT (Real-Time Emergency Management via Satellite) project to encourage greater use of satellite technologies in emergency management. This project is a joint undertaking of the European Space Agency (ESA) and the Canadian Space Agency (CSA). Other partners include Telesat Canada, BC Forest Service, Simon Fraser University and BC Ambulance Service.

Software Defined Radio (SDR)

The Issue: Deployment of a new radio technology that will help police, firefighters and other emergency personnel communicate with each other during a crisis.

CRC's Response: SDR is single radio for multiple communications services, standards and protocols. CRC is developing this unique radio technology, which works a lot like a desktop computer. Just as a home or office computer is able to carry out many functions based on the software loaded onto it, SDR will allow a single radio to adapt to different communications environments and systems by selecting the software that is best suited to the situation. It would enable public safety organizations using different radios to communicate with each other when responding to emergencies.

Central to the SDR technology is the software core framework, called the Software Communications Architecture (SCA), which allows deployment and configuration of the radio software. CRC is a world-renowned expert in the SCA, and is currently developing different SCA implementations to respond to various segments of the SDR market as well as development tools such as code generators, component editors, a waveform builder and a radio manager module. CRC also provides support to industry, government labs or universities for the development of SDR technologies through on-site courses and technical advice to organizations developing SCA-based radios.

Meeting Future Challenges

CRC's existing research is designed to meet emerging threats to public safety, and critical infrastructure and services delivered using public and private networks throughout the country. Its R&D program has the technical expertise and experience to react quickly and effectively to emerging network security threats.

For more information and to find out about opportunities for collaboration, please visit: **www.crc.ca**.