

▼ Northrop Grumman Cybersecurity Research Consortium

The Northrop Grumman Cybersecurity Research Consortium (CRC) was established in 2009 to enhance Northrop Grumman's technology capabilities in the area of Cybersecurity through a collaborative research partnership with top universities in the country. Current university members are Carnegie Mellon University (CMU), the Massachusetts Institute of Technology (MIT), and Purdue University. The goals of the Consortium include creating technological differentiators for our

business pursuits, further branding of our thought leadership, remaining at the state-of-the-art in technology, and further recruiting of top technical talent.

Northrop Grumman sponsors research projects at member universities on a yearly basis and transitions the results of the research to the marketplace through its Independent Research and Development (IR&D) program as well as through Contract R&D and customer projects.

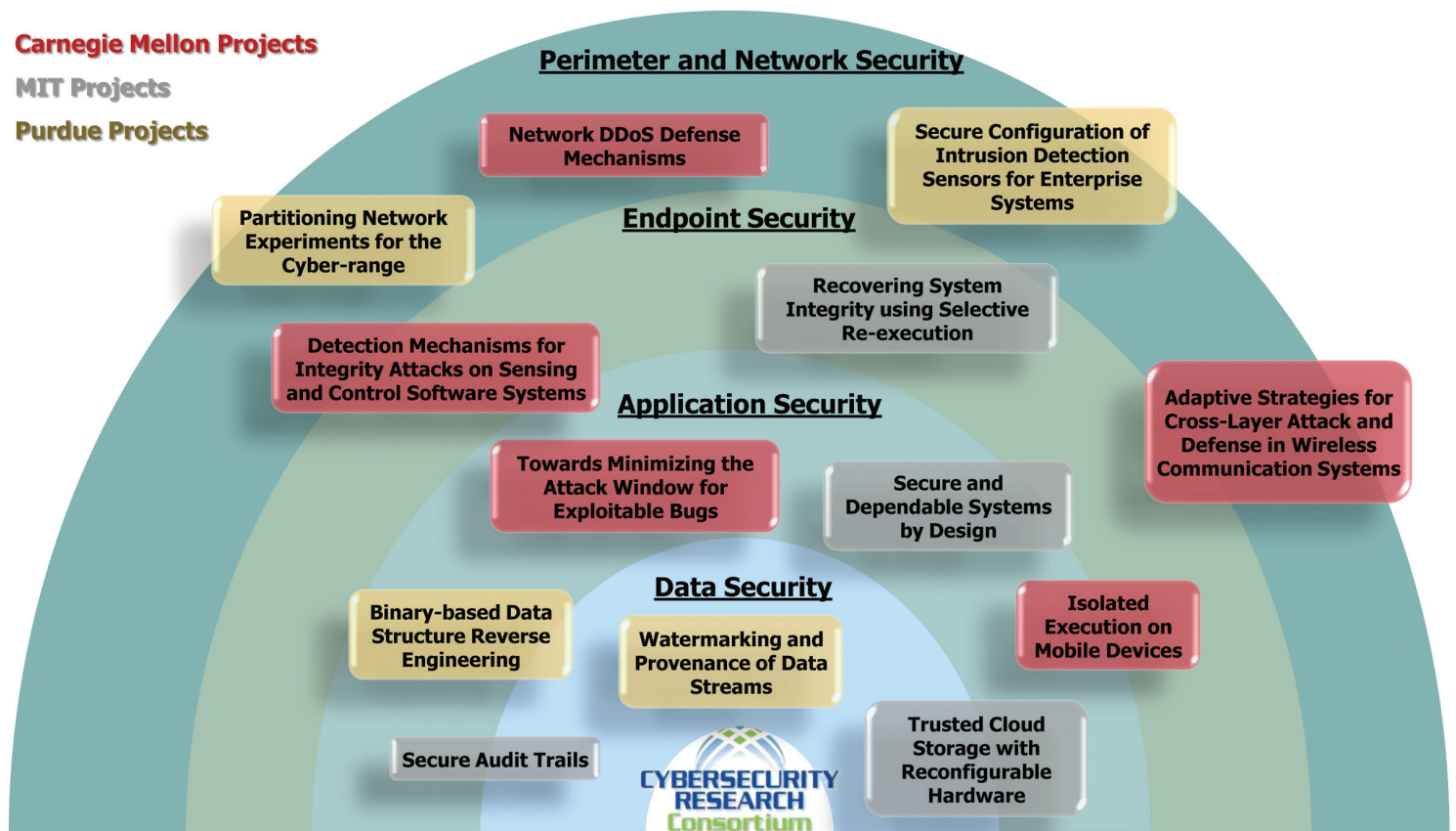
The Northrop Grumman CRC holds a semi-annual symposium to foster the exchange of ideas and results among consortium members and Northrop Grumman cybersecurity technologists, practitioners, and business developers.

The Northrop Grumman CRC is a key component of Northrop Grumman's strategy to secure our nation and its critical infrastructure against ever-evolving cyber threats.

Carnegie Mellon Projects

MIT Projects

Purdue Projects



Perimeter and Network Security

Adaptive Strategies for Cross-Layer Attack and Defense in Wireless Communication Systems assesses impact of combined layered attacks (e.g. jamming, MAC misbehavior, malicious routing/forwarding) on wireless networks and provides appropriate defense mechanisms.
Patrick Tague – CMU

Network DDoS Defense Mechanisms analyses link flooding attacks targeting a network infrastructure and provisions effective defense mechanisms.
Virgil Gligor – CMU

Partitioning Network Experiments for the Cyber-range partitions Internet-scale network experiments into a set of smaller experiments that are sequentially executed to approximate the results of the original experiment.
Sonia Fahmy – Purdue

Secure Configuration of Intrusion Detection Sensors for Enterprise Systems enables dynamic sensor configuration in enterprise computing systems that adapt to system changes and attacks.
Saurabh Bagchi – Purdue

Endpoint Security

Detection Mechanisms for Integrity Attacks on Sensing and Control Software Systems provides software-based attestation mechanisms and model-based schemes to detect and respond to integrity attacks on control systems.
Bruno Sinopoli, Adrian Perrig – CMU

Recovering System Integrity using Selective Re-execution enables recovering from cyber intrusions and restoring the integrity of the system by undoing both the direct and indirect effects of the attack.
Nickolai Zeldovich, Frans Kaashoek, Robert Morris – MIT

Application Security

Binary-based Data Structure Reverse Engineering for Memory Forensics and Application Vulnerability Discovery automatically identifies data structures in binary programs for use in forensics and security application scenarios.
Dongyan Xu, Xiangyu Zhang – Purdue

Isolated Execution on Mobile Devices protects relevant data on mobile devices and assures security properties (e.g., secrecy, integrity, authenticity) remain intact.
Jonathan McCune – CMU

Secure and Dependable Systems by Design ensures security and reliability in systems by construction, rather than relying on testing and inspection.
Daniel Jackson – MIT

Towards Minimizing the Attack Window for Exploitable Bugs automatically identifies vulnerabilities in software code and generates corresponding exploits.
David Brumley – CMU

Data Security

Secure Audit Trails enables detecting security violations in large scale distributed systems through automated aggregation and analysis of audit trails.
Barbara Liskov – MIT

Trusted Cloud Storage with Reconfigurable Hardware enables integrity and privacy guarantees for high-performance cloud storage systems using only two trusted low-cost components.
Srini Devadas, Nickolai Zeldovich – MIT

Watermarking and Provenance of Data Streams for Information Attribution securely and efficiently collects provenance metadata for streaming data from sensor networks and assesses trustworthiness of the data.
Elisa Bertino – Purdue

For more information, please contact:

Northrop Grumman Information Systems
7575 Colshire Drive
McLean, VA 22102

Dr. Kenneth C. Brancik
703-217-6707
kenneth.brancik@ngc.com

Dr. Donald D. Steiner
703-556-2115
donald.steiner@ngc.com