THE VALUE OF PERFORMANCE.

NORTHROP GRUMMAN

Northrop Grumman Cybersecurity Research Consortium

The Northrop Grumman Cybersecurity Research Consortium (CRC) is a unique industry/academia partnership established in 2009 to advance research in this field and develop next-generation solutions to counter the complex and growing cyber threats facing our economic and global security.

The CRC facilitates collaboration among top scientists from the nation's leading cybersecurity research institutions. Current university members include Carnegie Mellon University (CMU), the Massachusetts Institute of Technology (MIT), Purdue University, and the University of Southern California (USC).

Over the past few years, Northrop Grumman has funded over 30 game-changing technology projects, which have led to customer engagements where we can transition these innovative approaches to help address some of the most pressing cyber challenges.

The company sponsors research projects at member universities on a yearly basis in the areas of perimeter, network, endpoint, application, and data security as well as identity control and access management. This approach maps back to the Northrop Grumman-developed architecture model known as "The FAN™" (see back page) - a layered cybersecurity defensive technology reference model. Northrop Grumman then transitions research results to the marketplace through its Independent Research and Development (IR&D) program as well as through Contract R&D and customer projects.

To foster information sharing, the Northrop Grumman CRC holds a semi-annual symposium among university researchers and Northrop Grumman cybersecurity technologists, practitioners, and business developers. In addition to coordinating research projects, members of the consortium develop curricula, write joint case studies and other publications, and provide numerous learning opportunities and applications for students and the global security community.

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

Perimeter and Network Security

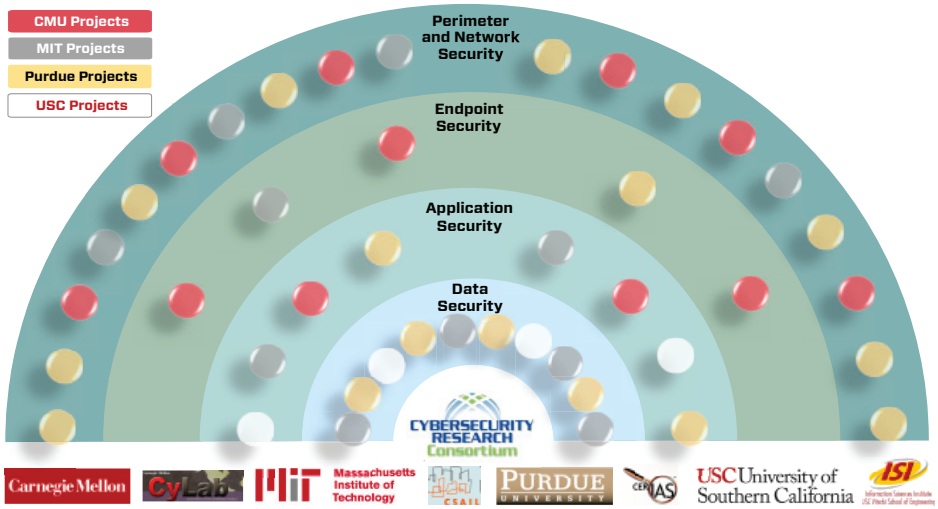
- Accurate and Fast Semantic Intrusion Detection
- Context-based Dynamic Defense
- Integrated Cyber-Physical Situational Awareness for Energy Operations and Infrastructure*
- Distributed Denial of Service Defense
- Modeling and Mitigating RF Vulnerabilities of Cellular Networks for UAS Communication*
- Moving Target Defense for Cloud
- Partitioning Network Experiments
- Relating Classes of Defense to Classes of Attack
- Security in Cyber-Physical Systems
- Sensor Configuration and Deployment
- Testbed Resource Mapping
- Using Deception as a Defense Mechanism
- Visualizing Event Correlation in Cyber-Physical Networks
- Visualizing Dynamic Patterns in Multi-Source Events*
- Wireless Communication Security
- Behavior-based Modeling for Detecting Novel Network Attacks*

Endpoint Security

- Dynamic System Recovery
- Mobile Device Forensics
- Real-time Execution Trace Analysis
- SCADA Sensor Integrity
- Threat Behavior Modeling

Application Security

- Automated Exploit Generation
- Cloud Security Policy Enforcement
- Data Reverse Engineering
- Adaptive Intrusion Management*
- Mobile Device Security
- Secure Cloud-based Multi-Party Computing*
- Security, Attribution and Trust
- Secure Systems by Design



The Northrop Grumman-developed FAN provides a framework for aligning the research projects across the various cyber dimensions.

Data Security

- Data Privacy in Cloud-Based Analytics
- Data Stream Provenance
- Integrity of Cloud-Based Analytics
- Mining Anonymized Data
- Trusted Cloud Storage
- Integrity of Cloud-Based Analytics
- Mining Anonymized Data*
- Practical Applications of Partial Homomorphic Encryption
- Privacy-Preserving Data Dissemination and Adaptable Service Composition*
- Retroactive Discovery and Synthesis of Cyber Datasets*
- Secure Audit Trails
- Secure Big Data Management and Analytics
- Secure Cloud Applications
- Trusted Cloud Storage

Identity Control and Access Management

- Browser Cryptography Standards
- Standardized User-Centric Authentication Systems for Trusted Clouds*
- Secure Browser Authentication Standards

**Represents the 2016 projects*

Northrop Grumman Cybersecurity Research Consortium Collaborators

CMU: David Brumley, Yang Cai, Virgil Gligor, Bob Iannucci, Adrian Perrig, Bruno Sinopoli, Patrick Tague, Amit Vasudevan, Joy Zhang

MIT: David Clark, Srini Devadas, Daniel Jackson, Jeff Jaffe, Frans Kaashoek, Barbara Liskov, Robert Morris, Ron Rivest, Howard Shrobe, Vinod Vaikuntanathan, Nickolai Zeldovich

Purdue: Saurabh Bagchi, Elisa Bertino, Bharat Bhargava, Ricardo Calix, Chris Clifton, Patrick Eugster, Sonia Fahmy, Arif Ghafoor, Feng Li, Richard Mislan, Eugene Spafford, Dongyan Xu, Xiangyu Zhang, Xukai Zou

USC: Blaine Burnham, John Heidemann, Prem Natarajan, Cliff Neuman, Don Paul, Viktor Prasanna, Roger Schell

For more information, please contact:

Northrop Grumman
Information Systems
7575 Colshire Drive
McLean, VA 22102

Dr. Donald Steiner
703.556.2115

www.northropgrumman.com

IS9480913 - B 10/30/15

THE VALUE OF PERFORMANCE.

NORTHROP GRUMMAN