Foreword

During the early 1990's more and more attacks were launched against the networks of the U.S. Department of Defense. In response to these attacks and increasing military reliance on the commercial Internet, DARPA started on a journey into the Information Survivability domain.

A new Information Security program was approved in 1994."Jumpstart" funds, provided in FY 1995, were used to establish and strengthen security components of existing programs. Since DARPA was funding the development of innovative networking and systems technologies, there was an opportunity to insert security into this early research, rather than have a completely separate security program that would have to address these technologies after they had been developed. Early focus areas included network security and electronic commerce.

The first Broad Agency Announcement (BAA) was published in January 1995. This BAA called for research in infrastructure protection, protection of end systems, and assurance. Infrastructure protection called for research to address networking vulnerabilities as well as the creation of new network security services. End-system security called for research on higher-assurance policy-independent firewalls, security management technology, configurable and reusable security policy enforcing modules, and security assessment tools. Assurance called for research in security specification languages, security analysis methods that could apply to complex distributed and networked systems, as well as metrics for security assessment.

During 1995, a DARPA-sponsored Information Science and Technology (ISAT) study on Survivability led to a new program segment aimed at developing means for hardening legacy systems by retrofitting security and survivability technologies. The Assurance segment of the program was changed into the Wrappers and Composition program to satisfy this new requirement. The Infrastructure Protection segment was renamed High Confidence Networking, and End-system Protection was renamed High Confidence Computing. Anticipating an increase in the interest of protecting critical infrastructure, a new program segment Survivability of Large Scale Systems was also added.

Subsequent BAAs (BAA 96-40 and 98-04) called for survivability research inspired by biological models, research in intrusion detection and response in large-scale systems, large-scale intrusion assessment, and survivable highly decentralized systems. Complementing the major thrust in intrusion detection and response were projects that recognized the need for Defense systems to sustain mission critical operations in the face of attack. These projects explored capabilities such as decentralized (e.g., market-based) resource allocation, adaptivity, and artificial diversity that led to the concept of Inherent Survivability and helped form the basis for a follow-on program in Intrusion Tolerant Systems.

The DARPA Information Survivability program consisted of four research areas. A short description of each research area is listed below.

High Confidence Networking

The High Confidence Networking program was aimed at creating network barriers that would prevent network disruption while facilitating secure communication for heterogeneous users and services. This program was designed to develop protocols and services to protect the integrity of internet-based fabrics and guarantee their preferential availability to critical applications as well as the health of the network in time of attack. Higher-level applications need network-wide security services, and this program was designed to supply the security technology for sharing and protecting enterprise facilities and for safe communication among dynamically negotiated sets of peers. This included the development of high assurance methods and algorithms that work with current and emerging network software and hardware.

Activities within this program included the development of secure protocols for key network functions such as routing, name service, mobile internets, data transport, multicast, key management, user authentication and network management. In addition, the development of tools and their application of formal methods for analyzing the security of such protocols were an important part of the program.

Research for secure group communication is seen as a basis for virtual private networks, also known as enclaves, and the associated policy negotiation languages are critical for their establishment. Lastly, resource allocation mechanisms, which satisfy quality of service requests of mission-critical priority clients, were developed as part of this program.

High Confidence Computing

The High Confidence Computing program was aimed at developing and demonstrating operating systems (OS) and computing environments with integral security designed to be strong against a powerful adversary and not trail commercial trends in functionality and performance. Its emphasis on policy neutrality and configurability was intended to lead to a technology base of commercially viable secure systems, easily tailored to defensive military needs. As Defense systems must simultaneously satisfy a number of mission-critical properties, High Confidence Computing developed technologies that integrated support for security, dependability, and real-time operation and explored tradeoffs and interactions among these constraints.

Activities within this program included enabling configurable OS security through policy-neutral access control mechanisms, policy languages for ease of specification and management of security rules, and a policy "compiler" that maps these rules into the access control mechanisms. These technologies ensure increased strength against attack by leveraging innovative language and compiler technology to provide low-cost tools for high assurance operating system construction. Development of partitioned OS resource management techniques that provide security through process isolation and resource use limitation were completed as part of this program. Research in security for extensible operating systems led to innovative techniques for assuring the safety and security of mobile code. This program was responsible for incorporating compatible security mechanisms into standard distributed computing environments (e.g., CORBA) to support secure interoperability across administrative domains. This facilitated the survivability of mission-critical applications through technologies which permit dynamic binding of security and fault-tolerance services to applications in response to policy or threat environment changes and are coupled to OS and distributed enforcement mechanisms.

Survivability of Large Scale Systems

The Survivability of Large-Scale Systems program was aimed at developing, evaluating, and demonstrating intrusion detection techniques. This included protocols that allow system elements (such as network managers, firewalls, and filtering routers) to react to detected events, algorithms to redirect resources to the most important tasks and whose behavior is difficult for an adversary to predict, and techniques for reconfiguring to a state not susceptible to the original attack. This program focused on providing detection technologies for local intrusion detection as well as larger-scale tactical indications, assessment, and warning.

Activities within this program included the development of intrusion detection technologies capable of detecting known attacks with high confidence and beginnings at detecting unknown attacks. These techniques offer much improved false alarm rates and higher detection accuracy than the prior existing state-of-the-art. These techniques were also validated in realistic testbeds subject to red-teaming. To address the problem of tactical indications and warning, efficient methods were developed for peer-to-peer cooperative detection and reporting. Probes and sensors were developed for monitoring large-scale systems for attack. This program investigated technologies to estimate the extent of damage, and developed protocols for automated response and reconfiguration. In addition, techniques for resource allocation were developed that assign remaining resources to the most critical tasks. This program explored diversity techniques to ensure that no single attack can completely take out any capability and techniques for recovery to a state not susceptible to the original attack.

Wrappers and Composition

The Wrappers and Composition program was aimed at developing toolkits for integrating security and survivability functionality into legacy systems and developing tools for assessing the security and survivability of components and their composition. Department of Defense systems contain a high percentage of legacy and off-the-shelf components that do not provide the properties needed for survivable systems (e.g., security, robustness). This program was designed to develop the techniques to assess aspects of the trustworthiness of a component and develop tools which transform existing components into ones, which have the properties, needed for survivability. This included the development of formal engineering rules for composing components so as to preserve these properties, and tools for embodying these rules to assist an integrator in assembling components and wrappers in a trustworthy manner.

Activities within this program included the development of tools for automatically generating security and survivability "wrappers." Wrappers encapsulate an existing component by intercepting all input and output to the component, and thereby add security and survivability functionality; e.g., encrypting the traffic or filtering access requests to the component. The demonstration of these wrappers for candidate systems provides security and robustness functionality. Underlying these tools is a rigorous methodology for "survivable composition" to allow an integrator to predict the security and survivability characteristics of compositions of components and wrappers.

These Proceedings

This publication represents the DARPA Information Survivability Conference and Exposition (DISCEX) proceedings and contains research papers describing the projects in the four areas of the Information Survivability program described above. Contributions from 24 academic institutions, 18 industrial research laboratories, and 3 government research laboratories describe progress in the research performed for survivable information systems. These proceedings have been peer reviewed, although not strictly in the traditional sense of a refereed conference or journal, and participating reviewers are noted in the Acknowledgements section. We're confident these proceedings represent high quality papers describing the research carried out at each institution. In addition, we view these proceedings as a technology transfer vehicle for anyone interested in information survivability and the technology available today. We believe these proceedings will be valuable for future information survivability researchers as they see where we've been and they can leverage this previous research as they proceed ahead.

The sections of these proceedings are grouped by program with the papers arranged by topic so similar research projects can be studied together. We are confident these proceedings will provide an excellent source of ideas and insight for the rapidly growing community of survivable information systems. It is our hope that these proceedings will convey the many ideas and results from the information survivability researchers and the results presented will catalyze the discovery of new techniques for securing our nation's information systems.

World Wide Web

Even though the DARPA Information Survivability program is coming to a close, current descriptions of all activities within this program are maintained with links to performers' sites at http://www.darpa.mil/ito/research/is. This will provide the reader with opportunities for contact and collaboration to accelerate the technology transfer process and, hopefully, the progress of research and development of survivable information systems.

Gary Koob
DARPA / ITO
gkoob@darpa.mil

Douglas Maughan
DARPA / ITO
dmaughan@darpa.mil

Sami Saydjari
DARPA / ISO
ssaydjari@darpa.mil