Experiments in Adaptable Distributed Systems
(Supported by NSF)

Bharat Bhargava
Department of Computer Sciences
Purdue University
West Lafayette, IN 47906

Abstract

An adaptable system can gracefully reconfigure based on its environment during execution. We propose to conduct a series of experiments that will lead in the development of policies for adaptability at the application, system, and network layer to meet the quality of service requirements. We study the impact of system constraints in determining the quality of service that can be guaranteed to the user. We plan to identify adaptability guidelines and mechanisms that will be implemented in the application and system software. We will evaluate how adaptability impacts in meeting the quality of service requirements in different applications. We focus on two fundamental research problems: Adaptability mechanisms and infrastructure and Adaptable quality of service provision and control for distributed systems. This will lead toward developing expert rules/guidelines for system adaptability and its impact on various applications. This will allow the research on the behavior of system software and its impact on various emerging applications such as electronic commerce, digital libraries, and video conferencing systems. This research will allow experiments with advanced system services, protocols, techniques and their experimental evaluation. This knowledge is applicable to various system software used in collaborative computing, distributed file systems, multimedia application, and real-time processing.
Secure Mobile Systems
(Supported by NSF)

Bharat Bhargava
Department of Computer Sciences
Purdue University
West Lafayette, IN 47906

Abstract

Survivability and secure communications are essential in a mobile computing environment. We propose to conduct a series of experiments that will lead to the development of new authentication and key management techniques for wireless Communications. We study the implementation of various authentication schemes on the overall system performance. We propose a technique to achieve fault-tolerant mobile node authentication in an efficient way. We plan to identify guidelines for authentication between an upstream domain and a DiffServ ingress router in a QoS enabled network. We will evaluate how various secure group communication and access control techniques fit into the wireless world by conducting scientific experiments in a systematic way. We will solve the problem of providing secure multimedia communication under mobile environments where the resources available to mobile hosts such as CPU power and network bandwidth are very limited. We have developed a series of light-weight video encryption algorithms which encompass video compression and video encryption in one step. This will lead towards an adaptable encryption system.
Experiments in Security and QoS in Mobile Systems
(Supported by NSF)

Bharat Bhargava
Department of Computer Sciences
Purdue University

Abstract

Disaster recovery after emergency such as earthquake, terrorist attack, war depends on mobile systems for communications. Security and Quality of Service(QoS) are of utmost importance. Providing security and QoS is a difficult problem in mobile systems because the availability of network and other resources may change as the mobile host moves or comes under intentional or unintentional attack or simply fails. We have proposed a technique to achieve fault-tolerant mobile node authentication in an efficient way. It eliminates single point of failure, distributes the load, enhances scalability and survivability, and makes failures transparent to users. We propose to conduct a series of experiments that will evaluate this technique under a variety of variables and lead to the development of new authentication and key management techniques. We plan to identify guidelines for authentication between an upstream domain and a DiffServ ingress router in a QoS enabled network. We will evaluate how various secure group communication and access control techniques fit into the wireless world. We plan to explore the adaptability requirements when considering security as a QoS parameter. By participating in this research and experimental studies, the postdoc will conduct research that cuts across security, mobile systems, and Quality of Service. The CERIAS security center at Purdue will provide an intellectually stimulating environment for her.
Formalizing Evidence and Trust for User Authorization
(Supported by NSF)

Bharat Bhargava
Department of Computer Sciences
Purdue University
West Lafayette, IN 47906

Abstract

Research is proposed to develop authorization mechanisms for secure information access by a large community of users in an open environment. The research problem is to formalize the trust that is associated with each user for granting privileges of access to data warehouse and the World Wide Web. Evidence is used to prove certain properties of a user in order to build a trust model. Evidence is formalized and a computational model for the reliability of evidence is developed. This research combines the concepts of role-based access control, user behaviors and profiles, mathematical theory of evidence, and data mining. This research contributes to the design and development of a trust-enhanced role-mapping server. For adaptive user authorization, this server cooperates with existing role-based access control mechanisms. A series of experiments are planned to study the performance issues of the trust model prototype. An efficient and adaptive algorithm for role assignment will be developed as a result of these experimental studies. This research will provide a framework for secure authorization systems with applications in the Semantic Web, e-commerce, airport security procedures, intelligence gathering and policymaking in military, homeland security, and database access in general.
Abstract
The proliferation of multimedia applications and high speed networks increase the demand for high quality of service (QoS) and congestion control in the Internet. Poor network performance by excessive delays and losses experienced by the users’ applications are not acceptable. Internet security lapses have cost U.S. corporations 5.7 percent of their annual revenue, as reported by economist Frank Bernhard from University of California at Davis. To improve the QoS, we focus on congestion and unfairness in network resource allocation problem. Proper traffic conditioning (marking, shaping) with unresponsive flow control can solve the congestion and unfairness problem. Continuous monitoring of network activity is required to maintain confidence in the security of networks with QoS support. These solutions have to be scalable otherwise it will not be deployable in the heterogeneous Internet.

This research studies and designs coordinated traffic conditioning, network monitoring, flow control, and provisioning the network properly to meet the demands for data and multimedia traffic in various applications. Proper network provisioning plays a vital role to provide QoS by the providers as promised to the users. We propose to design edge routers component to monitor the network from any service level agreement (SLA) violation and bandwidth theft attack. Users can inject excessive and illegitimate traffic from several different entry points to create distributed denial of service (DoS) attacks. This network monitoring scheme involves only edge routers. The conditioner and flow control components alleviate the congestion and unfairness in the resources allocation problem. The edge routers share the congestion information with upstream routers to save resources wastage in the downstream domains. Designing a scalable edge router is a challenging research task because all of the components of an edge router should not use excessive per-flow information and can not involve core routers. We follow this principle in designing edge routers to achieve scalability. We propose to solve the following research problems and evaluate them using analytical models as well as through a series of experiments.
In Ad Hoc networks, it is hard to employ static routes, link-state based protocols and complex public-key encryption algorithms. Routing protocols must be dynamic and robust against malicious attacks. One type of attacks targets the route discovery phase. By initiating false route queries and distorting the routing information, an attacker can overwhelm a network with excessive traffic load or partition the network [2]. Second threat occurs in the forwarding phase. An adversary host on the route can intentionally drop packets, obtain the content of the traffic, or analyze the traffic pattern even if the data is encrypted. An appropriate routing protocol will filter erroneous query and routing information and determine a route that only involves trustworthy hosts. We consider the trustworthiness as the metric of a route, which is determined by the trustworthiness of all hosts along it.
Vulnerability Analysis and Threat Assessment/Avoidance
(Supported to NSF)

Bharat Bhargava
Leszek Lilien
Department of Computer Sciences
Purdue University
West Lafayette, IN 47907-1398

Abstract

Existing vulnerabilities are a serious threat to computer systems and organizations. Research in security is needed to identify vulnerabilities in systems, evaluate the threat, and devise mechanisms that avoid them. Formalizing vulnerability, building quantitative models of threat, and experimental studies will allow us to discover and evaluate solutions for dealing with threats to life and economy. This will result in algorithms, observations based on experiments, and infrastructure that can deal with expected and unexpected attacks in an adaptable and graceful manner. It will allow us to provide guidelines for building secure systems and databases. We plan to build upon our research on failures, fault-tolerance and reliability/safety. We reduce vulnerabilities by keeping an attacker uncertain and unaware about the latest version of databases/software and routing information that are in operation.
Secure Wireless Command and Maintenance Environment
Submitted to Navy

Bharat Bhargava
Department of Computer Sciences
Purdue University
West Lafayette, IN 47906

Abstract

A Command and Maintenance Environment (CME) that optimizes the instruction and maintenance process by integrating data, information, and logistics across the bases, battle ships, and battle groups will support all strategies for reducing the maintenance and manning burden throughout the fleet. As an important part of the Smart Ship Science and Technology Program of Navy, wireless/mobile networks have been deployed on battle ships to provide increased responsiveness, visibility, and accessibility of information to the commander and crew. But there are security risks that threaten the safety and efficiency of the system (e.g. jamming the channel, sending false routes, or conducting illegal data accesses). These threats can come from all layers of the wireless networks. They must be mitigated before these networks can be installed on a broader scale.
SENSORS: Self-configuration and Data Aggregation in Microsensor Systems
(Submitted to NSF)

Bharat Bhargava
Department of Computer Sciences
Purdue University
West Lafayette, IN 47906

Abstract

Any system, structure, or environment is vulnerable to malicious and hostile activities. Detecting malfunctions, failures, and natural disasters require constant real-time monitoring. The technical challenge is to replace human monitoring with sensors that detect and determine events that lead to safe operations of any enterprise. The reliability, security, and accuracy of these sensors and wireless devices can affect timely access to information used in decision making. When deployed in large numbers and embedded deeply with in large scale physical systems, microsensors gain the ability to measure aspects of physical environment in unprecedented detail. Wireless sensor networks are envisioned to consist of large number of devices, each capable of limited computation, communication, and operating in an unattended mode with limited energy. Sensors are characterized by severe energy constraints. A variety of sensors that detect temperature, pressure, electromagnetic fields, acoustics, optical, chemical, biological, radiation, humidity etc are have become available due to advances in electronics, physics, chemistry, and biology.
Secure Shadow Networking for Scientific Research Collaboration

(Submitted to CISCO)

Bharat Bhargava
Department of Computer Sciences
Purdue University
West Lafayette, IN 47906

Abstract

Security and quality of service in mobile/wireless ad hoc networks will contribute to scientific research collaboration. We investigate the development of a suite of protocols and algorithms that enable researchers to securely collaborate over mobile ad hoc networks as well as the wired backbone. A series of experiments in key management, malicious intruder identification, and detection of denial of service attacks will be conducted. A close collaboration with Purdue ITaP on shadow network will provide realistic parameters and measurements for network management.
Abstract

Spatial disorientation (SD), a false perception of one’s attitude or orientation, is a major problem facing pilots and NASA astronauts alike. Spatial disorientation mishaps cost the Department of Defense $300 million annually in lost aircraft, dozens of lives and can give astronauts debilitating motion sickness. This project is a continuation of previous experiments investigating haptic (touch) perception in altered-gravity environments. Data collected during two previous flights under the NASA Reduced Gravity Student Flight Opportunities Program showed that (1) haptic performance deteriorated in zero-gravity environment; and (2) this deterioration was not due to a change in hardware performance, or a change in perceived intensity of haptic signals in zero-g. The current project will investigate the role of cognitive load in affecting haptic performance in zero-g environment. Cognitive load will be manipulated by immobilizing one of the flight crew members during the parabola flight thereby creating a lower demand on cognitive load. Performance will be assessed by comparing accuracy in identifying a haptic stimulus on the torso by the flying and the immobilized member, and by comparing information transmission through the multi-tactor vests worn by these two flight members. Results will be of interest throughout the aerospace community. Properly designed tactile displays could give astronauts additional orientation awareness during EVAs (Extra-Vehicular Activities) and discrete communication to covert ops soldiers would be made easy. This haptic technology could be used for navigational information to disabled, elderly or the blind when combined with a Global Positioning System (GPS) and a wearable computer.
Abstract

This research addresses privacy and trust issues in interactions ranging from simple transactions to the most complex collaborations. Dissemination and sharing of private data is often required by law. Mechanisms are needed to guarantee that privacy is preserved and enforced. Privacy and trust can be in a symbiotic or in an adversarial relationship. More research is called for to help users in giving up only the degree of privacy absolutely necessary to gain a level of trust required by applications they want to use. Metrics are needed for privacy assessment. This research integrates ideas from cooperative information systems, collaborations, privacy, trust, and information theory. The applications to location-based services and electronic supply chain management systems are illustrated. The ideas are applicable to diverse computer systems, ad hoc networks, peer-to-peer systems, and the Semantic Web.
A middleware for peer-to-peer streaming
(Submitted to NSF)

Bharat Bhargava
Department of Computer Sciences
Purdue University
West Lafayette, IN 47906

Abstract

Data sharing among large number of participants spreaded over a wide geographical area involves discovery, propagation, and aggregation of information. Internet as well as wireless networks are providing the underlying communication capabilities. Poor scalability and single points of failure lead us towards a decentralized peer-to-peer solution. Research in data integrity, trust, and privacy along with network-aware dispersion and aggregation of information in a collaborative environment can lead to deployment of systems that provide high quality of service. Experimental studies will integrate ideas from networking, replicated systems, and security research and will answer questions about performance and implementation of large systems. They will also provide us with empirical parameters and observations that can be used in other fields of computer science.