

Research Plan for Bharat Bhargava

Lack of trust, privacy, security, and reliability impedes information sharing, particularly among distributed entities. The potential for theft, fraud, harassment, and destruction of critical private data continues to exist. My research plans is to create knowledge and learning in secure networking, systems, and applications. Much of this research is based on using scientific principles for designing, building, evaluating systems in a living laboratory.

There are fundamental research problems in privacy, trust, and security issues in collaborative systems. I briefly describe my planned objectives as follows:

- The first objective is to develop models of cyber attacks, identify vulnerabilities in systems and networks, and assess threats and losses. The risks associated with various types of attacks need to be studied. The timing, extent, scope, and duration of attacks will determine the adaptive strategy to deal with them. This research extends the best ideas from research in reliability and fault-tolerance. The research has direct impact on nuclear waste transport, bio-security, disaster management, and homeland security.
- The second objective is to investigate new ideas for privacy and security in networks. For mobile wireless networks research is needed in intruder identification under wormhole and gang attacks, and fault-tolerant authentication. For Internet the research questions deal with network monitoring and differentiated services for avoiding congestion and for the detection of service violations due to misbehaviors or attacks.
- The third objective is to formalize trust and fraud. Existence of system vulnerabilities provide opportunities for conducting fraud and create a threat to trusted collaborations. We plan to investigate fraud countermeasures and schemes for detection of swindler's fraudulent intentions. Fraudsters can be impersonators or swindlers. Experiments are planned to show effectiveness for various types of swindler's strategies. This research has applications to e-commerce and collaborations.
- The fourth objective is to research ideas that can help with dissemination of private sensitive data. This includes measures of privacy and trust and tradeoffs between the two. This research has applications to sharing of data among hospitals, government agencies, and commercial institutions. A series of experiments for adaptability, quality of service, P2P multimedia streaming, congestion in mobile ad hoc networks, and privacy and trust tradeoffs will be carried out. Past research has resulted in several successful grants. Research on vulnerability/threat assessment and security and privacy in databases have resulted in new measures, identification of tradeoffs, and practical schemes. Several prototype systems are under development to provide tools, measurements, and guidelines. All these ideas and scientific experiments contribute to the building of peer-to-peer systems, mobile ad hoc networks, and internet.

The details of ongoing research are available on my web site. I briefly present the current research activities.

A. Research in developing distributed monitoring schemes that use edge-to-edge measurements and collect statistics of delay, loss, and bandwidth in Internet is underway. The objective is to reduce the overhead for core routers, deal with large scale network domains, and identify congested links to capture the misbehaving flows. Such flows violate service-level-agreements and inject excessive traffic that leads into denial of service attacks. The challenge is to investigate techniques to identify intruders and improve the performance for normal users. A network service called CollectCast has been designed and implemented. CollectCast serves the applications that operate in diverse and dynamic networks. CollectCast can perform the topology inference, monitoring, and adaptation. The topology inference employs network tomography techniques to infer the performance (e.g., segment-wise loss rate and available bandwidth) of the underlying network with a low overhead. Network tomography infers the internal characteristics of a network by only probing it from the edge nodes. We are conducting similar research in wireless networks. Research involves the study of algorithm, protocol, and architecture design to improve quality of service (QoS) and security. Research topics include routing, security, and inter-networking in ad hoc/cellular integrated networks, multi-rate communication and real-time service over multi-hop wireless connections, and location privacy in ad hoc networks. For congestion measurements and avoidance in ad hoc networks, we are building a SAGA protocol. SAGA uses intermediate delay (IMD) instead of hop count in routing decisions. The use of IMD enables selection of routes that bypass hot spots.

B. Research on intruder identification in ad hoc networks correctly identifies the malicious hosts in self organized infrastructures. This research is being done in the context of the AODV (Ad hoc On-demand Distance Vector) protocol. We are investigating gang attacks and wormhole attacks. Research involves host authentication and key management, secure routing and dealing with malicious hosts, adaptability to attacks, and experimental studies. Cellular-Assisted Mobile Ad hoc (CAMA) is network software for ad hoc mobile nodes that takes advantage of a cellular system. Cellular network works as a centralized control in a position-based routing algorithm to handle the ad hoc network management of routing and security. Experiments are conducted on throughput, cellular signaling, and robustness to imprecise position information.

C. Research in privacy and trust involves activities that range from simple transaction-based interactions to the most complex collaborations. This involves algorithms to evaluate privacy loss and trust gain, mechanisms for disseminating data without compromising privacy, and assessment metrics that measure the privacy. Guidelines are being developed for a variety of applications for developing privacy policies, building trust, and determining strategies for disseminating data to trusted or unknown users. Research is underway in formalizing trust and fraud. Applications in e-commerce and transportation security are being tested in a prototype system. An authorization for an access is based on the policies, the evidence, and the trust value assigned to a user. The reliability of evidence is determined by the trust value of the evidence provider and her own confidence level with respect to her opinions about the evidence. A user interacts

with a role-based access control (RBAC) enhanced application server to provide role assignment information and obtain data on users' behaviors. Users' trust information is submitted to the reputation server. When the server encounters a new user or an old user in a new context, it requests the reputation server to compute the personalized reputation of the user by using the specified reputation evaluation algorithm. If there were any previous interactions with the user, a valid reputation value will be returned. This value is used as the trust value for role assignment and access. Using the TERA prototype (details on my web site), experiments will study the evaluation of (a) behavior-based trust-building algorithms, (b) uncertain evidence handling mechanisms, and (c) personalized reputation calculation algorithms.

Based on TERA, we are building a comprehensive prototype system called PRETTY (private and trusted system). PRETTY implements research ideas in privacy-preserving data dissemination by using the quantification of the tradeoff between privacy and trust. PRETTY utilizes the server/client architecture. The client component of PRETTY consists of the user application, the credential manager, the evaluator of trust gain and privacy loss, the privacy negotiator, and a set of privacy policies. The server component consists of the server application, the TERA server, privacy negotiator, set of privacy policies, the database, and the data disseminator. PRETTY provides a platform to simulate privacy violators and users with different levels of trust. It will serve as a test bed for experimental studies on (a) clean self-destruction and proximity-based evaporation of data, (b) effectiveness and efficiency of the probability-based and lattice-based privacy loss evaluation methods, and (c) evaluation of the dynamic mappings between trust levels and distortions of data.

D. Research is underway in peer to peer multimedia streaming and video-on-demand applications. The system organizes peers in network-aware clusters that can allow for fast dissemination of multimedia files and control of traffic on the underlying network. File contents are distributed over the Internet in a cost-effective manner while achieving the desired quality of service. The study includes economic models, privacy issues, verification of integrity of packets received by a peer, and privacy preservations. The description of various systems and prototypes are available in the activity report on my web site.

My research plan is based on current grants, ongoing student thesis, and submitted proposals. Collaboration with faculty in Computer Science department and the Center for Trustworthy Networked Systems can lead to proposals to Darpa and NSF. One of my major objectives is to win a ten year grant to establish a NSF Science and Technology center.